

Emergency Operations Plan

2022-2023

INTRODUCTION

Emergency Operations Plan

OVERVIEW

The Emergency Operations Plan (EOP) provides an organized process to initiate, manage, and recover from a variety of emergencies, both external and internal, which could confront Opportunity Enterprises, Inc. (OE) and the surrounding community. The Emergency Management Committee (EMC) participates in the development of this EOP.

The EOP identifies the Agency's capabilities and establishes response procedures for when the Agency cannot be supported by the local community in OE's efforts to provide communications, resources and assets, security and safety, staff, utilities, or Client care for at least 72 hours.

The EOP describes a comprehensive "all-hazards" command structure for coordinating the six critical areas: communications, resources and assets, safety and security, staffing, utilities, and clinical and support activities. The overall response procedures include single emergencies that can temporarily affect demand for services, along with multiple emergencies that can occur concurrently or sequentially that can adversely impact Client safety and the ability to provide care, treatment, and services for an extended length of time. OE has updated emergency plans to establish the necessary policies and procedures to achieve preparedness and respond to and recovery from an incident. The newly revised plans, policies, and procedures will be exercised and reviewed to determine and measure functional capability.

OE's EOP describes the recovery strategies and actions designed to help restore the systems that are critical to providing care, treatment, and services after an emergency.

The EOP describes the processes for initiating and terminating OE's response and recovery phases of an emergency, including under what circumstances these phases are activated.

The EOP identifies the individual(s) who has the authority to activate the response and recovery phases of the emergency response.

The EOP identifies alternative sites for care, treatment, and services that meet the needs of its Clients during emergencies.

If OE experiences an actual emergency, it implements its response procedures related to care, treatment, and services for its Clients.

Members of the Emergency Management Committee (EMC), comprised of OE's Executive Team and Director of Nursing (DON) as applicable, shall review and revise the EOP on an annual basis. Documentation of this review shall be noted by the revision date in the footer on the front page of the EOP. Modifications made to the EOP are documented in the EMC minutes.

RESPONSIBILITIES

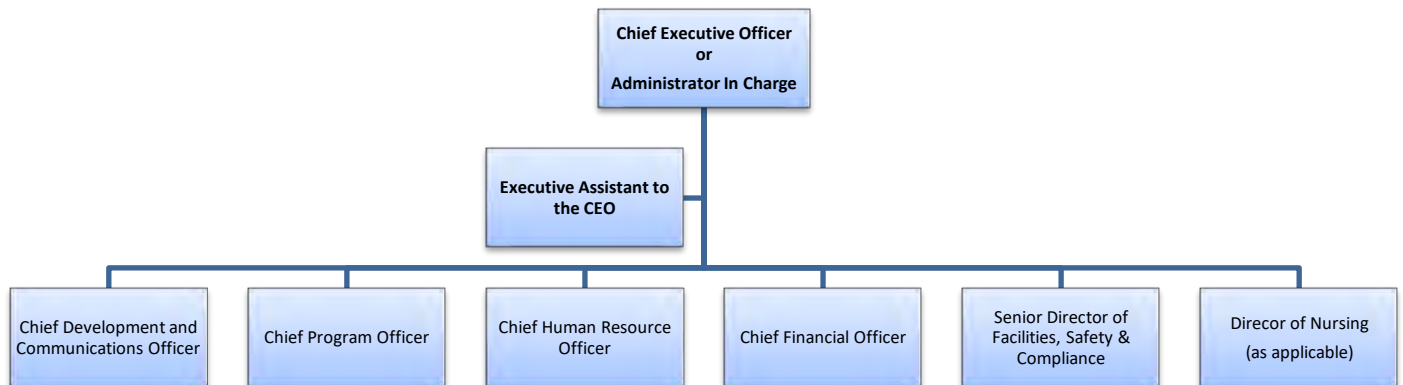
During an emergency, the Emergency Response System (ERS) will be in place. The staff have been trained in the ERS system.

The Emergency Management Committee (EMC)

Vital to successful planning for any disaster is involving local agencies such as police, fire/emergency medical services, emergency management, and public health in committee deliberations helps clarify the roles and responsibilities of all staff, including back up and PRN, specific to the actual emergency incident. This familiarization will help promote much-needed priority setting, information sharing, and joint decision-making during a real incident.

Emergency Response System (ERS)

The Agency has implemented the Emergency Response System (ERS) to assist in improving emergency management planning, response, and recovery capabilities for unplanned and planned events.



ESSENTIAL SERVICES

Opportunity Enterprises, Inc. (OE) is an employer who operates continuously 24 hours a day. Even on days when day service programs are cancelled or the Main and/or Lakeside campuses are declared closed due to inclement weather or other extraordinary situation, OE must provide adequate staffing in “Essential Services.” It is up to the department Directors to make sure such services are provided.

Closure of services can result from either scheduled events or suspension of normal operations, as described below. Each situation may affect each department differently. The nature, severity and impact of each circumstance determine the Essential Services required to maintain vital operations. OE has established two categories of emergency and nonemergency closures to plan more easily for and enable efficient communication, staffing levels required (including specific skill sets needed) and pay administration during various situations.

The Administrator in Charge is responsible for monitoring acceptable levels of risk for the organization and for determining the appropriate category and emergency response.

Scheduled (non-emergency) Scheduled situations or events are typically planned, nonemergency, short-term and require certain staff members to perform Essential Services when all or most offices are closed. Examples include but are not limited to events or needs that:

- occur on OE recognized holidays (New Year’s Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, Friday after Thanksgiving Day, Christmas Eve and Christmas Day)

Directors who are responsible for planning special events should anticipate staffing needs as far in advance as possible to designate some or all staff members as Essential Services staff for the specific event or time period

**Suspension
Of Normal
Operations
(emergency)**

Suspensions of normal operations are unscheduled situations or emergencies when OE would have to suspend normal operations and/or modify work schedules. While events requiring the suspension of normal operations are typically not scheduled, appropriate responses may be anticipated and planned ahead of time. Essential Services required will be determined by each situation.

These situations may impact the activities of the entire organization or portions of the organization, affect the ability of employees to travel, disrupt scheduled programs or events, close offices and have short-term or long-term impact.

Essential Services are required to ensure the health and welfare of the clients served, keep the organization secure and safely operating, and/or protect and preserve OE property.

Although unlikely or rare, employees must plan for serious or extreme emergencies that threaten the health or safety of the organization and/or the local region. There may be additional functions that require Essential Services staffing to maintain financial, technology and/or other infrastructure transactions.

Most or all offices may be closed and residential services and day programs may not be cancelled, depending on the severity of the threat or impact.

Examples include but are not limited to:

- bomb threats/terrorism
- extended network interruptions
- extended power interruptions
- fire/explosion
- natural gas leaks
- flooded roads or buildings
- hazardous material or other environmental hazard
- inclement weather
- interruption of vital supplies
- public health threat
- transportation/aviation Accident
- Pandemic
- violence or civil unrest

Employees providing Essential Services are required to report to work if so informed by their supervisors. Departments providing Essential Services will have a written plan for providing these services, including which employees and/or positions are needed, their steps to continually monitor staffing levels throughout the emergency and a system of notification to the EMC if staffing shortages are projected. Written plans are to be kept on file with the Director of each department.

These are the Essential Services of OE:

- Supported Living
- Group Homes
- Facilities
- Information Technology
- Human Resources
- Nursing
- Administration

Some departments or personnel might be able to provide some Essential Services from an off-site location. Department Directors can make these determinations.

Employees of non-Essential Service departments will be called on in order to maintain adequate staffing levels.

PROGRAM MANAGEMENT

HAZARD VULNERABILITY ANALYSIS

OE identifies the potential hazards, threats, and adverse events and assesses the impact on the care, treatment, and services sustained during an emergency. A Hazard Vulnerability Analysis (HVA) is used for the assessment for the organization. A list of priority concerns will be developed from the HVA and are evaluated annually. The HVA will include the ability to provide services, the likelihood of those events occurring, and the consequences of those events. The Agency's HVA is reviewed annually by the EMC.

The EMC will develop appropriate specific emergency response plans based on priorities established as part of the HVA. Each Emergency Response Plan/Policies will address the four phases of emergency management activities:

- | | |
|-----------------------|---|
| MITIGATION - | Activities designed to reduce the risk of and potential damage due to an emergency (i. e., the installation/utilization of safety equipment, training). |
| PREPAREDNESS - | Activities that will organize and mobilize essential resources (i. e., plan-writing, employee education, preparation with outside agencies, acquiring and maintaining critical supplies). |
| RESPONSE - | Activities the agency undertakes to respond to disruptive events. The actions are designed with strategies and actions to be activated during the emergency (i. e., control, warnings, and evacuations). |
| RECOVERY - | Activities the agency undertakes to return the facility to complete business operations. Short-term actions assess damage and return essential services to minimum operating standards. The long-term focus is on returning all agency operations back to normal or an improved state of affairs. |

COMMUNITY INVOLVEMENT

OE has established a relationship with the community. In conjunction with the community, priorities have been set among the potential emergencies identified in the hazard vulnerability analysis. The communication has been established on what the needs and vulnerabilities are for OE. It has identified the capabilities that the community can contribute to aid in meeting the needs of the facility. During a disaster, the agency's role within the community is to care for the Clients who receive services from the agency. The agency and community are involved through:

- Collaboration with Local Emergency Management Agency
- United Way COAD

INITIATION ACTIVITIES

DEFINITIONS

1. Internal Emergency

An Internal Emergency involves an incident within the agency that disrupts normal agency operations. Incidents include bomb threats, utility failures, hostage situations, epidemics, and Client elopements.

2. External Emergency

An External Emergency involves an incident beyond the immediate boundaries of the agency. Such an incident can include snowstorms, utility outages, and tornados.

PLAN INITIATION

To facilitate the orderly initiation of the response to an emergency, the following steps of the EOP will be initiated.

1. Information received by OE concerning an external emergency facing the community or an internal emergency involving the function of the agency will be passed directly to the Administrator in Charge (AIC).
2. When notified of a potential disaster, the AIC will:
 - Evaluate the issues such as location of incident (internal, external), the distance from OE, the scope of the incident (single individual, mass casualty, or malicious attack), and weather conditions (seasonal and current).
 - Discuss the operations pertaining to the conversion of the agency to disaster status.
 - Plan care of Staff/Clients during a disaster.
 - Will evaluate the information concerning this emergency and determine if initiation of the Emergency Operation Plan (EOP) is warranted.
3. Once it has been determined to activate the EOP, the individual who takes the role of AIC will notify the EMC. The EMC will then implement the communication plan to staff, clients, and families.

Incident Phases

1. Phase I – When notified of an incident that occurred within the facility.
 - Situation that most likely can be managed with the staff already on duty.
 - Staff should remain on duty and review their department specific procedures to be prepared to respond to the next level if situation requires an upgrade.
 - The Agency Command Center (ACC) may be set up.
2. Phase II – May require additional support from external authorities.
 - Situation may require additional staff to be called.
 - Staff should remain on duty and review their department specific procedures to be prepared to respond to the next level if situation requires an upgrade.
 - The ACC will be set up to coordinate the EOP.
3. Phase III – Significant issues have occurred and the need for extensive support will be addressed.
 - The ACC will be set up to coordinate disaster operations.

- This major event will require mobilization of most aspects of the ERS in the EOP, including planning for staff relief over an extended period.
4. The plan may be called All Clear for the disaster situation while the recovery efforts continue until the agency is back to normal operations.

*Please note, the EMC will assess at each phase, if any current state approved flexibilities apply, how they will implemented, communicated and phased out when appropriate.

AGENCY COMMAND CENTER

1. The Agency Command Center (ACC) will be established upon notification of an event that could disrupt normal operations. The ACC is generally established in the Training Room at Main and/or at the Horton Room at LAKESIDE. If the Training Room is not available, the Board Room has been designated as the alternate site. The phone numbers for these rooms are provided in the Communications Section. **At off-site locations the ACC will be established by the AIC present when the event occurs.**
2. The ACC will be activated by the AIC at 2801 Evans Ave. The most appropriate person present at the time the event occurs will establish command. This will vary according to the type of event and whether it is a pre-planned or unexpected event.
3. The EMC report to the ACC.
4. Deployment of Command Center Supplies
Supplies and materials for use in the ACC shall be deployed upon the decision to implement the ACC.

Supplies or materials
EMC vests
Job Action Sheets with clipboards
EOP, ERS Forms, and Emergency Response Plans (policies and procedures)
Note pads and pens
Two-way radios
Portable PC and printer
Bottled water and non-perishable refreshments
Portable signs for temporary treatment areas
Security Lockdown packet (signs to post at entrances during lockdown) and signs to advertise the Radio STAT frequency.

Administrator In Charge (AIC)

AIC will organize and direct the ACC and give overall direction for agency operations and, if needed, authorize evacuation.

The AIC manages the incident, which includes establishing the strategic objectives of the operation ordering and releasing resources. ERS will be assumed by the most appropriate and qualified person available at the scene when the event occurs.

Agency administrative staff and other assigned personnel will support the AIC.

Role of the AIC:

- a) Direct overall emergency operations for the agency
- b) Activate the ACC and initiate the appropriate emergency operating procedures
- c) Appoint ACC staff in the ERS configuration and supervise their activities
- d) Act upon information received from any source in a timely & effective fashion
- e) Internally and externally.
- f) Authorize the EMC to implement the communication plan.
- g) Notify Board of Directors (BOD).

CHIEF HUMAN RESOURCE OFFICER (CHRO)

Ensure adequate staffing to serve in essential services.

Ensure staff have adequate training to serve in essential services.

CHIEF DEVELOPMENT AND COMMUNICATIONS OFFICER (CDCO)

Responsible for the coordination of all internal and external communication, including press release.

CHIEF FINANCIAL OFFICER (CFO)

Ensure the IT and Financial needs of the agency are being met.

Communicate with lenders.

CHIEF PROGRAM OFFICER (CPO)

Ensure safety of all clients (including but not limited to; medications, food, shelter, etc.) while maintaining individuals' rights and choices.

Report status and plans to overseeing bodies.

SENIOR DIRECTOR OF FACILITIES, SAFETY AND COMPLIANCE (SDFSC)

Responsible for the coordination of all safety measures; assist to ensure the EOP is implemented and identify any hazards and unsafe conditions; ensure staff have adequate emergency supplies.

EXECUTIVE ASSISTANT TO THE CEO

Coordination of the EMC to the ACC; ensuring adequate planning supplies for the ACC; recording discussions and outcomes in relation to the situation/emergency at hand.

STAFF RESPONSE

1. All Staff on duty will report to their departments and **STAND-BY** (i. e., being ready, willing, and able to perform assigned duties) for further instruction.
2. Staff away from their department or duty station, who cannot report physically to the department, will communicate with the department and identify their current location and status of activity.
3. Client care activities being conducted away from the department will continue until a point of completion is reached.
4. The Client and staff will return to the appropriate area as soon as possible or receive instructions to secure the Client in an ancillary location if necessary.
5. The Staff will notify their Director/Manager of the location of the Client and staff member.
6. Staff will continue their designated Client care activities in preparation for response to the directions provided by the ACC.
7. All staff requesting to go off duty must obtain the approval of a member of the EMC. Staff must not leave their workstations until relief has arrived or until dismissed by the Department Supervisor/Manager.

DEPARTMENTAL AND OFFSITE RESPONSE

1. Each Department Director will assess the status of their Staff to maintain normal operation.
2. Each Department Director, or designee, will identify available resources, such as beds, personnel, and equipment, which could be allocated to the emergency response.
3. The Department Director will **STAND-BY** with information on status of department.
4. The Department Director will provide information to the EMC when requested.
5. When the departments receive the notification of the specific emergency, the Department Directors will initiate the appropriate departmental location response plan for the emergency.
6. The Department Directors will report any problems or concerns to the EMC.
7. No department should reduce its hours of operation without prior approval from the EMC.

Site	Location	Alternate Care Site Potential	Events Occurring at This Site	Events at Main or Lakeside Buildings
Appletree Group Home	203 Appletree Ln Valparaiso, IN 46383	Appletree Group Home may be used as an alternate care site during evacuation due to power failure. Generator on site.	For most events occurring at this facility, you will shelter in place or evacuate and close. Every satellite facility should have flashlights and a plan for alternate food supply in the event that the site is isolated. Maintain safety of Clients and staff during any event at this location. Notify a member of the EMC to request support.	When notified that there is an event at the Main or Lakeside locations, a member of the EMC will contact to assign a role if required. Staff may be diverted to the affected site or alternate care sites
Annabelle Group Home	451 Sheffield Drive Valparaiso, IN 46383		For most events occurring at this facility, you will shelter in place or evacuate and close. Every satellite facility should have flashlights and a plan for alternate food supply in the event that the site is isolated. Maintain safety of Clients and staff during any event at this location. Notify a member of the EMC to request support.	When notified that there is an event at the Main or Lakeside locations, a member of the EMC will contact to assign a role if required. Staff may be diverted to the affected site or alternate care sites
Rebecca Group Home	501 Albert Street Valparaiso, IN 46383		For most events occurring at this facility, you will shelter in place or evacuate and close. Every satellite facility should have flashlights and a plan for alternate food supply in the event that the site is isolated. Maintain safety of Clients and staff during any event at this location. Notify a member of the EMC to request support.	When notified that there is an event at the Main or Lakeside locations, a member of the EMC will contact to assign a role if required. Staff may be diverted to the affected site or alternate care sites

Sheffield Group Home	355 Sheffield Drive Valparaiso, IN 46383	Sheffield Group Home may be used as an alternate care site during evacuation due to power failure. Generator on site.	For most events occurring at this facility, you will shelter in place or evacuate and close. Every satellite facility should have flashlights and a plan for alternate food supply in the event that the site is isolated. Maintain safety of Clients and staff during any event at this location. Notify a member of the EMC to request support.	When notified that there is an event at the Main or Lakeside locations, a member of the EMC will contact to assign a role if required. Staff may be diverted to the affected site or alternate care sites
Fiesta Group Home	5949 Fiesta Avenue Portage, IN 46368		For most events occurring at this facility, you will shelter in place or evacuate and close. Every satellite facility should have flashlights and a plan for alternate food supply in the event that the site is isolated. Maintain safety of Clients and staff during any event at this location. Notify a member of the EMC to request support.	When notified that there is an event at the Main or Lakeside locations, a member of the EMC will contact to assign a role if required. Staff may be diverted to the affected site or alternate care sites
Airport Group Home	3102 Airport Road Portage, IN 46368	*Effective 10/15/22 Airport Group Home may be used as an alternate care site during evacuation due to power failure. Generator on site.	For most events occurring at this facility, you will shelter in place or evacuate and close. Every satellite facility should have flashlights and a plan for alternate food supply in the event that the site is isolated. Maintain safety of Clients and staff during any event at this location. Notify a member of the EMC to request support.	When notified that there is an event at the Main or Lakeside locations, a member of the EMC will contact to assign a role if required. Staff may be diverted to the affected site or alternate care sites
Lute Group Home	6381 Lute Road Portage, IN 46368	Lute Group Home may be used as an alternate care site during evacuation due to power failure. Generator on site.	For most events occurring at this facility, you will shelter in place or evacuate and close. Every satellite facility should have flashlights and a plan for alternate food supply in the event that the site is isolated. Maintain safety of Clients and staff during any event at this location. Notify a member of the EMC to request support.	When notified that there is an event at the Main or Lakeside locations, a member of the EMC will contact to assign a role if required. Staff may be diverted to the affected site or alternate care sites
Main Building	2801 Evans Ave. Valparaiso, IN 46383		For most events occurring at this facility, you will shelter in place or evacuate and close. Every satellite facility should have flashlights and a plan for alternate food supply in the event that the site is isolated. Maintain safety of Clients and staff during any event at this location. Notify a member of the EMC to request support.	When notified that there is an event at the Main or Lakeside locations, a member of the EMC will contact to assign a role if required. Staff may be diverted to the affected site or alternate care sites

Vocational Training Center	3101 Evans Ave. Valparaiso, IN 46383		For most events occurring at this facility, you will shelter in place or evacuate and close. Every satellite facility should have flashlights and a plan for alternate food supply in the event that the site is isolated. Maintain safety of Clients and staff during any event at this location. Notify a member of the EMC to request support.	When notified that there is an event at the Main or Lakeside locations, a member of the EMC will contact to assign a role if required. Staff may be diverted to the affected site or alternate care sites
Lakeside Building	32 Fish Lake Rd. Valparaiso, IN 46385	Can be used as an alternate care site during evacuation due to power failure. Generator on site.	For most events occurring at this facility, you will shelter in place or evacuate and close. Every satellite facility should have flashlights and a plan for alternate food supply in the event that the site is isolated. Maintain safety of Clients and staff during any event at this location. Notify a member of the EMC to request support.	When notified that there is an event at the Main or Lakeside locations, a member of the EMC will contact to assign a role if required. Staff may be diverted to the affected site or alternate care sites
Lakeside Apartments	27 Fish Lake Rd. Valparaiso, IN 46385	Can be used as an alternate care site during evacuation due to power failure. Generator on site.	For most events occurring at this facility, you will shelter in place or evacuate and close. Every satellite facility should have flashlights and a plan for alternate food supply in the event that the site is isolated. Maintain safety of Clients and staff during any event at this location. Notify a member of the EMC to request support.	When notified that there is an event at the Main or Lakeside locations, a member of the EMC will contact to assign a role if required. Staff may be diverted to the affected site or alternate care sites
Supported Living Sites	46383, 46385, 46307		For most events occurring at this facility, you will shelter in place or evacuate and close. Every satellite facility should have flashlights and a plan for alternate food supply in the event that the site is isolated. Maintain safety of Clients and staff during any event at this location. Notify a member of the EMC to request support.	When notified that there is an event at the Main or Lakeside locations, a member of the EMC will contact to assign a role if required. Staff may be diverted to the affected site or alternate care sites
Respite (Lake County)	1819 W. 64 th Pl. Merrillville, IN 46410		For most events occurring at this facility, you will shelter in place or evacuate and close. Every satellite facility should have flashlights and a plan for alternate food supply in the event that the site is isolated. Maintain safety of Clients and staff during any event at this location. Notify a member of the EMC to request support.	When notified that there is an event at the Main or Lakeside locations, a member of the EMC will contact to assign a role if required. Staff may be diverted to the affected site or alternate care sites

Respite (Porter County)	478 High Meadows Circle Valparaiso, IN 46385		For most events occurring at this facility, you will shelter in place or evacuate and close. Every satellite facility should have flashlights and a plan for alternate food supply in the event that the site is isolated. Maintain safety of Clients and staff during any event at this location. Notify a member of the EMC to request support.	When notified that there is an event at the Main or Lakeside locations, a member of the EMC will contact to assign a role if required. Staff may be diverted to the affected site or alternate care sites
--------------------------------	---	--	---	---

Ongoing Communication with Staff

Staff will receive information and instructions from a member of the EMC at the following intervals:

- The onset of the event
- As updates occur
- Any time additional action is required
- The conclusion of the event.

This information could be relayed via a meeting, a written form sent by email, or by a runner. Additional meetings will be setup to disseminate information throughout the emergency until the “All Clear.”

Communication with additional sites will be via email, phone, fax, and text. The AIC will determine the appropriate decision regarding keeping each alternate site open or closed during the event.

EMERGENCY COMMUNICATION AND NOTIFICATIONS

INTERNAL & STAFF NOTIFICATION LEVELS

During an emergency, staff will be alerted via one of the following communication mechanisms; email, personal notification devices (radios, walkie-talkies, cell phone), overhead paging, radio, or television. Internal communications will be limited to disaster-related issues once emergency has been initiated, therefore, do not attempt to contact the EMC unless directed to do so.

CODE ALERTS

Event	Audible Notification
Fire	Fire Alarm
Fire All Clear	"All Clear"
Intruder Alert	"Mr. Gray to [location of intruder]"
All Clear	"Code Gray all clear"
Tornado Warning	"Tor-na-do, please seek shelter" repeated 3 times
All Clear	"Tor-na-do All Clear"
Physical Harm Emergency CPI trained personnel needed	"Code Yellow to [location of event]"
All Clear	"Code Yellow All Clear"
Nursing Emergency	"Will a nurse report to [location of event]"
Bomb Threat	Code Red
All Clear	Code Red All Clear
Active Shooter	Code Blue
All Clear	Code Blue All Clear
Elopement	Code Green on "client name"
All Clear	Code Green All Clear

List of External Contacts

Operations Support		
Pharmacy	InTouch Pharmaceuticals	1.219.464.7055
Auto Repairs	Dave's Auto	1.219.465.1971
Commercial Banking	Centier Bank	1.888.236.8437
Commercial Insurance	Gibson	1.574.245.3500
Commercial Bus Fleet	NIRPC	1.219.763.6060
Medline	PPE Supplier	1.219.308.2214 / 1.866.497.0655 ext. 6368293
Utilities and Associated Supplies ALSO REFER TO ESSENTIAL UTILITIES GRID WHICH FOLLOWS THIS SECTION		
Utility Power (for 46383, 46410, 46360)	NIPSCO	1.800.4NIPSCO 1.888.689.8669
Generator Supplier/Service	NWI Generators	1.219.313.4317
Utility Power (For all 46385 & 46307 Sites)	KVREMC	1.800.552.2622
Natural Gas	NIPSCO	1.800.4NIPSCO 1.888.689.8669
Portable medical gas tank supplier	Alick's Home Medical Equipment	1.219.872.1000
General Contractor	Chester, Inc.	1.219.465.7555
Fire Suppression Contractor	Shambaugh	1.888.217.7055
Electrical Contractor	Ellis Electric	1.219.926.7400
Plumbing Contractor	Better Rooter	1.219.462.5868
HVAC Contractor	Bloomfield Mechanical	1.219.763.7470
Telecommunications Contractor	Midwest Telecom	1.219.531-9029
Information technology service provider	In-house/ Chester IT	1.219.464.9999
Local suppliers of hardware and household materials	Home Depot	1.219.531.6687
Local suppliers of hardware and household materials	Menards	1.219.462.8647
Cellular Service Provider	Verizon	1.800.837.4966 / 1.219.789.2799
Clinical and Client Support		
Security Service	EMA Cert Team	1.219.465.3490
Emergency Services	9-1-1	9-1-1
Towing Service	Greens Valparaiso	1.219.464.1173
Police (Non- emergency)	Valparaiso	1.219.462.2135
	Portage	1.219.762.3122
	Merrillville	1.219.769.3722
	Michigan City	1.219.874.3221
	Winfield	1.219.779.9326

NOTIFICATION & COMMUNICATION WITH EXTERNAL AUTHORITIES

1. All appropriate external authorities will be notified to facilitate effective response, continuing operations, and recovery from an emergency that disrupts the normal Client care and/or business operations of the organization
2. When an emergency plan is initiated, the appropriate external authorities and community resources will be notified
3. External authorities include, but are not limited to:

Office of Emergency Management (OEM)	911 or 1.219.465.3490
Fire Department	911
Law enforcement agencies	911
EMS	911
Centers for Disease Control	1.770.488.7100
Poison Control	1.800.222.1222
Red Cross of America	1.219.462.8534
Post-Tribune	1.219.477.6010
NWI Times	1.219.462.5151
WLJE Radio	1.219.462.8125
WYIN TV	1.219.756.5656

3. The CDCO has the responsibility for media and public information as it pertains to an event that involves the agency and has established working relationships with local media, emergency management office, and public health prior to an event.

COMMUNICATION WITH CLIENTS & FAMILY

The AIC or designee will establish a Family Support Center/Family Information Center to coordinate the needs and information to family members of Clients, to coordinate the information of the location of Clients, anticipated return to original environment and to provide critical incident stress debriefing.

Clients, their Families and other Interdisciplinary team members as appropriate, will receive information and instructions from a member of the EMC at the following intervals:

- The onset of the event
- As updates occur
- Any time additional action is required
- The conclusion of the event.

The Family Support Center/Family Information Center location will be determined by the AIC according to the type, magnitude, and size of the event. The Family Support Center/Family Information Center will serve as the location for relatives and friends of Clients/Staff.

Information will be sent to clients' families via phone (through auto-calling software). Families and outside residential providers will be asked to pick up their loved one to ensure their health and safety in a familiar environment. In emergencies where clients are not able to be transported or are sheltering in place at an OE facility, an emergency call center will be established where families and providers can call in for information regarding the well-being of their loved ones.

BACKUP COMMUNICATIONS

OE will maintain a current listing of backup communication systems or devices. A listing of all communication of primary or secondary communication systems or devices should be listed below:

1. Email will only be available as the infrastructure is working.
2. The overhead address or paging system is not tied into the telephone or fire system only. These systems should work independently in case of infrastructure damage.
3. Inter-departmental radios may be used as backup communication. Training must be achieved along with an instruction card attached for those that do not use the equipment often.
4. Cellular telephones have the risk of running out of battery during a long-term emergency. Homes will be provided with USB power packs to extend the life of the phones.
5. Runners if all other means of communication fail.

EVACUATION ACTIVITIES

1. An evacuation of OE for a situation, which renders the facility/site no longer capable of providing the necessary client care, will be directed by the AIC. The evacuation will be handled in cooperation with local Police or Fire and/or local EMA.
2. The local Police or Fire and/or the EMA will be notified as soon as the potential for evacuation is considered and will be kept updated on an ongoing basis to begin the process for identification of the availability of vehicles to relocate the clients.
3. Transporting clients, their medications, equipment, staff, and pertinent information to alternate care sites when the environment cannot support care, treatment and services is managed through by the EMC. Please see Memorandum of Understandings for Non-OE shelter sites.

**RESOURCE
AND
ASSET MANAGEMENT**

OBTAINING & REPLENISHING MEDICAL & NON-MEDICAL SUPPLIES

The amounts, locations, processes for obtaining and replenishing of medical and non-medical pharmaceutical supplies, including personal protective equipment, will be determined at the onset of the event by the EMC. Medical supplies would include anything used in the care of Clients. Non-medical supplies would include food, linen, water, fuel, and transportation vehicles.

OE will obtain and replenish medications and related supplies, non-medical supplies, and personal protective equipment by storing extra critical supplies off site at various OE properties.

For those items that usage would exceed par levels as a result of a large scale incident or dates that would expire (e. g., additional antibiotics, vaccines, PPE), OE would collaborate with partnering businesses to expedite receipt of items when needed.

The amounts and locations of current supplies will need to be evaluated to determine how many hours the facility can sustain before replenishing. This will give the facility a par level on supplies and aid in the projection of sustainability before terminating services or evacuating if supplies are unable to get to the facility. The inventory of assets and resources is the starting point of par levels.

The processes for obtaining and replenishing those supplies once the par level has decreased will need to be identified. This would include a list of the vendors and contractors that deliver and manufacture the supplies. Most facilities have just-in-time delivery of supplies. A stockpile within the company or corporation, stockpile with the local vendor, prepayment of supplies to be used in times of emergency, or regional purchase of supplies to be stockpiled in a warehouse are some ways of obtaining and replenishing supplies. The disadvantage of these methods is the idea that one vendor would have enough for all Agencies within the region to deliver, but the supplies are not checked often for expiration or not located in a controlled environment, or the local, county, or state resources would pull that stockpile before Agencies could access the supplies for field use. It is ideal to have other vendors outside of regional and state areas also available for delivery of supplies. A disadvantage to supplies offsite would be a natural disaster where delivery of supplies would not be possible.

The importance of how many hours of sustainability on supplies is crucial to determine if services can still be rendered during a disaster. The planning of the sustainability of OE, without the support of the community within the first 72 hours, should be a coordinated effort of the EMC and the departments affected at the onset of the disaster. Where supplies and alternative means are required to sustain 72 hours, resources and assets, alternative sources, and the sustainability at that point must be identified. If near or around 72 hours cannot be sustained, policies and procedures must be in place on the response that the facility may conceivably evacuate or temporarily close. OE will identify resources and assets needed for sustainability.

MANAGING STAFF SUPPORT IN EMERGENCY SITUATIONS

During activations of the EOP, various modifications and accommodations are made for staff to assist them in coming to the agency to provide needed services. The following accommodations are authorized:

1. Where travel is difficult or impossible because of weather conditions, OE will work with groups with appropriate vehicles to assist staff in getting to and from the affected site.
2. Where necessary because of conditions, OE accommodates staff that need to sleep, eat, and/or other services in order to be at the site to provide needed services.
3. The Human Resource Department handles the needs of staff during the emergency. The CHRO is authorized to modify the normal use of agency space and/or to work with local hotels and motels to provide accommodations for staff. Meal service for staff is authorized where approved by the CHRO.
4. OE will be prepared for incident stress debriefings. These areas will be staffed by community mental health services, clergy, and others trained in incident stress debriefing as available. As part of planning for mass casualty and similar incidents, staffing and alternatives will be identified and contacted to determine facilities and processes to be used.
5. Communication to staff family members will also be arranged through the Human Resource Department in addition to utilizing auto calling software (Robotalker) and setting up a designated call-in number for more information.
6. If staff are unable to physically work in a client's home, the AIC may decide to allow clients to be supported in a staff's home.

MANAGING CLIENT SUPPORT IN CRITICAL STAFFING SHORTAGES

In order to ensure the health and safety of the clients of Opportunity Enterprises (OE), all staff are expected to deliver the required level of care per an individual's state assigned ALGO level, even in critical staffing shortages.

1. It will be the responsibility of staff to maintain the appropriate level of supervision at all times.
2. It will be the responsibility of the Supported Living Scheduler/Supervised Group Living Manager to ensure appropriate staffing is in place by way of OE's scheduling system.
3. If the department experiences a shortage in staffing; the following tiered coverage system will be implemented:
 - a. All other homes/sites will be assessed to see if there are extra staff to be pulled to the open shift.
 - b. In the event that no extra staff are available to cover a shift, the Chief Human Resource Officer or Chief Program Officer will send an All User email notice to the Respite, Day Service DSP's, QIDP's and office staff requesting assistance in covering the open shift(s).

- c. If not all shifts are covered, members of the Administration will be expected to cover the open shift.
- d. As a last resort, mandatory overtime will be implemented to fill the need.

EMERGENCY PREPAREDNESS AND EVACUATION PROCEDURES

POLICY: To establish emergency procedures that detail appropriate actions to be taken for promoting safety in all types of emergencies. Being prepared and knowing what to do help the persons served and personnel to respond in all emergency situations, especially those requiring evacuation.

PURPOSE: These emergency preparedness and evacuation procedures will assist staff in assessing the situation, taking appropriate planned actions, and laying the foundation for continuation of essential services. These procedures can be used for natural disasters (tornado, flooding, snow, or other inclement weather), as well as other types of disasters/emergencies (fire, power failure, train derailment, airline crash, toll road accident, or active shooter)

Client Evaluation

Each person served will have an annual Fire and Emergency Risk Assessment completed. This will determine at-risk clients and help determine staff response in fire and emergency situations.

Evacuation Routes

- Evacuation route maps have been posted in each work area. The following information is marked on evacuation maps:
 - Emergency exits
 - Primary and secondary evacuation routes
 - Locations of fire extinguishers
 - Fire alarm pull stations' location
 - Assembly points
- Site personnel should know at least two evacuation routes.

Fire evacuation:

When fire is discovered:

- Activate the nearest fire alarm (if installed)
- Notify the local Fire Department by calling 911
- If the fire alarm is not available, notify the supervisory personnel about the fire emergency by voice or paging.

Upon being notified about the fire emergency, occupants must:

- Leave the building using the designated escape routes.
- Assemble in the designated area (specify location)
- Remain outside until the competent authority (Designated Official or designee) announces that it is safe to reenter.

Fire Drill Procedures

- Use a stopwatch or clock that has a second hand.
- Pull alarm pull station (or announce drill) and start timer.
- If clients are involved, teach evacuation skills as you observe drill. Assist as needed.

- As soon as everyone has exited and is at the designated assembly spot, stop timer and shut off alarm.
- Record each client's response to the drill as called for on the F-1 form.
- Fill out appropriate fire drill reports and submit to appropriate supervisors for review.

Relocation Drill Procedures

- Corvillia QIDP will direct staff to execute an evacuation drill and designate the relocation facility.
- Staff will load totes containing food supply and clothes, along with medications and binders with client medical information into group home vans
- Staff will assist all clients into group home vans or designated transportation and do a headcount of all evacuating prior to leaving
- When arriving at designated location staff will inform the Director of Operations of their location. The Compliance Officer will serve as a secondary contact.
- The Director of Operations/Compliance Officer will record both clients and staff present.
- Staff will complete Evacuation Drill worksheet

Tornado:

- When a warning is issued by sirens or other means, seek inside shelter.
 - Proceed to designated shelter areas. If there are no designated shelter areas, consider the following:
 - Small interior rooms on the lowest floor and without windows,
 - Hallways on the lowest floor away from doors and windows, and
 - Rooms constructed with reinforced concrete, brick, or block with no windows.
- Stay away from outside walls and windows.
- Use arms to protect head and neck.
- Remain sheltered until the tornado threat is announced to be over.

POWER FAILURE SAFETY PROCEDURES

- These emergency procedures for power failures should be carried out when power is out and conditions dictate (too hot, too cold, etc.) evacuation to assure the safety of the residents.
- Three (3) emergency flashlights with fresh batteries will be in a strategic location in each group home in case of power failure.
 - The batteries in these emergency flashlights will be marked with the date of installation and changed every 6 months.
 - Home managers will inspect these flashlights monthly to ensure that they are working properly.
- In the event of a power failure:
 - Locate and activate emergency lighting.
 - Place emergency lighting at strategic locations in the home to enable the residents' safe passage.

- Call the QIDP who will then call the power company and establish a timeline for repair.
- If extreme cold or heat, or other conditions dictate, the home will be evacuated. The QIDP will call the Director of Operations(DO) who will coordinate the evacuation, and contact CEO. See Emergency Relocation Plan.

DISASTER PROCEDURES

In the event of a disaster or threat of disaster the following steps will be taken to ensure the safety and welfare of the residents and staff.

- Staff will first ensure that residents are in or are put into a safe environment.
- Staff will call 911 if there is a need and then call the QIDP who will notify the DO.
- The home's QIDP will be called who will ensure that the home is adequately staffed. Staff working at the time of the disaster must be prepared to work extra hours if necessary. Staff will remain with residents until they are relieved by another staff member. The QIDP will call in extra staff as needed.
- Primary means of communication will be telephone land lines, cell phones, radio(WSBT).
- The CEO and administrative team will organize a plan to ensure the safety of both residents and staff. This evaluation will include determining if Corvillia facilities could be used by local emergency response agencies.
- Items to be evaluated in considering safety will be access to food, water, medical and pharmaceutical needs. Also evaluated will be the is there power to offer adequate temperature for clients and the food provisions. Is the fire detection still available? If not, Staff must start the Fire Watch procedure.
- Consideration will be given to if waste and sewage disposal is available.
- If it is determined that the group home is not a safe environment, the Emergency Relocation Plan will be put into effect.
- Corvillia will evaluate its ability to collaborate with official Government response to individual disaster situations.
- Staff will continue to use the online documentation service to maintain accurate communication and documentation of program and medical information. If the online documentation service is unavailable, written documentation will begin and be communicated to QIDP by phone or in person.
- Should the CEO not be available the *Administrative and Operational Coverage Policy* will be implemented.
- All locations will have weather radios along with emergency radios powered by batteries or self-powered. WSBT (960 AM and 96.1 FM) will be used for communication purposes.

EMERGENCY RELOCATION PLAN

- In case of an emergency; fire, tornado, flood, explosion, toxic spill, etc. Residents will be evacuated from the facility and other arrangements will be made until their home can be repaired and made a safe environment again. The CEO or a designee will coordinate the EMERGENCY RELOCATION PLAN.

- Full or partial evacuation will require contacting the Indiana State Department of Health at the ISDH contact number is 317-460-7287.
- Parents and guardians will be asked to offer short term help, if possible.
- Hotels and motels will be utilized in the short term.
- Corvilla's main office can be utilized in an emergency. There are enough portable cots for all clients. Food supplies and clothing will also be stored for possible emergencies.
- Clothing and food for three days will be stored in totes at the group homes. This will help facilitate a quick evacuation if needed. Homes will also have binders that will include face sheets, MARS, copies of birth certificates, social security cards, and insurance information.
- Location of all on duty staff and clients will be reported to Corvilla's Director of Operations.
- If any clients are missing, staff will follow the procedures in the *Elopement and Missing Persons Policy*
- Area agencies will be contacted about the possibility of temporary placement while repairs are being made to the damaged facility.
- Staff will continue to document using the online documentation services for programming and medication administration. If the online documentation service is unavailable, written documentation will begin and be communicated to QIDP by phone or in person.
- When relocating, all staff, contracted entities, client medical contacts and necessary volunteers will be contacted on a as needed basis by residential management staff.
- Relocations will be reported as necessary to Federal/State/Local emergency preparedness staff, ISDH, BDDS, and APS.
- Relocation drills will take place twice a year

BOMB THREATS

In the event of a bomb threat, the person receiving the threat should keep the caller on the phone. They should have another staff member call 9-1-1 and evacuate the building if directed by emergency personnel. Remain calm. At the end of the conversation, complete the Bomb Threat Report Form located in the Safety Manual and give it to the Bomb Squad as soon as possible. Responsible staff should account for all clients during the evacuation.

ACTIVE SHOOTER

See attached Active Shooter Policy

PANDEMIC

See attached Pandemic Policy

Origination Date: May 2018

Last Review/Revision: September 2021

Approved: Board of Directors

SAFETY AND HEALTH

8. A. POLICY REGARDING ACCESSING EMERGENCY OR MEDICAL INFORMATION

Purpose: To ensure emergency and medical information is confidential, but able to be accessed in case of an emergency.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees and Clients

Policy: It is the policy of Goodwill Industries to have emergency and medical information accessible in case of an emergency.

Procedures:

EMPLOYEE

When an employee is hired a Classification and Emergency Information Sheet is completed. This information is kept in the employee's medical file. This information is also kept in a locked box by the time clock at each store location, and in the break room at Magnavox Way, for quick access. This information is updated at least annually, or when an employee submits updated information.

In the event of an emergency, these forms will be used to notify the emergency contact, or inform medical personnel of any pertinent information. If the emergency occurs during office hours, Human Resources will access the emergency information. If the emergency occurs at any other time management can access the information in the locked box.

CLIENT

When a client is entered into programming, an Emergency Information form is completed. This information is kept in both the case file and a locked briefcase assigned to all Employment Services Department employees who have direct contact with the client.

In the event of an emergency, these forms will be used to notify the emergency contact, or inform medical personnel of any pertinent information. The assigned staff person will be responsible for accessing the emergency information.

This information is updated at least annually, or when a client submits updated information.

Forms: HR203 Classification and Emergency Information
R202 Emergency Information

Date Adopted: May 1994

Date Revised: March 2003

Date Reviewed: March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023

8. B. POLICY REGARDING BLOOD BORNE PATHOGENS

Purpose: To comply with OSHA's Blood borne Pathogens Standard (29 CFR 1910.1030) and reduce the possibility of infection.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees and Clients

Policy: It is the policy of Goodwill Industries to reduce occupational exposure to Hepatitis B Virus (HBV), Human Immunodeficiency Virus (HIV) other blood borne pathogens that employees may encounter in their workplace.

Procedures: Goodwill Industries believes that there are a number of "good general principles" that should be followed when working with blood borne pathogens and infectious diseases. These include that:

- It is prudent to minimize all exposure to blood borne pathogens and infectious diseases.
- Risk of exposure to blood borne pathogens and infectious diseases should never be underestimated.
- Our facilities should institute as many work practice and engineering controls as possible to eliminate or minimize employee exposure to blood borne pathogens and infectious diseases.

We have implemented this Exposure Control Plan to meet the letter and intent of the OSHA Blood borne Pathogens Standard. The objective of this plan is twofold:

- To protect our employees from the health hazards associated with blood borne pathogens and infectious diseases.
- To provide appropriate treatment and counseling should an employee be exposed to blood borne pathogens or an infectious disease.

GENERAL PROGRAM MANAGEMENT

A. Responsible Persons

There are four major "Categories of Responsibility" that are central to the effective implementation of our Exposure Control Plan. These are:

- The "Exposure Control Officer"
- Department Managers and Supervisors
- Education/Training Instructors
- Our Employees

The following sections define the roles played by each of these groups in carrying out our plan. (Throughout this written plan, employees with specific responsibilities are identified. If, because of promotion or other reasons, a new employee is assigned any of these responsibilities, the Human Resource Department is to be notified of the change, so that they can update their records.)

EXPOSURE CONTROL OFFICER

The "Exposure Control Officer" will be responsible for overall management and support of our facility's Blood borne Pathogens Compliance Program. Activities which are delegated to the Exposure Control Officer typically include, but are not limited to:

- Overall responsibility for implementing the Exposure Control plan for all ten locations.
- Working with management and other employees to develop and administer any additional blood borne pathogen-related policies and practices needed to support the effective implementation of this plan.
- Looking for ways to improve the Exposure Control Plan, as well as to revise and update the plan when necessary.
- Collecting and maintaining a suitable reference library on the Blood borne Pathogens Standard and blood borne pathogens safety and health information.
- Knowing current legal requirements concerning blood borne pathogens.
- Acting as a liaison during OSHA inspections.
- Conducting periodic facility audits to maintain an up-to-date Exposure Control Plan.

The Human Resources and Safety Director has been appointed as the Exposure Control Officer for all facilities.

We have determined that the Exposure Control Officer will require assistance in fulfilling the responsibilities. The Safety and Wellness Committee will assist in fulfilling these duties. The Safety and Wellness Committee is composed of the following people:

Human Resources and Safety Director
One employee from each store and each department

DEPARTMENT DIRECTORS AND SUPERVISORS

Department Directors and Supervisors are responsible for exposure control in their respective areas. They work directly with the Exposure Control Officer and our employees to ensure that proper exposure control procedures are followed.

EDUCATION/TRAINING COORDINATOR

Our Education/Training Coordinator will be responsible for providing information and training to all employees who have the potential for exposure to blood borne pathogens or infectious diseases. Activities falling under the direction of the Training Coordinator include:

- Maintaining an up-to-date list of facility personnel requiring training.
- Developing suitable education/training programs.
- Scheduling periodic training seminars for employees.
- Maintaining appropriate training documentation such as "sign-in sheets", quizzes, etc.
- Periodically reviewing the training programs with the Exposure Control Officer, Department Managers, and Supervisors to include appropriate new information.

The Human Resources and Safety Director has been selected to be the Education/Training Coordinator for all locations.

EMPLOYEES

As with all of Goodwill's activities, our employees have the most important role in our blood borne pathogens compliance program, for the ultimate execution of much of our Exposure Control Plan rests in their hands. In this role they must do things such as:

- Know what tasks they perform that have occupational exposure.
- Attend the blood borne pathogens training sessions.
- Plan and conduct all operations in accordance with our work practice controls.
- Develop good personal hygiene habits.

AVAILABILITY OF THE EXPOSURE CONTROL PLAN TO EMPLOYEES

To help employees with their efforts, our Exposure Control Plan is available to them at any time. Employees will be advised of this availability during their education/training sessions. Copies of the Exposure Control plan are kept in the following locations:

- Store Manager's Office at each store location
- Policy and Procedure Manual available on the computer public drive.

REVIEW AND UPDATE OF THE PLAN

We recognize that it is important to keep our Exposure Control Plan up to date. To ensure this, the plan will be reviewed and updated under the following circumstances:

- Annually, on or before **October 31st** of each year
- Whenever new or modified tasks and procedures are implemented which affect occupational exposure of our employees.
- Whenever our employees' jobs are revised such that new instances of occupational exposure may occur.
- Whenever we establish new functional positions within any location that may involve exposure to blood borne pathogens or infectious diseases.

EXPOSURE DETERMINATION

We have prepared the following lists to identify exposure situations:

- Job Classifications in which all employees have occupational exposure to blood borne pathogens and/or infectious diseases.
- Job Classifications in which some employees have occupational exposure to blood borne pathogens and/or infectious diseases.
- Tasks and procedures in which occupational exposure to bloodborne pathogens occur. These tasks and procedures are performed by employees in the job classifications shown on the following lists.

Our Exposure Control Officer will work with Department Directors and supervisors to revise and update these lists as our tasks, procedures, and classifications change.

JOB CLASSIFICATIONS IN WHICH ALL EMPLOYEES HAVE POTENTIAL EXPOSURE TO BLOODBORNE PATHOGENS AND/OR INFECTIOUS DISEASES

Below are listed the job classifications in our facility where all employees may come into contact with human blood or other potentially infectious materials, which may result in possible exposure to blood borne pathogens and/or infectious diseases:

JOB TITLE

Retail Sales Director	Support Supervisor
Store Manager	Janitor
Assistant Store Manager	Material Handler
Assistant Manager in Training	Clerk
Operations and Logistics Director	Truck Driver
Clothing Processor	Donation Attendant
Student Transition Coordinator	Student Transition Specialist
Procurement Specialist	Quality Specialist

JOB CLASSIFICATIONS IN WHICH SOME EMPLOYEES HAVE POTENTIAL EXPOSURE TO BLOODBORNE PATHOGENS AND/OR INFECTIOUS DISEASES

JOB TITLE: Maintenance Technician, Maintenance Assistant

WORK ACTIVITIES INVOLVING POTENTIAL EXPOSURE TO BLOODBORNE PATHOGENS AND/OR INFECTIOUS DISEASES

Below are listed the tasks and procedures where employees may come into contact with human blood or other potentially infectious materials which may result in exposure to blood borne pathogens or other infectious diseases:

Administering first aid
Sorting donations
Store/plant clean up
Collecting donations

METHODS OF COMPLIANCE

We understand that there are a number of areas that must be addressed in order to effectively eliminate or minimize exposure to blood borne pathogens and infectious diseases in our facility. The first five areas we deal with in our plan are:

- The use of Universal Precautions
- Establishing appropriate Engineering Controls
- Implementing appropriate Work Practice Controls
- Using necessary Personal Protective Equipment
- Implementing appropriate Housekeeping Procedure

Each of these areas is reviewed with our employees during their blood borne pathogens related training (see the "Information and Training" section of this plan for additional information). By rigorously following the requirements of OSHA's Blood borne Pathogens Standard in these five areas, we feel that we will eliminate or minimize our employees' occupational exposure to blood borne pathogens and infectious diseases as much as possible.

A. UNIVERSAL PRECAUTIONS

In our facilities, we practice "Universal Precautions". As a result, we treat all human blood and body fluids such as urine, semen and vaginal secretions as if they are known to be infectious for Hepatitis B, Hepatitis C, HIV, CMV, and other blood borne pathogens and infectious diseases.

In circumstances where it is difficult or impossible to differentiate between body fluid types, we assume all body fluids to be potentially infectious.

The Human Resources and Safety Director is responsible for overseeing our Universal Precautions Program.

B. ENGINEERING CONTROLS

One of the key aspects to our Exposure Control Plan is the use of Engineering Controls to eliminate or minimize employee exposure to all blood borne pathogens and infectious diseases. As a result, employees use cleaning, maintenance and other equipment that is designed to prevent contact with blood or other potentially infectious materials.

The Human Resources and Safety Director periodically works with Department Directors and supervisors to review tasks and procedures performed in our facilities where engineering controls can be implemented or updated. As part of this effort, a facility survey was completed identifying three things:

- Operations where engineering controls are currently employed.
- Operations where engineering controls can be updated.
- Operations currently not employing engineering controls, but where engineering controls could be beneficial.

Each of these lists will be examined during our annual Exposure Control Plan review and opportunities for new or improved engineering controls will be identified. Any existing engineering control equipment is also reviewed for proper function and needed repair or replacement every three months, in conjunction with the Department Director or supervisor where the equipment is located.

ENGINEERING CONTROL EQUIPMENT

The following operations have Engineering Control Equipment to eliminate or minimize our employees' exposure to blood borne pathogens. .

<u>DEPT/OPERATION</u>	<u>CONTROL EQUIPMENT</u>
First Aid	Latex Gloves CPR Masks
Janitor	Latex Gloves Bleach Spill Kits
Sorting	Latex Gloves Non-Latex Gloves Cotton Gloves Polyurethane Gloves

In addition, the following engineering controls are used throughout all locations:

Containers which are:

- Leak-proof
- Color-coded and/or labeled with a biohazard warning label
- Puncture resistant, if necessary

are provided for disposal of contaminated or potentially contaminated items.

C. WORK PRACTICE CONTROLS

In addition to engineering controls, our facilities will use a number of Work Practice Controls to help eliminate or minimize employee exposure to all blood borne pathogens and infectious diseases.

The person responsible for overseeing the implementation of these work practice controls is the Human Resources and Safety Director. This person will work with Department Directors, supervisors, and trainers to implement the controls.

Goodwill has adopted the following Work Practice Controls as part of our blood borne pathogen compliance program.

1. Employees must wash their hands immediately or as soon as feasible after removal of potentially contaminated gloves or other personal protective equipment.
2. Following any contact of body areas with blood or any other potentially infectious materials, employees must wash their hands and any other exposed skin with soap and water as soon as possible. They also must flush exposed mucous membranes with water.
3. Eating, drinking, smoking, applying cosmetics or lip balm and handling contact lenses is prohibited in work areas where there is a potential for exposure to blood borne pathogens and/or infectious diseases.
4. Food and drink may not be kept on countertops, tables, or in storage areas where blood or other potentially infectious materials are present.
5. Any items containing blood or other potentially infectious materials are placed in designated leak-proof containers, appropriately labeled with a biohazard warning label, for handling, storage, and disposal.

When a new employee comes to our facility, or an employee changes jobs within the facility, the following process takes place to ensure that the employee is trained in the appropriate work practice controls:

1. The employee's job classification and the tasks and procedures that they will perform are checked against the Job Classification and Tasks lists which we have identified as those in which occupational exposure may occur.
2. If an employee is transferring from one job to another within our facilities, their classification's tasks/procedures are checked against the lists to identify any new source of potential exposure.
3. By "cross-checking" we can identify occupational exposures that the employee may come in contact with and then the training coordinator can provide the employee with training on any work practice controls that the employee is not experienced with.

D. PERSONAL PROTECTIVE EQUIPMENT

Personal Protective Equipment is our employee's "last line of defense" against blood borne pathogens. Goodwill will provide (at no cost to the employee) the personal protective equipment that the employees need to protect themselves against exposure. This equipment includes but is not limited to:

- a) Gloves
- b) Face Masks (CPR)
- c) Goggles

The Human Resources and Safety Director is responsible for working with Department Directors and supervisors to ensure that all departments and work areas have the appropriate personal protective equipment available for all employees.

Our employees will be trained regarding the use of the appropriate personal protective equipment for their job classification and the tasks and procedures they perform.

To ensure that personal protective equipment is not contaminated and is in the appropriate condition to protect employees from potential exposure, we will adhere to the following practices:

1. All personal protective equipment will be inspected periodically and repaired or replaced as needed to maintain its effectiveness.
2. Reusable personal protective equipment is cleaned, laundered and decontaminated as needed.
3. Single-use personal protective equipment (or equipment that for whatever reason cannot be decontaminated) is to be disposed of by placing the item in the appropriate container that will be color-coded (red) or labeled with a biohazard label.

Our employees must adhere to the following practices in order to ensure that the personal protective equipment is used correctly and effectively:

1. Any garments penetrated by blood or infectious materials are removed immediately, or as soon as feasible.
2. All potentially contaminated personal protective equipment is removed prior to leaving a work area.
3. Gloves are worn in the following circumstances:
 - a. Whenever employees anticipate hand contact with potentially infectious materials.
 - b. When handling or touching contaminated surfaces.
4. Disposable gloves are replaced as soon as practical after contamination or if they are torn, punctured or otherwise lose their ability to function as an "exposure barrier".
5. Utility gloves are decontaminated for reuse unless they are cracked, peeling, torn, or exhibit other signs of deterioration, at which time they are disposed of.

E. HOUSEKEEPING

Maintaining our facilities in a clean and sanitary condition is an important part of our blood borne pathogens compliance program. We will set up a written schedule for cleaning and decontamination of appropriate areas of the facilities. The schedule will include the following information:

1. The area to be cleaned/decontaminated.
2. Day and time of scheduled work.
3. Cleansers and disinfectants to be used.
4. Any special instructions that are appropriate.

Along with the schedule our custodian staff will use the following practices:

1. All equipment and surfaces will be cleaned and decontaminated after contact with blood or other potentially infectious materials. This is to be done immediately or as soon as practical, when surfaces are apparently contaminated and at the end of the shift if the surface may have been contaminated during that shift.
2. Protective coverings (such as plastic trash bags or absorbent paper) are removed and replaced as soon as it is practical when it is apparent that they are contaminated and/or at the end of the work shift if they may have been contaminated during the shift.
3. All trash containers, pails, bins, and other receptacles intended for use are routinely inspected, cleaned, and decontaminated as soon as possible if visibly contaminated.
4. Potentially contaminated broken glassware is picked up using mechanical means (such as dustpan and brush).

The Retail Sales Director is responsible for making sure the cleaning and decontamination schedule is carried out within our facilities.

We must also be careful in our handling of regulated waste (including used bandages, feminine hygiene products and other potentially infectious materials). The following procedures will be used with all types of wastes:

1. The waste will be discarded in containers that are:
 - a. closeable
 - b. leak-proof, if the potential for spill or leakage exists
 - c. puncture resistant, if the discarded materials could penetrate the container.
 - d. red in color or labeled with the appropriate biohazard warning label.
2. Containers for the regulated waste will be placed in locations with easy access and as close as possible to the sources of waste.
3. Waste containers are maintained upright, routinely replaced, and are not allowed to overfill.

The janitor at each site is responsible for the collection and handling of our contaminated waste.

HEPATITIS B VACCINATION, POST EXPOSURE EVALUATION, AND FOLLOW-UP

Goodwill recognizes that even with good adherence to all of our exposure prevention practices, exposure incidents can occur. As a result, we have implemented a Hepatitis B Vaccination Program as well as set up procedures for post-exposure evaluation and follow-up, should exposure to blood borne pathogens occur.

VACCINATION PROGRAM

Goodwill's Hepatitis B vaccination program is available, at no cost, to all employees who have occupational exposure to blood borne pathogens.

The vaccination program consists of a series of three inoculations over a six month period. As part of the blood borne pathogens training, our employees will receive information regarding hepatitis B vaccination, including its safety and effectiveness.

The Human Resources Department is responsible for setting up and operating the vaccination program.

Vaccinations will be performed under the supervision of a licensed health practitioner. Employees who decline to take part in the program will need to sign a "Vaccination Declination Form".

POST EXPOSURE EVALUATION AND FOLLOW-UP CARE

All post exposure evaluations and follow-up care shall be administered by a licensed health practitioner. If an exposure incident occurs the exposed employee shall complete an exposure incident investigation form and a critical incident report will be completed. The original form shall be given to the Exposure Control Officer. The employee shall take a copy of the investigation form and report directly to a licensed health practitioner.

After the information regarding how exposure occurred has been gathered and evaluated, a summary will be prepared and recommendations given on ways to avoid similar incidents in the future.

After consent is obtained, the source individual's blood will be tested for HBV and HIV. Even if the source individual is already known to be infected with HBV or HIV a blood test is still required. If the source individual does not give consent for HIV testing, the laboratory will retain the blood for ninety (90) days in case the employee later elects to have the test performed.

Goodwill will provide appropriate medical evaluation and measures designed to preserve health and prevent the spread of disease at no cost to the employee. Physician counseling and evaluation of reported illness will be provided whether or not the employee elected to have a baseline HBV or HIV test. The physician's written opinion will be provided to the employee within fifteen days of the exposure incident. The opinion will include:

1. Whether hepatitis B is indicated.
2. Confirmation that the employee has been informed of the results of the evaluation.
3. Whether the employee has received the vaccine.
4. Confirmation the employee has been told about any medical conditions resulting from exposure to blood or other potentially infectious materials which may require further evaluation and or treatment.

All other findings or diagnoses will remain confidential and will not be included in the written report. Post exposure evaluation and follow-up care shall be provided to the employee at no cost to the employee.

We recognize that much of the information involved in this process must remain confidential, and we will do everything possible to protect the privacy of all those involved.

LABELS AND SIGNS

The biohazard warning label is the most obvious warning of possible exposure to blood borne pathogens. The labeling Goodwill will use includes biohazard labels and/or stickers and/or red "color coded" containers. We will use labels or stickers on the following items in our facilities:

1. Containers of regulated waste.
2. Other containers used to store, transport or ship blood or other infectious materials.
3. Contaminated equipment.

INFORMATION AND TRAINING

All employees who have the potential for exposure to bloodborne pathogens will be put through a comprehensive training program. Employees will be retrained at least annually. In addition, any employee who changes jobs or job functions will be given any additional training their new position requires. Human Resources is responsible for seeing that all employees who have potential to exposure to blood borne pathogens and/or infectious diseases receive training.

The topics of our training program will include:

1. The blood borne pathogens standard.
2. The symptoms of blood borne diseases.
3. The modes of transmission of blood borne pathogens.
4. Goodwill's exposure control plan.
5. Appropriate methods for recognizing tasks and other activities that may involve exposure to blood and other potentially infectious materials.
6. Use (and limitations) of methods that will prevent or reduce exposure including engineering controls, work practice controls, and personal protective equipment.
7. Selection and use of personal protective equipment including types available, proper use, location at each facility, removal, handling, decontamination, and disposal.
8. Visual warnings of biohazards (labels, color coded containers).
9. Information on the Hepatitis B Vaccine, including our free vaccination program.
10. Actions to take and procedures to follow if an exposure incident occurs.
11. Information on post exposure evaluation and follow-up.

Forms: HR210 Vaccination Declination Form
 HR615 Critical Incident Report

HR606 Exposure Incident Investigation
HR607 Post Exposure Evaluation and Follow-up Checklist

Date Adopted: **May 1994**

Date Revised: **March 2003, May 2014, May 2016, May 2017, April 2018, June 2021**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. C. POLICY REGARDING BUSINESS CONTINGENCY

Purpose: To ensure procedures are in place in case of an emergency/disaster.

Responsibility: President/CEO

Personnel Affected: All Goodwill Employees

Policy: It is the policy of Goodwill Industries to have procedures in place in case of an emergency/disaster.

Procedures:

These procedures are not intended to stand alone, but will be put into place concurrently with Crisis Communication, IT Disaster Recovery, and our Risk Management Plan. In the event of a disaster (tornado, flooding, fire, terrorist attack or other public emergency such as a flu pandemic) this plan will be implemented as follows:

Initial Preparation

Goodwill has determined that no service that we provide would be considered an essential service (such as health care) and will temporarily cease or minimize services if providing services would put clients, employees or the public at risk. In the event of a disaster, Goodwill stores, operations and offices will cease operations when:

1. Federal, State and/or Local officials request that all businesses close
2. The President/CEO of Goodwill Industries determines it is appropriate to close

Store Closing Procedures

Store management is responsible for maintaining a current employee contact list for all employees of their facility. If it is determined that the store will be closed for more than 5 days, store management will deposit all funds (including change fund and petty cash) in the bank upon the direction of the Retail Sales Director.

The President/CEO and the Retail Sales Director will maintain current contact information for store management and the Maintenance Department employees and contact information for critical contacts such as landlords. The Executive Management Staff will maintain current contact information for each other. Contact information is also available through the appropriate database and is stored off site in a fire proof safe.

Temporary work locations:

In the event of a store facility incurring damage to the extent that it became inoperable, the Plant Store/Distribution Center, 3127 Brooklyn Avenue, Fort Wayne will serve as a temporary work location for the dislocated employees.

If the Plant facility is not operable, the dislocated employees will report to the Goodwill Corporate Office, 1516 Magnavox Way, Fort Wayne and will be given a temporary work location at another facility as available.

If the Corporate Office facility is not operable, all other facilities may become temporary work sites. Corporate Office employees will initially report to The Plant Store/Distribution Center and will be assigned a temporary work site as appropriate.

Procedures when all facilities must be closed:

If Goodwill must close all facilities for an extended period (more than 3 days) Goodwill will operate with a skeleton crew. If the closure is due to a flu pandemic the designated employees will, whenever possible, work staggered shifts to avoid contact. Executive staff will have appropriate network access from home.

Payroll

Human Resources and Finance Departments will, as resources permit, process payroll. Employees who are eligible to use their accrued PTO time will be paid from their accrued time. The Human Resources and Safety Director and the CFO will complete payroll and direct deposit will continue, providing power utilities, our computer network and banking institutions are operational. We will mail paychecks by US mail for

employees who are not on direct deposit to the last known address, (as long as the U.S. mail system is operational).

Communication when all facilities are closed:

Employees: The President/CEO and/or the Retail Sales Director will contact store, operations, employment services and administrative management personnel with updated information. The managers will then contact their employees. If the resources are available, we will post information to our website: www.fwgoodwill.org and on Facebook and Twitter. We will also contact the Goodwill Industries International Office in a severe situation. You may also be able to obtain information from their website: www.goodwill.org or by phone at (800)741-0197.

Clients: All clients will automatically be placed on "Interrupt" status. If resources are available, we will post information to our website: www.fwgoodwill.org. When we are able to resume services, our clients will be contacted.

Mail collection

The President/CEO, Retail Sales Director, or their designee will make arrangements to collect the mail for each location.

Preventing flu and other communicable disease transmission at work:

Goodwill employees will be required to take steps to prevent the spread of illness in the workplace as follows:

Hand washing: Clean hands often with soap and water or an alcohol-based hand cleaner (especially after coughing sneezing or using the rest room). Hand sanitizer is to be kept at all registers.

Cough Etiquette: Cover mouth and nose with a tissue each time you cough or sneeze. If a tissue is not available, sneeze or cough into sleeve.

Stay home when ill: Employees are not permitted to come to work with a fever. If they do, they will be sent home.

Social distancing: Avoid close contact with people who are sick. Maintain a 3 foot distance when possible. Gloves and masks will be available. An employee who comes to work with a cough may be required to wear a mask if they will be working in close contact with others.

Forms: Not Applicable

Date Adopted: **May 2003**

Date Revised: **June 2009, May 2016**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. D. POLICY REGARDING COMPREHENSIVE SAFETY INSPECTIONS

Purpose: To enhance and maintain health and safety practices.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees

Policy: All facilities utilized for providing employment services (owned, leased or rented by Goodwill Industries of Northeast Indiana), will undergo regular, comprehensive inspections.

Procedures: Once each year an external company will conduct a comprehensive inspection at each facility. The inspection will include physical structures, equipment, machinery, emergency systems and safety policies and procedures. The inspector will verify compliance with OSHA regulations as well as fire code compliance.

A written report detailing any compliance deficiencies will be reviewed with the Executive staff and the safety committee. A plan to correct any deficiencies will then be developed.

The inspection report along with the correction plan will be reviewed with all affected employees, the Board of Directors and the safety committee.

Additionally, on a semi-annual basis, the Human Resources and Safety Director will conduct internal comprehensive inspections. The internal inspection will follow the same format as the external inspection.

All inspection reports will be maintained in the master safety binder.

Forms: Safety Checklist

Date Adopted: **March 2003**

Date Revised: **March 2004**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. E. POLICY REGARDING DRIVER'S LICENSES/INSURANCE/SEATBELTS

Purpose: To ensure all employees driving in the course of their work for Goodwill Industries are properly trained, licensed, and insured.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees

Policy: It is the policy of Goodwill Industries to allow only properly trained, licensed and insured employees to drive on company business.

Procedures:

Truck Drivers:

In order to drive a truck for Goodwill, employees must have a valid chauffeur's or CDL license and be insurable by our insurance carrier. At the time of hire for or promotion to a truck driver position, a copy of the individual's driver's license will be used to verify the driving record through the Bureau of Motor Vehicles.

All drivers must have and maintain a satisfactory driving record in order to drive for Goodwill Industries. Employees are required to inform Goodwill of any changes affecting their driving privileges. Training will be provided by Goodwill for all truck drivers, at new hire, and annually thereafter.

Driving records for truck drivers will be verified annually. Truck drivers are required to keep their license with them at all times while driving for Goodwill.

Goodwill Industries will not be responsible for any traffic or parking violations.

Due to safety concerns, all employees are required to wear seatbelts and may not eat, drink, smoke, or use a cell phone while in a Goodwill truck.

Goodwill expects drivers to obey all speed limits and all other traffic rules.

Personal Cars:

Employees driving personal cars on company business will be required to have a valid driver's license and carry the proper insurance. Copies of employee's driver's licenses will be used to verify the driving record through the Bureau of Motor Vehicles. Driving records will be verified annually

Employees must also submit proof of insurance, at minimum levels of 100,000/300,000/50,000 (bodily injury/property damage). Upon hire and at renewal every employee driving their personal vehicle on Goodwill business is required to submit a copy of their new policy to Human Resources. It is each employee's responsibility to maintain insurance at the approved levels.

Any employee who does not have the required amounts of insurance will have 90 days in which to obtain it. If the employee is transporting clients, the required insurance must be obtained within 30 days.

Employees who drive on Goodwill business must have and maintain a satisfactory driving record in order to drive for Goodwill Industries. Employees are required to inform Goodwill of any changes affecting their driving privileges.

Driver's training will be provided by Goodwill at new hire, and annually thereafter. Employees who transport clients will receive additional training in assisting passengers with disabilities.

Goodwill Industries will not be responsible for any traffic or parking violations.

Any employee on Goodwill business in a personal or company vehicle, as a driver or passenger, is required to wear a seatbelt.

Goodwill expects drivers to obey all speed limits and other all traffic rules.

Goodwill employees may not text while driving. Hands free cell phone use is permitted, but not encouraged or required.

All employees transporting clients will keep a roadside emergency packet in their vehicles, along with a fleet safety kit.

Forms: Drivers Licenses
 Identification (Business) Cards
 Insurance Verifications
 Drivers License Verifications
 Driver's Training Checklist

Date Adopted: **May 1994**

Date Revised: **May 2013, May 2017, April 2018**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. F. POLICY REGARDING DRUG-FREE WORKPLACE

Purpose: To maintain a safe, healthful and productive working environment in compliance with the Drug-Free Workplace Act of 1988.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees

Policy: It is the policy of Goodwill Industries to prohibit the possession, use or sale of an illegal drug, or alcohol in the workplace and to conduct random drug testing to ensure compliance with this policy.

Procedures:

1. ALCOHOL

Possession, use or being under the influence of alcohol by an employee while at work or on Company property or on Company business is prohibited.

2. ILLEGAL DRUGS

Possession, use, sale, purchase or being under the influence of an illegal drug by an employee while at work or on Company property or on Company business is prohibited.

3. SEARCHES

The Company may conduct searches for illegal drugs or alcohol on Company property when there is reasonable cause to suspect that illegal drugs or alcohol are present. Searches may include an employee's personal property including, but not limited to the employee's automobile, clothing, lunch box, cooler, purse, parcels, and similar items.

4. LEGAL DRUGS

An employee's use of a legal drug can pose a significant risk to the safety of the employee or others. The use of, or being under the influence of, any legally obtained drug while at work or on Company property or on Company business is prohibited if such use or influence may affect the safety of the employee, his or her co-workers or members of the public.

An employee who has reason to believe that the use of a legal drug may present a safety risk to himself or others must report such drug use to the Company to determine job-related consequences. The Company may require the employee to take a leave of absence or comply with other appropriate remedies determined by management.

5. DRUG AND ALCOHOL TESTING

The Company may require a blood test, breathalyzer test, urinalysis, saliva testing or other drug/alcohol testing of an employee whom the Company has reasonable cause to suspect of using or being under the influence of a drug or alcohol while at work or on Company property or on Company business. This may include an employee who has been involved in a plant accident and is reasonably suspected of being under the influence of drugs and/or alcohol.

Note: The symptoms of influence are not confined to those consistent with misbehavior, nor to obvious impairment of physical or mental ability, such as slurred speech or difficulty in maintaining balance. A determination of influence can be established by a professional opinion, a scientifically valid test, and, in some cases, by a layperson's opinion.

An alcohol test which reveals any alcohol in the employee's blood stream will be considered conclusive evidence that the employee was "under the influence" of alcohol within the meaning of this Substance Abuse Policy.

If a drug test reveals that an employee has illegal drugs in his/her system, the test results will be considered with other evidence that the employee was "under the influence" of illegal drugs at the time of the test.

If an employee is required to leave work for a drug or alcohol test, the Company will pay the employee for time lost from scheduled work for that day, provided the employee's test results are negative.

6. DRIVERS

- a. Employees who are hired to drive for Goodwill will be tested post offer.

7. RANDOM TESTING

Goodwill will randomly test employees for compliance with its drug-free workplace policy. As used in this Policy, "random testing" means a method of selection of employees for testing, performed by an outside third party. The selection will result in an equal probability that any employee from a group of employees will be tested. Furthermore, Goodwill has no discretion to waive the selection of an employee selected by this random selection method.

8. SUBSTANCES COVERED BY DRUG/ALCOHOL TESTING

Employees will be tested for their use of commonly-abused controlled substances, which include: Amphetamines, Barbiturates, Benzodiazepines, Opiates, Cocaine, Marijuana, Methadone, Methamphetamines, Methaqualone, Phencyclidine (PCP), Propoxyphene, and chemical derivatives of these substances as well as alcohol.

Employees must advise testing lab employees of all prescription drugs taken in the past month before the test, and to be prepared to show proof of such prescription to testing lab personnel.

9. SUBSTANCE ABUSE TESTING

Goodwill uses drug and alcohol testing to help administer this policy. Testing is done under the following circumstances:

1. Employees will be tested for reasonable suspicion or probable cause.
2. Post accident (including forklift) testing: In the event of a work related injury testing will be discretionary depending on the facts and circumstances of the case.
3. Random drug screening of the employee population on a periodic basis using random selection.

10. TESTING METHODS AND PROCEDURE

All testing will be conducted by a licensed independent medical laboratory, which will follow testing standards established by the State or federal government. Confirmation testing will be conducted on a urine sample provided by the employee to the testing laboratory under procedures established by the laboratory to insure privacy of the employee, while protecting against tampering/alteration of the test results.

Employees will be considered to be engaged at work for the time spent in taking the initial screening test, and will be compensated for such time at their regular rate.

Goodwill will pay for the cost of the testing, including the confirmation of any positive test result by gas chromatography. The testing lab will retain samples in accordance with State law, so that an employee may request a retest of the sample at his/her own expense if the employee disagrees with the test result.

11. POSITIVE TEST

If an employee tests positive on an initial screening test, the employee will be temporarily suspended while the confirmation test is being conducted. Upon receipt of positive test results on the confirmation test, the employee will be subject to disciplinary action, up to and including discharge.

12. RIGHT TO EXPLAIN TEST RESULTS

All employees and applicants have the right to meet with the testing laboratory personnel, and with Goodwill, to explain their test results. These discussions shall be considered confidential except that information disclosed in such tests will be communicated to personnel within Goodwill or within the Lab who need to

know such information in order to make proper decisions regarding the test results or regarding the employment of the individual.

13. RIGHT TO REVIEW RECORDS

Employees have a right to obtain copies of all test results from the testing laboratory, or from Goodwill. When the individual disagrees with the test results, the individual may request that the testing laboratory repeat the test. Such repeat test shall be at the expense of the individual, unless the repeat test overturns the original report of the Lab, in which case Goodwill will reimburse the employee for the costs incurred for the retest.

14. CONFIDENTIALITY REQUIREMENTS

All records concerning test results will be kept in medical files which are maintained separately from the personnel file of the employee.

Testing laboratories may conduct testing only for substances included on the disclosure list provided to the individual, and may not conduct general testing related to the medical conditions of the individual which are unrelated to drug usage.

15. RETESTING

Employees may request a retest of their positive test results, within five (5) working days after notification by Goodwill of such positive test result. This retest is at the expense of the individual, unless the original test result is called into question by the retest.

Where the employee/applicant believes that the positive test result was affected by taking of lawful or prescribed substances, the individual may be suspended without pay pending receipt of confirming information to substantiate the claims of the individual. Normally, the individual will be provided no more than two (2) business days in which to provide this additional information.

Once Goodwill has determined whether or not there is evidence to indicate that the test results are incorrect, Goodwill will advise the individual of its decision.

16. TERMINATION AND REHIRE

Employees who test positive for any drug(s) listed on the Disclosure List may be discharged immediately and will not be considered for rehire.

17. DISCIPLINARY ACTION

Violation of any of the provisions of this Substance Abuse Policy may result in termination, even for a first offense.

An employee's refusal to consent to a drug/alcohol search or test under the provisions of this policy may also result in termination, even for a first refusal.

An employee who is participating in a chemical dependency treatment program may be required to undergo periodic drug/alcohol testing at any time at the sole discretion of management during the treatment, and for up to two years following completion of any chemical dependency treatment program.

An employee who has successfully gone through treatment and who subsequently is found to be "under the influence" or who tests positive on a periodic test as described in this Substance Abuse Policy may be terminated.

18. DEFINITIONS FOR THE PURPOSE OF THIS POLICY

"Under the influence" means that the employee is affected by a drug or alcohol or the combination of a drug and alcohol in any detectable manner.

"Legal Drug" means prescribed drugs and over-the-counter drugs which have been legally obtained and are being used for the purpose for which they were prescribed or manufactured.

"Illegal Drug" means any drug (a) which is not legally obtainable or (b) which is legally obtainable but has not been legally obtained. The term includes prescribed drugs not legally obtained and prescribed drugs not being used for prescribed purposes. It also includes marijuana.

As mandated by the Drug-Free Workplace Act of 1988, employees must report any convictions under a criminal drug statute for violations occurring on or off Company premises while conducting Company business. Report of a conviction must be made to the Company within five (5) days after the conviction. The Company will then notify the appropriate contracting officer within ten (10) days after receiving notice from either the employee or from another source. Within thirty (30) days of learning of a conviction, the Company will discipline the employee.

Training will be held annually (and at new hire orientation) to explain Goodwill's Substance Abuse Policy. This will include discussion of the hazards of substance abuse in the workplace. The impact of drug or alcohol abuse within the workplace is a serious matter. All employees must be alert to the signs of substance abuse.

Forms: Not Applicable

Date Adopted: **May 1994**

Date of Revision: **July 2013, May 2014, May 2016**

Date Reviewed: **May 2012, July 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. G.

POLICY REGARDING EMERGENCY PROCEDURES

Purpose: To ensure employees are aware of what to do in the event of an emergency.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees

Policy: It is the policy of Goodwill Industries to ensure all employees, customers, clients, volunteers, interns, and visitors have a safe environment, with provisions planned in advance in case of an emergency.

Procedures: Each Goodwill office has an Emergency Procedures flip chart that is a quick reference detailing what needs to be done in each type of emergency.

In the event any of our locations need to be evacuated, employees, customers, clients and visitors are to report to the designated areas. After the situation is assessed, further directions will be announced.

Employment Services staff is responsible for making sure any clients in the building are evacuated or are in the safety zone as appropriate.

Any employee who may require assistance will be assigned a "buddy", upon request, who will assist when any emergency actions must be taken.

One of the following types of drills will be held or reviewed each month on each shift at each location: Fire, Tornado, Bomb Threat, Medical Emergency, Violent/Threatening Situation and Power Failure. At least one drill per quarter will require everyone to evacuate the building.

A written analysis of each drill will be completed in order to determine the effectiveness of the procedures. The results of the drill will be discussed at the next Safety Committee meeting, and a copy will be given to the President/CEO.

Safety Captains are designated for each area of the facility and it is their responsibility to be sure that all employees are out of the building and in the designated areas. All persons must evacuate the building immediately during drills. If the Safety Captain is not at work, store management has been trained to serve this function.

FIRE

All locations are equipped with heat detectors, manual pull alarms and strobe horns. The manual pull alarms are located next to the exits at each location.

If you discover smoke or fire:

1. Pull the nearest fire alarm.
2. Evacuate the building.
3. Leave all lights on and close all doors.
4. Once outside everyone must meet in the parking lot. Everyone must stay at least 50 yards away from the building. At the plant store everyone must go to the back of the employee parking lot (by the fence).
5. At the Corporate office the administrative assistants are responsible for ensuring the building is evacuated. Management is responsible for this function at all other locations.

Fire extinguishers have been placed throughout Goodwill. These extinguishers are to be used only if the fire is blocking an exit. **NEVER** attempt to extinguish a fire unless there is no alternative way to evacuate the building.

Fire drills will be held quarterly at all locations.

CAUTION: Do not attempt to operate the terminal or any other electrical equipment when a fire has been spotted.

TORNADO

In the event of a tornado or other serious weather conditions we have designated areas at each location as **Safety Zones**.

The **Safety Zone** at **Angola** is the hallway to the public restroom.

The **Safety Zone** at **Auburn** is the break room.

The **Safety Zone** at **Glenbrook** is the hall way.

The **Safety Zone** at **Covington** is the restroom hallway

The **Safety Zone** at **Dupont** is the restroom hallway .

The **Safety Zone** at **Huntington** is the emergency exit hallway.

The **Safety Zone** at **Magnavox Way** is the hallway by the mail room.

The **Safety Zones** at the **Plant Store** are the locker hallway and the front hallway between the store and the break room, whichever is closer.

The **Safety Zone** at **Chapel Ridge** is the break room and hallway.

The **Safety Zone** at **East State** is the break room and back room (by the break room)

A manager will lock the entrance and exit doors and no one will be permitted to leave the building until the "all clear" is given either by radio, siren, or other notification.

Tornado drills will be held semi-annually at all locations.

BOMB THREAT

In the event of a bomb threat or discovery of a suspicious package, a fire drill will be called to evacuate the building. The employee answering this type of call will be

encouraged not to panic, to complete the bomb threat checklist, and notify management. Everyone will meet in the same areas as for a fire and the safety captains are responsible for seeing that everyone is out of the building.

The store manager or Human Resources and Safety Director is to call 911. We will follow whatever directives are given us from the Police Department. The President will determine how to implement the Police Department directives. If the President is unavailable, the Human Resources and Safety Director will make this decision.

MEDICAL EMERGENCY

In the event of a medical emergency, first aid will be administered only by trained, qualified persons. Only those employees who are trained may administer first aid. The first aid kit at Magnavox Way is located in the break room, at Huntington it is located outside the store office and at all other locations the first aid kits are located by the time clock. Notify your supervisor if you require first aid.

The following employees have been trained in First Aid and CPR:

- Assistant Store Managers
- Assistant Managers in Training
- Employment Specialists
- Human Resources and Safety Director
- Job Support Specialists
- Maintenance Technician and Assistant
- Operations and Logistics Director
- Student Transition Coordinators
- Student Transition Specialists
- Support Supervisors
- Store Managers

Call 911 if the injured or ill person is:

- a) Unconscious or confused
- b) Gasping for breath or blue
- c) In shock (very weak, pale, cold and clammy)
- d) Bleeding severely
- e) In severe pain

After 911 has been called, send a co-worker outside to guide the emergency response personnel to the injured person.

When an employee is hired an Emergency Information Sheet is completed. This information is kept in the employee's confidential information file. It is also kept in a locked box by the time clock for quick access. This information is updated at least annually, or when an employee submits updated information.

In the event of an emergency, these forms will be used to notify the emergency contact, or inform medical personnel of any pertinent information. If the emergency occurs during office hours, Human Resources will access the emergency information. If the emergency occurs at any other time the store management has access to the information in the locked box by the time clock.

All accidents and medical emergencies **MUST** be reported immediately to your supervisor.

An accident report will be completed for each accident, even if it is minor and medical treatment is not required.

All non-life threatening occupational injuries are to be sent to our company doctor. If the injury is not life threatening, the employee may be transported in a personal or company vehicle.

Redi-Med:

Southwest	7333 West Jefferson	435-7334
Business Health	5932 West Jefferson	436-2273
North	315 E. Cook Road	458-3800
Northeast	3717 Maplecrest Road	486-7334
Huntington	2708 Guilford Street	355-3580
Auburn	1310 E. 7 TH St. Suite D	925-9511

Parkview Occupational:

North	3978 New Vision Drive	672-4680
South	9318 Airport Drive	373-9330
Central	3415 Hobson Road	373-9300
Huntington	2855 N Park Ave, Suite 102	355-3570
Columbia City	1270 E. S.R. 205, Suite 040	248-9490

Hours vary by location. Please call for current operating hours.
Angola employees should go to:

Urgent Care of Cameron Hospital

1381 N. Wayne

665-8222

Referrals for treatment are required to be eligible for company coverage. Referrals may be obtained from the store management, Department Directors or Human Resources.

ACTIVE SHOOTER

In the event of an active shooter, research has shown it is best to flee the area. Therefore individuals should first try to run away from the shooter. If you cannot run, your next safest move is to hide. If there is a locked room, hide there. If that is not available, find anything close by to hide behind. Your last choice is to fight. Try to find a fire extinguisher, chair, scissors, or anything you can use as a weapon.

Remember – RUN, HIDE, FIGHT

POWER FAILURE

All locations are equipped with battery back-up emergency lighting and a weather radio.

All customers must leave the building and the manager will lock the doors. Employees and clients are to stay in the building if possible. The Retail Sales Director must be notified if the power is not restored within 30 minutes. Any further instructions from the Retail Sales Director will then be followed. If the Retail Sales Director is unavailable, the Human Resources and Safety Director is to be notified and will provide instructions as to what further steps are to be taken.

INCLEMENT WEATHER (INCLUDING FLOODS, SNOW/ICE STORMS)

Goodwill will be open unless the President/CEO or Retail Sales Director decide otherwise. If the President/CEO decides not to open Goodwill operations, all Department Directors will be notified, and they will be responsible for notifying their department employees. Goodwill will also attempt to announce the closing in the local media (radio and TV) and on social media.

In the absence of the President/CEO, the Operations Director and the Retail Sales Director will make the determination as to whether or not to close.

Employees who feel they cannot safely travel to or from Goodwill are required to contact their immediate supervisor to make arrangements. Weather-related tardies may be dismissed at the discretion of Human Resources.

Partial day or closings for weather-related incidents will be paid for salaried employees.

Weather-related absences for hourly employees will be paid if the employee has benefit time available. Otherwise, the absence will be unpaid.

VEHICLE ACCIDENT

In case of an accident involving a company vehicle, there is a yellow envelope from our insurance carrier explaining what to do. This envelope will be kept in the vehicle. In addition to what the insurance carrier requires, the driver or material handler on the truck must call the Operations and Facilities Director, and report the incident as soon as possible. An accident report (First Report of Injury) is to be completed if there is a personal injury.

BURGLARY

In the event an employee reports to work to find one of our locations has been broken into, do not enter the building. Go to the nearest telephone and call 911 to report the burglary. After reporting the burglary, call the Retail Sales Director. If you are unable to

reach the Retail Sales Director, call the President/CEO . Do not enter the building, or allow others to enter, until the police have arrived.

ROBBERY

In the event of a robbery, complete cooperation is required. If you are asked to give the person any money or items, do so immediately. Try to get a good description of the individual. As soon as possible call 911 to report the robbery. Inform the President/CEO and Retail Sales Director immediately after calling 911.

CHEMICAL SPILL

If there is a spill of a chemical at Goodwill, refer immediately to the Safety Data Sheet (SDS) to determine the appropriate method of containing and cleaning up the spill. Follow directions exactly.

If there is a chemical spill in the vicinity of one of our locations, employees are to follow the instructions given by the police or hazardous material team. Call the Retail Sales Director to report the occurrence immediately.

CRISIS

If a crisis situation arises that could paralyze operations the following procedures are to be followed:

- Protect people first, property second
- Follow safety procedures as required
- Remain calm
- Do not excite others
- Be patient
- If possible listen to radio for news and instructions
- Follow the advice of local emergency official
- Do not light matches or candles or turn on electrical switches
- Notify management in this order:
 1. President/CEO
 2. Retail Sales Director
 3. Human Resources
 4. Manager

The management at each location is responsible to:

- Check for fires or fire hazards
- Check for injuries, give first aid, and get help for seriously injured people
- Sniff for gas leaks, starting with the water heater
- If you smell gas or suspect a leak, turn off the gas valve, open windows and get everyone out side quickly
- Shut off any other damaged utilities from diagram at each location

Critical business records (insurance policies, bank account numbers, computer back-up tapes) are housed at another Goodwill location..

A Critical Incident Report will be completed if necessary.

CONTINUANCE OF SERVICES

If a facility must be temporarily closed, services will be re-located to another facility.

Forms: Not Applicable

Date Adopted: **May 1994**

Date Revised: **May 2013, May 2014, April 2015, May 2016, May 2017, April 2018**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. H POLICY REGARDING HAZARDOUS COMMUNICATION

Purpose: To comply with OSHA's Hazardous Communication Standard (29 CFR 1910.1200 and 29 CFR 1926.59)

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees

Policy: It is the policy of Goodwill Industries to determine hazardous chemicals in the workplace and inform employees of the hazards associated with each chemical.

Procedures:

I. Hazard Determination

- A. Goodwill Industries will be relying on Safety Data Sheets from material suppliers to meet hazard determination requirements.
- B. The Safety Committee is given the authority to approve all chemicals used at Goodwill.

II. Labeling

- A. The Human Resources and Safety Director will be responsible for seeing that all containers coming in are properly labeled.
- B. All incoming labels shall be checked for: Identity, hazard warning, and name and address of responsible party.
- C. All containers used in the work areas will be labeled with identity and hazard warning.
- D. The Human Resources and Safety Director shall review and update label information on a semi-annual basis.

III. Safety Data Sheets (SDS)

- A. The Human Resources and Safety Director will be responsible for compiling the master SDS file. It will be kept in the Human Resources offices.
- B. Copies of SDSs for all hazardous chemicals to which employees may be exposed will be kept posted in their work area, by the time clock.
- C. SDSs will be available for review to all employees during each work shift. Copies will be available upon request to the supervisor.

- D. The Human Resources and Safety Director shall make requests for SDSs on all purchase orders. A file of follow up letters shall be maintained for all shipments received without SDSs.
- E. The Human Resources and Safety Director shall provide postings notifying employees of new or revised SDS.

IV. Employee Information and Training

- A. The Human Resources and Safety Director and Retail Sales Director shall be responsible for training, coordinating and maintaining records of training conducted at Goodwill.
- B. Before starting work, each new employee will attend a safety orientation which will have information on:
 - details of Goodwill's Hazardous Communication Program
 - chemicals and their hazards in their work areas
 - methods used to detect the presence or release of a hazardous chemical
 - procedures to follow if they are exposed to these chemicals
 - how to read and interpret labels and SDSs used at Goodwill
 - protective measures implemented at Goodwill

Training will consist of individual or classroom training, as appropriate. Each employee will sign or initial that they received the safety training.

Before any new hazardous chemical is introduced into a section, each employee will be given information in the same manner as during the safety class. The Human Resources and Safety Director will be responsible for seeing that MSDSs on the new chemical are available.

Department meetings will be held regularly, and safety issues, including Hazardous Materials, will be discussed as needed. Attendance at these meetings is mandatory for all employees.

A complete review of the Written Hazardous Communication Program will be done annually.

Training on hazards of non routine tasks will be provided before these tasks are assigned.

Notices will be posted that provide the location of the Written Hazard Communication Program and SDS locations.

V. Informing Contractors

- A. It is the responsibility of the Safety Director to provide the contractors and their employees with the following information:
- hazardous chemicals to which they may be exposed while on the job site
 - measures the employees may take to lessen the risks
 - steps the company has taken to lessen the risks
 - SDSs for all hazardous chemicals are on file in the plant office
 - procedures to follow if they are exposed
- B. The Human Resources and Safety Director will coordinate with the supervisor to ensure that contractor's employees are given this information prior to entering the work site.

VI. Consumer Products

Consumer products that are purchased in small quantity will be labeled by the manufacturer as to identity and hazard warning.

VII. Ordering chemicals

Any suggestions for additional or replacement chemicals are to be given to the Human Resources and Safety Director.

VIII. Retail Products

Any retail location that sells products containing chemicals will have the Safety Data Sheets at the register.

A Critical Incident Report will be completed if necessary.

Forms: Safety Data Sheets (SDS)
 HR615 Critical Incident Report

Date Adopted: **May 1994**

Date Revised: **May 2013, April 2018**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. I. POLICY REGARDING HEALTH AND SAFETY EXPECTATIONS

Purpose: To control the work environment so that employees are protected and accidents are avoided.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees

Policy: It is the policy of Goodwill Industries to ensure workplace safety and health by letting employees know what is expected of them and providing them with opportunities to correct their behavior before an accident occurs.

Procedures: Goodwill Industries follows the standards set forth in the Federal Occupational Safety and Health Act of 1970 and Indiana Occupational Safety and Health Act of 1974. A comprehensive external inspection of all facilities will be completed annually. Additionally, comprehensive internal inspections will be held semi-annually. The reports and recommendations from these inspections will be reviewed by the, Human Resources and Safety Director, President and Board of Directors. Any recommendations will be completed according to the timetable assigned by the inspector.

All employees have the right to raise a safety or health concern without retaliation. Any employee who believes that a violation of a safety standard exists should bring the situation to the attention of their supervisor or the Human Resources and Safety Director. If corrective action has not been taken or a satisfactory explanation has not been given, you may request a safety inspection by sending a signed notice to the Department of Labor.

Employees will be informed of any specific safety and health rules that are in effect in their work area. Basic safety and health rules throughout Goodwill Industries include, but are not limited to:

- Wearing of protective equipment (gloves, goggles, etc.)
- No horseplay
- Storing equipment safely after each shift
- Reporting all accidents to the supervisor
- Keeping aisles clear
- No unauthorized extension cords
- No food or drink in plant or store, except water in a closed container
- Evacuating building when required for drills or emergencies
- No unauthorized use of first aid kits
- Keeping floors clean and dry
- No unauthorized fans/heaters
- No careless or neglectful behavior
- Using only labeled and approved chemicals/cleaning supplies
- No one under 18 operating baler or compactor
- No unauthorized or excessive breaks
- Possession of a weapon (as determined by management)

Goodwill Industries utilizes a progressive discipline approach for violations of safety and health policies. This approach includes verbal and written warnings, suspensions and discharge.

Discharge may be used as a first step, only for major violations.

Major violations, include, but are not limited to:

- Smoking in unauthorized areas
- Fighting
- Blatant disregard of any safety rule
- Neglect or carelessness which results in serious damage to Goodwill property or equipment, or results in serious personal injury
- Unauthorized removal of machine tags/locks
- Possession, use or being under the influence of alcohol or illegal drugs

Three-day suspensions without pay will be utilized for serious violations, which include, but are not limited to:

- Not following universal precautions
- Unauthorized use of equipment (forklift, baler, saws, etc.)

Safety violations of a less serious nature, but still unacceptable, will be handled in the following manner:

- | | |
|-------------------|--|
| First violation— | For the Record Of (Verbal warning) |
| Second violation— | First Written Warning |
| Third violation— | Second Written Warning |
| Fourth violation— | Three (3)-day suspension without pay |
| Fifth violation— | Discharge (within 12 months of first occurrence) |

Individual supervisors will be responsible for ongoing monitoring of their employees work and safety habits. These supervisors will have the opportunity to observe how work is performed and to correct any problems before a serious situation develops. The effectiveness of this supervision depends on a quick response to a hazardous situation or problem, correction before any punishment, and a relationship between employees and their supervisors that allows them to discuss problems and reach mutually agreed-upon solutions.

Forms: HR404 For The Record Of
 HR405 First Written Warning
 HR406 Second Written Warning
 HR407 Suspension
 HR208 Notice of Termination

Date Adopted: **May 1994**

Date Revised: **July 2005, May 2017**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. J. POLICY REGARDING HOUSEKEEPING

Purpose: To ensure a clean and safe environment for employees.

Responsibility: Retail Sales Director

Personnel Affected: All Goodwill Employees

Policy: It is the policy of Goodwill Industries to maintain a clean, orderly and safe workplace.

Procedures: The necessity for maintaining good housekeeping is stressed at orientation. Employees are expected to keep their offices and workspace neat and orderly. Wet floors, trash, tripping hazards, or other unclean or unsafe environments are not permitted. Employees are required to clean their workstation and properly store equipment before leaving at the end of their shift.

Employees at all locations are expected to clean up after themselves and keep all common areas neat and clean.

Forms: Not Applicable

Date Adopted: **May 1994**

Date Revised: **June 2000**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. K. POLICY REGARDING INFECTIOUS/COMMUNICABLE DISEASES

Purpose: To eliminate the spread of infectious and communicable diseases.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees and Clients

Policy: It is the policy of Goodwill Industries to comply with all federal and state laws concerning infectious and communicable diseases in the workplace, including cytomegalovirus (CMV), rubella, staph infections, hepatitis, human immunodeficiency virus (HIV), head lice, and tuberculosis.

Procedures: Training will be conducted at new hire orientation, and annually, to educate employees on the prevention and control of infectious and communicable diseases.

No prospective employee, current employee or client will be excluded from employment or services solely on the basis of a diagnosis of an infectious disease. Goodwill will rely on opinions from physicians as to individual outcomes.

Employees or clients who have an infectious or communicable disease must promptly notify their supervisor or Human Resources whenever a condition exists that could transmit the disease to others. Records of infectious diseases of employees and clients will remain confidential.

Employees who are absent due to a communicable disease will be excused if proper documentation is provided.

Hepatitis B immunizations are offered at no cost to employees whose job classifications have been determined to have exposure to blood borne pathogens.

Restrooms and break areas are cleaned with appropriate disinfectant.

Gloves are provided and readily available to employees who are at risk of exposure to infectious or communicable diseases.

Hands are to be washed thoroughly.

All first aid providers have received training in the prevention of infectious diseases.

In the event of an "outbreak" of an infectious disease, a Critical Incident Report will be completed and Goodwill's company doctor will be contacted and all recommendations will be followed.

Please refer to our extensive Blood Borne Pathogen policy for further information.

Forms: HR203 Classification and Emergency Information
 HR210 Vaccination Declination Form
 HR615 Critical Incident Report

Date Adopted: **May 1994**
Date Revised: **March 2003**
Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**
8. L. **POLICY REGARDING INVESTIGATING ACCIDENTS**

Purpose: To prevent accidents from reoccurring.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees

Policy: It is the policy of Goodwill Industries to review any accident requiring medical attention (other than first aid) resulting in time off work or an accident that qualifies as a critical incident.

Procedures: A member of the Safety and Wellness Committee, or management, will review any accident considered a critical incident or one requiring medical attention (other than first aid) or resulting in time off work, within 48 hours of the accident. If the safety committee member is unable to conduct the investigation within 48 hours the Human Resources and Safety Director is to be contacted to conduct the investigation.

The Human Resources and Safety Director will review all investigations to determine if any further action is needed.

A Critical Incident Report will be completed if necessary.

Forms: HR601 Employee Report of Accident, Injury or Illness
 First Report of Injury (on-line)
 HR604 Accident Investigation Report
 HR615 Critical Incident Report

Date Adopted: **May 1994**

Date Revised: **March 2003**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. M. POLICY REGARDING LIFT TRUCKS

Purpose: To ensure only qualified employees operate the lift trucks.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees

Policy: It is the policy of Goodwill Industries to permit only trained and licensed employees to operate the lift trucks.

Procedures:

TRAINING PROGRAM

Goodwill employees must be licensed through Goodwill to operate our lift trucks. Before an employee may be licensed to operate the lift truck, the employee must complete on-site lift truck training. The training program includes classroom instruction, PowerPoint presentations, "on-the-truck" evaluation and training, written tests and instructor evaluations. Equipment maintenance responsibilities, safe operation, capacity and factors which can affect capacity, proper use of controls and hints for safe,

efficient truck operation are the primary topics covered in the class. The class outline includes a PowerPoint presentation, review of the actual equipment, review of “data plate” information, review of proper maintenance of industrial batteries and a test.

Operators need to work the machines and have a closely supervised chance to practice the tasks required on their jobs. Specific training on the lift trucks utilized by Goodwill is provided on-the-job.

On-the-Truck training by Goodwill consists of the operator learning to move and load bales of salvage onto a highway truck. The operator must be able to safely enter and exit trucks and be able to maneuver bales into appropriate positions.

DAILY CHECKLIST/INSPECTION

OSHA requires that lift trucks are inspected at the beginning of each shift. If ANYTHING is found to be wrong with the forklift it must be taken out of operation immediately.

The inspection should include the following:

1. Safety equipment

- a) Overhead guard and load backrest extension. Inspect and record the condition of the overhead guard and load backrest extension. Check for loose or missing parts or fasteners. Damage to these parts can weaken the guard or backrest.
- b) Operator restraints. Check for cuts, tears, and proper condition.
- c) Warning decals. Make sure all decals are in place and readable.
- d) Warning devices. Test all audible and visual warning devices on the equipment. These devices must be working at all times.
- e) Forks and fork retention. Inspect forks for cracks, heel wear, tip wear, and tip alignment. Check service procedures for the forklift. If forks are worn beyond limits, replace them. DO NOT attempt to straighten or weld forks.

Fork stop devices are mounted at the ends of the fork bar. These, along with the load backrest extension prevent the forks from sliding off the end. If the fork retainers are removed, worn, or broken, they must be repaired or replaced.

2. Tires

- a) All tires must be inspected for cuts, breaks, and signs of wear.
- b) If material has become embedded in solid tires it must be removed.

- c) The tires are mounted on a split rim. A split rim that is damaged or not installed properly can come apart under high pressure.

3. Batteries

- a) Special procedures, equipment, and personal protective clothing are required when working on or around forklift batteries. Other than the following basic inspections, operators should not work on batteries.
- b) Battery plug connection. Be sure that the battery plug connection is tight.
- c) Battery discharge indicator. With the key on, the needle of the battery discharge indicator should be in the green area.
- d) Battery load test. Watch the battery discharge indicator while holding the tilt lever on full back tilt. If the needle falls to the red area, the battery doesn't have enough charge to operate the truck properly.

4. Hour Meter

This must be written in at the top of the form. Also operator must check that this meter is functioning during operation.

5. Obvious Damage and Leaks

Check fitting for fluid leaks. The most common leak would be hydraulic fluid.

6. Horn

Press on horn and listen. Audible devices must be working at all times.

7. Steering

Check by turning left and right. Check for looseness or tightness.

8. Service Brakes

Check for leaks, if they are loose or grab.

9. Parking Brakes

Engage brake. When the brake is engaged the power automatically shuts off.

10. Hydraulic Controls

Test by moving forks up and down; side-to-side shift, and tilt.

FAULTY EQUIPMENT AND MAINTENANCE

If, at any time, the forklift is not operating properly, stop immediately and report this to your supervisor.

GENERAL LIFT TRUCK OPERATION

LEAVING THE FORKLIFT

Whenever an operator leaves the forklift, the forks must be fully lowered, the controls must be in neutral, and the brakes set. If the operator goes 25 feet or more away from the forklift, or is out of sight, the power must be shut off and the wheels chocked.

LOAD HANDLING

Only stable and safely arranged loads within the rated capacity of the lift truck should be handled.

When handling long or high loads, watch your clearance and remember, these loads can reduce capacity.

When picking up a load, place the forks under the load as far as possible and carefully tilt the mast backward just enough to stabilize the load.

When raising a load use extra caution. An elevated load must not be tilted forward except when the load is in the correct position to be deposited. When stacking, use only enough backward tilt to stabilize the load.

GRADES

Travel up and down grades slowly. Loaded lift trucks should be operated with the load upgrade. Unloaded trucks should be operated with the forks downgrade. The load should be tilted back and raised only as high as necessary to clear the surface.

LOADS

1. Center loads evenly on the forks. Check the fork length. Forks must be at least $\frac{2}{3}$ (two-thirds) the length of the load. The load should rest against the vertical portion of the forks or load backrest.
2. All loads must be made stable by either interlocking the objects or strapping the load to prevent individual objects from falling off.
3. Long loads, such as carpet rolls, reduce the stability of the load and require more room.

PARKING THE LIFT TRUCK

1. Bring the forklift to a complete stop before getting off.
2. Lower the forks completely. Be sure that the forks are flat on the floor then tilt the upright forward.
3. Place the forklift in neutral.

4. Apply the parking brake.
5. Never leave forklift parked on a dock ramp, dock leveler, or in a trailer.
6. Turn off the power supply and remove the keys.

GRADES, RAMPS, SLOPES, AND INCLINES

Travel straight up and straight down. Never turn on ramps, slopes, and inclines. Wait until on a level surface.

PEDESTRIANS

1. Sound the horn at intersections and blind spots.
2. Watch for people. They may not be watching for you.
3. If your view is blocked because of the load, travel backwards. If you must move forward make sure that people are out of the way and move the lift truck slowly. If you can't see, don't move.
4. Watch for employees working around you. Do not let anyone walk under raised forks or load. Keep people off the lift truck. This means that people are not allowed on the forks, not on the load, and not on the lift truck. They must be off and completely away.

DOCK OPERATIONS

1. Travel slowly on the dockboards or bridgeplates. High speed travel or sudden acceleration can jar them loose.
2. Trailers must be chocked and the condition of the trailer floor inspected before a forklift may enter.

RULES FOR SAFE LIFT TRUCK OPERATION

1. Operate the lift trucks only if trained and authorized.
2. Before boarding a highway truck the brakes (on the truck) must be set and wheel chocks placed under rear wheels.
3. No one is allowed to stand or pass under the elevated lift whether loaded or empty.
4. No one is permitted to ride on forks, on the load, or any part of the lift truck. The lift truck is for the express use of the operator only and no one else is to ride it.
5. Before backing out from under a load the operator should look behind.
6. Arms and legs should be kept inside the lift truck.

7. The daily checklist must be completed before starting to work.
8. If leaving the forklift unattended, the load should be fully lowered, forks pointed downward, controls neutralized, power shut off, brake set, and key or connector plug removed.
9. A safe distance should be maintained from the edge of ramps or platforms while on any elevated dock, or platform.
10. The overhead guard must be in place as protection against falling objects from the load or from backing into stacks of material.
11. The load back rest extension must be used whenever necessary as protection from part or all of the load falling rearward.
12. Caution must be used on wet or slippery floors.
13. All traffic rules and signs as to speed should be observed. Cross aisles should be approached slowly, with horn sounding.
14. Loads should be carried 3 to 6 inches off the floor and tilted backwards to provide better stability.
15. Stunt driving and horseplay will not be permitted.
16. Running over loose objects on the roadway surface must be avoided.
17. The lift truck must be operated at a speed which permits stopping in a safe manner under all conditions.
18. Any unsafe operating condition of the lift truck must be reported to management.
19. Goggles and gloves must be worn when checking battery fluids.
20. Do not remove the battery under any circumstance.

All licensed lift truck drivers will receive training annually, and will be recertified every four years.

Lift truck licenses are located in the Master Safety Book, and individual personnel files.

Any accident involving a lift truck must be reported to a supervisor. A Critical Incident Report will be completed if necessary.

Forms: Fork Lift License
 O106 Driver's Daily Checklist for Electric Forklift
 HR615 Critical Incident Report
 HR618 Forklift Operator Performance Evaluation Checklist

HR619 Walker Stacker Test
HR620 Forklift Test
Forklift Operator Excellence PowerPoint

Date Adopted: **May 1994**

Date Revised: **June 2009, May 2014**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. N. POLICY REGARDING LOCK-OUT/TAG-OUT

Purpose: To comply with OSHA's Lock-Out/Tag-Out Program (29 CFR 1910.150)

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees

Policy: It is the policy of Goodwill Industries to ensure that machines and equipment are isolated from all potentially hazardous energy and locked-out/tagged-out before employees perform any servicing or maintenance activities where the unexpected energization, start up or release of stored energy could cause injury.

Procedures:

TRAINING

All employees shall be instructed in the safety significance of the lock-out/tag-out procedure when they are initially hired. Employees transferred to work operations that are or may be in an area where energy control procedures may be utilized shall again be instructed in the purpose and use of the lock-out/tag out procedure. Retraining will occur if there is a change in machines, equipment, procedures or processes. Goodwill Industries will also provide yearly review to employees of the lock-out/tag-out program. Only specific lock-out/tag-out devices will be utilized for this program. These include Lock-out tags, red hasps and padlocks. They are located in the Operation and Logistics Director's Office.

SEQUENCE OF LOCK-OUT/TAG-OUT PROCEDURES

All affected employees shall know the type and magnitude of energy that the machine or equipment utilizes and shall understand the hazards thereof.

Only the Maintenance Technician and Assistant, Operations and Logistics Director, or Support Supervisors will be allowed to install lock-out/tag-out devices. Only Qualified persons will be allowed to work on equipment that needs to be repaired. A qualified person will have had training in avoiding the electrical hazards of working on or near exposed energized parts. The Maintenance Technician has been determined qualified for voltages 110 or less based on their previous on-the-job training.

1. If the machine or equipment is operating, shut it down by the normal stopping procedure.
2. Operate the switch, valve or other energy isolating device so that the equipment is isolated from its energy source. Stored energy must be dissipated or restrained.
3. Lock-out or tag-out the energy isolating devices. Lock-out is the preferred method if the equipment is compatible. Tag-out will be utilized when lock-out is not possible, but it does not afford the same protection as a lock.
4. After ensuring that no personnel are exposed, and as a check on having disconnected the energy sources, operate the push button or other normal operating controls to make certain the equipment will not operate.

RESTORING MACHINE/EQUIPMENT TO NORMAL OPERATION

1. After servicing and/or maintenance is complete and equipment is ready for normal production operations, check the area around the machines or equipment to ensure that no one is exposed.
2. After all tools have been removed from the machine or equipment, guards have been reinstalled and employees are in the clear, remove all lock-out/tag-out devices. Operate the energy isolating devices to restore energy to the machine or equipment.

BASIC RULES

All equipment shall be locked-out/tagged-out to protect against accidental or inadvertent operation when such operation could cause injury to personnel.

Do not attempt to operate any switch, valve or other energy isolating device where it is locked-out/tagged-out.

Only the individual who locked-out/tagged-out the equipment is authorized to remove the lock or tag. If the individual is unavailable, permission to remove the lock or tag must be obtained from the Human Resources and Safety Director.

TYPES OF EQUIPMENT/ENERGY/HAZARDS

1. Balers

The electrical panels for the balers are located on the rear of the machines. This box is to be locked-out when any work is being performed. The opening on the pit baler will also be manually blocked using a two inch steel bar to prevent the table from lowering.

2. Compactor

The electrical panel for the compactor is to the left of the door as you leave the dock on the north side of the building. This box is to be locked-out when any work is being performed.

3. Boiler

The electrical panel for the boiler is in the boiler room. This box is to be locked-out when any work is being performed.

4. Electrical Panels

Electric panels at all locations will be locked-out when any work is being performed.

PERIODIC INSPECTION

An inspection of the energy control procedures shall be conducted annually. This inspection shall be designed to correct any deviations or inadequacies observed.

A Critical Incident Report will be completed if necessary.

Forms: HR615 Critical Incident Report

Date Adopted: **May 1994**

Date Revised: **March 2003, May 2016, April 2018**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. O. POLICY REGARDING MEDICATION

Purpose: To ensure medication taken is the responsibility of each individual.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees and Clients

Policy: It is the policy of Goodwill Industries to prohibit dispensing any medication to any client, and to prohibit dispensing any medication to employees other than what is contained in the approved first aid kits.

Procedures: Any medication taken by clients is the sole responsibility of the client. Goodwill does not administer, handle, store or dispose of any medications for clients.

Any employee requiring medication is to bring it to work in the original, labeled container. Medication is to be kept only in offices, lockers, or on your person. Any medication that must be refrigerated is to be brought to the immediate supervisor or Human Resources to be labeled. Medication, including over the counter, is not to be shared.

Any employee taking medication should update their Emergency Information Sheet to include this information. If the medication could impair their ability to perform their job safely it is to be reported immediately to the supervisor, who will discuss the situation with Human Resources and appropriate remedies will be taken.

A Critical Incident Report will be completed in necessary.

Forms: HR203 Classification and Emergency Information
HR615 Critical Incident Report

Date Adopted: **May 1994**

Date Revised: **March 2003**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. P. **POLICY REGARDING PERSONAL PROTECTIVE EQUIPMENT**

Purpose: To ensure employees are protected when performing job duties.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees

Policy: It is the policy of Goodwill to review all job duties to determine if any personal protective equipment is required, and, if so, what type is most effective.

Procedures: All job duties, tasks, and procedures will be audited to determine if hazards exist that would require personal protective equipment (PPE). If personal protective equipment is required, all affected employees will be informed of the necessity of wearing the equipment. The required personal protective equipment will be provided by Goodwill at no cost to the employee.

Each location will be audited annually to determine what personal protective equipment is required. The audit will consist of a survey of all locations, reviewing accident records, identifying and evaluating equipment and processes, and reevaluating the suitability of previously selected PPE.

PPE alone should not be relied on to provide protection. We will try first to engineer the hazard out.

SURVEY

Goodwill will conduct a walk-through survey of all areas during the semi-annual internal safety inspection to identify sources of hazards to workers and co-workers. During this survey the following items will be considered:

impact	heat
penetration	harmful dust
compression (roll-over)	light (optical) radiation
chemical	

During the walk-through survey the following items will be observed:

1. Sources of motion (machinery or processes) where any movement of tools, machine elements or particles could exist or movement of personnel that could result in collision with stationary objects.
2. Sources of high temperature that could result in burns, eye injuries, or ignition of protective equipment, etc.
3. Types of chemical exposure, sources of harmful dust, sources of light radiation, welding, brazing, cutting, furnaces, heat treating and high intensity lights.
4. Sources of falling objects or potential for dropping objects.
5. Sources of sharp objects which might pierce the feet or cut the hands.
6. Sources of rolling or pinching objects which could crush the feet.
7. Layout of the workplace and location of co-workers.
8. Electrical hazards.

SELECTION OF PPE

Hazards will be compared with the capabilities of the available protective equipment. Selection of the protective equipment will be done to ensure a level of protection greater than the minimum required to protect employees from the hazards and, if appropriate, fit the user for the PPE and give instructions on care and use of PPE.

PPE TRAINING

PPE training will cover:

- when a PPE is necessary
- what type of PPE is necessary
- how to don, doff, adjust and wear the PPE
- limitations of PPE
- proper care, maintenance, useful life and disposal of PPE

Employees must demonstrate an understanding and ability of how to use PPE before being allowed to perform work requiring its use.

Re-training may be required in instances where there are changes in the workplace, changes in the types of PPE to be used, inadequacies in the employee's knowledge or use of the assigned PPE indicate that the employee has not retained the understanding or skill.

HAND PROTECTION

Goodwill shall select and require employees to use appropriate hand protection when employees' hands are exposed to hazards such as those from bloodborne pathogens,

skin absorption of harmful substances, severe cuts or lacerations, severe abrasions, punctures, chemical burns, thermal burns, and harmful temperature extremes.

EYE AND FACE PROTECTION

Each affected employee shall use appropriate eye or face protection when exposed to eye or face hazards from flying particles, caustic liquids, chemical gases or vapors, molten metal, liquid chemicals, acids, or potentially injurious light radiation.

Each affected employee shall use eye protection that provides side protection when there is a hazard from flying objects.

Each affected employee who wears prescription lenses while engaged in operations that involve eye hazards shall wear eye protection that can be worn over the prescription lenses without disturbing the proper position of the prescription lenses or the protective lenses.

Protective helmets designed to reduce electrical shock hazard shall be worn by each such affected employee when near exposed electrical conductors which could contact the head.

FOOT PROTECTION

Each affected employee shall wear protective footwear when working in areas where there is a danger of foot injuries due to falling and rolling objects, or objects piercing the sole and where employees' feet are exposed to electrical hazards.

Forms: HR612 Hazard Assessment Survey

Date Adopted: **May 1995**

Date Revised: **April 1997, May 2014**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. Q. **POLICY REGARDING PREVENTING WORKPLACE
VIOLENCE AND MANAGING UNSAFE BEHAVIORS**

Purpose: To be alert to, and prepared for, potentially violent situations and to protect employees, visitors, customers and clients from violence in our workplace.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees and Clients

Policy: It is the policy of Goodwill Industries to ensure safety by taking seriously and dealing appropriately with instances of violent or disruptive behavior.

Procedures: All employees will receive training regarding recognizing potentially violent situations, actions to be taken to minimize risk, procedures to respond to violent incidents, and how to report violent incidences. Management will also be trained in their additional duties.

PREDICTING VIOLENCE

The following is a list of warning indicators that could predict the potential for violent behavior:

1. Verbally or physically aggressive behavior (bullying, intimidating, harassing or belligerent behaviors, using profanity, defying authority).
2. Numerous conflicts with customers, co-workers, and supervisors.
3. Bringing a weapon into the workplace.
4. Making references to guns or making idle threats about using a weapon to harm someone.
5. Statements indicating the approval of the use of violence to resolve a problem.
6. Statements indicating desperation (over family, financial, or personal problems) to the point of considering suicide.
7. Direct or veiled threats of harm.
8. Substance abuse.
9. Extreme changes in normal behaviors.
10. Prior violence.
11. Feelings of humiliation, inferiority, boredom, grief, or powerlessness.
12. Experiencing childhood abuse or aggression in the home.
13. Feelings of injustice or oppression.

Even if you do not have any information about a person's past history or current emotional state, look for the following signs: clenching of fists or jaw, tightening of

muscles, pacing or fidgeting, speaking in a loud voice or becoming verbally abusive, seeming to be out of touch with reality, having a “wild” look in their eyes.

MINIMIZING RISK

The following list details ways to reduce tension and begin to diffuse the situation:

1. Remain calm and speak in a calm tone.
2. Maintain a calm demeanor.
3. Do not tell the person to calm down.
4. Talk about the problem or frustration that has come up.
5. Remember that the person is frustrated at the situation, not at you.
6. Defensiveness on your part validates the angry person, increasing the tension.
7. Move slowly, and avoid putting your hands on your hips.
8. Avoid extensive eye contact and physical closeness.
9. Do not touch an angry person.
10. Do not stand between the person and the door.
11. Offer the person choices, such as talking later or agreeing to a cooling down period.
12. **Do not** use humor - it can be too easily misunderstood.
13. Be patient. It may take 30 – 45 minutes to calm down from anger.

RESPONDING TO A VIOLENT SITUATION:

EMPLOYEE RESPONSIBILITIES

1. If you believe you are at risk of injury, remove yourself from the situation and seek help.
2. If there is an active shooter, Goodwill policy is to Run, Hide, Fight. Research has shown it is best to flee the area. Therefore individuals should first try to run away from the shooter. If you cannot run, your next safest move is to hide. If there is a locked room, hide there. If that is not available, find anything close by to hide behind. Your last choice is to fight. Try to find a fire extinguisher, chair, scissors, or anything you can use as a weapon.
3. Know the pre-arranged distress signals.
4. Report strangers who are in areas not intended for the public.
5. Report any threats (physical or verbal) (in person or over the phone).
6. Report disruptive behavior of any person.
7. Report any violent behavior.
8. Do not confront individuals who are a threat.
9. Take all threats seriously.
10. If it is your supervisor, notify that person’s manager.
11. Know that Goodwill prohibits retaliation against those who report violent behavior or participate in an investigation.

MANAGERS & SUPERVISORS RESPONSIBILITIES

1. Determine a code or distress signal.
2. Ensure employees have been trained in workplace violence issues and the emergency action plan.
3. Respond to potential threats and escalating situations.
4. Take all threats seriously.
5. Notify the Human Resources Department of any concern.
6. Utilize the EAP, security and the police department as appropriate.
7. If it is a client, customer or someone you supervise, evaluate the situation and take steps to ensure the safety of others.
8. Account for all employees if a facility is evacuated.
9. Ensure that no one is retaliated against for reporting violent behavior or participating in an investigation.

HUMAN RESOURCES RESPONSIBILITIES

1. Keep a comprehensive directory of personnel up-to-date with copies maintained off site.
2. Maintain training records.
3. Assists managers with investigations and help determine appropriate course of action.
4. Identify safe places to escape to inside and outside of each facility.

STEPS TO ENSURE THE SAFETY OF OTHERS

1. Question strangers who are in an area not intended for the public.
2. Use the distress code or signal to alert others.
3. After closing, walk to the parking lot as a group.
4. Do not allow non-employees in the stores after closing.

PERSONAL SAFETY

1. Do not meet with a client alone in the office outside of business hours.
2. Arrange meetings outside of the building in public areas (restaurant, library, etc.).
3. Bring cell phone.

IF AGGRESSION OCCURS

1. Protect yourself from head injuries. Block blows with pillows, arms, clipboard, etc.
2. If you fall, block the attack with your feet and legs.
3. If your **arm is grabbed**, break the hold by twisting quickly toward the person's thumb.
4. If you are **choked**, raise both arms straight up and quickly turn around. Your arms and shoulders will break the hold.

5. If you are **bitten**, push into the bite, don't pull away.
6. If your **hair is pulled**, press down on the person's hand with both of your hands.
7. If the person has **a weapon, NEVER** reach for the weapon. Encourage the person to talk.

All locations have a "distress" signal that is to be announced over the phone system in the event any employee feels threatened, or requires assistance.

A Critical Incident Report will be completed if necessary.

Forms: HR615 Critical Incident Report

Date Adopted: **March 2003**

Date Revised: **July 2005, May 2014**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. R. POLICY REGARDING REPAIR TAG

Purpose: To ensure employees have access only to items in good repair.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees

Policy: It is the policy of Goodwill Industries to remove from service any items that need repair.

Procedures: Employees finding equipment, such as carts or tools, unsafe to use or operate, are to contact their immediate supervisor for a Repair Tag. The Repair Tag will be completed by the supervisor and the item placed aside, out of use, until repair or replacement is completed. Repair or replacement of the item will be completed by only employees who have been trained. The Repair Tag will then be removed, completed and turned in to the Operations and Logistics Director.

Forms: Repair Tag

Date Adopted: **May 1994**

Date Revised: **April 1997, May 2016, April 2018**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. S. POLICY REGARDING REPORTING ACCIDENTS

Purpose: To ensure all accidents occurring in the workplace are reported in a timely and approved manner.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees

Policy: It is the policy of Goodwill Industries to give employees the right to report all workplace accidents, however minor, to the immediate supervisor at the time of the accident. Accidents involving customers, clients or visitors are also required to be reported.

Procedures: Any employee having an accident at work has the right to report the accident immediately to their supervisor. The supervisor is responsible for handling the situation, including completion of the Employee Report of Accident, Injury or Illness form and contacting a trained first aid provider or ambulance, if necessary. The list of trained first aid providers is posted by the first aid kit at each location. Human Resources will complete the First Report of Injury form.

Any injury requiring medical treatment, other than minor first aid, or calling of an ambulance, will be treated by the company doctor. Goodwill will not be responsible for treatment obtained by a family or other doctor. Supervisors will either call or send a treatment slip with the employee to the company doctor. Employees who are being treated for work-related injuries will be paid for the time they are required to attend medical treatment.

In the case of an accident involving a customer or visitor, the Department Director or supervisor is to complete a General Liability form. In the event the customer or visitor refuses to give the necessary information to complete the General Liability form, the Department Director or supervisor is to complete the form to the best of their ability, indicating the injured party refused to cooperate. This form is then to be given to Human Resources. Treatment can be obtained by their personal physician. Goodwill's insurance carrier will provide the follow-up on these incidences. A Critical Incident Report will be completed if necessary.

Forms: HR601 Employee Report of Accident, Injury or Illness
 First Report of Injury (on-line)
 HR602 General Liability
 HR615 Critical Incident Report
 Treatment Slip

Date Adopted: **May 1994**

Date Revised: **March 2003, May 2016**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. T. POLICY REGARDING RETURN TO WORK AND LIGHT DUTY

Purpose: To ensure employees are able to return to work safely.

Personnel Affected: All Goodwill Employees

Responsibility: Human Resources and Safety Director

Policy: It is the policy of Goodwill Industries to require a doctor's release to return to work if an employee has been off work under a doctor's care.

Procedures: Goodwill Industries has developed a light duty policy. In case of temporary work restrictions Goodwill will attempt to modify job duties or reassign the employee to another position until the restriction has been lifted.

A light duty assignment may not necessarily be within the employee's normal department.

Exceptions to this light duty policy include return to work under the Family and Medical Leave Act.

A Doctor's statement will be required for an employee to return to work if the employee has been off work three (3) days or more.

Forms: Doctor's statement

Date Adopted: **May 1994**

Date Revised: **June 2000**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. U. POLICY REGARDING SAFETY AND WELLNESS COMMITTEE

Purpose: To ensure Goodwill employees have a safe and healthy working environment.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees

Policy: It is the policy of Goodwill Industries to have a Safety Committee that meets monthly to discuss safety policies, review safety suggestions, detect and correct unsafe conditions and review accident reports to improve Goodwill's overall safety.

Procedures: The Safety and Wellness Committee is headed by the Human Resources and Safety Director. The committee consists of one member from each store, Operations and the Corporate office. Appointments to the Safety and Wellness Committee are on an annual basis. Committee members are required to review their respective areas and bring these checklists to the meeting. These monthly safety checklists and accident reports are discussed, along with any business carried over from the last meeting, new business and announcements. Safety committee members are also required to check fire extinguishers and emergency lighting each month.

Safety and Wellness Committee members are designated as Safety Captains and it is their responsibility to make sure all restrooms, conference rooms, offices, fitting rooms and stock rooms have been vacated and check that all doors are closed and equipment has been turned off.

If a Safety Captain is not at work, store management has been trained to serve this function.

Safety Captains will make sure everyone stays at least 50 yards away from the building during drills and actual emergencies.

Forms: HR603 Monthly Safety Checklist

Date Adopted: May 1994

Date Revised: May 2013, May 2017

Date Reviewed: March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023

8. V. POLICY REGARDING SAFETY SUGGESTIONS

Purpose: To solicit suggestions to improve the overall safety of the workplace.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees

Policy: It is the policy of Goodwill Industries to solicit safety suggestions at each of our locations.

Procedures: Each location has a Suggestion Box located by the time clock. At Magnavox Way, the suggestion box is in the break room. Employees with suggestions are encouraged to complete a safety suggestion form. The box will be emptied periodically, and suggestions will be discussed at the next Safety and Wellness Committee meeting.

Awards may be given to employees submitting the most useful suggestions.

Forms: Safety Suggestion Form

Date Adopted: **May 1994**

Date Revised: **April 1997**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. W. POLICY REGARDING SMOKING

Purpose: To ensure a safe and healthy working environment.

Responsibility: Retail Sales Director

Personnel Affected: All Goodwill Employees, Clients, Customers, Volunteers, Interns, and Visitors

Policy: It is the policy of Goodwill Industries to prohibit the sale of smoking products, and to limit their use to designated areas only.

Procedures: Use of tobacco or other smoking products (including e-cigarettes and vaping) is strictly prohibited in retail stores, trucks, storage areas, offices, conference rooms and restrooms. Smoking is permitted in designated areas only. In Fort Wayne no smoking is allowed within 20 feet of a door, or windows that open. Indiana state law requires no smoking within 8 feet.

Smoking is not permitted during any meetings, regardless of location.

Forms: Not Applicable

Date Adopted: **May 1994**

Date Revised: **October 2013, May 2017, April 2018**

Date Reviewed: **March 2012, May 2013, October 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**

8. X. POLICY REGARDING SPACE HEATERS/FANS

Purpose: To ensure the safety of employees and property.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees

Policy: It is the policy of Goodwill Industries to allow the use of space heaters and fans only with prior approval of Department Directors and Human Resources.

Procedures: For safety reasons, careful consideration must be given to the use of space heaters and fans. Before anyone may use a space heater or fan it must first be

approved by the Department Director. After approval it will be inspected by Human Resources to make certain it meets OSHA standards.

Employees may not leave space heaters or fans running when they are not in the area and must turn off and unplug the heater or fan when it is not in use.

The area around the space heater or fan must be kept clear and free of clutter.

Forms: Not Applicable

Date Adopted: **May 1994**

Date Revised: **March 2004**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022**

8. Y. POLICY REGARDING USE OF EQUIPMENT

Purpose: To ensure safety of employees and safe and proper use of equipment.

Responsibility: Human Resources and Safety Director

Personnel Affected: All Goodwill Employees

Policy: It is the policy of Goodwill Industries to allow only trained employees to use equipment.

Procedures: Employees who are assigned to use equipment will first be trained in the use of the equipment by their immediate supervisor. Detailed steps of operation will be explained, along with any protective equipment required. If any equipment does not appear to be operating properly, employees must turn the equipment off and notify their supervisor immediately.

Equipment includes, but is not limited to, such items as the baler, hand tools, forklift, mower, snow blower, and compactor.

Forms: Not Applicable

Date Adopted: **May 1994**

Date Revised: **April 1997**

Date Reviewed: **March 2012, May 2013, May 2014, April 2015, May 2016, May 2017, April 2018, June 2019, Sept 2020, June 2021, May 2022, August 2023**



May 6, 2022

BQIS Reporting

Re: Emergency Management Plan

To Whom it May Concern:

Attached please find LOGAN's revised emergency management plan and related documents as requested. We believe we have addressed all the issues identified in our Corrective Action Plan. Since we believe most of the issues identified were already contained in the documents previously submitted, we attempted to provide more clarity.

Not one of these policies and procedures listed below is intended to be taken as the sole document to reference in a case of an emergency. LOGAN's policy and procedure manual is intended to be referenced as a whole, with each document supported by another. As was stated previously, I did not include each of the documents LOGAN has related to emergency preparedness since it is too massive for an email. For your purposes, we have provided for review the policies and procedures we believe are most pertinent to your review. I have attached the table of contents for the Health and Safety Section of LOGAN's policy manual for your review.

Group Living has developed an Emergency Preparedness Plan and an Emergency Preparedness Plan for COVID-19. These are reviewed by Life Safety Code surveyors from Indiana Department of Health when they complete annual surveys at our seven group homes. I have included in this attachment the table of contents for each of these plans as they are extensive.

The following documents are included in this attachment.


- Policy S-01-02: Total Evacuation Plan/Identification of Essential Services
- Policy S-04-01: Infectious Disease
- Policy S-04-05: COVID-19
- Policy S-04-06: Mandatory COVID-19 Vaccination -- SGL
- Policy S-04-06-01 LOGAN - Vaccination Medical Exemption Form
- Policy S-04-06-02 LOGAN - Vaccination Religious Exemption Form
- Policy S-05-01: Emergency Management Plan – Residential Services
- Policy S-05-02: Staff Shortage Procedures – Residential Services
- Policy S-05-03: Pandemic Procedures – Residential Services
- Procedure SL-011: Emergency On-Call Procedure for Supported Living
- Procedure SL-011-02: Management of the Supported Living Emergency On-Call Phone
- Procedure GL-005: Emergency On-Call Procedure for Group Living
- Procedure GL-005-02: Management of the Group Living Emergency On-Call Phone
- Table of Contents Health and Safety Section of LOGAN Policy Manual
- Table of Contents SGL Emergency Preparedness Plan
- List of Appendices SGL Emergency Preparedness Plan for COVID-19

We will be happy to provide any additional information or documents upon request.

We believe we have met compliance expectations in terms of our emergency preparedness plan for residential services.

Thank you.

Sincerely,


Cheryl Schade
VP/Chief Program Officer

PROCEDURE: TOTAL EVACUATION PLAN/IDENTIFICATION OF ESSENTIAL SERVICES

In the event of a fire, natural disaster or other event which results in the total evacuation of LOGAN Center or LOGAN Industries, the following occurs as needed.

A. Identification of Temporary Shelter:

1. Should the need to evacuate either LOGAN Center or LOGAN Industries result in seeking temporary shelter, the building which remains functional would be used.
2. In the event both are unusable, St Anthony Parish on Jefferson Boulevard would be used as a temporary shelter.
3. LOGAN provides housing to 52 persons in 7 LOGAN owned group homes. Should one or more of the houses become uninhabitable for any reason shelter will be sought in nearby hotels.
4. LOGAN supports individuals in their own homes or apartments, apart from family. Should the homes of one or more of these individuals become uninhabitable for any reason, shelter will be sought in nearby hotels.
5. LOGAN Policy S-05-01 Emergency Management Plan – Residential Services outlines specific details to be followed in the event of an emergency.

B. Identification of Essential Services:

1. The group home services LOGAN provides are essential services. Temporary housing can be obtained in hotels or persons can live with a family member for a short period of time. Should more long-term housing arrangements be needed LOGAN would be responsible to secure alternate housing. LOGAN employees assigned to the Group Living Department are required to be available for duty at all times.
2. For those individuals who received residential support through LOGAN's Supported Living Program., the residential support LOGAN provides is an essential service. Temporary housing can be obtained in hotels or persons can live with a family member for a short period of time. Should more long-term housing arrangements be needed LOGAN would assist the individual in securing alternate housing. LOGAN employees assigned to the Supported Living Department are required to be available for duty at all times.
3. LOGAN Protective Services Caseworkers are to be available at all times for those individuals for whom LOGAN serves as corporate guardian.
4. Dependent on the nature of the event, LOGAN Industries manufacturing operations may continue even when other services may be closed.
5. All other services LOGAN provides are non-essential services and could be closed for a period of time.
6. In all circumstances members of the Leadership Team are available for duty.
7. All key personnel have cell phones. A list of all home and cell phone numbers for all key personnel and emergency services is updated and distributed regularly.
8. Each Program Director is responsible to maintain an up-to-date list of contact information for all personnel.
9. Client Master Files and Employee Personnel Files are maintained electronically and the back up system is off site and could easily be retrieved in the event of a disaster.

C. Decision-Making Responsibility:

1. Decisions regarding the need for temporary shelter are made by the CEO and other LOGAN Officers.

2. Decisions regarding the continuation of essential services are made by CEO and other LOGAN Officers.

Date: April 30, 2022	By: VP/Chief Program Officer Program
----------------------	--------------------------------------

POLICY # S-04-01

POLICY: INFECTIOUS DISEASE

RELATED POLICIES:

S-01-23	Head Lice Diagnosis and Treatment Protocol
S-01-23-01	Quick Guide for Managing Head Lice
S-01-23-02	Documentation of Treatment Form-ALC
S-04-02	Post Exposure Follow-up --Employees
S-04-03	Employee Tuberculosis Screening Program
S-04-05	COVID-19
S-04-06	Mandatory COVID-19 Vaccination -- SGL

POLICY STATEMENT:

LOGAN will take all reasonable precautions to promote a safe and healthy environment and to avoid the spread of infectious disease.

GENERAL PROCEDURES:

1. The health status of an individual is a private and confidential issue. Every reasonable step will be taken to protect the confidentiality of medical status and records. The Program Directors will be responsible for the central management of the medical records of individuals served. The Human Resources Department will be responsible for central management of employee medical records.
2. The agency will provide, upon request, to all employees, service recipients and their families, guardians, and advocates:
 - A. Information or education about infectious diseases, particularly those prevalent for residents and employees of congregate settings.
 - B. Referrals to appropriate medical and social service agencies.
 - C. Information regarding insurance or other benefits.
3. All requests for employee accommodations should be made in writing to the Human Resources Department and supported by a written statement from a physician or health care provider. LOGAN may require an examination by a physician approved by LOGAN. The final decision as to whether accommodations can be made available, and if so, the type of accommodations, rests with LOGAN.
4. In some cases, LOGAN may request a physician's statement that a specific medical condition does not pose a threat to the workforce or the people we support. LOGAN reserves the right to ask for an examination by a LOGAN approved physician. Should the physicians' opinion differ, LOGAN will rely on the opinion received from the LOGAN approved physician or an independent third party.
5. If LOGAN obtains medical advice that an individual receiving service or an employee with a medical condition poses a threat to the safety of the work environment, necessary reasonable precautions will be taken to protect other individuals in accordance with the physician's recommendations.

6. In all day services, service recipients who show symptoms of a contagious illness or condition (e.g., fever, vomiting, diarrhea, head lice, staph infections, rubella, Tuberculosis, COVID-19, etc.) will be immediately reported to the LOGAN Program Director, as applicable; Primary Care Physician, as appropriate; and local authorities, as appropriate. They will be excluded immediately from the day services and may not return until 24 hours after the occurrence of the last symptom or when given clearance by his/her physician. See below for more return-to-day services criteria.
7. Employees are encouraged to practice similar precautions as described in #6 and to take all appropriate measures to prevent the spread of communicable disease. See below for more return-to-work criteria.
8. Employees, who provide home-based services will use Universal Precautions and will disinfect all toys and other materials used prior to providing services to another individual.
9. Training will be provided to all employees in New Staff Orientation and annually on the Universal Precautions, Bloodborne Pathogens, Tuberculosis, Communicable Diseases, and availability of vaccination against Hepatitis B.
10. To prevent the transmission of infectious diseases, Universal Precautions will be implemented in the handling of all body secretions. Employees who fail to use Universal Precautions when handling body fluids may be subject to disciplinary corrective action, up to and including termination.

RETURN TO WORK PROCEDURES -- Employees

1. If staff call off ill, they need to specify the reason with their supervisor, especially if staff have a potentially contagious condition, so a potential return time frame can be discussed.
2. If staff is sent home ill for any reason (i.e.: vomiting, fever, diarrhea, etc.), the person must be symptom free for a **full 24 hours** prior to return. They would minimally be absent the very next day. There may be special situations that require a different (modified) time frame. This will be specified at the time the staff is sent/goes home or speaks with their supervisor who will get direction from the Program Director.
3. If staff are off work for five (5) consecutive days due to a medical/health reason, a physician signed Authorization to Return must be received stating that they may return to work. Any restrictions or special orders must be noted specifically. This ensures that the staff is ready to return, as well as any special health considerations are noted and will be followed during their shift(s), if accommodations allow. This must be received **prior** to staff return.
4. If staff receive any emergency treatment or medical intervention (i.e.: trip to urgent care or an emergency room), a physician signed release (or notation on medical /discharge paperwork from the urgent care center or emergency room) must be received stating that the employee may resume their normal work activities. Restrictions or follow up care that applies to work hours must be specifically noted. This ensures that any special considerations or restrictions that need to be followed during work hours are specifically noted, providing staff's supervisor and Human Resources with this necessary information.
5. If the staff is diagnosed with anything contagious (i.e.: influenza, conjunctivitis; ringworm; shingles; impetigo; etc.), a physician signed Authorization to Return must be received stating that they are no longer considered contagious and that they may return to work. If staff are prescribed medication for a contagious condition, staff must be on the prescribed medication a full 24 hours prior to return.

RETURN TO WORK PROCEDURES – Individuals in Day Services

1. If a service recipient stays home from program due to illness, they need to specify the reason with their Program Coordinator, especially if the individual has a potentially contagious condition, so a potential return time frame can be discussed.
2. If a service recipient is sent home ill for any reason (i.e.: vomiting, fever, diarrhea, etc.), the person must be symptom free for a **full 24 hours** prior to return. They would minimally be absent the very next day. There may be special situations that require a different (modified) time frame. This will be specified at the time the individual is sent/goes home or speaks with their Program Coordinator who will get direction from the Program Director.
3. If a service recipient is out of program for five (5) consecutive days due to a medical/health reason, a physician signed Authorization to Return must be received stating that the individual may return to normal activities. Any restrictions or special orders must be noted specifically. This ensures that the individual is ready to return, as well as any special health considerations are noted and will be followed during their program day, if accommodations allow. This must be received **prior** to the individual's return to program.
4. If a service recipient receives any emergency treatment or medical intervention (i.e.: trip to urgent care or an emergency room), a physician signed release (or notation on medical /discharge paperwork from the urgent care center or emergency room) must be received stating that the individual may resume their normal activities. Restrictions or follow up care that applies to day program hours must be specifically noted. This ensures that any special considerations or restrictions that need to be followed during program hours are specifically noted, providing the individual's support team with this necessary information.
5. If the individual receiving service is diagnosed with anything contagious (i.e.: influenza, conjunctivitis; ringworm; shingles; impetigo; etc.), a physician signed Authorization to Return must be received stating that they are no longer considered contagious and that they may return to program. If the individual receiving service is prescribed medication for a contagious condition, the service recipient must be on the prescribed medication a full 24 hours prior to return.

SPECIAL CONDITIONS

TUBERCULOSIS

Employees

1. All staff will be required prior to assuming their work duties, and annually thereafter for Supervised Group Living staff, to submit written evidence that a TB test or Chest X-ray was completed.

Service Recipients

1. As criteria of admission to the LOGAN Group Living, Supported Living and adult day programs, LOGAN will require proof of negative TB test or Chest X-ray within the last 90 days. Program applicants who do not supply this evidence will not be accepted for services.
2. Annually, individuals served in LOGAN Group Living must show evidence of a negative TB test.

HEPATITIS B

Employees

1. Informed consent will be required of all employees or post-offer applicants prior to any testing, screening, or vaccination for Hepatitis B. This consent will be documented and become part of the individual's master file or personnel file.
2. All employees who have a significant potential for coming into contact with the body fluids of others, will be required to present proof of immunity from Hepatitis B, be vaccinated at LOGAN's expense, or sign a declination agreement.

Service Recipients

1. As criteria of admission to the LOGAN Group Living, Supported Living, Community Habilitation, Family Supports and adult day service programs, LOGAN will require proof of immunity (documented laboratory evidence of either current or past infection with the subsequent development of immunity) or vaccination against Hepatitis B. Program applicants or their guardians who choose not to be vaccinated must sign a declination agreement.
2. Should an applicant to the LOGAN group living program be admitted without proof of immunity or vaccination against Hepatitis B, antigen screening for hepatitis will be administered by the physician.

COVID-19

1. See separate policies pertaining to this infectious disease.

Approved: October 28, 1987
Board of Directors

Date: By:
November 29, 2021 VP/Chief Program Officer

Status:
Revised

POLICY # S-04-05

POLICY: COVID-19

RELATED POLICIES:

S-04-01 Infectious Disease

S-04-06 Mandatory COVID-19 Vaccination -- SGL

POLICY STATEMENT:

LOGAN will take all reasonable precautions to promote a safe and healthy environment and to avoid the spread of infectious disease. This policy pertains specifically to COVID-19 but is to be considered in conjunction with the Infectious Disease and the Mandatory COVID-19 Vaccination – SGL Policies.

A. GENERAL PROCEDURES

1. In that the COVID-19 was a novel coronavirus in 2020, all policies set forth below are subject to change as frequently as indicated by the CDC. In this rapidly changing environment, if state or federal mandates change before we can update existing LOGAN policies, state and federal mandates will supersede LOGAN policies.
2. Vaccination for COVID-19 has become widely available. LOGAN employees are encouraged to get vaccinated for COVID-19, including booster shots when eligible. Vaccines are effective at preventing COVID-19, especially severe illness, and death. Booster shots are now being recommended for those who have been fully vaccinated for at least six months. Guidance surrounding protocols for vaccinated and unvaccinated people is evolving, which may result in changes to safety protocols. Given what we know now, even people who have had their vaccines should continue taking basic prevention steps.
3. All employees of the LOGAN group living department, other LOGAN employees who work in the group homes as a regular part of their duties (e.g., Maintenance and IT department employees and moonlighters), and other LOGAN employees who have frequent interaction with group home employees and residents (e.g., day program, production, etc.) are required to meet one of the following conditions:
 - a. Have been fully vaccinated
 - b. Have been granted a qualifying exemption
 - c. Have a pending request for a qualifying exemption
 - d. Are identified as having a temporary delay as recommended by the CDC
4. General screening questions are required to enter a LOGAN facility and report to work. Employees and service recipients are expected to stay home when feeling unwell and/or displaying COVID-19 related symptoms. Employees and service recipients are encouraged to get tested for COVID-19 when they are exhibiting COVID-19 symptoms. When a person is in doubt about whether they should pursue testing, employees and service recipients are urged to contact their doctor and get tested if recommended.
5. COVID-19 symptoms may include but are not limited to fever or chills, cough, shortness of breath or difficulty breathing, fatigue, muscle or body aches, headache, new loss of taste or smell, sore throat, congestion or runny nose, nausea or vomiting, and diarrhea. Symptoms may appear 2-14 days after exposure and symptoms may be mild or severe. Displaying any of these

symptoms does not necessarily mean the person has COVID-19; only testing can confirm COVID-19.

6. Employees are expected to practice safety protocols including frequent handwashing and social distancing as appropriate to prevent the spread of COVID-19.
7. Face masks are optional at LOGAN facilities; however, each department director may set and enforce specific mask requirements as necessary to meet licensing requirements (i.e. group homes licensed as ICF/ID's) or to ensure the safety and wellbeing of all individuals. Masks are required for periods of time (as defined below) in certain exposure/infection circumstances. By regulation, masks are required for employees when in LOGAN group homes. When in the community on behalf of LOGAN, employees must adhere to requirements of local businesses and federal mandates (e.g., public transportation).
8. If at any time, an employee has questions or uncertainty about LOGAN COVID-19 protocols, they must seek guidance from their supervisor or director.

B. COMMUNICATION ABOUT COVID-19

1. LOGAN requires employees to promptly notify their supervisor or program director when they have tested positive for COVID-19, have been diagnosed with COVID-19 by a licensed healthcare provider, or have been exposed to COVID-19, whether at LOGAN or outside of LOGAN. Service recipients must also notify LOGAN in case of a positive test or exposure.
2. Living, work, and program spaces at LOGAN may be zoned to make it easier to address confirmed or suspected exposure to cases of COVID-19. When staff or service recipients have been exposed or presumed to have been exposed to COVID-19, meaning they have been in physical contact less than 6 feet for more than 15 minutes with this individual, each staff or service recipient in the affected zone will be informed so that appropriate measures can be taken. All efforts to protect the identity of the staff or service recipient who was confirmed or presumed positive will be taken as this is HIPAA protected information. The measures to be taken are outlined below. Guidance for group homes, which are licensed through the Indiana State Department of Health as ICF/ID's, may be subject to slightly different protocols than are listed below.

C. EXPOSURE TO COVID-19

1. Exposure is defined as being in physical contact, with an individual positive for COVID-19, less than 6 feet for more than 15 minutes.
2. LOGAN employees are considered essential healthcare workers and as such county, state, and CDC guidance pertaining to essential healthcare workers is used to determine policies.
3. Fully vaccinated employees who have come into close contact with someone with COVID-19 or believe they may have been exposed to someone with COVID-19 are expected to continue to work if they are asymptomatic. They must be tested immediately, but not earlier than 2 days after the exposure and, if negative, again 5-7 days after exposure. They must wear a mask in indoor settings for 14 days or until they receive a second negative test result. They need to isolate only if they have tested positive. Most fully vaccinated people with no COVID-like symptoms do not need to quarantine or be restricted from work following an exposure to someone with suspected or confirmed COVID-19, if they follow the testing and masking recommendation above.

4. Fully vaccinated service recipients follow the same protocols as fully vaccinated employees, although it is acknowledged that not all service recipients can tolerate masks. Service recipients may choose to quarantine in lieu of testing procedures.
5. Unvaccinated employees who have come into close contact with someone with COVID-19 or believe they may have been exposed to someone with COVID-19 must be off work until they have been tested twice (*except in cases of residential staff and residential moonlighters – see #7 below). They must be tested immediately, but not earlier than 2 days after the exposure and, if negative, again 5-7 days after exposure. They must wear a mask in indoor settings for 14 days or until they receive the second negative test result. They need to isolate only if they have tested positive.
6. Unvaccinated service recipients follow the same protocols as unvaccinated employees. Service recipients who live at home with family may choose to quarantine in lieu of testing.
7. Regardless of vaccination status, if they are asymptomatic, staff in residential programs are still expected to work while awaiting test results. Unvaccinated residential moonlighters, if they are asymptomatic, can work only in residential programs, and not in their primary position, while awaiting test results.

D. CONFIRMED OR SUSPECTED CASES OF COVID-19

1. Return to Work Procedures -- Employees

Use one of the below symptom-based strategies to determine when LOGAN personnel may return to work. Choose whichever is appropriate for the staff's specific circumstances.

a. Staff – Tested for COVID 19

If staff have had the COVID-19 testing, completed at certified testing site or with an FDA emergency approved test kit brand (list included at the end of the document), have the documentation, and have tested positive, staff will be excluded from work until:

- 10 days from test date or onset of symptoms, whichever comes sooner. Only 5 days are required if staff are asymptomatic regardless of vaccination status.
AND
- Resolution of fever without the use of fever -reducing medications (such as Tylenol) for at least 24 hours
AND
- Improvement in respiratory symptoms (e.g., cough, shortness of breath)
AND
- Other symptoms of COVID-19 are improving (loss of taste and smell may persist for weeks or months and need not delay the end of isolation).

CDC guidelines state that for mild to moderate illness, the individual is no longer considered contagious after the 14-day period of isolation and the symptoms should dissipate within that time frame as well. For those with severe to critical illness the symptoms may persist for up to 20 days.

If symptoms persist beyond the 10 days, the COVID-19 Officer Team will determine when the employee can return to work, taking the individual's specific health conditions into consideration in addition to CDC guidelines.

b. Staff – Symptomatic but not tested for COVID 19

If staff have not been tested but have been instructed by health care professional to self-isolate until fever is gone and symptoms have improved, staff will be excluded from work until:

- At least 24 hours have passed since recovery defined as resolution of fever without the use of fever-reducing medications and improvement in respiratory symptoms (e.g., cough, shortness of breath).
- AND
- At least 10 days have passed since symptoms first appeared.

c. Return to Work Practices and Work Restrictions -- Employees

After returning to work, staff should:

- Adhere to hand hygiene (frequent and thorough handwashing) and respiratory hygiene and cough etiquette (cover nose and mouth when coughing or sneezing and dispose of tissues in waste receptacles immediately).
- Self-monitor for symptoms and seek re-evaluation from occupational health if respiratory symptoms recur or worsen.

2. Return to Program Practices and Restrictions – Service Recipients

If a service recipient tests positive for COVID-19, they will be asked to shelter in place at their own home and return to program following procedures noted below.

- a. If a LOGAN residential service recipient tests positive for COVID-19, all service recipients of the same home will be treated as positive. They will shelter in place with assigned staff staying in the group or supported living residence with them for the required quarantine period. Quarantine period is 10 days from test date or onset of symptoms, whichever comes sooner. Only 5 days is required if service recipient is asymptomatic, regardless of vaccination status. A longer period of quarantine may be required based on displayed symptoms. As required, medical care will be secured.

- b. Use one of the below symptom-based strategies to determine when a non-residential service recipient may return to program. Choose whichever is appropriate for the service recipient's specific circumstances.

1. Service Recipient -- Tested for COVID-19

If a service recipient had the COVID-19 testing, completed at certified testing site or with an FDA emergency approved test kit brand (list included at the end of the document), have the documentation, and have tested positive, staff will be excluded from work until:

- 10 days from test date or onset of symptoms, whichever comes sooner. Only 5 days is required if the service recipient is asymptomatic, regardless of vaccination status.
AND
- Resolution of fever without the use of fever -reducing medications (such as Tylenol) for at least 24 hours
AND
- Improvement in respiratory symptoms (e.g., cough, shortness of breath)
AND
- Other symptoms of COVID-19 are improving (loss of taste and smell may persist for weeks or months and need not delay the end of isolation).

CDC guidelines state that for mild to moderate illness, the individual is no longer considered contagious after the 14-day period of isolation and the symptoms should dissipate within that time frame as well. For those with severe to critical illness the symptoms may persist for up to 20 days.

If symptoms persist beyond the 10 days, the COVID-19 Officer Team will determine when the service recipient can return to work, taking the individual's specific health conditions into consideration in addition to CDC guidelines.

2. Service Recipient -- Symptomatic but not tested for COVID-19

If service recipient has not been tested but has been identified as a close contact, and/or is symptomatic, and/or has been instructed by health care professional to self-isolate, service recipient will be excluded from day services until:

- At least 24 hours have passed since recovery defined as resolution of fever without the use of fever-reducing medications and improvement in respiratory symptoms (e.g., cough, shortness of breath).
AND
- At least 10 days have passed since symptoms first appeared.

E. FDA EMERGENCY APPROVED TEST KITS

The following tests have emergency use authorization from the FDA to test for COVID-19, and the most recent information is always available from the FDA (Antigen or Molecular) by searching "home test" and including quotes. Check with your local pharmacy or online for availability.

1. Abbott Diagnostics Scarborough, Inc. BinaxNOW tests
 - a. BinaxNOW COVID-19 Antigen Self-Test
 - b. BinaxNOW COVID-19 Ag Card Home Test
 - c. BinaxNOW COVID-19 Ag Card 2 Home Test
2. Access Bio, Inc. - CareStart COVID-19 Antigen Home Test
3. ACON Laboratories, Inc - Flowflex COVID-19 Antigen Home Test
4. Becton, Dickinson and Company (BD) - BD Veritor At-Home COVID-19 Test
5. Celltrion USA, Inc. - Celltrion DiaTrust COVID-19 Ag Home Test
6. Cue Health Inc. - Cue COVID-19 Test for Home and Over The Counter (OTC) Use
7. Detect, Inc. - Detect Covid-19 Test
8. Ellume Limited – Ellume COVID-19 Home Test

9. iHealth Labs, Inc. - iHealth COVID-19 Antigen Rapid
10. InBios International Inc.
11. Lucira Health, Inc.
 - a. Lucira CHECK-IT COVID-19 Test Kit
 - b. Lucira COVID-19 All-In-One Test Kit (Prescription)
12. OraSure Technologies, Inc.
 - a. InteliSwab COVID-19 Rapid Test
 - b. InteliSwab COVID-19 Rapid Test Rx
13. Quidel Corporation
 - a. QuickVue At-Home OTC COVID-19 Test
 - b. QuickVue At-Home COVID-19 Test.

Infectious Disease Policy Approved:

October 28, 1987
Board of Directors

Date:
April 30, 2022

By:
VP/Chief Program Officer

Status:
Revised

POLICY # S-04-06

POLICY: MANDATORY COVID-19 VACCINATION -- SGL

RELATED POLICIES:

S-04-01 Infectious Disease

S-04-05 COVID-19

S-05-03 Pandemic Procedures – Residential Services

POLICY STATEMENT:

LOGAN will take all reasonable precautions to promote a safe and healthy environment and to avoid the spread of infectious disease. Vaccination is a vital tool to reduce the presence and severity of COVID-19 cases in the workplace, in communities, and in the nation as a whole. LOGAN has adopted this policy on mandatory vaccination to safeguard the health of our employees from the hazard of COVID-19. This policy complies with *CMS Omnibus COVID-19 Health Care Staff Vaccination Interim Final Rule* for individuals working in specified Medicare and Medicaid participating facilities; for LOGAN this applies to Intermediate Care Facilities for individuals with Intellectual Disabilities (ICF/ID), or in other words LOGAN group homes. Henceforth, this will be referred to as the CMS Vaccine Mandate.

This mandatory COVID-19 vaccination policy only applies to all employees of the LOGAN group living departments, other LOGAN employees who work in the group homes as a regular part of their duties (e.g., Maintenance and IT department employees and moonlighters), and other LOGAN employees who have frequent interaction with group home employees and residents (e.g., day program, production, etc.).

PROCEDURES:

1. All employees of the LOGAN group living department, other LOGAN employees who work in the group homes as a regular part of their duties (e.g., Maintenance and IT department employees and moonlighters), and other LOGAN employees who have frequent interaction with group home employees and residents (e.g., day program, production, etc.) are required to meet one of the following conditions:
 - a. Have been fully vaccinated
 - b. Have been granted a qualifying exemption
 - c. Have a pending request for a qualifying exemption
 - d. Are identified as having a temporary delay as recommended by the CDC
2. Compliance with this requirement is a term and condition of employment at LOGAN for employees of the LOGAN group living department and other LOGAN employees who work in the group homes as a regular part of their duties. All employees hired into these departments are required to meet this requirement.
3. Employees are considered fully vaccinated two weeks after completing primary vaccination with a COVID-19 vaccine, with, if applicable, at least the minimum recommended interval between doses. For example, this includes two weeks after a second dose in a two-dose series, such as the Pfizer or Moderna vaccines, two weeks after a single-dose vaccine, such as the Johnson & Johnson vaccine, or two weeks after the second dose of any combination of two doses of different COVID-19 vaccines as part of one primary vaccination series.

4. All required staff must receive any recommended booster doses, and any recommended additional doses for individuals who are immunocompromised, in accordance with the recommended timing of such doses.
5. All employees are required to report their vaccination status and to provide proof of vaccination. Employees must provide truthful and accurate information about their COVID-19 vaccination status.
6. Employees may schedule their vaccination appointments at any available location.
7. Employees may request a vaccine exemption from the COVID-19 vaccination requirements in the following circumstances:
 - If the vaccine is medically contraindicated for the employee or medical necessity requires a delay in vaccination.
 - If the vaccination conflicts with a sincerely held religious belief, practice, or observance.All requests for employee exceptions pertaining to this mandatory vaccination policy should be made in writing to the Human Resources Department by the employee using the applicable exception request form. All such requests will be handled in accordance with applicable laws and regulations and LOGAN's Infectious Disease Policy (H-04-01).
8. Human resources will track and securely document the COVID-19 status, granted medical exemptions, and granted religious exemptions for all required staff.
9. All medical information collected from employees, including vaccination information, test results, and any other information obtained because of testing, will be treated in accordance with applicable laws and policies on confidentiality and privacy.
10. Failure to comply with this policy is considered a Type C Violation (H-12-01 General Work Rules and Disciplinary Corrective Action) and as such is subject to immediate termination.

VACCINATION STATUS AND ACCEPTABLE FORMS OF PROOF OF VACCINATION:

1. All vaccinated employees are required to provide proof of COVID-19 vaccination, regardless of where they received vaccination. Proof of vaccination status must be submitted to the Human Resources Department. It is the responsibility of the employee to ensure the proof was received by the Human Resources Office.
2. Acceptable proof of vaccination status includes any one of the following:
 - The record of immunization from a healthcare provider or pharmacy.
 - A copy of the COVID-19 Vaccination Record Card.
 - A copy of medical records documenting the vaccination.
 - A copy of immunization records from a public health, state, or tribal immunization information system.
 - A copy of any other official documentation that contains the type of vaccine administered, date(s) of administration, and the name of the healthcare professional(s) or clinic site(s) administering the vaccine(s).
3. Proof of vaccination generally should include the employee's name, the type of vaccine administered, the date(s) of administration, and the name of the healthcare professional(s) or clinic site(s) that administered the vaccine. In some cases, state immunization records may not

include one or more of these data fields, such as clinic site; in those circumstances LOGAN will still accept the state immunization record as acceptable proof of vaccination.

4. LOGAN will pay employees for the time it requires to get vaccinated. Hourly employees will need to clock in if they are not already at the time of the appointment and clock out after the vaccination process is completed.
5. LOGAN does not pay for the rare instance of adverse reactions to the vaccine. If you experience any side effects and need to stay home after being vaccinated, you will need to use PTO or supervisor approved unpaid time off for your absence. LOGAN reserves the right change this at any time.

EXEMPTION REQUESTS:

1. Employees may request an exemption from this mandatory vaccination policy.
2. Medical exemptions will be granted if the vaccine is medically contraindicated for the employee or medical necessity requires a delay in vaccination. Certification signed and dated by a licensed medical practitioner, who is not the individual requesting the exemption, and who is acting within their respective scope of practice, is required providing the clinical reasons for contraindications that form the basis of the exemption request.
3. Medical exemptions will be granted if a medical necessity requires a temporary delay in vaccination, as recommended by the CDC, due to clinical precautions and considerations, including, but not limited to, individuals with acute illness secondary too COVID-19 or individuals who received monoclonal antibodies or convalescent plasma for COVID 19 treatment.
4. Religious exceptions will be granted if the vaccination conflicts with a sincerely held religious belief, practice, or observance.
5. All requests for employee exceptions pertaining to this mandatory vaccination policy should be made in writing to the Human Resources Department by the employee using the applicable exception request forms.
6. All such requests will be handled in accordance with applicable laws and regulations and LOGAN's Infectious Disease Policy (S-04-01) and LOGAN's COVID-19 Policy (S-04-05).

INFECTION PREVENTION AND CONTROL:

1. LOGAN will take measures to prevent the transmission and spread of COVID-19 in the group home.
2. General screening questions are required of employees and visitors prior to entering a group home. Hourly employees will answer screening questions when clocking in.
3. The temperatures of the employees and visitors are taken upon entering the home. Entry will not be permitted for individuals with a temperature at or above 100.4.
4. Employees are expected to stay home when feeling unwell and/or displaying COVID-19 related symptoms and are expected to stay home. Testing for COVID 19 is required for employees exposed to COVID-19 and when they are exhibiting COVID-19 symptoms.

5. Regardless of vaccination status, employees are expected to practice safety protocols including the wearing of face masks over the nose and mouth and frequent handwashing to prevent the spread of COVID-19. Employees are required to wear masks in the group home and in all other program areas, which includes occupying a vehicle with other people.
6. Employees who have not been vaccinated must always wear face masks over the nose and mouth when indoors and outdoors when social distancing cannot be maintained.
7. The following exceptions are made for not wearing a face mask.
 - For a limited time, while an employee is eating or drinking at the workplace can an employee not wear a face mask.
 - When an employee is alone in a room with floor to ceiling walls and a closed door.
 - When the employee has determined the use of a face covering is infeasible or creates a greater hazard, such as when the work requires an uncovered mouth, or when it presents a risk of serious injury or death to the employee.
8. Employees will be attentive to how infection spreads in the residential setting. They will minimize personal contact except what is required for personal care. When providing personal care, they will wear PPE such as masks and gloves to prevent infection spread.
9. LOGAN will supply residential sites with Personal Protective Equipment (PPE) including but not limited to face masks (cloth, surgical, KN95, and N95), gloves, face shields, and gowns.
10. Typically, N95 face masks, face shields, and gowns are reserved for working with COVID-19 positive residents. However, employees may wear as much as PPE as desired when no COVID 19 positive exists.
11. Staff will have access to EPA-registered hospital grade disinfectants, including hand sanitizer, to allow for frequent cleaning of high touch surfaces and shared client equipment/bathrooms, etc. Staff are required to sanitize a minimum of four times per day or more often as necessary.

Infectious Disease Policy Approved:

October 28, 1987
Board of Directors

Date:
April 30, 2022

By:
VP/Chief Program Officer

Status:
Revised



Request for Accommodation: Certification for Medical Exemption from the LOGAN COVID-19 Mandatory Vaccination Policy

To request an exemption from LOGAN's COVID-19 Mandatory Vaccination Policy, please complete section 1 below and have your health care provider complete section 2 before returning this form to the Human Resources department.

Section 1

Name (print):	Date:
Dept.:	Position:

I have read and understand LOGAN's COVID-19 Mandatory Vaccination Policy and am requesting a medical exemption.

I certify that the information I am submitting to substantiate my request for exemption is true and accurate to the best of my knowledge. I understand that submitting false information will lead to disciplinary action, up to and including termination.

I further understand that LOGAN is not required to provide this exemption if doing so would pose a direct threat to myself or others in the workplace or would create an undue hardship for LOGAN.

Employee Signature:	Date:
---------------------	-------

Section 2

Health Care Provider Certification for Vaccination Exemption

Employee Name: _____

Dear Health Care Provider,

LOGAN requires its employees to be vaccinated against COVID-19. A copy of LOGAN's COVID-19 Mandatory Vaccination Policy is attached. The individual named above is seeking an exemption to this policy or some aspect of this policy due to medical reasons. Please complete this form to assist LOGAN in deciding whether to grant the exemption request.

NOTICE TO HEALTH CARE PROVIDER: Please provide only the answers to the questions listed herein. The Genetic Information Nondiscrimination Act of 2008 (GINA) prohibits employers and other entities covered by GINA from requesting or requiring genetic information of an individual or family member of the individual, except as specifically allowed by this law. To comply with this law, we are asking that you not provide any genetic information when responding to this request for medical information. "Genetic information" as defined by GINA, includes an individual's family medical history, the

results of an individual's or family member's genetic tests, the fact that an individual or an individual's family member sought or received genetic services, and genetic information of a fetus carried by an individual or an individual's family member or an embryo lawfully held by an individual or family member receiving assistive reproductive services.

The above person should not be immunized for COVID-19 or subject to some other aspect of the policy for the following reasons (Please check all that apply):

- ☐ The above person should not be immunized for COVID-19 because of a history of previous allergic reaction to indicate an immediate hypersensitivity reaction to a component of the vaccine.
- ☐ The physical condition of the person or medical circumstances relating to the person are such that immunization is not considered safe. In the space below, please indicate the specific nature and probable duration of the medical condition or circumstances that contraindicate immunization with the COVID-19 vaccine.
- ☐ Other – In the space below, please indicate the accommodation requested and the specific nature and probable duration of the medical condition or circumstances that support the request for a medical exemption.

This exemption is:

☐ Temporary, expiring on: __/__/__, or when _____

☐ Permanent

I certify the above information to be true and accurate, and request exemption from the COVID-19 vaccination for the above-named individual.

Health Care Provider Name (print):	
Health Care Provider Signature:	Date:
Practice Name & Address:	Provider Phone:

COVID-19 VACCINE EXEMPTION – HR USE ONLY

To be completed by Human Resources Department

Date of initial request: __/__/__

Date sufficient certification received: __/__/__

Interactive discussion date(s) / notes of discussion, if applicable. Attach additional pages as necessary:

Accommodation request:

Approved __/__/__

Describe specific accommodation details:

Describe alternative safety precautions required, if any:

Denied __/__/__

Describe why accommodation is denied:

Alternative accommodation considered, if any:

Denial approved by Human Resources and Operations: __/__/__

Date Employee Was Notified of Decision: __/__/__

Name of HR Representative Completing This Form: _____

Date: _____



Request for Religious Exemption/Accommodation Related to COVID- 19 Vaccination Policy

LOGAN is an equal opportunity employer and is committed to complying with all laws protecting employees' religious beliefs and practices. When requested, LOGAN will provide an exemption/reasonable accommodation to its COVID-19 vaccination policy for employees' religious beliefs and practices which prohibit the employee from receiving a COVID-19 vaccine, provided the requested accommodation is reasonable and does not create an undue hardship for LOGAN or pose a direct threat to the health and/or safety of others in the workplace and/or to the requesting employee.

To request an Exemption/Accommodation related to LOGAN's COVID-19 vaccination incentive policy, please complete this form, and return it to Human Resources as soon as possible. This information will be used by Human Resources or other appropriate personnel to engage in an interactive process to determine whether an employee is eligible for a reasonable accommodation to the COVID-19 vaccination policy and if so, to determine what reasonable accommodations are available to the employee.

Part 1 – To Be Completed by Employee:

Name: _____

Date of Request: _____

Please explain below why you are requesting an Exemption/Accommodation from the COVID-19 vaccine requirement:

Verification and Accuracy

I verify that the information I am submitting in support of my request for an accommodation is complete and accurate to the best of my knowledge, and I understand that any intentional misrepresentation contained in this request may result in disciplinary action.

I also understand that my request for an accommodation may not be granted if it is not reasonable, if it poses a direct threat to the health and/or safety of others in the workplace and/or to me, or if it creates an undue hardship on LOGAN.

Signature: _____ Date: _____

Print Name: _____

Part 2 – To be completed by Human Resources Representative

Date Form Received by Human Resources: _____

Interactive Discussion Date(s) if applicable: _____

Exemption/Accommodation granted? ☐ Yes ☐ No

If yes, describe Exemption/Accommodation: _____

If Exemption/Accommodation granted, list required alternative safety precautions required:

If Exemption/Accommodation is denied, explain why:

Name of HR Representative: _____

Signature of HR Representative: _____

Date: _____

POLICY # S-05-01

POLICY: EMERGENCY MANAGEMENT PLAN -- Residential Services

RELATED POLICIES:

Policy S-01-02: Total Evacuation Plan/Identification of Essential Services

Policy S-04-01: Infectious Disease

Policy S-04-05: COVID-19

Policy S-04-06: Mandatory COVID-19 Vaccination -- SGL

Policy S-05-02: Staff Shortage Procedures – Residential Services

Policy S-05-03: Pandemic Procedures – Residential Services

All LOGAN Health and Safety Procedures in the LOGAN Policy Manual

LOGAN SGL Emergency Preparedness Plans

Procedure SL-011: Emergency On-Call Procedure for Supported Living

Procedure SL-011-02: Management of the Supported Living Emergency On-Call Phone

Procedure GL-005: Emergency On-Call Procedure for Group Living

Procedure GL-005-02: Management of the Group Living Emergency On-Call Phone

POLICY STATEMENT:

LOGAN is prepared to act in the event an emergency so that individuals receive needed supports and services. Emergencies may include a natural or manmade disaster, a pandemic, or staff shortage. Residential services are defined as Supervised Group Living (SGL) and the following waiver services: Residential Habilitation Services – Hourly and Daily, Structured Family Caregiving, and Participant Assistance and Care.

A. Leadership

1. Decision-Making Authority

- a. In emergency situations impacting the whole agency, the seven LOGAN Officers (President and Chief Executive Officer, Vice President/Chief Program Officer for Adult Services, Vice President/Chief Financial Officer, Chief Human Resources Officer, Chief Program Officer for Child and Adolescent Services, Chief Marketing Officer, and Chief Philanthropy Officer) will serve as the decision-making authority.
- b. In the event of emergency situations impacting residential services, the three residential directors (Director of Group Living, Director of Supported Living, and Director of Family Supports) the President and Chief Executive Officer, and the Vice President/Chief Program Officer for Adult Services will serve as the decision-making authority.
- c. Each residential director will be the decision-making authority for site specific issues within their department.
- d. Residential directors in collaboration with the President and Chief Executive Officer and the Vice President/Chief Program Officer for Adult Services will be responsible for coordination of residential services and related health services.

2. Critical Services

- a. The group home services LOGAN provides are essential services. In the event of an emergency, temporary housing can be obtained in hotels or persons can live with a family member for a short period of time. Should more long-term housing

arrangements be needed LOGAN is responsible to secure alternate housing. LOGAN employees assigned to the Group Living Department are required to be available for duty at all times.

- b. For those individuals who received residential support through LOGAN's Supported Living Program., the residential support LOGAN provides is an essential service. In the event of an emergency, temporary housing can be obtained in hotels or persons can live with a family member for a short period of time. Should more long-term housing arrangements be needed LOGAN will assist the individual in securing alternate housing. LOGAN employees assigned to the Supported Living Department are required to be available for duty at all times.

3. Policy Development

- a. LOGAN will follow any mandates and guidelines that are communicated from governmental agencies, including but not limited to, the Center for Disease Control, the Indiana and County Departments of Health, Indiana's Governor's Office, Department of Homeland Security, and the Family and Social Services Administration, Division of Disability and Rehabilitative Services, Bureau of Developmental Disabilities, and the Bureau of Quality Improvement Services.
- b. Based on the above referenced mandates and guidance, the Vice President/Chief Program Officer for Adult Services, in conjunction with LOGAN Officers and residential directors, will develop policies, procedures, and protocols related to each emergency, which will then be communicated to staff through an intentional and strategic approach to ensure each staff are aware of the role they play in the event of an emergency.
- c. Located in the LOGAN Policy Manual are detailed procedures relative to Health and Safety including but not limited to Identification of Essential Services, Emergency Management, Evacuation, Severe Weather, Bomb Threat, Workplace Violence, Infectious Disease, and COVID-19. Also, in the health and safety section of the manual are policies related to the staff shortages.
- d. At a minimum, LOGAN reviews its policies on an annual basis. As new guidance is issued or as LOGAN's needs change, the policies and procedures are reviewed and revised as necessary.

4. Timelines

- a. The timing of decisions in each of the aforementioned areas is dependent on the emergency and its impact on the health and wellbeing of individuals served and staff. Time is of the essence in most emergencies, so decisions must be made thoughtfully but quickly.

5. Training

- a. At a minimum of annually, each staff member will receive documented training specific to LOGAN policy S-05-01 Emergency Management Plan – Residential Services and related policies and procedures.
- b. As policies, procedures, and protocols are revised, staff receive documented training.
- c. In the event of a prolonged emergency, such as what was experienced with COVID-19, each staff member will receive documented training on procedures and protocols specific to the emergency as they are developed and/or revised, which may be as often as weekly.

B. Communication

1. Communication Authority
 - a. In the event of an emergency impacting the whole agency, the President and Chief Executive Officer will be responsible for external communication to LOGAN constituents and internal communication to all LOGAN staff. The Chief Marketing Officer will serve as backup. The President and Chief Executive Officer will approve all communication to be disseminated to constituents (e.g. individuals served, guardians, family members, staff, Board members, volunteers, and community at large).
 - b. When communication in addition to that described above and specific to residential services is necessary, the Vice President/Chief Program Officer for Adult Services will be responsible for the communication to constituents. The President and Chief Executive Officer will approve all communication to be disseminated to constituents.
2. Communication Methods
 - a. Communication will be sent to constituents via email and posted on the LOGAN Website. Links to this communication will be posted as well on LinkedIn, Facebook, Twitter, and Instagram.
 - b. As necessary, the message on LOGAN's main telephone line(s) may be changed to provide status and actions to anyone that calls that number. Similarly, information may be posted on the LOGAN website.
 - c. Signs posted on doors and main locations and throughout the facility will also communicate information to staff and visitors.
 - d. Communication to residential staff will include distribution of printed emails, distribution of documents to residential sites, formal staff meetings, zoom calls or phone calls.
 - e. Each department will develop and maintain methods to contact staff persons. This will include email addresses, home telephone numbers, cell phone numbers, addresses, and other work telephone numbers as applicable.
 - f. When an emergency appears to be imminent as defined in the related policies listed above, each department will utilize the phone tree to relay important and necessary information to staff.
 - g. LOGAN has a text alert system to communicate important and necessary information to staff.
 - h. Communication to individuals, families, guardians, advocates, case managers, and teams of those served residentially will most typically be sent via email. For those not having email, the printed communication will be mailed or hand-delivered to the pertinent party. If time disallows sending by mail, then a phone call will be made to the pertinent party. Scheduled zoom calls with this constituent group will also be utilized to communicate pertinent information.
 - i. Individual Support Team meetings will also be used as a vehicle for decision making and communication.
 - j. Each department will maintain current contact information for individuals and their families in as many modes as possible (e.g. telephone numbers, cell phone numbers, email addresses, etc.).
 - k. Telephone numbers and contact information will be maintained for other agencies that may be resources to LOGAN in the event of the emergency. These include the Red Cross, the local County Department of Health, and the main local hospitals.
3. Residential Individuals, Families, Guardians, Advocates, Case Managers, and Teams
 - a. Communication to individuals, families, guardians, advocates, Case Managers, and teams of those served residentially must outline specific information regarding any

change in service delivery and implementation of Appendix K flexibilities. Such communication may include but is not limited to any of the following:

1. Day Programs

- Suspension of day program
- Day services being provided at the group home rather than day program facility
- Day services being provided at the supported living residence rather than day program facility
- Change from face-to-face services to telemedicine
- Visitor guidelines
- Safety Protocols

2. Residential Services

- When consolidation of sites will or may occur
- When relocation of sites will or may occur
- When the individual can expect to return to their home
- How rent and other expenses will be handled when the individual is not residing in their legal residence
- Having sleep staff overnight
- Visitor guidelines
- Safety Protocols
- Managing COVID positive cases

- b. Individuals should have the support, information, and resources needed for them to be an active decision-maker in discussions about visitor guidelines and other safety protocols established for their home. If the individuals residing in the home do not agree on the guidelines or safety protocols, all individuals' support teams should convene as a group to discuss and make these determinations.
- c. This emergency management plan for residential services acknowledges that individuals served have individual-specific plans. At no time, will this plan infringe on the individual's rights or choice.

4. Timing and Frequency

- a. The timing and frequency of communication is dependent upon the emergency. This may vary from daily to monthly to quarterly. In the event of a prolonged emergency, bi-weekly zoom calls will be held with staff and monthly zoom calls will be held with families, guardians, advocates, and teams.
- b. When a change or service delivery occurs or Appendix K flexibilities are utilized as outlined above, the Individual Support Team will at least monthly discuss their continuation, phase-out period, or termination. At all times the specific needs of the individual and their likes and preferences is considered in making these determinations. The nature of the emergency will determine the frequency of review.

C. Staff Deployment

- 1. The Vice President/Chief Program Officer for Adult Services, working with residential directors will be responsible for deployment of staff.
- 2. Staffing Capacity
 - a. Each residential director will maintain a list of the number of hours of staffing needed to provide services for their area of responsibility each day. The number of staff needed is site specific, based on the needs of the individual, the resources available to the individual on their Waiver NOA or the licensure category of the group home.

- b. Residential directors maintain a system for providing after hours support (e.g. On-Call) for their area of responsibility. See related procedures.
 - c. A list of who is trained to work in each service site or group home is maintained by the residential director and is available to the management staff on-call.
 - d. LOGAN assumes full responsibility to ensure that individuals receiving group living or supported living services, particularly those in 24/7 settings, receive continued supports during an emergency. Whatever means necessary will be used to ensure necessary supports are provided to individuals.
3. Assessment and Monitoring of Staff Need
- a. While site specific schedules are maintained, the staffing needs vary from time to time due to scheduled time off, call off's, unexpected absences, and other unplanned issues.
 - b. The staffing needs of each site per shift are assessed daily by the Program Manager, Program Coordinator, and Case/Service Coordinator responsible for the site to assure individuals' needs are met.
 - c. These same staff ensure that trained staff are assigned to shifts to ensure individual needs are met.
 - d. Staff persons who normally work in a site or group home will be utilized to work in that site or group home whenever possible. When needed, people who are unable to work will be replaced with subs, part time staff, or any other staff who have been trained to work at that site or group home.
 - e. Administrative staff may be deployed as needed. Prior to working at a site or group home, the administrative staff will be properly trained to support the individual(s).
 - f. Each site or group home may be assessed at a different level since the assessment of need is site specific.
 - g. Staffing needs at each service site or group home for each shift may be placed in one of three assessment levels or tiers as defined below:
 - Optimum: There is the ideal number of staff available to meet the needs of the needs of the individuals' based on group home licensure category or Waiver NOA.
 - Sufficient: There is the minimum number of staff to meet the individuals' basic needs.
 - Critical: There is no staff available to fill a shift
4. Sufficient Tier
- a. The Sufficient Tier related to staff shortage as defined above is the minimum number of staff are available to meet the individuals' basic needs. This may be a short-term issue but may be more of a long-term issue.
 - b. Short-term is defined as an occasional shift or specific shifts but generally, the staffing of the home is able to meet needs and support individuals effectively.
 - c. Long-term is defined by an inability to provide staffing at no more than the very minimal level for the individuals. Full utilization of hours on the NOA or available to the group home is not occurring.
 - d. In adherence to the HCBS settings rule, individuals receiving waiver services will have individual specific emergency back up plans developed by their support team. Individual specific emergency specific plans will be honored, and decisions made by LOGAN will not infringe on individual rights and choices.
 - e. LOGAN will communicate early and often with case managers, individuals, and families when staffing and/or other typical support options are not available so that back up plans can be reasonably enacted.
 - f. Short-Term

1. When there is only sufficient staffing as defined above, individuals, guardians or advocates may consider alternate residential option while the provider increases its efforts to hire and train the needed staff to reach the Optimum Tier.
- g. Long-Term
 1. When there is only sufficient staffing as defined above, individuals, guardians or advocates may consider alternate residential options while the provider increases its efforts to hire and train the needed staff to reach the Optimum Tier.
 2. Remote supports will be considered by teams. An assessment will be done to evaluate the needs of the individual and how their needs can be met with remote supports. Remote supports will be used only when supported by the team and written in the individual Support Plan. See related policy.
 3. As vacancies occur in waiver sites, effort to consolidate sites will be taken to reduce the number of overall staffing need. This will be considered as are other admissions. The likes and preferences of the individual are considered as are the needs of the potential new housemates.
5. **Critical Tier**
 - a. The Critical Tier in staff shortage as defined above is no staff available to fill a shift. This may be a short-term issue but may be more of a long-term issue.
 - b. Short-term is defined as only one shift or several consecutive shifts. Short-term staff shortage would not exceed three consecutive days or a weekend.
 - c. Long-term staff shortage is defined by more than three consecutive days.
 - d. In adherence to the HCBS settings rule, individuals receiving waiver services will have individual specific emergency back up plans developed by their support team. Individual specific emergency specific plans will be honored, and decisions made by LOGAN will not infringe on individual rights and choices.
 - e. LOGAN will communicate early and often with case managers, individuals, and families when staffing and/or other typical support options are not available so that back up plans can be reasonably enacted.
 - f. Short-Term
 1. In the event of a critical staff shortage as defined above, any of the following may be utilized to ensure the individual receives needed supports for a short period of time.
 - b. Follow individual specific emergency backup plan developed by the Individual Support Team.
 - c. Locate a family member to take the individual to their home and provide needed services for a specified length of time. Most likely this person has been identified in the individual's emergency backup plan or is already someone who takes the individual home frequently.
 - d. For individuals with the Waiver, if the individual lives with a family member temporarily, Appendix K flexibilities may be considered by the Individual Support Team allowing the family member to receive reimbursement for the time spent caring for the individual in their home.
 - e. For group home residents who temporarily live with a family member, the individual cannot exceed the available number of therapeutic leave days, or they jeopardize group home placement. It is noted that Appendix K increased the number of therapeutic leave days available during the health emergency from 60 to 120.
 - f. Arrange for the individual to go to another supported living or group living site, whichever is appropriate, for a specified length of time, which would not include an overnight.

- g. The needs and preferences of the individuals being served will be considered when relocating individuals, even if temporarily.
 - h. Arrange for a staff member to live in residence with the individual(s). Approval from the individual(s) support team(s) will be acquired in such instances as staff will be permitted to sleep while in residence.
- h. Long-Term
- 1. In the event of a critical staff shortage as defined above, any of the following may be utilized to ensure the individual receives needed supports for a longer period of time. The needs and preferences of the individual will be considered.
 - a. Follow individual specific emergency backup plan developed by the Individual Support Team.
 - b. Locate a family member to take the individual to their home and provide needed services for a specified length of time. Most likely this person has been identified in the individual's emergency backup plan or is already someone who takes the individual home frequently.
 - c. For individuals with the Waiver, if the individual lives with a family member, Appendix K flexibilities may be considered by the Team allowing the family member to receive reimbursement for the time spent caring for the individual in their home.
 - d. For group home residents who live with a family member, the individual cannot exceed the available number of therapeutic leave days, or they jeopardize group home placement. It is noted that Appendix K increased the number of therapeutic leave days available during the health emergency. From 60 to 120.
 - e. The needs and preferences of the individuals being served will be considered when relocating individuals, even if temporarily.
 - f. Arrange for a staff member to live in residence with the individual(s). Approval from the individual(s) support team(s) will be acquired in such instances as staff will be permitted to sleep while in residence.
 - 2. Remote supports will be considered by teams. An assessment will be done to evaluate the needs of the individual and how their needs can be met with remote supports. Remote supports will be used only when supported by the team and written in the individual Support Plan. See related policy.
 - 3. As vacancies occur in waiver sites, effort to consolidate sites will be taken to reduce the number of overall staffing need. This will be considered as are other admissions. The likes and preferences of the individual are considered as are the needs of the potential new housemates.
- h. Family Supports
- 1. For those receiving residential services at home with family, LOGAN will work with families to ensure that necessary services are provided either by LOGAN staff or family members. Appendix K flexibilities will be used as determined necessary by the team.
 - 2. In times of emergency, the individual's family may choose to go without service until the emergency is over.
- i. Structured Family Caregiving
- 1. LOGAN provides Structured Family Caregiving to only two individuals. These individuals are considered members of the family as they have lived in their home for many, many years. LOGAN will ensure that necessary services are provided in their home and will use Appendix K flexibilities as determined necessary by the team.

D. Supplies

1. Each residential director is responsible for procurement and delivery of needed supplies. Collaboration with other directors will occur to assure cost effectiveness and efficiency in pricing and delivery.
2. Each department will maintain a supply of medical items predicted to be needed for infection control including masks, gloves, thermometers, etc. and will dispense to individual program sites as necessary.
3. Each department will maintain a supply of infection control items for cleaning and sanitizing environments and will dispense to individual program sites as necessary.
4. Each residential location will maintain an emergency food and water supply.
5. As appropriate, supplies will be shipped directly to the service site or group home. Groceries may be ordered to go or to be delivered as appropriate.

Date:
5/6/22

By:
VP/Chief Program Officer

Status:
Revised

POLICY # S-05-02

POLICY: STAFF SHORTAGE PROCEDURES – Residential Services

RELATED POLICIES:

Policy S-05-01: Emergency Management Plan – Residential Services

Procedure SL-011: Emergency On-Call Procedure for Supported Living

Procedure SL-011-02: Management of the Supported Living Emergency On-Call Phone

Procedure GL-005: Emergency On-Call Procedure for Group Living

Procedure GL-005-02: Management of the Group Living Emergency On-Call Phone

POLICY STATEMENT:

LOGAN is prepared to support individuals receiving residential services in the event of a staff shortage so that individuals receive needed supports and services. Residential services are defined as Supervised Group Living (SGL) and the following waiver services: Residential Habilitation Services – Hourly and Daily, Structured Family Caregiving, and Participant Assistance and Care.

A. General

1. The Vice President/Chief Program Officer for Adult Services, working with residential directors will be responsible for deployment of staff.

B. Communication

1. Communication to individuals, families, guardians, advocates, Case Managers, and teams of those served residentially must outline specific information regarding any change in service delivery and implementation of Appendix K flexibilities. Such communication may include, but is not limited to any of the following:
 - a. When consolidation of sites will or may occur
 - b. When relocation of sites will or may occur
 - c. When the individual can expect to return to their home
 - d. How rent and other expenses will be handled when the individual is not residing in their legal residence
 - e. Having sleep staff overnight
 - f. Visitor guidelines
 - g. Safety Protocols
 - h. Managing COVID positive cases
2. Individuals should have the support, information, and resources needed for them to be an active decision-maker in discussions about visitor guidelines and other safety protocols established for their home. If the individuals residing in the home do not agree on the guidelines or safety protocols, all individuals' support teams should convene as a group to discuss and make these determinations.
3. This emergency management plan for residential services acknowledges that individuals served have individual-specific plans. At no time, will this plan infringe on the individual's rights or choice.
4. Staffing Capacity
 - a. Each residential director will maintain a list of the number of hours of staffing needed to provide services for their area of responsibility each day. The number of staff needed is site specific, based on the needs of the individual, the resources available to the individual on their Waiver NOA or the licensure category of the group home.

- b. Residential directors maintain a system for providing after hours support (e.g. On-Call) for their area of responsibility. See related procedures.
- c. A list of who is trained to work in each service site or group home is maintained by the residential director and is available to the management staff on-call.
- d. LOGAN assumes full responsibility to ensure that individuals receiving group living or supported living services, particularly those in 24/7 settings, receive continued supports during an emergency. Whatever means necessary will be used to ensure necessary supports are provided to individuals.

C. Assessment and Monitoring of Staff Need

- 1. Each residential director will maintain the current schedule of staff deployed in their service sites or group homes.
- 2. While site specific schedules are maintained, the staffing needs vary from time to time due to scheduled time off, call off's, unexpected absences, and other unplanned issues.
- 3. Each residential director will maintain a system for monitoring the daily attendance of staff and ensuring that at any given time the service site or group home has the staff needed to provide the individual(s) needed supports and services.
- 4. Residential directors will maintain a system for providing after hours support for their area of responsibility. See related procedures.
- 5. The staffing needs of each site per shift are assessed daily by the Program Manager, Program Coordinator, and Service Coordinator responsible for the site to assure individuals' needs are met.
- 6. These same staff ensure that trained staff are assigned to shifts to ensure individual needs are met.
- 7. Staffing needs at each service site or group home for each shift may be placed in one of three assessment levels or tiers as defined below:
 - Optimum: There is the ideal number of staff available to meet the needs of the needs of the individuals' based on group home licensure category or Waiver NOA.
 - Sufficient: There is the minimum number of staff to meet the individuals' basic needs.
 - Critical: There is no staff available to fill a shift

Staffing needs will be identified in terms of short-term and long-term needs. Short-term is defined as only one shift or several consecutive shifts. Short-term would not exceed three consecutive days or a weekend. Long-term is defined by more than three consecutive days.

D. Deployment of Staff

- 1. Staff persons who normally work in a site or group home will be utilized to work in that site or group home whenever possible. When needed, people who are unable to work will be replaced with subs, part time staff, or any other staff who have been trained to work at that site or group home.
- 2. Administrative staff may be deployed as needed. Prior to working at a site or group home, the administrative staff will be properly trained to support the individual(s).
- 3. Each site or group home may be assessed at a different level since the assessment of need is site specific.
- 4. Financial incentives/bonuses have been predetermined for use as an inducement to secure needed staff to work open shifts. Financial incentives/bonuses in addition to overtime may be given to staff to entice them to work. This is to be done only with the approval of the residential director.
- 5. In the event of a staff shortage, 24/7 supported living sites and group homes will be given priority in terms of staffing. Needs in non-24/7 supported living sites will be assessed and prioritized based on results.

6. As a last resort, paid time off will be revoked or postponed to secure needed staff.

E. Group Living – Supervised Group Living

1. LOGAN assumes full responsibility to ensure that individuals receiving group living services receive continued supports during a staff shortage. Whatever means necessary will be used to ensure necessary supports are provided to individuals.
2. Staff persons who normally work in each group home will be utilized to work in that group home whenever possible. When needed, people who are unable to work will be replaced with subs, part time staff, or any other staff who have been trained to work at that group home.
3. A list of who is trained to work in which group homes will be maintained by the Director of Group Living and will be available to the management staff on-call.
4. Administrative staff may be deployed as needed. Prior to working at a group home, the administrative staff will be properly trained to support the individual(s).
5. The needs and preferences of the individuals being served will be considered when relocating individuals, even if temporarily. Decisions made by LOGAN will not infringe on individual rights and choices.
6. LOGAN will communicate early and often with individuals, and families when staffing and/or other typical support options are not available so that alternate plans can be set in motion.
7. Sufficient Tier
 - a. The Sufficient Tier related to staff shortage as defined above is the minimum number of staff are available to meet the individuals' basic needs. This may be a short-term issue but may be more of a long-term issue.
 - b. Short-term is defined as an occasional shift or specific shifts but generally, the staffing of the home is able to meet needs and support individuals effectively.
 - c. Long-term is defined by an inability to provide staffing at no more than the very minimal level for the individuals. Full utilization of hours available to the group home is not occurring.
 - d. Short-Term
 1. When there is only sufficient staffing as defined above, individuals, guardians or advocates may consider alternate residential option while the provider increases its efforts to hire and train the needed staff to reach the Optimum Tier.
 - e. Long-Term
 1. When there is only sufficient staffing as defined above, individuals, guardians or advocates may consider alternate residential options while the provider increases its efforts to hire and train the needed staff to reach the Optimum Tier.
8. Critical Tier
 - a. The Critical Tier in staff shortage as defined above is no staff available to fill a shift. This may be a short-term issue but may be more of a long-term issue.
 - b. Short-term is defined as only one shift or several consecutive shifts. Short-term staff shortage would not exceed three consecutive days or a weekend.
 - c. Long-term staff shortage is defined by more than three consecutive days.
 - d. Short-Term

In the event of a critical staff shortage as defined above, any of the following may be utilized to ensure the individual receives needed supports for a short period of time.

 1. Locate a family member to take the individual to their home and provide needed services for a specified length of time. Most likely this person is already someone who takes the individual home frequently.

2. For group home residents who temporarily live with a family member, the individual cannot exceed the available number of therapeutic leave days, or they jeopardize group home placement. It is noted that Appendix K increased the number of therapeutic leave days available during the health emergency from 60 to 120.
 3. Arrange for the individual to go to another group home for a specified length of time, which would not include an overnight.
 4. Arrange for a staff member to live in residence with the individual(s). Approval from the individual(s) support team(s) will be acquired in such instances as staff will be permitted to sleep while in residence.
- e. Long-Term
- In the event of a critical staff shortage as defined above, any of the following may be utilized to ensure the individual receives needed supports for a longer period of time. The needs and preferences of the individual will be considered.
1. Locate a family member to take the individual to their home and provide needed services for a specified length of time. Most likely this is already someone who takes the individual home frequently.
 2. For group home residents who live with a family member, the individual cannot exceed the available number of therapeutic leave days, or they jeopardize group home placement. It is noted that Appendix K increased the number of therapeutic leave days available during the health emergency. From 60 to 120.
 3. Arrange for a staff member to live in residence with the individual(s). Approval from the individual(s) support team(s) will be acquired in such instances as staff will be permitted to sleep while in residence.
 4. As vacancies occur in group homes, consolidation of group homes may be considered to reduce the number of overall staffing need.

F. Supported Living – Residential Habilitation Hourly and Daily and Participant Assistance and Care

1. LOGAN assumes full responsibility to ensure that individuals receiving supported living services receive continued supports during a staff shortage. Whatever means necessary will be used to ensure necessary supports are provided to individuals.
2. Staff persons who normally work in specific waiver sites will be utilized to work in those specific sites whenever possible. When needed, people who are unable to work will be replaced with subs, part time staff, or any other staff who have been trained to work at that site.
3. A list of who is trained to work in which sites will be maintained by the Director of Supported Living and will be available to the management staff on-call.
4. Administrative staff may be deployed as needed. Prior to working at a supported living site, the administrative staff will be properly trained to support the individual(s).
5. The needs and preferences of the individuals being served will be considered when relocating individuals, even if temporarily. Decisions made by LOGAN will not infringe on individual rights and choices.
6. LOGAN will communicate early and often with case managers, individuals, and families when staffing and/or other typical support options are not available so that back up plans can be reasonably enacted.
7. **Sufficient Tier**
 - a. The Sufficient Tier related to staff shortage as defined above is the minimum number of staff are available to meet the individuals' basic needs. This may be a short-term issue but may be more of a long-term issue.

- b. Short-term is defined as an occasional shift or specific shifts but generally, the staffing of the home is able to meet needs and support individuals effectively.
 - c. Long-term is defined by an inability to provide staffing at no more than the very minimal level for the individuals. Full utilization of hours on the NOA is not occurring.
 - d. In adherence to the HCBS settings rule, individuals receiving waiver services will have individual specific emergency back up plans developed by their support team. Individual specific emergency specific plans will be honored, and decisions made by LOGAN will not infringe on individual rights and choices.
 - e. Short-Term
 - 1. When there is only sufficient staffing as defined above, individuals, guardians or advocates may consider alternate residential option while the provider increases its efforts to hire and train the needed staff to reach the Optimum Tier.
 - f. Long-Term
 - 1. When there is only sufficient staffing as defined above, individuals, guardians or advocates may consider alternate residential options while the provider increases its efforts to hire and train the needed staff to reach the Optimum Tier.
 - 2. Remote supports will be considered by individual support teams. An assessment will be done to evaluate the needs of the individual and how their needs can be met with remote supports. Remote supports will be used only when supported by the team and written in the individual Support Plan. See related policy.
 - 3. As vacancies occur in waiver sites, effort to consolidate sites will be taken to reduce the number of overall staffing need. This will be considered as are other admissions. The likes and preferences of the individual are considered as are the needs of the potential new housemates.
8. Critical Tier
- a. The Critical Tier in staff shortage as defined above is no staff available to fill a shift. This may be a short-term issue but may be more of a long-term issue.
 - b. Short-term is defined as only one shift or several consecutive shifts. Short-term staff shortage would not exceed three consecutive days or a weekend.
 - c. Long-term staff shortage is defined by more than three consecutive days.
 - d. In adherence to the HCBS settings rule, individuals receiving waiver services will have individual specific emergency back up plans developed by their support team. Individual specific emergency specific plans will be honored, and decisions made by LOGAN will not infringe on individual rights and choices.
 - e. LOGAN will communicate early and often with case managers, individuals, and families when staffing and/or other typical support options are not available so that back up plans can be reasonably enacted.
 - f. Short-Term

In the event of a critical staff shortage as defined above, any of the following may be utilized to ensure the individual receives needed supports for a short period of time.

 - 1. Follow individual specific emergency backup plan developed by the Individual Support Team.
 - 2. Locate a family member to take the individual to their home and provide needed services for a specified length of time. Most likely this person has been identified in the individual's emergency backup plan or is already someone who takes the individual home frequently.
 - 3. For individuals with the Waiver, if the individual lives with a family member temporarily, Appendix K flexibilities may be considered by the Individual

Support Team allowing the family member to receive reimbursement for the time spent caring for the individual in their home.

4. Arrange for the individual to go to another supported living site for a specified length of time, which would not include an overnight.
5. Arrange for a staff member to live in residence with the individual(s). Approval from the individual(s) support team(s) will be acquired in such instances as staff will be permitted to sleep while in residence.

g. Long-Term

In the event of a critical staff shortage as defined above, any of the following may be utilized to ensure the individual receives needed supports for a longer period of time. The needs and preferences of the individual will be considered.

1. Follow individual specific emergency backup plan developed by the Individual Support Team.
2. Locate a family member to take the individual to their home and provide needed services for a specified length of time. Most likely this person has been identified in the individual's emergency backup plan or is already someone who takes the individual home frequently.
3. For individuals with the Waiver, if the individual lives with a family member, Appendix K flexibilities may be considered by the Team allowing the family member to receive reimbursement for the time spent caring for the individual in their home.
4. Arrange for a staff member to live in residence with the individual(s). Approval from the individual(s) support team(s) will be acquired in such instances as staff will be permitted to sleep while in residence.
5. Remote supports will be considered by individual support teams. An assessment will be done to evaluate the needs of the individual and how their needs can be met with remote supports. Remote supports will be used only when supported by the team and written in the individual Support Plan. See related policy.
6. As vacancies occur in waiver sites, effort to consolidate sites will be taken to reduce the number of overall staffing need. This will be considered as are other admissions. The likes and preferences of the individual are considered as are the needs of the potential new housemates.

G. Family Supports – Residential Habilitation Hourly and Participant Assistance and Care

1. Family Supports at LOGAN is provided to those individuals who live at home with family.
2. LOGAN assumes full responsibility to ensure that individuals receive continued supports even during instances of staff shortages. Whatever means necessary will be used to ensure necessary supports are provided to individuals.
3. Staff persons who normally work in specific family homes will be utilized to work in those homes whenever possible. When needed, people who are unable to work will be replaced with subs, part time staff, or any other staff who have been trained to work in that home.
4. A list of who is trained to work in which sites is maintained by the Director of Family Supports and the management staff on-call.
5. In adherence to the HCBS settings rule, individuals receiving family supports living services will have individual specific emergency plans developed by their support team. Individual specific emergency specific plans will be honored, and decisions made by LOGAN will not infringe on individual rights and choices.

6. For those receiving residential services at home with family, LOGAN will work with families to ensure that necessary services are provided either by LOGAN staff or family members. Appendix K flexibilities will be used as determined necessary by the team.
7. If the individual lives with a family member, and staff are not available to support the individual, Appendix K flexibilities may be considered by the Team allowing the family member to receive reimbursement for the time spent caring for the individual in their home.
8. In times of emergency, the individual's family may choose to go without service until the staffing has improved or the emergency is over.

H. Structured Family Caregiving

1. LOGAN provides Structured Family Caregiving to only two individuals. These individuals are considered members of the family as they have lived in their home for many, many years. LOGAN will ensure that necessary services are provided in their current home and will use Appendix K flexibilities as determined necessary by the team.

Date:
4/26/22

By:
VP/Chief Program Officer

Status:
Revised

POLICY # S-05-03

POLICY: PANDEMIC PROCEDURES -- Residential Services

RELATED POLICIES:

Policy S-05-01: Emergency Management Plan – Residential Services

Policy S-04-01: Infectious Disease

Policy S-04-05: COVID-19

Policy S-04-06: Mandatory COVID-19 Vaccination -- SGL

LOGAN SGL Emergency Preparedness Plans

POLICY STATEMENT:

LOGAN is prepared to support individuals receiving residential services in the event of a pandemic so that individuals receive needed supports and services. Residential services are defined as Supervised Group Living (SGL) and the following waiver services: Residential Habilitation Services – Hourly and Daily, Structured Family Caregiving, and Participant Assistance and Care.

A. Critical Services

1. The group home services LOGAN provides are essential services. In the event of an emergency, temporary housing can be obtained in hotels or persons can live with a family member for a short period of time. Should more long-term housing arrangements be needed LOGAN would be responsible to secure alternate housing. LOGAN employees assigned to the Group Living Department are required to be available for duty at all times.
2. For those individuals who received residential support through LOGAN's Supported Living Program., the residential support LOGAN provides is an essential service. In the event of an emergency, temporary housing can be obtained in hotels or persons can live with a family member for a short period of time. Should more long-term housing arrangements be needed LOGAN would assist the individual in securing alternate housing. LOGAN employees assigned to the Supported Living Department are required to be available for duty at all times.

B. Decision-Making Authority

1. In emergency situations impacting the whole agency, the seven LOGAN Officers (President and Chief Executive Officer, Vice President/Chief Program Officer for Adult Services, Vice President/Chief Financial Officer, Chief Human Resources Officer, Chief Program Officer for Child and Adolescent Services, Chief Marketing Officer, and Chief Philanthropy Officer) will serve as the decision-making authority.
2. In the event of emergency situations impacting residential services, the three residential directors (Director of Group Living, Director of Supported Living, and Director of Family Supports) the President and Chief Executive Officer, and the Vice President/Chief Program Officer for Adult Services will serve as the decision-making authority.
3. Each residential director will be the decision-making authority for site specific issues within their department.
4. Residential directors in collaboration with the President and Chief Executive Officer and the Vice President/Chief Program Officer for Adult Services will be responsible for coordination of residential services and related health services.

C. Policy Development

1. LOGAN will follow any mandates and guidelines that are communicated from governmental agencies, including but not limited to, the Center for Disease Control, the Indiana and County Departments of Health, Indiana's Governor's Office, Department of Homeland Security, and the Family and Social Services Administration, Division of Disability and Rehabilitative Services, Bureau of Developmental Disabilities, and the Bureau of Quality Improvement Services.
2. Based on the above referenced mandates and guidance, the Vice President/Chief Program Officer for Adult Services, in conjunction with LOGAN Officers and residential directors, will develop policies, procedures, and protocols related to each emergency, which will then be communicated to staff through an intentional and strategic approach to ensure each staff is aware of the role they play in the event of an emergency.
3. Located in the LOGAN Policy Manual are detailed procedures relative to Health and Safety including but not limited to Identification of Essential Services, Emergency Management, Evacuation, Severe Weather, Bomb Threat, Workplace Violence, Infectious Disease, and COVID-19. Also, in the health and safety section of the manual are policies related to the staff shortages.
4. At a minimum, LOGAN reviews its policies on an annual basis. As new guidance is issued or as LOGAN's needs change, the policies and procedures are reviewed and revised as necessary.
5. In the event of a pandemic, frequent revisions to policies, and procedures will occur based on direction from the local and state health authority as well as CDC guidance.
6. The group homes operated by LOGAN must follow all regulations for ICF/ID facilities.

D. Timelines

1. The timing of decisions in each of the aforementioned areas is dependent upon the emergency and its impact on the health and wellbeing of individuals served and staff. Time is of the essence in most emergencies, so decisions must be made thoughtfully but quickly.
2. Policies and procedures need to be updated and revised as immediately as possible after required protocols or guidance has changed.

E. Training

1. At a minimum of annually, each staff member will receive documented training specific to LOGAN policy S-05-01 Emergency Management Plan – Residential Services and related policies and procedures.
2. As policies, procedures, and protocols are revised, staff will receive documented training.
3. In the event of a prolonged emergency, such as what was experienced with COVID-19, each staff member will receive documented training on procedures and protocols specific to the emergency as they are developed and/or revised, which may be as often as weekly.

F. Communication

1. Residential Individuals, Families, Guardians, Advocates, Case Managers, and Teams Communication to individuals, families, guardians, advocates, Case Managers, and teams of those served residentially must outline specific information regarding any change in service delivery and implementation of Appendix K flexibilities. Such communication may include but is not limited to any of the following:
 - a. Day Programs
 - Suspension of day program
 - Day services being provided at the group home rather than day program facility
 - Day services being provided at the supported living residence rather than day program facility

- Change from face-to-face services to telemedicine
- Visitor guidelines
- Safety Protocols
- b. Residential Services
 - When consolidation of sites will or may occur
 - When relocation of sites will or may occur
 - When the individual can expect to return to their home
 - How rent and other expenses will be handled when the individual is not residing in their legal residence
 - Having sleep staff overnight
 - Visitor guidelines
 - Safety Protocols
 - Managing COVID positive cases
- c. Individuals living in supported living waiver sites will be given the support, information, and resources needed for them to be an active decision-maker in discussions about visitor guidelines and other safety protocols established for their home. If the individuals residing in the home do not agree on the guidelines or safety protocols, all individuals' support teams should convene as a group to discuss and make these determinations.
- d. This emergency management plan for residential services acknowledges that individuals served have individual-specific plans. At no time, will this plan infringe on the individual's rights or choice.
- e. The staff and residents of group homes must follow all regulations for ICF/ID facilities.

G. Screening Protocols

1. Protocols around temperature taking and other screening protocols will be based on the current guidance from the CDC and the local and state health authority.
2. General screening questions are required to enter a LOGAN supported living site or group home. Hourly employees will answer screening questions when clocking in.
3. The temperatures of employees and visitors are taken upon entering a group home. Entry will not be permitted for individuals with a temperature at or above 100.4.
4. Staff are expected to stay home when feeling unwell and/or displaying COVID-19 related symptoms and are expected to stay home.
5. Individuals served residentially are monitored for other COVID-19 symptoms.
6. The temperatures of individuals living in group homes are taken daily and more often if warranted. Temperatures at or above 100.4 will warrant staying home from day services and continued regular temperature monitoring. Individuals are similarly monitored for other COVID-19 symptoms.
7. The temperatures of individuals living in supported living sites are taken when experiencing COVID-19 symptoms. Temperatures at or above 100.4 will warrant staying home from day services and continued regular temperature monitoring.
8. Refer to the LOGAN Policy S-04-05: COVID-19 for more detail.

H. Cleaning and Sanitizing Protocols

1. Protocols around cleaning and sanitizing will be based on the current guidance from the CDC and the local and state health authority.

2. Employees are expected to practice safety protocols including frequent handwashing and social distancing, when possible, to prevent the spread of COVID-19.
3. Staff will be attentive to how infection spreads in the residential setting. They will minimize personal contact except what is required for personal care. When providing personal care, they will wear PPE such as gloves to prevent infection spread.
4. Each residential department will use established protocols for cleaning and sanitizing homes and vehicles.
5. LOGAN will supply residential sites with cleaning and sanitizing products including hand sanitizer. Residential directors will be responsible for procurement and distribution of cleaning and sanitizing supplies.

I. Personal Protective Equipment

1. Protocols around the use of personal protective equipment (PPE) will be based on the current guidance from the CDC and the local and state health authority.
2. At the height of the pandemic face masks were required. Face masks are optional at LOGAN facilities; however, each department director may set and enforce specific mask requirements as necessary to meet licensing requirements or to ensure the safety and wellbeing of all individuals.
3. Masks are required for periods of time (as defined below) in certain exposure/infection circumstances.
4. By regulation, masks are required for employees when in LOGAN group homes.
5. When in the community on behalf of LOGAN, employees must adhere to requirements of local businesses and federal mandates (e.g., public transportation).
6. LOGAN will supply residential sites with Personal Protective Equipment (PPE) including but not limited to face masks (cloth, surgical, KN95, and N95), gloves, face shields, and gowns. Residential directors will be responsible for procurement and distribution of PPE.
7. Typically, N95 face masks, face shields, and gowns are reserved for working with COVID-19 positive individuals. However, staff can wear as much PPE as desired when no COVID 19 positive exists.

J. Vaccinations

1. LOGAN group and supported living clients and those in Structured Family caregiving sites are prioritized for COVID-19 vaccination and boosters. On-site clinics will be set up to provide these vaccinations.
2. Residential clients living at home with family will be given information about the vaccine and ways to receive the vaccine.
3. Residential directors will maintain a system to track which clients have been vaccinated.
4. LOGAN residential staff will be provided information regarding the COVID-19 vaccination and booster and encourage vaccination. On-site clinics will be set up to provide these vaccinations.
5. Group living staff will be required to be fully vaccinated for COVID-19 or file a religious or medical exemption in accordance with the CMS Vaccination Mandate effective 1/14/22. The Director of Group Living, in conjunction with HR, will maintain a system to track vaccination and exemption status of staff.
6. The Director of Supported Living and the Director of Family Supports will maintain a system to track the vaccination status of staff.

K. Testing Protocols

1. Service recipients will get tested for COVID-19 when they are exhibiting COVID-19 symptoms.
2. When exhibiting COVID-19 symptoms, employees are urged to be tested.
3. Testing for COVID- 19 is required for employees and service recipients exposed to COVID-19.
4. Refer to LOGAN Policy S-04-05: COVID-19 for more detail.

L. COVID-19 Exposure

1. When staff or service recipients have been exposed or presumed to have been exposed to COVID-19, meaning they have been in physical contact less than 6 feet for more than 15 minutes with this individual, each staff or service recipient in the affected residential site will be informed so that appropriate measures can be taken. All efforts to protect the identity of the staff or service recipient who was confirmed or presumed positive will be taken as this is HIPAA protected information.
2. Exposure to COVID-19 is treated differently dependent upon vaccination status. See LOGAN Policy S-04-05: COVID-19 for how exposure incidents will be handled.
3. LOGAN will provide as much on-site testing to residential clients and staff as testing kits are available.

M. COVID-19 Positive

1. LOGAN will complete a BDDS reportable incident for each residential client who tests positive for COVID-19.
2. Staff who test positive for COVID-19 will be reported to HR. HR will report all COVID-19 positives for staff in congregate settings to BDDS using the on-line COVID-19 Employee Reporting Form as required in Appendix K.
3. If a LOGAN group or supported living service recipient tests positive for COVID-19, all service recipients of the same home will be treated as positive. They will shelter in place with assigned staff staying in the group or supported living residence with them for the required quarantine period. Quarantine period is 10 days from test date or onset of symptoms, whichever comes sooner. Only 5 days is required if service recipient is asymptomatic, regardless of vaccination status. A longer period of quarantine may be required based on displayed symptoms. As required, medical care will be secured.
4. Alternate housing options may be considered if remaining in the home seems contraindicated. In such instances, LOGAN will consider use of a hotel or the gym or day program space at the Hannah and Friends LOGAN location.
5. In most instances of client positive cases, staff member(s) will live in residence with the individual(s). Approval from the individual(s) support team(s) will be acquired in such instances as staff will be permitted to sleep while in residence.
6. See LOGAN Policy S-04-05: COVID-19 for more details as to how COVID-19 positive cases will be handled.

N. Visitors

1. The Directors of Group Living and Supported Living, in conjunction with the President and Chief Executive Officer and the Vice President/Chief Program Officer for Adult Services, will be involved in making decisions about visitors to the homes. If LOGAN determines that visitor restrictions must be imposed, individuals and their families will be notified of the restrictions and protocols imposed.

2. In supported living sites, allowing visitors to the home will be decided by the individuals and their support teams as they determine the level of risk which they are willing to take.
3. Individuals living in supported living waiver sites will be given the support, information, and resources needed for them to be an active decision-maker in discussions about visitor guidelines and other safety protocols established for their home. If the individuals residing in the home do not agree on the guidelines or safety protocols, all individuals' support teams should convene as a group to discuss and make these determinations.
4. Group living may have restrictions different than those in supported living as they are subject to ICF/ID requirements in addition to BDDS requirements.

O. Community Activities

1. Individuals living in supported living sites or group homes will be permitted to engage in activities in the community or at home with family. Based on the community spread, discernment is needed to decide if participating in the activity is advised. This will be decided on a case-by-case basis.
2. The Directors of Group Living and Supported Living, in conjunction with the President and Chief Executive Officer and the Vice President/Chief Program Officer for Adult Services, will be involved in making decisions about participating in community activities or visits at homes of family and friend. If LOGAN determines that restrictions of such activities must be imposed, individuals and their families will be notified of the restrictions and protocols imposed.
3. In supported living sites, participating in community activities and visiting in the homes of families and friends will be decided by the individuals and their support teams as they determine the level of risk which they are willing to take.
4. Group living may have restrictions different than those in supported living as they are subject to ICF/ID requirements in addition to BDDS requirements.
5. For those receiving Family Supports, the individual and their family will decide the level of the individual's community participation.

P. Meetings in LOGAN Offices

1. In a pandemic LOGAN Officers will serve as the primary team for making needed decisions about allowing visitors to LOGAN offices and holding client meetings or staff meetings. LOGAN Officers will take one of the following actions:
 - a. LOGAN offices will remain fully open with no restrictions.
 - b. LOGAN offices will remain open with restricted access.
 - c. LOGAN offices will remain open but closed to all visitors.
 - d. LOGAN offices will be closed with only essential personnel working in the office.
 Evaluation of the above will be based on the current guidance from the CDC and the local and state health authority.
2. During a pandemic, indoor gatherings of individuals in small spaces is discouraged.
3. During a pandemic most client meetings will be held virtually. Face to face meetings will be held only if desired by the individual, guardian, or family member. If held, proper social distancing will be maintained. Appendix K flexibilities will be considered for all client meetings.
4. During a pandemic, staff meetings will be held in settings that allow for social distancing.

Date:
4/26/22

By:
VP/Chief Program Officer

Status:
Revised

Procedure # SL-011

Procedure: Supported Living Emergency On-Call Procedure

Supported Living Emergency On-Call Phone: 574-340-8929

MEDICAL EMERGENCIES:

In the event of a medical emergency, staff are to contact 911 and ensure that the individual's medical issue is being addressed by professional medical staff. After medical personnel have arrived and are taking care of the individual, then the staff person should call the emergency on-call to tell them about the situation.

DANGEROUS SITUATIONS:

If staff feel they are in a dangerous or life-threatening situation, they are expected to call 911. Once the situation is resolved, help has arrived, or they are no longer in danger, staff are expected to call the emergency on-call.

WHEN to call:

1. Contact the Emergency On-Call only during non-business hours.
 - Between 5:00 pm and 8:00 am Monday through Friday.
 - All hours on weekends, holidays, and when the office is closed.
2. During business hours Monday through Friday call the designated Program Coordinator or Program Manager.

WHY to call:

1. Call only for emergencies as defined below. Issues that can wait for normal business hours must wait, and do not warrant a call to the Emergency On-Call.
2. If the phone is not answered, leave a voice message. The management staff will respond with a phone call or text if warranted.
3. Staff are not to call the LOGAN nurse on-call directly. If warranted, the manager on-call will contact the LOGAN nurse on-call.

Call or leave a voice mail in the following situations:

1. Medical emergencies that are life threatening and require more than first aid.
2. Falls
3. Staff calling off for a shift that will occur before the next business day.
4. Police activity in the neighborhood or similar threatening situation.

Leave voice mail or text in the following situations:

1. Medical issues that require first aid.
2. Incident reports.
3. Running emergency drills.
4. Relief staff has not arrived. Staff cannot leave a shift until their replacement staff have arrived.

Procedure # SL-011-02

Procedure: Management of the Emergency On-Call Phone

Purpose: LOGAN's Supported Living Department supports the needs of individuals served and staff after normal business hours by having management staff available by phone or text.

Procedure:

1. Program Managers will share the responsibility for carrying on the on-call phone on a weekly rotation beginning on Friday each week.
2. A schedule will be developed for the rotation and will equally and fairly distribute coverage for holidays.
3. The manager on-call will maintain a log of each call, recording who called, the nature of the call, and the resolution or direction given.
4. Phone calls, voice messages, and texts will be promptly responded to by the manager on-call in accordance with the urgency of the situation.
5. The manager on-call will attempt to resolve the issue without involving fellow program managers unless necessary to effectively resolve or address the issue.
6. The Supported Living Director will be notified of each medical emergency and incidents involving the police.
7. The manager on-call will complete the BDDS reportable incident if the 24-hour requirement falls within non-business hours. Otherwise, the designated Program Manager will complete the BDDS reportable.
8. The manager on-call will contact the LOGAN nurse on-call if warranted. The nurse-on-call will be shared by the two LOGAN nurses (one in Group Living and another in Supported Living).
9. Accompanying the emergency on-call phone will be the following:
 - a. A list of Supported Living sites and phone numbers.
 - b. Accurate schedules for each SL site.
 - c. Supported Living staff names with accurate and current contact information.
 - d. A list of each staff and which site in which they are approved and trained to work.
 - e. A list of staff and which sites they are prohibited from working.
 - f. Contact and other demographic information of clients and guardians needed for completing incident reports.
 - g. Williams Brothers information for pharmacy related issues.
 - h. Night Owl information
 - i. Concentra and Physician's Urgent Care information for worker's compensation related issues.
 - j. LOGAN maintenance staff contact information.
 - k. South Bend and Mishawaka Police Department non-emergency phone numbers.
 - l. House key box codes as applicable.
 - m. Koorsen security codes as applicable.
 - n. Nurse on-call rotation list.
 - o. Program Manager on-call rotation list.

Procedure # GL-005

Procedure: Group Living Emergency On-Call Procedure

Group Living Emergency On-Call Phone: 574-220-1461

MEDICAL EMERGENCIES:

In the event of a medical emergency, staff are to contact 911 before calling Emergency On Call and ensure that the individual's medical issue is being addressed by professional medical staff. After medical personnel have arrived and are taking care of the individual, then the staff person should call the emergency on-call to tell them about the situation.

DANGEROUS SITUATIONS:

If staff feel they are in a dangerous or life-threatening situation, they are expected to call 911 first. Once the situation is resolved, help has arrived, or they are no longer in danger, staff are expected to call the Emergency On-Call.

WHEN to call the Emergency On- Call:

1. Contact the Emergency On-Call only during non-business hours.
 - Between 5:00 pm and 8:00 am Monday through Friday.
 - All hours on weekends, holidays, and when the office is closed.
2. During business hours Monday through Friday call the designated Program Coordinator for the group home. If there isn't a Program Coordinator for the group home, then call the Program Manager for that home first. If that {Program Manager is not available, THEN call the Emergency On-Call.

WHY call the Emergency On-Call:

1. Call only for emergencies as defined below. Issues that can wait for normal business hours must wait, and do not warrant a call to the Emergency On-Call.
2. If the On Call phone is not answered, leave a voice message. The Emergency On-Call will respond.
3. Staff are not to call the LOGAN nurse on-call directly. If warranted, the Emergency On-Call will contact the LOGAN Nurse On-Call.

Call or leave a voice mail in the following situations:

1. Any incident where a client or staff is injured to the extent of requiring medical attention. Staff must complete an internal incident report.
2. Any incident of major property destruction, especially if it would require maintenance to repair the damage. Staff must complete an internal incident report.
3. Any time the van is damaged or involved in an accident. IF the van is involved in an accident staff must call the 911 to complete a police report. Staff must complete an internal incident report.
4. Any time a medication has not been administered within the one hour window. Staff should not administer the medication unless authorized by the Emergency On-Call. Staff must complete a medication incident report.

5. Any time a medication is not available to give during a medication pass. Staff must complete a medication incident report.
6. Any time a medication is given to a wrong person. Staff must complete a medication incident report.
7. Any time there is client to client aggression of any degree. Staff must complete an internal incident report.
8. Any time money is off by more than \$5.00. An internal incident report needs to be completed when there is any missing monies.
9. Any time staff witness someone getting neglected or abused or exploited. Staff must complete an internal incident report.
10. Any time a client elopes from the group home, and you do not know the whereabouts. Staff must complete an internal incident report.
11. Any time power goes out for more than 30 minutes, and or it is extremely hot or cold.
12. Any time the home becomes uninhabitable for any reason.
13. Any time a staff calls off for the shift that is outside of regular business hours.
14. Any time a staff is over 15 minutes late for their shift.

INVALID REASONS FOR CALL THE EMERGENCY ON-CALL:

1. The home is out of a certain grocery item.
2. The home is out of a cleaning supply.
3. Staff want to know who is going to relieve them.
4. If the staff has a missing punch.
5. If there is an Accel issue.

These are all issues that can wait and talk with your supervisor and not deemed an emergency.

IMPORTANT FACTS TO REMEMBER:

1. In the situation where relief staff does not show up and the Emergency On-Call cannot find someone to relieve staff from their shift, staff must stay on the home until the replacement arrives. Under no circumstance are staff permitted to leave clients by themselves.
2. Staff are employees of LOGAN. Even though staff are designated to one site they may be pulled by the Emergency On- Call to go to another home. Refusal to go to another site can result in disciplinary action, up to and including termination from employment.
3. All internal incident reports must be turned in to the Program Manager within 24 hours of the incident.

Written by: Cheryl Groves, Director of Group Living 4/1/22

Procedure # GL-005-02

Procedure: Management of the Group Living Emergency On-Call Phone

Purpose: LOGAN's Group Living Department supports the needs of individuals served and staff after normal business hours by having management staff available by phone or text.

Procedure:

1. Program Managers and the Case Coordinator will share the responsibility for carrying on the on-call phone on a weekly rotation beginning on Monday each week at 8:00am.
2. A schedule will be developed for the rotation and will equally and fairly distribute coverage for holidays.
3. The manager on-call will maintain a log of each call, recording who called, the nature of the call, and the resolution or direction given.
4. Phone calls, voice messages, and texts will be promptly responded to by the manager on-call in accordance with the urgency of the situation.
5. The manager on-call will attempt to resolve the issue without involving fellow program managers unless necessary to effectively resolve or address the issue.
6. The Group Living Director will be notified of each medical emergency and incidents involving the police.
7. The manager on-call will complete the BDDS reportable incident if the 24-hour requirement falls within non-business hours. Otherwise, the designated Program Manager will complete the BDDS reportable.
8. The manager on-call will contact the LOGAN nurse on-call if warranted. The nurse-on-call will be shared by the two LOGAN nurses (one in Group Living and another in Supported Living).
9. Accompanying the emergency on-call phone will be the following:
 - a. A list of group home and phone numbers.
 - b. Accurate schedules for each home.
 - c. Group Living staff names with accurate and current contact information.
 - d. A list of each staff and in which home they are approved and trained to work.
 - e. A list of staff and which homes they are prohibited from working.
 - f. Contact and other demographic information of clients and guardians needed for completing incident reports.
 - g. Williams Brothers information for pharmacy related issues.
 - h. Concentra and Physician's Urgent Care information for worker's compensation related issues.
 - i. List of after hour phone numbers for maintenance emergencies
 - j. South Bend and Mishawaka Police Department non-emergency phone numbers.
 - k. House key box codes as applicable.
 - l. Koorsen security codes as applicable.
 - m. Nurse on-call rotation list.
 - n. Program Manager and Case Coordinator on-call rotation list.

LOGAN COMMUNITY RESOURCES, INC.

POLICY MANUAL INDEX

SECTION 5: HEALTH AND SAFETY

S-01-01	Health and Safety
S-01-02	Total Evacuation Plan/Identification of Essential Services
S-01-03	LOGAN Center Evacuation Plan
S-01-04	LOGAN Center Severe Weather Procedure
S-01-05	LOGAN Power Failure Procedure
S-01-06	LOGAN Bomb Threat Procedure
S-01-07	LOGAN Workplace Violence Procedure
S-01-08	LOGAN Industries Evacuation Plan
S-01-09	LOGAN Industries Severe Weather Procedure
S-01-10	Hannah and Friends Evacuation Plan
S-01-11	Hannah and Friends Severe Weather Procedure
S-01-13	Day Services Emergency Response Procedures
S-01-14	Granger ALC Evacuation Plan
S-01-15	Granger ALC Severe Weather Procedures
S-01-20	St. Joseph, MI ALC Evacuation Plan
S-01-21	Weather Closing Procedure
S-01-22	Bed Bug Protocol
S-01-23	Head Lice Diagnosis and Treatment Protocol
S-01-23-01	Quick Guide for Managing Head Lice
S-01-23-02	Documentation of Treatment Form -- ALC
S-01-23-03	Documentation of Treatment Form -- Day Program
S-02-01	Nurse Coordination of Care
S-02-02	Nurse Notification
S-02-03	Client Risk Plans
S-03-01	Employee Safety and Workers' Compensation
S-04-01	Infectious Disease
S-04-02	Post-Exposure Follow-Up -- Employees
S-04-03	Employee Tuberculosis Screening Program
S-04-03	Employee Tuberculosis Screening Program for Service Recipients
S-04-05	COVID-19
S-04-06	Mandatory COVID-19 Vaccination Policy -- SGL
S-04-06-01	Medical Exemption Request Form
S-04-06-02	Religious Exemption Request Form
S-05-01	Emergency Management Plan -- Residential Services
S-05-02	Staff Shortage Procedures -- Residential Services
S-05-03	Pandemic Procedures -- Residential Services
S-35-01	Medication Administration and Monitoring
S-35-02	Organized System of Medication Administration (Supported Living)
S-35-03	Medication Incident (Errors/Refusals) Report
S-35-03	Medication Incident Form (Day Program)
S-35-03	Medication Incident Form (Residential)
S-50-01	Smoke Free Environment
S-61-02	Building Access and Security
S-70-01	Equipment Use and Control
S-80-01	Transportation
S-80-02	Insurability Matrix -- Cincinnati

EMERGENCY PREPAREDNESS
LOGAN COMMUNITY RESOURCES
GROUP HOMES
TABLE OF CONTENTS

- 1. POLICY**
- 2. OBJECTIVES**
- 3. POPULATION SERVED**
- 4. COMMUNICATIONS**
- 5. MEDICAL RECORDS/MEDICATIONS**
- 6. RISK ASSESSMENT**
- 7. TYPES OF EMERGENCIES**
 - a. Active Shooter**
 - b. Flood**
 - c. Bomb Threat**
 - d. Missing Persons**
 - e. Fire**
 - f. Tornado**
 - g. Power Outage**
 - h. Severe Temperature**
- 8. DISASTER FOOD**
- 9. FIRST AID**
- 10. CLIENT/STAFF TRACKING**
- 11. FAMILY/GUARDIAN NOTIFICATION**
- 12. EMERGENCY LIGHTING**
- 13. TRANSPORTATION**

**GROUP LIVING
EMERGENCY PREPAREDNESS PLAN
COVID-19
List of Appendices**

Appendix A- Group Home Guardian List
Appendix B- Logan Initial Emergency Preparedness Plan
Appendix C- ISDH Covid-19 Home Cleaning Guidance
Appendix D- Covid-19 Sanitation Cleaning Checklist
Appendix E- Infectious Disease Policy
Appendix F- Client Temperature Checklist
Appendix G- Covid-19 Response for positive Covid- 19 in Congregate Residential Settings
Appendix H- No Visitor Sign
Appendix I- Limited Visitor Sign
Appendix J- Logan PTO Policy
Appendix K- Logan Unpaid Leave Policy
Appendix L- Covid-19 Screening for Staff
Appendix M- BDDS/DDRS Reporting Requirements for Covid-19
Appendix N- Staff Development Records for Training
Appendix O- DDRS Temporary Covid-19 DSP Training Requirements on Covid-19
Appendix P- DDRS Staff Development Record for DSP Training Covid-19
Appendix Q- Personal Protective Equipment Toolbox
Appendix R- Pharmacy Delivery Protocol
Appendix S- Guidelines for Clients Wearing Masks
Appendix T- Preparing Nursing Homes/Assisted Living Facilities for Covid-19
Appendix U- Covid-19 Emergency Declaration Blanket Waivers for Healthcare Providers- pages 27-28
Appendix V- Sanitation Guidelines for Cleaning Room of Sick Client
Appendix W- Covid19 Registered Cleaning and Sanitation Agents
Appendix X- Guidelines for Return to Day Program
Appendix Y-Group Home Visits and Admissions
Appendix Z- Miscellaneous Documents
 a. Procedure for communicating a positive Covid-19 case

PATHFINDER SERVICES, INC.

POLICY/PROCEDURE



Number: 503

Sponsor: Safety Committee

Subject: **Disaster and Fire Evacuation Procedures**

Original Date: January 21, 1987

Revised/Reviewed Date: January 14, 2020

PROCEDURE - DISASTERS:

If the National Weather Service issues a tornado warning for the immediate area (County), a member of the staff will immediately notify the Person in Charge (PIC). The PIC will determine whether or not to issue an announcement of a tornado drill. In the absence of the PIC, staff on duty will assume those duties. The PIC is to monitor the weather information. Upon notification from the Weather Information Service that the tornado has left the area and does not pose a continuing threat, the PIC will notify all personnel and operations will return to normal.

All Pathfinder Services, Inc. locations will utilize the internet for weather updates.

For Office Locations: In the event the PIC determines it prudent to instruct the Receptionist to make an announcement of a tornado warning, an announcement should be made over the intercom system.

Following the announcement of the above information by a member of the Office staff, he/she will remove the visitor and employee sign in/out sheet and the staff and client emergency information book to the severe weather shelter area.

Safety committee members shall insure that a portable first aid kit is available.

All Pathfinder Services, Inc. staff are to assist in the movement of all persons to their severe weather shelter area. Staff should assure that flashlights are in working order.

If and when a tornado has a noticeable effect upon the building, the PIC will notify all persons to place head on knees, and cover head with hands. No one is to move from this position until the tornado has passed.

Roll call will be taken by an assigned staff and this person will report all accounted for or anyone unaccounted for to the PIC. In the event of injury to any individual, first aid trained staff are requested to administer first aid as necessary. Emergency personnel will be notified if necessary.

PROCEDURE - FIRE EVACUATION AND DRILLS:

In the event a fire is discovered by anyone, the following are required procedures:

- Remove anyone in immediate danger.
- Close the door to the room or area in which fire is located.
- Turn on the alarm: Pull wall alarm closest to you; if time, call 911 number and report location of fire in building and best door for fire fighters to enter the building.
- Assist in the evacuation of building per "Pathfinder Services, Inc. Evacuation Checklist" assignments, which are given to each staff.

- All individuals are to report to the parking lot of Pathfinder Services, Inc. locations and stay clear for fire equipment to arrive.

Pathfinder Services, Inc. staff is responsible for the removal of the visitor and agency sign/out logs and emergency information books. Upon arrival at parking lot, roll call will be taken by assigned staff as per "Evacuation Checklist". Assigned staff report all accounted for or anyone unaccounted for to the PIC. The names of persons found to be unaccounted for will be brought to the attention of the first arriving fire fighters.

All individuals are to remain clear of the building until fire department representatives give authorization to enter. Or in a drill, until PIC gives signal to re-enter.

In the event a quick return into the building is not possible, all individuals will evacuate to assigned locations. Safety drills are done monthly as weather permits.

PROCEDURE - BOMB THREAT:

In the event of a bomb threat, a designated person will order the building to be evacuated using same procedure as for fire, with the following exceptions:

- The police and fire departments will be contacted by phone as soon as possible.
- Evacuated persons shall be removed to a distance of no less than 75 feet from the building pending the arrival of safety personnel.

In the event of receiving a bomb threat telephone call, the staff receiving the phone call will write down the following information:

- Is the caller male or female?
- Does the voice sound young or old?
- Is there any recognizable background noise?
- Ask the caller where the bomb is located.
- Ask the caller what time the bomb will go off.
- The staff person receiving the telephone call will immediately notify the PIC and call 911.

Re-entry into the building will come only after the all clear is given by the appropriate authorities. Do not activate the Fire Alarm System as a bomb may be connected to the system.

PROCEDURE – OUT OF CONTROL SITUATION:

- Remove anyone in immediate danger.
- The Receptionist will immediately notify the PIC and call 911 if necessary.

For Office Locations: In the event of an out of control situation the Receptionist will page "Sam Beeks" to the operator or the location of the out of control situation. This is the code name letting staff know there is an out of control situation. The PIC will respond to the page and determine who needs to be involved in controlling the situation.

MISSING PERSONS – CODE ONE

If a person served is missing from a Pathfinder location, immediately call CODE ONE to the assigned location. The Code One team members will respond and take charge of the situation. The team leader

will hand out search assignments, assure all areas are promptly searched, communicate with other team members and determine when outside help will be requested. (Also refer to the policy on Reporting and Locating Missing Persons in the Customer Related section of this manual.)

PROCEDURE-POWER OUTAGE

- All customers are to report to the assigned location.
- Manufacturing employees need to report to their supervisor.
- Use your evacuation list to make sure everyone is accounted for.
- Take your flashlights and cell phones with you. There may be no phone service if you need to make calls, so you will need the cell phone.
- There is emergency water stored in the apartment in the closet at State Street.
- Use hand sanitizer as needed.
- Staff need to make sure that visitors report to the lobby.
- Staff without client responsibilities are to go to where clients are located.
- Time of day will help to determine if clients should be served offsite.

PROCEDURE - COMMUNITY OR NATURAL DISASTER:

Proceed according to the Civil Defense Emergency Operations Plan for each county.

EMERGENCY CONTACT NUMBERS:

	Home	Cell
John Niederman – CEO/President	260-356-4666	260-359-3720
Staci Wilkinson – Human Resource Manager	n/a	260-519-0861
Diana Laux – Chief Financial Officer	n/a	260-224-9880
Sandy Wing – Community Supports Director	260-356-1459	260-359-3721
Tim Federspiel- Real Estate Manager	n/a	260-359-3732

PATHFINDER POLICY

Owner: IT Services
Subject: Acceptable Use
Revision Date: April 20, 2023



1. Purpose

A strong Acceptable Use Policy serves as a basis of trust between Pathfinder and its stakeholders, enables Pathfinder to comply with applicable laws and regulations, and helps protect its earnings and capital by mitigating operational, compliance, and reputational risks associated with its critical information assets.

2. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Pathfinder business or interact with internal networks and business. It always applies to all Pathfinder locations. Compliance with this Acceptable Use Policy is mandatory for all Pathfinder employees, consultants, vendors, contractors, and temporary staff.

3. Acceptable Use

Pathfinder facilities and technology resources are intended to support the business objectives of Pathfinder. Given that these resources provide access to sensitive data, corporate infrastructure, and partner networks, it is essential that all employees conduct themselves in an ethical and legal manner. Acceptable use means respecting the rights of fellow employees; safeguarding corporate property and assets; protecting relationships and agreements with corporate partners; abiding by all federal, state, and local laws governing the use of technology resources. If an employee violates this Acceptable Use Policy, disciplinary action may be initiated that includes the possible loss of access to technology resources. Serious infractions can lead to termination.

- All internet/intranet/extranet-related systems constructed by or provided to Pathfinder's workforce, including but not limited to cloud infrastructure provider resources, production and/or development computer equipment, software, operating systems, files, storage media, databases, spreadsheets, graphics, information systems, network accounts providing email, internet browsing, SFTP, etc. are the property of Pathfinder
- Pathfinder's computing resources are intended for business purposes in serving the interests of Pathfinder, and of our clients during normal operations.

PATHFINDER POLICY

Owner: IT Services
Subject: Acceptable Use
Revision Date: April 20, 2023



- All technology related installations, upgrades, and removals, including hardware, software, and cloud services must be coordinated with and approved by IT Services. This includes all computing devices managed and administered by Pathfinder such as desktops, laptops, thin clients, and mobile devices.

Effective security and use of Pathfinder's resources require the participation and support of every member of Pathfinder's workforce. It is the responsibility of every individual to know these requirements, and to conduct their activities accordingly.

4. General Use and Ownership

- All data, technology resources, and information assets, including but not limited to, client-lists or client-information, stored, transmitted, or accessed with Pathfinder's resources are owned by Pathfinder or under the operational control and guardianship of Pathfinder and subject to examination by Pathfinder at any time.
- All data, technology resources, and information assets are required to be accessed for only intended business purposes in serving the interests of Pathfinder, and of our clients during normal operations.
- Computer resources and information assets should be afforded the same level of protection as any other important corporate asset.
- Pathfinder's computing resources are for business use with reasonable accommodation for personal use that does not violate this policy.
- All Pathfinder data elements remain the property of Pathfinder, including following an individual's departure from the corporation. Upon resignation or termination of employment, all technology resources, data, and information assets, including those which were developed by the departing employee, shall be turned over to the responsible manager and shall remain the property of Pathfinder. This includes storage of data on portable devices; regardless of who owns the device.
- The organization's computer systems and information assets are routinely audited and monitored for unauthorized activity and use. An expectation of privacy does not exist for employees, contractors and vendors when using Pathfinder's computer systems or information assets. Use of any Pathfinder computer or system to access the Internet, send or receive electronic mail, process information, or store information and files is subject to review, monitoring, and recording.
- For security and network maintenance purposes, authorized individuals within Pathfinder may monitor equipment, systems, and network traffic at any time.

PATHFINDER POLICY

Owner: IT Services
Subject: Acceptable Use
Revision Date: April 20, 2023



5. Unacceptable Use

The following activities are, in general, prohibited. Individuals may be exempted from these restrictions while performing their legitimate job responsibilities (e.g., IT Services staff may have a need to disable network access of a host if that host is disrupting production services). Under no circumstances is a member of Pathfinder workforce authorized to engage in any activity that is illegal under local, state, federal, or international law while using Pathfinder's computing resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are prohibited:

- The storage of confidential, private, or internal Pathfinder data, including but not limited to client-lists, client-information, or prospects on computing devices or cloud services that are not managed and administered by Pathfinder or a business partner with a signed and executed contract or agreement incorporating standard security provisions. This includes third-party Artificial Intelligence applications like ChatGPT, Bing Chat, Google Bard, etc.
- Unauthorized access, alteration, modification, falsification, or destruction of a technology resource or information asset. In appropriate circumstances, or when required by law or regulation, Pathfinder may refer matters to law enforcement authorities.
- Attempting to circumvent or subvert any security measure.
- Loading, adding, or removing any software/hardware on a computer, which includes cloud services, without prior authorization from the IT Director.
- Installing Pathfinder licensed software on a personal home computer.
- Introduction of malicious programs into the Pathfinder computing environment (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- The creation or transmission of any offensive, obscene, or indecent images, data, or other material or any links (any defamatory information regarding race, color, religion, sex, sexual orientation, nation origin, disability, or age).

PATHFINDER POLICY

Owner: IT Services
Subject: Acceptable Use
Revision Date: April 20, 2023



- Using a Pathfinder technology resource to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Port scanning or security scanning unless this activity is a part of the individual's normal job duties.
- Executing any form of network monitoring which will intercept data not intended for the individual unless prior approval is received from the IT Director.
- Establishing remote or external connectivity between a third-party and Pathfinder technology without prior authorization from the IT Director.
- Corrupting or destroying other users' data. Violating the privacy of other users by attempting to gain unauthorized access to Pathfinder data.
- Connecting non-Pathfinder computers, devices, or other computer software to a Pathfinder technology resource without prior authorization from the CSO and following the Pathfinder Bring Your Own Device (BYOD) Policy (section 9 of this policy).

Email Usage

All computer users can send and receive both internal and external electronic mail. The function of internal email is to facilitate the conduct of business within the company. The function of external email is to facilitate the conduct of Pathfinder related business with other organizations and individuals.

Prohibited activities include, but are not limited to, the following:

- Pathfinder email system may not be used for illegal activity of any kind.
- Pathfinder email system may not be used for personal business of any kind.
- Sending large amounts of unsolicited email messages, including the sending of "junk mail" or other advertising material directly to individuals who did not specifically request such material (email spam). Marketing shall coordinate all email advertising campaigns.
- Conducting or soliciting for political, religious, or charitable causes or for other commercial ventures outside the scope of their employment and responsibility to Pathfinder.
- Sharing chain letters and emails that contain threatening, obscene, defamatory, or abusive language and content.

PATHFINDER POLICY

Owner: IT Services
Subject: Acceptable Use
Revision Date: April 20, 2023



- Sending nonpublic (NP), personally identifiable information (PII), or protected health information (PHI) over the public Internet without the use of encryption.
- Requesting that a client or affiliate send an email containing NPI, PII, PHI over the public Internet without the use of encryption.
- Automatic forwarding of an individual's Pathfinder email to a non-Pathfinder email address (e.g., personal email).

Email may be monitored to ensure the system is being used in compliance with Pathfinder policy and for purposes of maintaining the integrity and effective operation of Pathfinder's email systems. All users should understand that no expectation of privacy exists regarding the use of Pathfinder email.

Pathfinder reserves the right to inspect and disclose the contents of email at any time.

Internet Usage

Pathfinder provides access to the Internet to help employees do their jobs and be well informed. Access between Pathfinder processing environments and the Internet, as well as other networks that connect to the Internet, is permitted only through Pathfinder approved and administered communication paths.

Only the Pathfinder provided browser may be used to access the Internet. The use of, or downloading of, other browsers is prohibited unless approved by the IT Director. Additionally, altering security and configuration settings on software provided to access the Internet is prohibited unless approved by the IT Director.

6. Individual Responsibility

Everyone is responsible for all activity associated with their User ID and password. Everyone should be familiar with Pathfinder policies on information security, email, and private information.

7. Clean Desk Policy

The following steps must be taken at all Pathfinder locations to properly secure private information when it is in a hard copy format, such as a document, computer printouts, or other print media:

PATHFINDER POLICY

Owner: IT Services
Subject: Acceptable Use
Revision Date: April 20, 2023



- Private information is not left on employees' desks or where they can be seen for extended periods when employees are not present, such as during breaks, at lunch, or after hours.
- Printed private information is not left out in open areas, such as around copiers, printers, or fax machines.
- Portable devices that access private information must never be left with the screen unlocked and unattended.
- Printed material containing private information and portable devices not taken home at the end of the day should be stored in lockable file cabinets, desk drawers, or behind a locked office door with limited key distribution. Such locations must be locked when not in use and checked prior to leaving work at the end of the day.
- Computer workstations must be locked when leaving workstations unattended.
- Computer screens should be angled away from the view of unauthorized persons. If not possible, reasonable measures must be taken to protect private information from visitors in the area.

8. Bring Your Own Device (BYOD) Policy

All employees have the option to use personally owned devices for work-related purposes. To protect both the employee's personal data and Pathfinder data, employees installing and using Pathfinder licensed mobile applications on their mobile device must install Pathfinder's Mobile Device Management (MDM) software on the device. This software will protect the employee's personal information and ensure it remains separated from company data. At no time will Pathfinder be able to access the employee's personal data. Alternatively, employees may safely use their browser to access website applications published through Pathfinder's secure web portal without need to enroll in the MDM.

Employees wishing to use a personal computer or laptop to access Pathfinder network or data systems must do so through Pathfinder provided web portals or VPNs, have a current operating system (within two most recent revisions), and active, current antivirus software installed on the PC or laptop.

If a personal device that was used to access any Pathfinder data, including web applications, is lost, or stolen, the employee must notify management immediately. The MDM will allow for company-related data to be wiped from a mobile device; any web applications will require a password change. Upon resignation or termination of employment, all company data on personal devices will be removed by IT Services.

PATHFINDER POLICY

Owner: IT Services
Subject: Acceptable Use
Revision Date: April 20, 2023



9. Referenced Standards

PCI DSS: 12.3

GLBA: Safeguards Rule

HIPAA: A-§164.310(d)(2)(iii)

PATHFINDER POLICY

Owner: IT Services
Subject: Access Control
Revision Date: April 4, 2023



1. Overview

All workforce members have appropriate access to private information and unauthorized individuals are prevented from improperly gaining access. Control over who has access to information as well as the procedure for accessing that information is vital to the protection of Pathfinder and is regulated strictly and consistently to ensure information is secure.

2. Provisioning

Workforce members are given access to private information as required for the performance of their assigned job responsibilities. The access is provided on a "need to know" basis, which means that access is granted with the least privileges required to fulfill job responsibilities. All Pathfinder access must be provisioned through IT services, or a designated department level administrator approved by the IT Director. Users must never subscribe to or obtain their own third-party software. User accounts must be integrated with Pathfinder's identity management solution with Single Sign-On (SSO) enforced whenever possible.

Background checks on new employees must be complete prior to hire. Within two weeks of being provided access, new employees must have read and acknowledged Pathfinder's Acceptable Use Policy.

When a new employee is hired, the Human Resources department must submit a ticket to the help desk with the appropriate details. The help desk will create the user account verifying all permissions with the hiring manager within 48 hours.

Third-party consultants must have a valid contract in place that meets the requirements of Pathfinder's Contract Management Policy before accounts can be provisioned. The IT Director must submit or approve help desk tickets for all third-party account provisioning. Third-party accounts must be set to automatically expire upon the planned duration of services in any systems that support such controls. If a system does not support such controls, an alternative tracking and monitoring system must be established to assure third-party access does not exceed the duration of contracted services.

3. Deprovisioning/Job Changes

Access is terminated within 48 hours (or immediately for urgent terminations) when the individual's job responsibilities for Pathfinder are concluded, or appropriately modified when the workforce member changes jobs within the organization. All user IDs assigned to a person who has left the organization will be immediately disabled and staged for deletion from all computer systems unless the deletion causes loss of required data. The Human Resources department must call or submit a ticket to the help desk officially requesting the changes to the user account. In the event of job change, the help desk will verify all necessary permissions and access with the employee's new manager prior to making the changes.

4. Privileged Access

ACCESS CONTROL POLICY/PROCEDURE

Any exceptions to this policy must be authorized and conform to the Security Exceptions Policy.

PATHFINDER POLICY

Owner: IT Services
Subject: Access Control
Revision Date: April 4, 2023



The following additional requirements exist for all user IDs granted privileged access. Privileged access includes platform-, system-, or administrative-level access that allows the use of system control programs or features, ability to configure functional parameters for a system or application, or other special purpose functionality beyond that of a standard user¹.

Privileged access is typically granted to system or database administrators (including third party and department level administrators), technical or computer support personnel, and security staff.

- Access to privileged functions is based upon the user's job function and responsibilities.
- All users requiring privileged access must be approved by the user's management and authorized by the CSO. Approvals are documented in the ticketing system.
- Users who are granted privileged access are assigned an additional user ID to be used for the elevated duties, which is different from the user ID used for normal business purposes.
- Users who have been granted privileged access must be revalidated at least annually by their management to ensure the privileged access is still required.
- Users designated as a department level administrator must be listed as application champions on application inventory documentation.
- Department level administrator accounts must be provisioned by IT Services only.
- Department level administrator passwords must be made available to them in a shared password vault that IT Services controls.

5. Leave of Absence or Suspension

Employees who are suspended or on a leave of absence are required to have their User IDs disabled until they return to work. The Human Resources department must notify the help desk of the need to for account suspension, and all must be documented in the ticketing system. The HR department must also notify the help desk when the suspended accounts should be reinstated.

6. User Access Reviews

User access reviews are performed at least annually for systems or applications that store or access private information or are deemed critical to the continuance of business. User access reviews for all other systems or applications are performed at least every three years. Access reviews will be conducted by the IT Services department collaboratively with any department level administrators who are involved with assigning user accounts within their departments.

7. Remote Access

It is the manager's responsibility to ensure that a valid business need exists for their direct reports' remote access to the Pathfinder managed network. All remote access to Pathfinder's managed

¹ Privileged access does not include group and team ownership in Microsoft 365 as it is a common feature available to standard users.

PATHFINDER POLICY

Owner: IT Services
Subject: Access Control
Revision Date: April 4, 2023



environment requires multi-factor authentication methods and the use of Pathfinder provided VPN or secure portal. Remote access technologies must automatically disconnect sessions managed by Pathfinder after 30 minutes of inactivity.

8. Inactive Accounts

IT services monitors user IDs for inactivity. Any user ID that has not been used for 90 days or longer will be disabled and/or removed.

9. Separation of Duties

To ensure risk of fraud is kept to an acceptable level, Pathfinder maintains a sound separation of duties around access and use of information. A matrix of roles defining separation of duties must be maintained by IT Services.

At the highest level and to the degree possible business functions are separated from IT functions and duties are segregated according to Authorization, Custody & Control, Recording, and Verification. Functions such as system design and configuration, applications development and programming, quality assurance/testing, change management, configuration management, network administration and security, data administration and internal audit are separated within Pathfinder as well as within third-party service providers by job description and line management.

Instances where separation of duties is not possible will be tracked via the Security Exceptions Policy and additional controls or oversight are implemented.

10. Referenced Standards

PCI DSS: 7.1, 7.2, 7.3, 8.1, 8.3, 8.7, 12.3, 12.7

HIPAA: R-§164.308(a)(3)(i), A-§164.308(a)(3)(ii)(A), A-§164.308(a)(3)(ii)(B), A-§164.308(a)(3)(ii)(C), R-§164.308(a)(4)(i), A-§164.308(a)(4)(ii)(B), A-§164.308(a)(4)(ii)(C), R-§164.312(a)(1)

GLBA: Safeguards Rule

POLICY

Owner: IT Services
Subject: Change Management
Revision Date: April 14, 2023



1. Purpose

All changes affecting the operational environment and infrastructure owned by Pathfinder are managed in a rational and predictable manner.

2. General Change Information

A change, as it applies to this policy and when within the means of Pathfinder's control, whether owned and hosted or not, is defined as any implementation of new functionality, enhancements, new technology products, scheduled upgrades, adjustments, corrections, or routine system maintenance to any production component or application of Pathfinder-owned operational information systems. Routine and scheduled patches are excluded from this policy, these are covered within the Network Security Policy.

All change requests are logged within the Pathfinder approved change management system. A documented audit trail must always be maintained and include change request documentation, approvals, testing, and outcome of the change. No single person can effect changes to production information systems without the approval of other authorized personnel.

3. Assess and Prioritize

Upon receipt of the change request, IT services performs a risk and impact assessment to identify the people and other systems potentially affected, estimate the cost and risk of implementation, and consider compliance with legislative requirements and standards. Using the results of the assessment, IT services confirms or denies the change and assigns a priority level and time frame to the change. If the change request was rejected, IT services will close the change request and notify the requestor, documenting the reason the change was not approved.

Changes deemed as large-scale change (deployment of a new software system for example) require a properly scoped out proposal on the approved Change Proposal form. These will then be documented in the change management system and treated as a project with a detailed plan.

4. Testing

All testing is performed in an isolated, controlled, and representative environment (where such an environment is feasible) before a change is promoted to production. The team making the changes performs tests to minimize the effect on the relevant business process, assess its impact on operations and security, and verify that only intended and approved changes were made.

As needed, user acceptance testing is performed by end users of the revised system to confirm that the change has been made properly and the system has not been changed in any other way. The performance of testing is documented in the change management system.

CHANGE MANAGEMENT POLICY

Any exceptions to this policy must be authorized and conform to the Security Exceptions Policy.

POLICY

Owner: IT Services
Subject: Change Management
Revision Date: April 14, 2023



5. Approval Requirements

All changes require IT Director approval before they are promoted to production. Approval of changes is based on formal acceptance criteria, such as confirming that the change request was made by an authorized user, an impact assessment was performed, the proposed changes were tested, and proper separation of duties was followed (or additional oversight where separation of duties is not possible). Large scale changes that impact or replace an entire IT system must be approved by the CSO and Executive over the department requesting the change on the approved Change Proposal form.

6. Fall back

Procedures for aborting and recovering from unsuccessful changes are documented for each change. Should the outcome of a change be different from the expected result, procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert to what they were prior to implementation of changes.

7. Types of Changes

a. Emergency Changes

An Emergency Change is a change that requires a fix in response to a critical situation that necessitates an immediate resolution. The following rules apply to Emergency Changes:

- Because of the nature of an Emergency Change situation, the fix may be installed before the approvals are acquired.
- The implementor of the change must ensure that a ticket/task card is created on the change board prior to implementation to ensure a record is initiated to support the change being made.
- Following implementation of an Emergency Change, the change will follow the normal approval execution path and must begin no later than the next business day.
- Approvals and other workflow tasks should be completed within three business days of implementation.

b. Standard Changes

A Standard Change is a change that follows an established path and is the accepted solution to a specific requirement or set of requirements. This standard applies to changes that have been pre-authorized to be processed as a Standard Change. The following rules apply to Standard Changes:

- Tasks are well known, repeatable, and proven.
- The change has no impact to users.
- Authority is effectively given in advance and the change is considered pre-authorized.
- Standard Changes do not require the rigors of the change management cycle.

POLICY

Owner: IT Services
Subject: Change Management
Revision Date: April 14, 2023



c. Normal Changes

A Normal Change is a change that is scheduled or planned and must follow the appropriate scoping, review, and approval process. It requires no special handling. Normal Changes must be reviewed and approved prior to the implementation start time.

8. Referenced Standards

PCI DSS: 1.1, 6.3, 6.4, 6.7

HIPAA: R- §164.308(a) (8)

GLBA: Safeguards Rule

PATHFINDER POLICY

Owner: IT Services
Subject: Contingency Planning
Revision Date: April 20, 2023



1. Policy Overview

Pathfinder has established a contingency plan to respond to emergencies or other occurrences that might damage information systems containing private information, recover those systems, and mitigate the effects to operations following a disruption in the event of an emergency or other occurrence, such as fire, vandalism, system failure, or natural disaster.

2. Data Backup

Pathfinder IT Services staff routinely backup the systems which store, process, transmit, or receive private or critical information. Nightly replications are performed and retained at a secure offsite datacenter where they are kept in ready operational state in case of disaster situation.

The IT Director will test and evaluate the backup procedures at least annually and document the results of the testing to determine the overall effectiveness. Data backup procedures will be revised as appropriate based on the results of testing and as needed in response to environmental or operational changes.

3. Disaster Recovery

Disaster recovery procedures are in place for restoring lost data and resuming performance of services following a disaster. The plan identifies the functions, operations, and resources necessary to restore and resume operations and assign responsibilities to designated personnel during periods of interruption. IT Services is responsible for implementing annual testing and evaluation of the plan and documenting the results to determine its overall effectiveness. Testing must include IT Services staff and key users with knowledge to evaluate the validity of recovered systems. The IT Director will revise the plan as appropriate based on the testing and evaluation and as needed in response to environmental or operational changes.

4. Business Continuity Planning

Through the efforts of the CSO, IT services, management, and third-party service providers, a Business Continuity Planning process for information systems and data is maintained. The process includes, but is not limited to, Board and senior management oversight, process, business impact analysis (BIA), risk management, Disaster Recovery, pandemic planning, training, continuous monitoring, and annual testing.

Pathfinder will identify reasonably foreseeable emergencies that could impact the information systems and the procedure to follow during and immediately following an emergency to maintain security processes and controls of private information while ensuring access to the data.

5. Critical Application and Data Analysis

CONTINGENCY PLANNING POLICY

Any exceptions to this policy must be authorized and conform to the Security Exceptions Policy.

PATHFINDER POLICY

Owner: IT Services
Subject: Contingency Planning
Revision Date: April 20, 2023



Through the BIA process, Pathfinder analyzes and documents the criticality of its private data and information systems. The criticality analysis serves as the basis for prioritization of data and information systems in the event of a disaster or other emergency which causes the information systems to become unavailable.

6. Referenced Standards

PCI DSS: 9.5

HIPAA: R-§164.308(a)(7)(i), R-§164.308(a)(7)(ii)(A), R-§164.308(a)(7)(ii)(B), R-§164.308(a)(7)(ii)(C), A-§164.308(a)(7)(ii)(D), A-§164.308(a)(7)(ii)(A), A-§164.310(a)(2)(i), A-§164.310(d)(2)(iv), R-§164.312(a)(2)(ii)

GLBA: Safeguards Rule

PATHFINDER POLICY

Owner: IT Services
Subject: Data Classification
Revision Date: April 18, 2023



1. Policy Overview

All Pathfinder information assets are classified according to their level of confidentiality. The specific classification level that is assigned to an information asset is based on the potential impact to the organization in terms of exposure, unwanted publicity, or loss in the event the information is lost, stolen, released without authorization, or disclosed without permission.

2. Default Classification

Information assets that do not possess a classification marking or identifier are classified as “private” by default and should be treated as such. A collection of information (e.g., data warehouse, repository, table, file, etc.) will carry the highest classification of any of its data.

3. Information Classification Matrix

The following table provides definitions and classification levels for various types of information assets.

Classification Label	Definition	Examples	Security Requirements
Public	Information or data of a public nature that is considered non-sensitive. If released or disclosed would have no negative impact.	Advertisements Marketing Material Public Web Pages	No restrictions. No specific security protection measures are necessary. No secure storage methods required.
Private	All non-public information or data that is considered sensitive. If released or disclosed would impact the organization, customers, and/or business operations.	Customer and Client Data NPI/PII/PHI ⁱ Internal Communications Employee Information	Access is restricted to those who require the access to perform their individual job responsibilities. Information should be protected from accidental disclosure and requires secure disposal. Electronic transmissions of the data outside of the Pathfinder network must be encrypted.

ⁱ Non-Public Information (NPI)

Nonpublic personal information: “Nonpublic personal information” generally is any information that is not publicly available and that:

PATHFINDER POLICY

Owner: IT Services
Subject: Data Classification
Revision Date: April 18, 2023



-
- a consumer provides to a financial institution to obtain a financial product or service from the institution;
 - results from a transaction between the consumer and the institution involving a financial product or service; or
 - a financial institution otherwise obtains about a consumer in connection with providing a financial product or service.

Personally Identifiable Information (PII).

Any instance of an individual's first name (or first initial) plus the last name and any one or more of the following: Social Security number

- Driver license or state-issued ID number
- Military ID number
- Passport number
- Credit card (or debit card) number, CVV2, and expiration date
- Financial account numbers (with or without access codes or passwords)
- Customer account numbers
- Unlisted telephone numbers
- Date or place of birth
- Mother's maiden name
- PINs or passwords
- Password challenge question responses
- Account balances or histories
- Wage & salary information
- Tax filing status
- Biometric data that can be used to identify an individual, including finger or voice prints
- Digital or physical copies of handwritten signature
- Personal E-mail addresses
- Medical record numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Medical histories
- National or ethnic origin
- Religious affiliation(s)
- Physical characteristics (height, weight, hair color, eye color, etc.)
- Insurance policy numbers
- Credit or payment history data
- Full face photographic images and any comparable images

DATA CLASSIFICATION POLICY

Any exceptions to this policy must be authorized and conform to the Security Exceptions Policy.

PATHFINDER POLICY

Owner: IT Services
Subject: Data Classification
Revision Date: April 18, 2023



-
- Certificate/license numbers
 - Internet Protocol (IP) address numbers

In general, personally identifiable information does not include information that is lawfully obtained from publicly available records, or from federal, state or local government records lawfully made available to the general public.

Protected Health Information (PHI)

Under HIPAA PHI is considered to be any identifiable health information that is used, maintained, stored, or transmitted by a HIPAA-covered entity – a healthcare provider, health plan or health insurer, or a healthcare clearinghouse – or a business associate of a HIPAA-covered entity, in relation to the provision of healthcare or payment for healthcare services. This data combined with the following identifiers is considered PHI.

Individually Identifiable Health Information:

1. Names
2. Zip Codes
3. All elements of dates (except year) for dates directly related to a client, employee, or family member, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Fax numbers
6. Electronic mail address
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificates/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web universal resource locators (URL's)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photograph images and any comparable images
18. Any other unique identifying number, characteristic, or code

PATHFINDER POLICY

Owner: IT Services
Subject: Data Classification
Revision Date: April 18, 2023



PHI excludes individually identifiable health information in:

- a. Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g
- b. Records described at 20 U.S.C. 1232g(a)(4)(B)(iv)
- c. Employment Records held by a Covered Entity in its role as an Employer
- d. Records of a person who has been deceased for more than 50 years

4. Referenced Standards

PCI DSS: 9.6

HIPAA: R-§164.514(d)(1), R-§164.514(d)(2)

GLBA: Safeguards Rule

PATHFINDER POLICY

Owner: IT Services
Subject: Data Management
Revision Date: April 18, 2023



1. Policy Overview

This policy ensures that Pathfinder adequately protects and maintains necessary data records and documents. This policy also ensures that records that are no longer needed by Pathfinder are discarded or destroyed at the appropriate time in the correct manner.

2. Data Retention

Only the minimum amount of private data, such as protected health information, cardholder data, and non-public customer and employee information is obtained, and its storage is limited to that which is required for legal, regulatory, and/or business requirements.

Pathfinder policies and procedures will be maintained for at least 6 years, which also includes maintaining revisions to the documents.

3. Data Destruction

When media containing private data is no longer required for business or legal reasons, it must be disposed of in a secure manner. Prior to destruction of electronic media, the IT Director will ensure, if appropriate, that a retrievable, exact copy of the required private information is retained.

- Hardcopy materials are cross-cut, shredded, incinerated, or pulped.
- Storage of materials to be destroyed must be retained in a secure area until destroyed.
- Private data is removed from all hardware and electronic media prior to disposal, using procedures that ensure that the data is not recoverable.
- Computing devices and electronic storage media must have the hard drives and any recording or memory units physically removed and destroyed or irreversibly wiped of all data.
- Removable storage media must be physically destroyed by shredding or pulverizing.

If any of the disposal activities are performed by a third-party service, a certificate of destruction is obtained to evidence the secure disposal. The certificate should include an itemized list to describe what was destroyed, and the process used for destruction. The itemized list should be cross-referenced to the internal listing of items sent for destruction to confirm that all items were destroyed.

4. Media Reuse

If electronic media devices that contain private information will be made available to third-parties or different users within the company for reuse, all private information must be irreversibly erased by IT services. Prior to removal, the IT Director will ensure that a retrievable, exact copy of any required private information is retained. If determined that the private information cannot be securely erased, the device must be securely destroyed in a way that it cannot be reconstructed, and, therefore, unavailable for reuse.

PATHFINDER POLICY

Owner: IT Services
Subject: Data Management
Revision Date: April 18, 2023



5. Removable Storage Media

Removable digital media containing private information must be encrypted. Any sharing or moving of unencrypted removable hardcopy media containing this type of data must be trackable, such as via a secure courier. Written manager approval is required prior to physically moving the media.

6. Documents Relevant to Actual or Potential Litigation and Governmental Investigations and Proceedings

If Pathfinder is confronted with or contemplates potential or actual litigation, or a potential or actual governmental investigation or proceeding, it has a duty to preserve records -- including electronic data, e-mails, and other documents that may be relevant to the potential or actual litigation or governmental investigation or proceeding. Consequently, upon the direction of a member of Pathfinder management that certain records may be relevant to actual or potential litigation, or a potential or actual governmental investigation or proceeding, employees have an obligation to preserve such records until management informs employees that the records are no longer needed. Such obligation includes turning off any automatic delete functions related to e-mail, voicemail, text messages, and instant messages.

Additionally, no employee may discard records based on a concern by the employee or others that the records could be harmful in potential or actual litigation or a potential or actual governmental investigation or proceeding. Accordingly, the retention period for the records potentially relevant to potential or actual litigation or governmental investigations or proceedings supersedes any established retention period identified in the Schedule of General Retention Periods in the [Document Retention Policy](#). Failure of employees to abide by these policies can carry severe civil and criminal penalties, as well as disciplinary action up to and including termination of employment.

7. Archiving

Data should not remain in production forever. Whether stored on-premises or in the cloud, data should be archived to mitigate any negative performance issues that could arise from a perpetually growing data set. IT services will ensure that data archiving be automated via policies and rules in databases or file directories whenever possible. When not possible, a manual archive will occur.

Archive rules:

- Migrate data older than 2 years to archive, unless a longer period is required by the user or business function for production.
- Destroy archived data according to the Schedule of Retention Periods in Pathfinder Services [Document Retention Policy](#).
- Archived data must be encrypted and backed up per backup protocols in Contingency Planning Policy.

DATA MANAGEMENT POLICY

Any exceptions to this policy must be authorized and conform to the Security Exceptions Policy.

PATHFINDER POLICY

Owner: IT Services
Subject: Data Management
Revision Date: April 18, 2023



8. Referenced Standards

PCI DSS: 3.1, 3.2, 4.2, 9.5, 9.6, 9.7, 9.8

HIPAA: R-§164.514(d)(4), R-§164.310(d)(1), R-§164.310(d)(2)(i), R-§164.310(d)(2)(ii), A-§164.310(d)(2)(iii), R-§164.316(b)(2)(i)

GLBA: Safeguards Rule

PATHFINDER POLICY

Owner: IT Services

Subject: Electronic & Digital Signature Policy

Revision Date: October 6, 2023

Purpose

The purpose of this policy is to define Pathfinder's use of electronic and digital signatures in compliance with the Indiana Uniform Electronic Transactions Act (IC 26-2-8) and the U.S. Electronic Signatures in Global and National Commerce (ESIGN) Act.

Scope

This policy applies to all employees, contractors, and third parties who use electronic or digital signatures within our organization.

Policy Statements

Pathfinder employees are authorized to use and collect electronic and digital signatures for company business. Electronic and digital signatures are as legal as a traditional ink signature and documents signed electronically are legally enforceable.

Pathfinder requires electronic documentation and signing of most internally created work records using secure protocols that meet the requirements of a digital signature.

To conduct business electronically with external parties, the other party must agree and clearly want to sign documents electronically. Consent can be implied with their actions of signing the document without objection. Should that party desire not to, they must be given an alternative. Pathfinder and the other parties must each get a copy of electronically signed documents.

Document-Specific Requirements

Most legal documents can be signed with an electronic signature, including contracts, agreements, forms, and even wills. However, some legal documents that get officially registered in the county recorder's office like deeds, mortgages, powers of attorney, affidavits require a notarized traditional ink signature in Indiana and other states.

Certain types of documents may require a higher level of security and verification, such as a digital signature. These might include documents related to healthcare, government, finance, and legal matters. The specific requirements can vary depending on the type of document and the context. Electronic records created and signed within secure information systems in compliance with Pathfinder's Access Control and Authentication policies typically meet the requirements for digital signature.

PATHFINDER POLICY

Owner: IT Services

Subject: Electronic & Digital Signature Policy

Revision Date: October 6, 2023

Pathfinder officials must consult legal counsel when uncertain about the signature requirements for records.

Definitions

- **Electronic Signatures:** An electronic signature means an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record.
- **Digital Signatures:** A digital signature is an advanced form of electronic signature that provides additional security and verification of the signer's identity through cryptographic techniques.
- **Electronic Records:** An electronic record means a record created, generated, sent, communicated, received, or stored by electronic means.
- **Automated Transactions:** An automated transaction means a transaction conducted or performed, in whole or in part, by electronic means or electronic records in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract.

REFERENCES

- Indiana Uniform Electronic Transactions Act (IC 26-2-8)
- U.S. Electronic Signatures in Global and National Commerce (ESIGN) Act

PATHFINDER POLICY

Owner: IT Services
Subject: Encryption
Revision Date: April 18, 2023



1. Policy Overview

Pathfinder guards against unauthorized access to private information being stored, transmitted, or received electronically.

2. Encryption Technology

All private information transmitted to a network outside Pathfinder must utilize an encryption mechanism of appropriate strength between the sending and receiving entities or the file, document, or folder containing the private information must be encrypted before transmission.

Technology and processes are implemented to ensure that all networks and information systems housing, transmitting, receiving or through which private information is accessed are appropriately secured.

3. Key Management

Encryption keys are generated only by cryptographic algorithms approved by Pathfinder. Keys are protected to ensure that only authorized users and applications can access the keys and are not stored on the same media as that data. Unique keys (or asymmetric key pairs) are not reused and access to the keys is restricted to the fewest number of custodians necessary.

4. Referenced Standards

PCI: 3.5, 3.6, 4.1, 4.3, 6.5

HIPAA: A- §164.312(a)(2)(iv), R- §164.312(e)(1), A- §164.312(e)(2)(ii)

GLBA: Safeguards Rule

PATHFINDER POLICY

Owner: Information Security Officer
Subject: Incident Response and Breach
Revision Date: April 18, 2023



1. Policy Overview

Pathfinder will promptly investigate any security incident or suspected breach involving private information, such as cardholder data, protected health information, and nonpublic customer and employee information to mitigate any harmful effect and to comply with applicable breach notification requirements.

2. Definitions

Breach - Any unauthorized acquisition, access, use, or disclosure of unsecured private information, which compromises the security or privacy of the data.

Potential breaches include but are not limited to:

- Unauthorized access to cardholder data, protected health information, or nonpublic customer and employee information maintained in paper or electronic form.
- Theft of data such as by stealing a laptop or paper documents.
- Interception or the receipt of mail or other communications intended for other recipients.

Breach excludes:

- Any unintentional acquisition, access, or use of private information by a workforce member if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure.
- Any inadvertent disclosure by a person who is authorized to access the private information at Pathfinder to another person authorized to access the private information at Pathfinder and the information received as a result of such disclosure is not further used or disclosed.
- A disclosure of private information where Pathfinder has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Security Incident - Any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Information Security Officer – The Pathfinder Services staff member designated to officially oversee implementation of Information Security policies and practices. The IT Director serves as the Information Security Officer

Privacy Officer – The Pathfinder Services staff member designated to officially oversee implementation of Privacy policies and practices. The Chief Strategy Officer serves as the Privacy Officer.

INCIDENT RESPONSE AND BREACH POLICY

Any exceptions to this policy must be authorized and conform to the Security Exceptions Policy.

PATHFINDER POLICY

Owner: Information Security Officer
Subject: Incident Response and Breach
Revision Date: April 18, 2023



3. Reporting a Possible Security Incident or Breach

Any person who discovers or suspects that they or someone else has acquired, accessed, used, or disclosed private information in an unauthorized manner shall immediately report the incident to their supervisor and the Information Security Officer.

4. Responding to a Possible Security Incident or Breach

Upon discovering a possible breach or security incident, Pathfinder will take immediate steps to limit the suspected breach or incident. Pathfinder will stop the unauthorized practice and seek the recovery or appropriate destruction of any private information. The Information Security Officer is responsible for responding to, containing, and investigating a suspected breach involving private information in collaboration with the Privacy Officer. All workforce members shall cooperate and assist as requested.

The response effort will include secure documentation and retention the following information:

- Description of what happened, including the date of the breach or security incident and the date of discovery, if known.
- Description of the types of information involved (such as whether full name, social security number, date of birth, home address, account number, or other types of information).
- Description of what is being done to investigate the matter, to mitigate harm to the individual(s), and protect against any further breaches or security incidents.
- List of all individuals notified (for example, the individual(s) who is the subject of the possible breach, police, Attorney General).
- Outcome of the incident.

Following the close of the incident response, the Information Security Officer must document vulnerabilities leading to the breach or security incident, assess business risk due to the incident, and formulate corrective actions to prevent further incidents, and record any follow up testing performed where appropriate to assure the effectiveness of the corrective action measures implemented.

5. Reporting Requirements

Pathfinder Services executive management will determine, in consultation with legal counsel as needed, whether a breach has occurred and any applicable notification requirements under state and/or federal law. Notification requirements may include the affected individual(s), Pathfinder's insurance company, the media, Secretary of HHS, State Attorney General's Office, the police, or other law enforcement.

6. Enforcement

Pathfinder will take appropriate enforcement action consistent with Pathfinder's Sanction Policy against individuals responsible for the breach or who otherwise fail to report a breach. Disciplinary actions may include up to termination and, in some instances, notifying law enforcement.

INCIDENT RESPONSE AND BREACH POLICY

Any exceptions to this policy must be authorized and conform to the Security Exceptions Policy.

PATHFINDER POLICY

Owner: Information Security Officer
Subject: Incident Response and Breach
Revision Date: April 18, 2023



7. Breach Prevention

Pathfinder will take appropriate actions to prevent future security incidents or breaches from occurring in a similar manner. Pathfinder will evaluate its physical, administrative, and technical safeguards if implicated in the breach or security incident, evaluate any security systems involved in the breach or incident, update its policies or training as appropriate, and review third-party service providers arrangements if involved with the breach or security incident.

8. Incident Response Plan

Pathfinder will develop and maintain an [Incident Response Plan](#) that operationalizes the requirements of this policy.

9. Referenced Standards

PCI DSS: 11.1, 12.10

HIPAA: R-§164.308(a)(6)(i), R-§164.308(a)(6)(ii), R-§164.414(a), R-§164.530(i), R-§164.530(j), R-§164.402, R-§164.404(a), R-§164.404(b), R-§164.404(c)(1), R-§164.404(d), R-§164.406, R-§164.408, R-§164.410, R-§164.412, R-§164.414(b)

GLBA: Safeguards Rule

INCIDENT RESPONSE PLAN (IRP)



Purpose & Scope

All information security and privacy incidents are different by nature. Therefore, the guidelines provided in this Incident Response Plan (IRP) do not comprise an exhaustive set of incident handling procedures. These guidelines document basic information about responding to incidents that can be used regardless of hardware platform or operating system. This plan describes the stages of incident identification and handling, with the focus on preparation and follow-up, including reporting guidelines and requirements.

Applicability

This IRP is part of the Written Information Security Program and applies to all employees, administrative consultants, contractors, temporary personnel, and the like who may experience or witness a security incident or possible data breach. After discovery, this process provides Information Technology Services with a checklist or outline for responding so that steps or information related to the incident are not missed. We are committed to protecting our information and responding appropriately to a security incident or data breach.

Compliance

Violations of this policy may lead to the suspension or revocation of system privileges and/or disciplinary action up to and including termination of employment or service contract. We reserve the right to advise appropriate authorities of any violation of law.

PLAN OBJECTIVES

The objectives of the Incident Response Plan (IRP) are to:

- Limit immediate incident impact to customers and business partners;
- Recover from the incident;
- Determine how the incident occurred;
- Find out how to avoid further exploitation of the same vulnerability;
- Avoid escalation and further incidents;
- Assess the impact and damage in terms of financial impact and loss of image;
- Update company policies, procedures, standards and guidelines as needed; and
- Determine who initiated the incident for possible criminal and/or civil prosecution.

INCIDENT RESPONSE TEAM (24x7)

To adequately respond to an intrusion or incident, predetermined teams should be formed to react to predetermined incident characteristics. As the situation develops and the impact becomes more significant, the various teams may be called to contribute.

Incident Response Team Roles (24x7 Key Personnel)	Role Description
Incident Response Coordinator. Chief Information Officer	Individual responsible for conducting and coordinating the Incident Response Plan (IRP).
Technical Support Team Lead. Network Administrator	Individual responsible for aiding IT Services, which could include support personnel, outside contractors, or individual users.
Management Team Lead. Chief Information Officer	Management representative responsible for interfacing with other managers/executives in areas, such as Legal, Human Resources, or other specialties, as required.

INCIDENT RESPONSE TEAM RESPONSIBILITIES

Incident Response Coordinator

- Receive and track all reported potential threats.
- Escalate Incident Response if the threat manifests itself.
- Determine relevant membership of the Technical Support Team.
- Alert applicable support organizations of the potential threat and any defensive action required.
- Alert management of the potential threat.
- Start a chronological log of events.
- Receive status from IT Services and report to management on a regular basis.

Technical Support Team

- Monitor all applicable sources for alerts or notification of a threat.
- Determine initial defensive actions required.
- Notify the Incident Response Coordinator.
- Determine the best course of action for the containment of the incident and eradication of the threat.
- Report actions taken and status to the Incident Response Coordinator.
- Continue to monitor all known sources for alerts looking for further information or actions to take to eliminate the threat.
- Continue reporting status and actions taken to the Incident Response Coordinator for the chronological log of events.
- Monitor effectiveness of actions taken and modify them as necessary.

Management Team

- Assume responsibility for directing activities about the incident.
- Actively participate in Incident Response operations, based on the effects to business operations.

- Determine whether escalation appropriate.
- Determine when the risk has been mitigated to an acceptable level.
- Contact local authorities, if deemed appropriate.
- Initiate breach notification procedures, if applicable.
- Ensure that all needed information is being collected to support legal action or financial restitution.

INCIDENT RESPONSE PROCESS

The Incident Response Process is an escalation process whereas the impact of the incident becomes more significant or widespread, the escalation level increases bringing more resources to bear on the problem. At each escalation level, team members who will be needed at the next higher level of escalation are alerted to the incident so that they will be ready to respond if they are needed.

Step		Responsible Entity	Incident Response Plan (IRP) Actions
1	1.0	Anyone	Determine If an Incident Occurred <i>If You See Something, Say Something.</i>
	1.1	Anyone	Analyze the precursors and indications. (Appendix A)
	1.2	Anyone	Look for correlating information. (Appendix A)
	1.3	Anyone	Perform research (e.g. search engines, vendor knowledge base, peer review, etc.)
2	2.0	Anyone	Notify IT Services
	2.1	Anyone	Any person who discovers or suspects that they or someone else has acquired, accessed, used, or disclosed private information in an unauthorized manner shall immediately report the incident to the CIO and email details of suspected incident to itservices@pathfinderservices.org with subject: Urgent – Suspected Security Event. The email should include screenshots of any evidence (if applicable) as well as descriptions of the following: <ul style="list-style-type: none"> • What was experienced or observed? • When was it first noticed? • Why do you think it is a security incident?
	2.2	IT Services	IT Services classifies the ticket type as: Security/Suspected Event and sets the initial priority to Medium.
	2.3	IT Services	If IT Services feels the event warrants a full investigation, IT Services should create a case file in IT Services SharePoint document library and link that folder to the ticket.
	2.4	IT Services	IT Services consolidates documentation and evidence and, if applicable, stores the documentation in the case file for the incident.
3	3.0	IT Services	Incident Prioritization
	3.1	IT Services	IT Services prioritizes handling the incident based on the business impact and urgency and sets the ticket priority to match.
	3.2	IT Services	IT Services will identify which IT resources have been affected and forecast which resources will be affected.
	3.3	IT Services	IT Services will estimate the current and potential technical effect of the incident.
4	4.0	IT Services	Incident Notification
	4.1	IT Services	IT Services will contact affected asset owners and business units, alerting them to the situation.

5	5.0	Multiple Entities	Incident Escalation (If Required)
	5.1	IT Services	If the incident is believed to be significant, the Incident Response Coordinator or asset owner is responsible for notifying management for escalation.
	5.2	Management	Management is responsible for coordinating further incident escalation steps, as required.
6	6.0	IT Services	Secure, Document, Acquire, Preserve & Analyze Evidence (If Required)
	6.1	IT Services	IT Services will follow its Standard Operating Procedures (SOP) for evidence seizure and analysis.
	6.2	IT Services	IT Services will begin an Information Incident Report to document the details of the incident as well as response throughout the life of the incident.
7	7.0	IT Services	Contain the Incident
	7.1	IT Services	IT Services will work with affected asset custodians and business units to determine a containment strategy.
	7.2	IT Services	Incident handlers will implement steps to contain the incident.
8	8.0	IT Services	Eradicate the Incident
	8.1	IT Services	Identify and mitigate all vulnerabilities that were exploited.
	8.2	IT Services	Remove malicious code, inappropriate materials, and other components.
9	9.0	IT Services	Recover from the Incident
	9.1	IT Services	Return affected systems to an operationally ready state.
	9.2	Multiple Entities	Confirm that the affected systems are functioning normally.
	9.3	Multiple Entities	If necessary, implement additional monitoring to look for future related activity.
10	10.0	Multiple Entities	Follow-Up
	10.1	IT Services	IT Services will finalize the Information Incident Report and distribute it appropriately.
	10.2	Management	Initiate Breach Notification Procedures if appropriate.
11	11.0	Multiple Entities	After Action Review (AAR)
	11.1	Multiple Entities	Hold an After-Action Review (AAR) / "lessons learned" meeting involving all key players.
	11.2	Multiple Entities	Update any changes needed to the Incident Response Plan (IRP) or other policy/procedure/standard.

POST INCIDENT

Following an incident, the Incident Response Coordinator should work with the Technical Support Team to prepare a report for management to include:

- Estimate of damage and impact.
- Action taken during the incident (not technical detail).
- Follow-on efforts needed to eliminate or mitigate the vulnerability.
- Policies or procedures that require updating.
- Efforts taken to minimize liabilities or negative exposure.
- Provide the chronological log and any system audit logs requested by the Management Team.
- Document lessons learned and modify the Incident Response Plan (IRP) accordingly.
- Recommend disciplinary action in the case that the incident was from an internal source.

BREACH NOTIFICATION PROCEDURES

In terms of incident reporting, the definition of a security breach is when an individual's unencrypted Personally Identifiable Information (PII) is reasonably believed to have been acquired by an unauthorized person or process. Good faith acquisition of PII by an authorized user or authorized agent for Pathfinder purposes does not constitute a security breach, provided that the PII is not used or subject to further unauthorized disclosure.

If a breach occurs, breach notification procedures should occur without unreasonable delay, except:

- When a law enforcement agency has determined that notification will impede a criminal investigation; or
- To discover the complete scope of the breach and restore the integrity of the system.

If a security incident is suspected to be a data privacy breach, take the following immediate actions:

1. Notify the Incident Response Team (IRT), including the General Counsel and Information Security.
2. Determine what information was suspected to be breached, i.e., specific individuals' first and last names with a type of PII.
3. When appropriate, bring in an incident response expert or law enforcement to investigate. Identify the scope, time frame and source(s) of breach, type of breach, whether data encryption was used and for what, possible suspects (internal or external, authorized or unauthorized, employee or non-employee user).
4. Review for other compromised systems.
5. Monitor all systems for potential intrusions.
6. Determine the notification requirements (statutory or contractual) and address within the required timeframe.

APPENDIX A: INCIDENT DISCOVERY

Malicious Actions	Possible Indications of an Incident
Denial of Service (DoS) Examples	You might be experiencing a DoS if you see...
Network-based DoS against a host	<ul style="list-style-type: none"> • User reports of system unavailability • Unexplained connection losses • Network intrusion detection alerts • Host intrusion detection alerts (until the host is overwhelmed) • Increased network bandwidth utilization • Large number of connections to a single host • Asymmetric network traffic pattern (large amount of traffic going to the host, little traffic coming from the host) • Firewall and router log entries • Packets with unusual source addresses
Network-based DoS against a network	<ul style="list-style-type: none"> • User reports of system and network unavailability • Unexplained connection losses • Network intrusion detection alerts • Increased network bandwidth utilization • Asymmetric network traffic pattern (large amount of traffic entering the network, little traffic leaving the network) • Firewall and router log entries • Packets with unusual source addresses • Packets with nonexistent destination addresses
DoS against the operating system of a host	<ul style="list-style-type: none"> • User reports of system and application unavailability • Network and host intrusion detection alerts • Operating system log entries • Packets with unusual source addresses
DoS against an application on a host	<ul style="list-style-type: none"> • User reports of application unavailability • Network and host intrusion detection alerts • Application log entries • Packets with unusual source addresses

Malicious Software (malware) Examples	You might be infected with malware if you see...
A virus that spreads through email infects a host.	<ul style="list-style-type: none"> • Antivirus software alerts of infected files • Sudden increase in the number of emails being sent and received • Changes to templates for word processing documents, spreadsheets, etc. • Deleted, corrupted, or inaccessible files • Unusual items on the screen, such as odd messages and graphics • Programs start slowly, run slowly, or do not run at all • System instability and crashes
A worm that spreads through a vulnerable service infects a host.	<ul style="list-style-type: none"> • Antivirus software alerts of infected files • Port scans and failed connection attempts targeted at the vulnerable service (e.g., open Windows shares, HTTP) • Increased network usage • Programs start slowly, run slowly, or do not run at all • System instability and crashes
A Trojan horse is installed and running on a host.	<ul style="list-style-type: none"> • Antivirus software alerts of Trojan horse versions of files • Network intrusion detection alerts of Trojan horse client-server communications • Firewall and router log entries for Trojan horse client-server communications • Network connections between the host and unknown remote systems • Unusual and unexpected ports open • Unknown processes running • High amounts of network traffic generated by the host, particularly if directed at external host(s) • Programs start slowly, run slowly, or do not run at all • System instability and crashes
Malicious mobile code on a Web site is used to infect a host with a virus, worm, or Trojan horse.	<ul style="list-style-type: none"> • Indications listed above for the pertinent type of malicious code • Unexpected dialog boxes, requesting permission to do something • Unusual graphics, such as overlapping or overlaid message boxes
Malicious mobile code on a Web site exploits vulnerability on a host.	<ul style="list-style-type: none"> • Unexpected dialog boxes, requesting permission to do something • Unusual graphics, such as overlapping or overlaid message boxes • Sudden increase in the number of emails being sent and received • Network connections between the host and unknown remote systems
A user receives a virus hoax message.	<ul style="list-style-type: none"> • Original source of the message is not an authoritative computer security group, but a government agency or an important official person • No links to outside sources • Tone and terminology attempt to invoke panic or a sense of urgency • Urges recipients to delete certain files and forward the message to others

Unauthorized Access Examples	You might be experiencing unauthorized access on your system or network if you see...
Root compromise of a host	<ul style="list-style-type: none"> • Existence of unauthorized security-related tools or exploits • Unusual traffic to and from the host (e.g., attacker may use the host to attack other systems) • System configuration changes, including— <ul style="list-style-type: none"> - Process/service modifications or additions - Unexpected open ports - System status changes (restarts, shutdowns) - Changes to log and audit policies and data - Network interface card set to promiscuous mode (packet sniffing) - New administrative-level user account or group • Modifications of critical files, timestamps, and privileges, including executable programs, OS kernels, system libraries, and configuration and data files • Unexplained account usage (e.g., idle account in use, account in use from multiple locations at once, unexpected commands from a particular user, large number of locked-out accounts) • Significant changes in expected resource usage (e.g., CPU, network activity, full logs, or file systems) • User reports of system unavailability • Network and host intrusion detection alerts • New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots) • Highly unusual operating system and application log messages • Attacker contacts the organization to say that he or she has compromised a host
Unauthorized data modification (e.g. Web server defacement)	<ul style="list-style-type: none"> • Network and host intrusion detection alerts • Increased resource utilization • User reports of the data modification (e.g., defaced Web site) • Modifications to critical files (e.g., Web pages) • New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots) • Significant changes in expected resource usage (e.g., CPU, network activity, full logs or file systems)
Unauthorized usage of standard user account	<ul style="list-style-type: none"> • Access attempts to critical files (e.g., password files) • Unexplained account usage (e.g., idle account in use, account for use from multiple locations at once, commands that are unexpected from a particular user, large number of locked-out accounts) • Web proxy log entries showing the download of attacker tools
Physical intruder	<ul style="list-style-type: none"> • User reports of network or system unavailability • System status changes (restarts, shutdowns) • Hardware is completely or partially missing (i.e., a system was opened, and a particular component removed) • Unauthorized new hardware (e.g., attacker connects a packet sniffing laptop to a network or a modem to a host)

Unauthorized data access (e.g., database of customer information, password files)	<ul style="list-style-type: none"> • Intrusion detection alerts of attempts to gain access to the data through FTP, HTTP, and other protocols • Host-recorded access attempts to critical files
---	---

Inappropriate Usage Examples	You might have identified inappropriate usage if you see...
Unauthorized service usage (e.g., Web server, file sharing, music sharing)	<ul style="list-style-type: none"> • Network intrusion detection and network behavior analysis software alerts • Unusual traffic to and from the host • New process/software installed and running on a host <ul style="list-style-type: none"> - Password cracking tools - Unauthorized website running - File transfer software - Peer-to-Peer (P2P) sharing software running • New files or directories with unusual names (e.g., “warez” server style names) • Increased resource utilization (e.g., CPU, file storage, network activity) • User reports • Application log entries (e.g., Web proxies, FTP servers, email servers)
Access to inappropriate materials (e.g., downloading pornography, sending spam)	<ul style="list-style-type: none"> • Network intrusion detection alerts • Eyewitness reports or complaints to management, HR • Pornographic or explicit content displayed • Application log entries (e.g., Web proxies, FTP servers, email servers) • Inappropriate files on workstations, servers, or removable media
Attack against internal party	<ul style="list-style-type: none"> • Network intrusion detection alerts • Inside party reports (e.g. management, HR, or ethics) <ul style="list-style-type: none"> - Harassing email or text messages sent to internal users - Pornographic or explicit content sent to internal users • Network, host, and application log entries
Attack against external party	<ul style="list-style-type: none"> • Network intrusion detection alerts • Outside party reports <ul style="list-style-type: none"> - Harassing email or text messages sent to external users - Pornographic or explicit content sent to external users - External attack traffic traced back to the company • Network, host, and application log entries

APPENDIX B: COMMON EFFECTS OF ATTACKS

There are at least four primary effects of attacks that affect Information Security:

- Denial of Service. Any action that causes all or part of the network's service to be stopped entirely, interrupted, or degraded sufficiently to impact operations is a denial of service. Examples of denial of service include network jamming, introducing fraudulent packets, and system crashes and/or poor system performance, in which people are unable to effectively use computing resources.
- Loss / Alteration of Data or Programs. An example of loss or alteration of data or programs would be an attacker who penetrates a system, then modifies an Operating System-level program/configuration file (e.g. audit) so that the intrusion will not be detected.
- Compromise of Data. One of the major dangers of a computer security incident is that information may be compromised. The release of classified information to people without the proper clearance or formal authorization jeopardizes our business' security. Efficient incident handling minimizes this danger.
- Loss of Trust in Computing Systems. Users may lose trust in computing systems and become hesitant to use one that has a high frequency of incidents or even a high frequency of events that cause the user to distrust availability or integrity.

APPENDIX C: INCIDENT RESPONSE STAGES

There are generally six (6) stages of incident response:

- Preparation. The most important aspect of a response plan is to know how to use it once it is in place. Knowing how to respond to an incident before it occurs can save valuable time and effort in the long run.
- Identification. Identify whether an incident has occurred. If one has occurred, the Incident Response Team can take the appropriate actions. Identification may come from Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), File Integrity Monitoring Systems (FIMS), or manual observance of an incident.
- Containment. Involves limiting the scope and magnitude of an incident. Because so many incidents observed currently involve malicious code, incidents can spread rapidly. This can cause the destruction and loss of data. As soon as an incident is recognized, the Incident Response Team must immediately begin working on containment.
- Eradication. Removing the cause of the incident can be a difficult process. It can involve virus removal, removing user permissions, and/or dismissing employees.
- Recovery. Restoring a system to its normal business status is essential. Once a restore has been performed, it is also important to verify that the restore operation was successful and that systems are back to its normal condition.
- Follow-up. Some incidents require considerable time and effort. It is common that once the incident appears to be contained and remedied; there is little interest in devoting any more effort to the incident. Performing follow-up activity is, however, one of the most critical activities in the response procedure. This follow-up can support any efforts to prosecute those who have broken the law. This includes changing any policies that may need to be narrowed down or be changed altogether.

APPENDIX D: INCIDENT CATEGORIES

An incident will be categorized as one of ten severity levels. These severity levels are based on the impact to the company and can be expressed in terms of financial impact, impact to operations, impact to sales, or impact to the company's image.

CAT	Severity	Situation	Category Description	Response Action	Response Time	Recovery Actions
0	Training	Exercise (e.g. Network Defense Testing)	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Depends on the type of exercise.	Exercise Dependent	There are no recovery procedures required for this event.
1	Criminal	Illegal Content	This category is used to respond to any suspected incidents involving either: - the possession or transmission of child pornography; or - possible terrorist-related activities.	<u>Stop the investigation immediately.</u> The incident handler must cease work and call the local office for the FBI and follow the FBI's response instructions.	Within 1 hour of event identification	There are no recovery procedures required for this event.
2	Serious	Successful Host Compromise (privileged-level access)	This is a root or administrator-level compromise of a system. A successful event of this nature means the intruder has total control over the host and access to all data stored on it or on systems that trust this host.	The system must be disconnected from the network. It should NOT be turned off. No action should be taken to investigate this incident or change anything on the system unless directed to do so by IT Services.	Within 1 hour of event identification	Do not start recovery procedures until directed to do so by IT Services. Normal recovery procedures from an event of this category are rebuilding the system from original media, installing all required patches, and scanning for vulnerabilities before reattaching to the network. Notify IT Services to arrange for a verification scan to be conducted.

3	Serious	Malicious Software (servers)	Any software code intentionally created or introduced into a server-class system for the distinct purpose of causing harm or loss to the computer system, its data, or other resources. Examples are spyware, adware, viruses, Trojans, worms, etc.	The system must be disconnected from the network. It should NOT be turned off. No action should be taken to investigate this incident or change anything on the system unless directed to do so by IT Services.	Within 1 hour of event identification	Do not start recovery procedures until directed to do so by IT Services. Normal recovery procedures from an event of this category are rebuilding the system from original media, installing all required patches, and scanning for vulnerabilities before reattaching to the network. Notify IT Services to arrange for a verification scan to be conducted.
4	Serious	Malicious Software (workstations)	Any software code intentionally created or introduced into a workstation-class system for the distinct purpose of causing harm or loss to the computer system, its data, or other resources. Examples are spyware, adware, viruses, Trojans, worms, etc.	The system must be disconnected from the network. It should NOT be turned off. IT Services will respond and follow company-approved procedures to remediate the malware infection.	Within 1 hour of event identification	Normal recovery procedures from an event of this category are rebuilding the system from original media, installing all required patches, and scanning for vulnerabilities before reattaching to the network. Notify IT Services to arrange for a verification scan to be conducted.
5	Serious	Denial of Service (DoS) Attack	A successful event of this nature means the intruder has successfully denied access to either the entire network, portion of the network or to critical systems or data.	Determine the cause, if possible. Contact IT Services for assistance in determining the source of the attack and removing the threat. Take no further action unless directed to do so by IT Services.	Within 1 business day	Review logs and configurations to determine if there is anything that can be done to prevent further occurrences of this type of the event and/or the cause of the current event.
6	Serious	Unauthorized Scan (internal network)	Any automated probe attacks (e.g. Nessus, Nmap, etc.)	Contact IT Services for assistance in determining if the scan is unauthorized.	Within 1 business day	Review system event logs and/or network logs to determine if any systems responded to the probe or scan and what information may have been obtained by the unauthorized scanner.

7	Significant	Successful Host Compromise (user-level access)	This is a user-level compromise. A successful event of this nature means the intruder has access to data, applications, and systems which the users can access.	The system must be disconnected from the network. It should NOT be turned off. No action should be taken to investigate this incident or change anything on the system unless directed to do so by IT Services.	Within 1 business day	Do not start recovery procedures until directed to do so by IT Services. Normal recovery procedures from an event of this category are rebuilding the system from original media, installing all required patches, and scanning for vulnerabilities before reattaching to the network. Notify IT Services to arrange for a verification scan to be conducted.
8	Significant	Attempted Access (unsuccessful)	An unsuccessful attempt to access or compromise an information system. An event of this nature means the intruder attempted a known exploit or attempted to log into an information system but was not successful in compromising it or in logging in.	No response is necessary. Report the event to IT Services and include as much data as possible about the intruder and the attempted compromise or intrusion. Take no further action unless directed to do so by IT Services.	Within 1 business day	There are no recovery procedures required for this event.
9	Significant	Poor Security Practice	Examples of poor security practices are root login using Telnet, FTP or HTTP; bad passwords; not using secure protocols to transfer sensitive data; downloading unauthorized software; peer-to-peer (P2P) software, etc.	The response depends on the event. The response ranges from disconnection from the network to a system rebuild, to no action required. An incident report should be sent to the department to follow appropriate actions (e.g. verbal or written counseling).	Within 1 business day	The recovery depends on the type of event.
10	Significant	Suspected/Unknown	If the threat is unclear, use this category until the threat or situation is investigated, and a final determination has been made.	Reassign to the proper category when a final determination is made.	Within 4 hours of event identification	Recovery is determined after the final determination and event category is determined.

PATHFINDER POLICY

Owner: IT Services
Subject: Information Risk Management
Revision Date: April 18, 2023



1. Policy Overview

Potential security risks and vulnerabilities that may affect the confidentiality, integrity, and/or availability of Pathfinder critical systems or private information is identified and addressed.

2. IT Risk Assessments

Annual IT risk assessments are performed to evaluate overall effectiveness and potential risks and vulnerabilities to the confidentiality, integrity, or availability of Pathfinder private information. Updates are performed whenever environmental or operational changes occur that may affect the security of private information, including the adoption of new technology.

The IT risk assessment identifies the systems which are critical to conducting Pathfinder business, including those that store, process, or transmit private information; identify threats and vulnerabilities to the system; consider current controls; assess the risk and identify risk mitigation strategies. Third-Parties that store or have access to Pathfinder Services' information must also be assessed for risk in accordance with Pathfinder's Contract Management Policy and incorporated into the IT risk assessment. The results of the IT risk assessment are documented and retained for six (6) years.

3. Risk Management

Using the results of the IT risk assessment, security measures and related policies and procedures are updated as appropriate to address risk areas, such as physical security measures, firewalls, passwords, encryption, and access controls. The nature of specific risks and the feasibility, effectiveness, and cost of specific safeguards are considered. Pathfinder retains documentation of measures implemented to remediate potential risks and/or vulnerabilities identified during the IT risk assessment for six (6) years.

4. Evaluations

In conjunction with the annual IT risk assessment, periodic technical and non-technical evaluations of security safeguards are performed to evaluate how well the practices and safeguards are being followed, along with how well they are protecting private information from unauthorized access or intrusion. Technical evaluations, such as vulnerability scans or penetration tests, are performed at least annually. Non-technical evaluations, such as audits over specific controls or processes are performed less often based on the level of risk.

Evaluations may include:

- Interviews with workforce members
- Access control and system activity audits
- Tests of intrusion detection systems
- Vulnerability Scans
- Penetration testing
- Review of Business Associate and service provider contracts

If any practices or controls are deemed insufficient or ineffective, action will be taken to implement other measure to address the compliance or security need.

RISK MANAGEMENT POLICY

Any exceptions to this policy must be authorized and conform to the Security Exceptions Policy.

PATHFINDER POLICY

Owner: IT Services
Subject: Information Risk Management
Revision Date: April 18, 2023



5. Referenced Standards

PCI: 12.2

HIPAA: R-§164.308(a), R-§164.308(a)(1)(ii)(A), R- §164.308(a)(1)(ii)(B), R- §164.308(a)(8)

GLBA: Safeguards Rule



Disaster Recovery Information Systems

Plan to recover Information Systems in the event of a disaster

Contents

Overview.....	1
Risk Assessment & Mitigation	1
Disaster Recovery as a Service (DRaaS)and the Cloud.....	1
Natural and Man-Made Risks.....	1
Technical Risks	2
Pre-Disaster Planning	3
Backups and Warm Site	3
Systems Documentation	3
In the event of a Disaster	4
Communication.....	4
Restoration of Systems and Critical Data.....	5
Prioritization of Restoration in Event of Disaster	5
Disaster at a Branch Office.....	6
Attachment A: DR Playbook	7
Attachment B: Failover of Phone Lines	9
Attachment C: Message Broadcasting	10
Attachment D: Web Site Communication Procedure	11
Attachment E: LastPass	12
Attachment F: IT Disaster Recovery Contacts	13
ITS Personnel.....	13
Emergency Contact Information	14
Attachment G: Tiered Software List for Restoration.....	15
Attachment H: Maintenance & Test Schedule	18

Overview

This plan documents the IT Services Department's preparations associated with Disaster Recovery, Backup, and Continuity of Business planning to minimize the effects of disasters on our IT Infrastructure.

This plan outlines preparations for not only a catastrophic disaster such as the loss of the headquarters building and data center, but also minor disasters such as extended power outages and the loss of telecom or internet service.

This plan is intended as a reference and guideline and should not replace sound judgment and common sense.

Risk Assessment & Mitigation

Pathfinder engages in an annual Risk Assessment of its natural and man-made risks to information systems and security. Severe weather, thunder and lightning storms, tornadoes, fire, and cyber security crimes pose the greatest risk to Pathfinder operations. This plan focuses on risk from the loss of data systems, not cyber security. That is addressed in a separate Written Information Security Program.

Disaster Recovery as a Service (DRaaS) and the Cloud

Whether natural or man-made, the primary risk is the loss of access to or destruction of business-critical information systems and data. Pathfinder subscribes to Disaster Recovery as a Service (DRaaS) provided by 4EOS's SafeHouse DataCenter. This includes daily incremental backups of our entire data store and all systems. It also includes a warm site and service to spin up all Tier 1 software and data to be remotely accessible via public internet within an hour. Details of this DRaaS are documented in a DR Playbook maintained by 4EOS and copied here in Attachment A. All other business critical information systems are hosted by remote third-party cloud vendors and are therefore immune to a localized disaster.

Natural and Man-Made Risks

The following strategies are focused on mitigation of risk to the main data center located at the North Campus, in Huntington. If the data center were lost, it would have a disastrous effect on the entire business. If any of the branch locations were lost, they would relocate and set up temporary operations including a connection back to the data center to resume access and use of Pathfinder hosted or third party hosted systems.

Fire: Exterior of North Campus building is brick and inside walls are built with metal studs. Automatic Fire Alarm on premise notifies Fire Dept. via Koorson Fire and Security Alarm Monitoring center. Fire alarm is powered by the backup generator. Fire extinguishers are placed throughout the building including one in the server room.

Tornado or Wind Damage: Brick building is unlikely to sustain major damage from an average thunderstorm. Tornado damage is possible. Tornado damage to even part of the building could affect power/internet reliability. Internet and telecommunications infrastructure enter the building in upstairs loft area above restrooms.

Flooding: Server Room Floor is approximately 18 in up from ground level in the back of the building. Surrounding Terrain slopes down away from the building to the North. No major water ways nearby. Nearest water ways are a drainage pond approximately 700 feet to the east (Between TCU & K of C) and a Drainage ditch/ravine approximately 600 feet to the north, across North Point Ave.

Evacuation: An event such as a chemical spill, bomb threat or large fire near the North Campus building could require the evacuation of all personnel. All can work remotely via Microsoft Teams, SharePoint and VPN with access setup on both of our internet connections into the North Campus building. Most functions of the ITS Department can continue off site. The Microsoft Teams phone system allows all calls to be received wherever the user is on their computer or mobile device. The ITS Department can also work with staff to work from other offices, such as State Street.

End-point Replacement: Destruction of any office space will likely also result in loss of the endpoints used by staff. In such a case, the IT Services staff will use its inventory log to immediately order replacement devices from its trusted vendors (either CDW or 4EOS) to be delivered and set up for use at home or alternate location.

Technical Risks

Power Outage: Power lines into the North Campus (where the data center is) are underground. Feed lines into the area are mostly above ground. Risk is largely mitigated with backup generator and an Uninterrupted Power Supply (UPS). If Natural Gas service is still intact and flowing to the building, generator can run for indefinite amount of time. Pathfinder Maintenance staff manages the maintenance on the generator and ensures that it is ready for an extended power outage. Preventative maintenance is to be performed yearly. Starting battery will be replaced every three years in line with general industry recommendations. The backup generator and UPS both run through automated test cycles each week. The UPS emails test results directly to the System Admin and IT Director weekly. The generator test run is audible (sounds like a lawn-mower) and can be heard running weekly on Friday mornings.

Loss of Internet/WAN/Telco Connectivity: Our IT infrastructure is reliant on connections from our data center to our branch offices and to the internet. We have mitigated this risk by having redundant connections to the internet from two separate providers into the Data Center, currently Metronet and Comcast. The two internet connections enter the building from opposite directions. All branch offices have private WAN connections as well as a VPN connection to the Data Center. Telephone connections are routed over the internet connections via two separate providers (Metronet and Comcast). As long as we maintain an internet connection our phone

will continue to operate as designed. See [Attachment B](#) for details on our phone provider's designed diversity and redundancy they have in place.

Pre-Disaster Planning

Backups and Warm Site

SafeHouse Data Center takes incremental snapshots of all locally hosted servers and data daily. These snapshots are kept in local storage and are also replicated to its remote servers in Northern Allen County, IN. Servers with software and data classified as Tier 1 (most critical to business operations) are maintained as a warm site ready to be made operational and accessible from any internet connection within one hour. This warm site will be mirrored to servers in an earthquake, tornado, fire, and flood resistant bunker also in Northern Allen County, IN. This service includes weekly maintenance of any changes to our data center to be replicated in the warm site, as well as monthly status reports and two annual tests where we will recover operations from the warm site. A DR playbook with procedures for testing and recovery from a disaster will be provided by 4EOS and attached to this plan in Attachment A.

Systems Documentation

4EOS also manages our production servers and infrastructure along with help desk support to end users. This includes a secure, remote web-based wiki (IT Glue) with all the system documentation necessary to help restore operations over the long term. 4EOS manages and backs up this documentation.

Pathfinder subscribes to Last Pass for Teams to securely store shared ITS team access credentials for all cloud-based web portals that we need to manage and restore our environment. Only members of the ITS team have credentials to access this site. Credentials cannot be published here for security reasons. Once access to the site is gained, all critical systems accounts with vendors will be easily identified in the vault and appropriate account credentials or other secure notes disclosed to access and manage any cloud-based system portals. [Attachment D](#) provides instruction for accessing LastPass.

Communication Devices

All senior management and IT Services staff have company provided mobile phones. The IT Services Department has a limited amount of air cards and Mobile Wi-Fi "JetPacks" devices available as "loaners". Air cards from other areas in the company can be reassigned as necessary in the event of a disaster. These air cards can be used for employees to access the network if a disaster affects an office or site other than North Campus. Due to our relationship with Verizon, we can quickly get additional cellular data devices, such as air cards or MiFi devices shipped to us overnight. These devices can be ordered by contacting our Verizon Rep Jeff Musselman at jeffrey.musselman@verizonwireless.com, or using [My Business Account Online](#) for account management. Customer Care is available at 800-295-1614. These devices could be used in any

disaster where additional access to the internet is needed, and land-based internet is not available.

Pathfinder's public websites and intranet are hosted by remote third parties and are immune to a localized disaster, remaining available for disaster related communication. MDD Hosting hosts all public sites. Microsoft hosts the intranet in Sharepoint Online services.

Pathfinder's email system is also remotely hosted in the Microsoft cloud through our Office 365 subscription, making it a resilient communication channel that will be available in a disaster.

Pathfinder subscribes to Dial My Calls for the ability to broadcast emergent communications to all staff and parents at Kids Kampus when necessary. Messages can go out as texts, emails, or phone calls. Human Resources maintains the staff contact list including their mobile phone numbers in that system. The Kids Kampus' Director is responsible to assure that the parent contacts are maintained. Dial My Calls is a cloud-based service accessible from any internet connection and therefore immune to a local disaster. [Attachment C](#) provides details on use of the system.

This plan and associated preparations will be reviewed and updated annually.

In the event of a Disaster

All disaster recovery operations and short-term decisions will be managed by the Chief Strategy Officer (CSO), with the IT Director acting as a backup. The CSO or IT Director will communicate with the CEO, and the entire senior and extended leadership teams, as necessary. Minor disasters will be managed by the CSO. In the event of a catastrophic disaster the CSO & President will collaborate to make the decision to officially declare a catastrophic disaster and begin the recovery process at which time the CSO or designee will activate the DR Service and restoration detailed in the DR Playbook (Attachment A).

Communication

ITS Staff will communicate by whichever means are functional and most convenient dependent on the situation. Communication devices available include:

- Cell Phone Voice Calls
- VOIP Voice Calls
- Microsoft Teams messaging
- Text Message/iMessage
- Company E-mail
- Personal E-mail
- Dial My Calls broadcast

- Microsoft Office 365 Groups
- Corporate Website
- Any other means available in an Emergency, such as Skype or Instant Messaging or social media.

Even in the event of a disaster, information security and privacy policies must be followed. Private information should not be communicated via a non-secure method.

If a catastrophic disaster has been declared, the CSO will notify the extended leadership team. The preferred method of notification will be via Dial My Calls broadcast to all cell phones and email. A companywide broadcast in Microsoft Teams will also occur. Phone calls will be made to the senior leaders with more detailed information and instruction. Senior Leaders will follow up with the extended leaders under their supervision. An alert with a link to an internal Disaster Recovery website will be posted on the home page of Pathfinder's public website and broadcast via text message and email to affected staff. The DR website will be a Microsoft SharePoint site created at the time of the disaster with plans published along with an internal newsfeed and ongoing discussion threads. Only staff effected by the disaster or considered relevant to its management will be invited into the site. Both the public and internal DR websites are hosted far offsite via cloud service providers and will be immune to any local disasters.

Restoration of Systems and Critical Data

In the event of a catastrophic disaster, ITS staff will meet at the North Campus location if it is safe to enter the area. If it is not safe, ITS staff will meet at the State Street location. If the event includes the loss of the North Campus building, the State Street office will be the recovery location to begin rebuilding the data center. This is the most ideal situation due to having the server room already in place in that building. Electrical, Cooling, and internet connections are already in place. In the rare event that both North Campus and State Street are not usable the Wabash or Plymouth offices can be used, with additional accommodations for power, cooling, security, etc. needing to be made, which will result in a longer recovery time.

A licensed electrician will be required to hookup our hardwired UPS device to power the servers and restore systems at a new restoration site. The following are preferred electricians depending on the location of the restoration site:

- Plymouth - Monty's 574-952-1127
- Huntington -Young's Electric 260-356-6223
- Wabash - Quality Electric 260-563-5772

Prioritization of Restoration in Event of Disaster

All systems have been prioritized by ITS and Senior Leadership based on a desired Recovery Point Objective and Recovery Time Objective. These objectives were determined according to business impact analysis. Full tiered list with RPO and RTO for each is attached in [Attachment E](#):

Tier 1 Systems are the systems that are prioritized for a warm site DRaaS and should become operational with 1-4 hours.

Payroll: Paylocity is our payroll vendor. If a disaster prevents the payroll staff from completing the payroll batches, Paylocity can pull the Import Payroll file for the last payroll and process that file to create an ACH file to send to the banks. Alternatively, Paylocity can process a file based on auto paying everyone. This way would only pay staff their rate times their default hours, no overtime would be included. Payroll adjustments can be made after services are restored to our time keeping services in Provide.

Disaster at a Branch Office

In the event of a disaster that affects a branch office, but the data center is unaffected most operations can continue as normal. The following provisions and decisions will need to be made by the CSO in collaboration as needed with the CEO /President, and/or other Senior leaders over the affected location.

- Salvage as much of the IT equipment as can safely be done and order replacement equipment as soon as possible.
- Make provisions for staff to work from other locations such as:
 - Staffs' own homes,
 - Other Pathfinder Locations, offices, group homes, etc.,
 - Temporary space available in the community such as community centers or libraries.
- Forward Phone calls to North Campus or some other number.
- Once arrangements are made for a more permanent office space, IT Services will plan for a rebuild of IT Infrastructure, and Internet Connections.

Attachment A: DR Playbook

The linked playbook serves as the recovery and testing procedure. Double click the image below to launch the playbook.



IT Disaster Recovery Playbook

Pathfinder Services



The 4EOS Family of Companies

This document is 4EOS controlled document. It is not intended for the client to share this document or its contents or its concepts with any entity outside of the Client Organization.

Attachment B: Failover of Phone Lines

We utilize Granite Communications for our Phone service provider and rely on measures they have put into place to make themselves resilient. See attached below for their steps taken.

Granite's nationwide network includes a fully redundant, geographically diverse, carrier-class Metaswitch softswitch platform that it uses to provide SIP-based voice over IP (VoIP) services such as Hosted PBX, SIP Trunking, Emulated PRIs, Emulated Business Lines, Direct Inward Dialing (DID) service, and Remote Call Forwarding (RCF). Granite has agreements with VoIP carriers such as Verizon Business, Level 3, Onvoy, and Inteliquent to originate and terminate voice traffic from rate centers across the country. As a certified CLEC in its own right, Granite fully complies with all federal and state mandates related to local number portability and E911.

In order to provide geographic diversity, Granite has deployed complete Voice over IP switch clusters in Los Angeles and New York City, as well as Session Border Controller (SBC) edges in Chicago and Dallas.

At a high-level, Metaswitch VoIP switch clusters consist of:

- Session Border Controllers (SBC) for industry-leading network protection and to facilitate SIP trunking to other licensed operators
- Call Feature Servers (CFS) and Enhanced Applications Servers (EAS) for IP call control, unified communications, voicemail, click-to-dial and a range of other features
- Media Resource Servers to support transcoding and media anchoring
- Universal Media Gateways for handling SS7 and PRI connections
- Service Assurance Servers (SAS) for always-on diagnostics including internal policy application as well as network protocol tracing
- Network Management System (NMS) servers for provisioning and management of the Metaswitch network elements
- Application Servers for hosting Music-on-Hold and Audio Conferencing.

The CFS supports the core IP softswitch functionality, while the EAS provides the SIP provisioning and CommPortal features. The Media Resource Server performs transcoding for G.711/G.729a coding and media anchoring. Layer 2 connectivity between all the voice/media servers is provided by a redundant dual core switching fabric with fabric extenders.

Redundancy and diversity have been designed into Granite's overall SIP architecture and topology to reduce single points of failure. Each cluster is part of an OSPF area for routing between clusters. The routing is tunneled across the Layer 3 core to interconnect the clusters at Layer 2. The diagram below illustrates the Granite VoIP architecture described above:

Attachment C: Message Broadcasting

Follow these steps to broadcast a message via text or phone and email using DialMyCalls.com

Go to: www.dialmycalls.com and log in using the shared credentials in Last Pass.

This service is prepaid, and you bank credits ahead of time or buy at time of broadcast.

1. Click on the Create Broadcast button on the Account overview page.
2. Select the type of service from Call or Text. Both will give the option to include an email when you send the message.
3. Follow the on-screen instructions that are presented to create your message or select one that was previously recorded. You should be able to type in the message or call a number and record your voice over the phone.
4. After the message is created, choose your contacts targeted for the broadcast. You can select one or more groups from among the Contacts Groups tab.
5. Follow instructions to select some additional settings like: email this message to my contacts to, or what caller ID to display and when to actually broadcast the message (i.e now or at a scheduled later time).
6. Confirm Broadcast settings, preview it and then click send broadcast now if it's satisfactory.

Attachment D: Web Site Communication Procedure

1. Notify Pathfinder's Digital Media Manager of situation and provide details for alert to be posted on Pathfinder Services.org or another appropriate web page.
2. Log into Office 365 via Admin account and create an Office 365 group *
 - a. Name the group appropriately, example: Huntington Disaster Recovery
 - b. Invite all effected and critical users and groups into the group.
 - i. Assign Owner status to CSO and any other users he delegates ownership responsibility to. User creating the group will automatically be an owner.
 - ii. Assign Member status to all other users.
 - iii. Invitations will go out via email to all invited user's Pathfinder email accounts with instruction on how to access and participate in the group.
 - c. Create and appropriately name channels according to the needs of the disaster response. Channels automatically create discussion threads by topic as well as a file structure for shared documentation that may need to be made available.
 - d. Create and maintain NewsFeed on group website.
 - e. Send link to the mobile app for Group to all essential and effected users.

*Instructions for Office 365 group creation, management and participation are provided via easy to follow onscreen step by step guides once the process for creation or acceptance of invitation is initiated by the user. Current, detailed instructions from Microsoft can be found at the site below:

<https://support.office.com/en-us/article/Learn-about-Office-365-groups-b565caa1-5c40-40ef-9915-60fdb2d97fa2?appver=MOE150>

Attachment E: Bitwarden

Log into Bitwarden account using an existing browser extension. If one doesn't exist on the browser being used, go to www.bitwarden.com and download and install the free extension and then log into team account using your individual user account. Only ITS Staff can access this and they each have their own individual user account. Nothing else needs to be published here.

Attachment F: IT Disaster Recovery Contacts

ITS Personnel

Name	Company	Position	Priority	Address	Phone	Email
Chris Kauffman	Pathfinder	CSO	Primary Contact	2824 Theater Ave Huntington, IN 46750	Office 260-356-1804 Cell 260-359-3736	ckauffman@pathfinderservices.org
Josh Goss	Pathfinder	IT Director	Primary Contact	2824 Theater Ave Huntington, IN 46750	Office 260-355-2547 Cell 260-224-9606	jgoss@pathfinderservices.org
Jim Powers	Pathfinder	System Admin	Primary Contact	2824 Theater Ave Huntington, IN 46750	Office 260-355-2548 Cell 260-359-2214	jpowers@pathfinderservices.org
Anton Talamantes	4EOS	Relationship Manager/VCIO	Primary Contact	9809 Dawsons Creek Blvd, Fort Wayne, IN 46825	Office 260 490-7740 Cell 260 452-7615	atalamantes@4eos.com
Brad Thompson	4EOS	Data Center Engineer	Primary Contact	9809 Dawsons Creek Blvd, Fort Wayne, IN 46825	Office 260-490-7740 Cell 260-449-0381	bthompson@4eos.com
Derek Felger	4EOS	Network Engineer	Secondary Contact	9809 Dawsons Creek Blvd, Fort Wayne, IN 46825	Office 260 490-7740 Cell 260 440-0132	dfelger@4eos.com

Jeremy Holle	4EOS	Interim CEO	Secondary Contact	9809 Dawsons Creek Blvd, Fort Wayne, IN 46825	Office 260 490-7740 Cell 260 804-4367	jholle@4eos.com
--------------	------	-------------	-------------------	--	--	--

Emergency Contact Information

Pathfinder Location	Critical Supplier	Contact Name	Contact Number
All	Police	NA	911
All	Fire	NA	911
Huntington	Power Company	Heartland REMC	260-758-3155
Huntington	Gas Company	Vectren	1-800-227-1376
Huntington	Telephone Provider	Granite Communications	1-866-847-5500
All	Primary ISP Provider	Metronet	1-844-684-0215
All	Alternate ISP Provider	Comcast	1-800-391-3000
All	Fire and Security Service	Koorsen Fire and Security	260-483-7557
All	Insurance Company	Assured Partners of Indiana, Christine Lang	(317) 595-7360 christine.lang@assuredpartners.com

Attachment G: Tiered Software List for Restoration

Recovery Point Objective (RPO) is the amount of work that is available for restoration in units of time.

Recovery Time Objective (RTO) is the amount of time that is desired to have a system recovered and back up and running after a disaster.

- All critical and high importance apps have a 24-hour recovery point objective and a 24-hour recovery time objective.
- All medium importance apps have a 36 plus hour RPO and RTO
- All low importance apps can be recovered as soon as possible after the other applications.

On Premises = Pathfinder Data Center.

SaaS = Software as a Service where data or system is hosted on vendors servers.

All applications and servers are documented in more detail and shared with 4EOS in IT Glue. [Click here to link to that site](#). Each 4EOS and Pathfinder IT user has an account. Below is the abbreviated list of business applications ranked for recovery.

Name	Type	Service Location	Importance	Business Impact	Application Champions
App4.Pro Planner Manager	Business Intelligence	Cloud	Low	CSO, IT Director	Josh Goss
Dial My Calls	Communications	Cloud	High	Corporate Wide	Chris Kauffman
ClassDojo	Communications	Cloud	Low	Early Learning Center	Jenna Wilkinson
Unifi Cloud Controller	Communications	Cloud	Medium	IT's Management of WAPs	Sam King
Child Plus	CRM	Cloud	Critical	Early Learning Center	Jenna Wilkinson
Salesforce	CRM	Cloud	Critical	Homeownership Center	Amy Lochner, Jeff Teusch

Bloomerang	CRM	Cloud	Critical	Marketing and Development Staff	Orion McCormack
BytePro Online	Database	Cloud	High	HOC	Jeff Teusch, Sam King
Stripe	E-Commerce	Cloud	Critical	Homeownership Center, Marketing, Accounting	Aleks Shcherbakov, Jeff Teusch
iCaremanager	ERP	Cloud	Critical	All disabilities services	Kelley Miller
Procare	ERP	Cloud	Critical	Early Learning Center	Jenna Wilkinson
Financial Edge NXT	Finance	Cloud	Critical	Accounting	Michelle Banks
QuickBooks Online	Finance	Cloud	High	Accounting	Michelle Banks
Concur Expense Management System	Finance	Cloud	High	All hourly employees	Joy Meyer, Michelle Banks
PaperSave Cloud for Financial Edge	Finance	Cloud	Medium	Accounting	Michelle Banks
Paylocity	Human Resources	Cloud	Critical	HR & Payroll; all users	Jessica Osborne, Rachel Zahm
Relias	Human Resources	Cloud	Medium	All users	Rachel Zahm
Adobe Creative Cloud	Marketing	Cloud	Medium	Marketing staff	Aleks Shcherbakov
Virtual Keypad (Koorsen)	Other	Cloud	High	Access and Alarm controls for Physical Security	Amanda Randel
Teaching Strategies Gold	Other	Cloud	High	Early Learning Center	Jenna Wilkinson
Know Be 4	Other	Cloud	Low	All users	Chris Kauffman, Sam King
Bitwarden	Other	Cloud	Medium	IT, Marketing, Accounting	Sam King

Office 365 (Word, Power Point, Excel, Outlook, Sharepoint, Teams, etc.)	Productivity	Cloud	Critical	All users	Sam King
Dynamics Field Services	Productivity	Cloud	High	Maintenance Department	Amanda Randel, Jim Powers
Adobe DC Pro	Productivity	Cloud	Low	HomeOwnership Center, FOC, Accounting and misc admin staff	Sam King
AccelTrax	CRM	On-premises	Critical	All hourly employees use it for time keeping for payroll. DSPs use it for client documentation.	Jim Powers
Provide HT	CRM	On-premises	Critical	Community Supports programs	Jim Powers
Power Plan Web	Finance	On-premises	Medium	Budget management unavailable	Michelle Banks, Sam King
Sage Employee Self Service	Human Resources	On-premises	Low	All users	Jessica Osborne
Postage Saver	Other	On-premises	Low	Administrative Assistant	Jennifer Jagger, Jim Powers
Intact	Productivity	On-premises	Low	Accounting, HR, Homeownership Center	Sam King
Faxcore	Productivity	On-premises	Low	All fax users	Josh Goss, Sam King

Attachment H: Maintenance & Test Schedule

Task	Time Frame	Responsible	Date of Last ¹	Date Validated	Validated By	Comments
UPS Test	Weekly Saturdays	IT Director	3/4/23	3/6/23	J. Goss	
Generator Test	Weekly on Friday	IT Director	9/29/23	9/29/23	J. Goss	
Generator Maintenance	Annually	IT Director	10/25/23	10/25/23	J. Goss	Performed by Evapar
Generator Battery Replacement	Every three years	IT Director	10/25/23	10/25/23	J. Goss	Handled by Evapar
Test recovery of Data Center/Data	Semi-annually	IT Director & 4 EOS	3/3/23	3/3/23	J. Goss	DR Test Completed successfully, found a few issues that are to be remediated.
DR Plan review and Update	Annually	CSO & IT Director	06/06/23	06/06/23	J. Goss	

¹ Date of Last is the date this task was last completed. If its an automated on going task, i.e daily backups or weekly generator tests, this refers to the date last confirmed at time of plan review.

PATHFINDER POLICY

Owner: IT Services
Subject: Network Security
Revision Date: April 14, 2023



1. Policy Overview

Pathfinder protects its network from internal and external security threats.

2. Information System Activity Review

Mechanisms are implemented to record and examine systems and applications which store, process, transmit, or receive private information. The IT Director ensures that information system activity is secure, retained, and reviewed on a regular basis, such as audit logs, log-in attempts, access reports, and security incident tracking reports for suspicious activity.

3. Virus Detection and Protection

Anti-virus software is installed on all workstations and configured to update automatically. Automatic notifications are sent to IT services, where appropriate investigations are conducted. Workforce members may not disable any anti-virus programs on devices that are approved for use by Pathfinder. Any malicious software identified or suspected must be immediately reported to the IT Director.

The IT Director ensures that periodic inspections are conducted of the system to ensure all virus protection and filtering software are functioning appropriately.

4. Security and Hardening Standards

Firewalls, switches, routers, and wireless access points are in place where necessary to ensure that network devices are secure and private information is isolated. Intrusion detection and/or prevention systems are employed in all sensitive network zones. These systems are configured to generate active alerts to IT services. Configuration standards are followed when setting up or servicing these devices. Changes to configurations follow the Change Management Policy and related procedures.

5. Patch Management

All Pathfinder computing resources are kept up to date with the latest vendor-supplied security patches. Guidelines are in place for ensuring computer resources such as applications, databases, and network devices are patched on a timely basis. The IT Director ensure that these systems are monitored for missing and available patches.

6. Referenced Standards

PCI: 1.1, 1.2, 1.3, 1.4, 1.5, 2.2, 5.1, 5.2, 5.3, 5.4, 6.2, 10.1, 10.2, 10.3, 10.5, 10.6, 10.7, 10.9, 11.4, 11.6

HIPAA: R- §164.306(b), R- §164.308(a), R- §164.308(a)(1)(ii)(D), A- §164.308(a)(5)(ii)(B), A- §164.308(a)(5)(ii)(C), R- §164.310(b), R- §164.312(b), R- §164.312(c)(1), A- §164.312(c)(2), A- §164.312(e)(2)(i)

GLBA: Safeguards Rule

PATHFINDER POLICY

Owner: IT Services
Subject: Payment Card Security
Revision Date: April 14, 2023



1. Policy Overview

This establishes Pathfinder's policy for securely handling sensitive credit/debit cardholder data including but not limited to magnetic strip data, Primary Account Numbers (PAN's), expiration date, and service code. This policy is intended to prevent data theft, destruction or compromise of confidential cardholder information.

2. Scope

This policy applies to all Pathfinder employees and systems used in the scope of processing payment card transactions. All such employees and systems are to be identified as In Scope.

3. Employee Access and Responsibility

Only employees designated by Pathfinder management will be authorized to conduct payment card transactions or handle cardholder data. It is the responsibility of every such employee to protect customer cardholder information from unauthorized access, modification, duplication, destruction, or disclosure. All In-Scope employees must complete PCI specific Security Awareness Training before handling transactions and annually thereafter and follow all prescribed security and privacy practices. Pathfinder's IT Director is responsible for security policy and oversight of control implementation.

All payment card transactions may only be processed using company provided technology and procedures including point of sale (POS) devices, applications or websites and follow prescribed security practices. Never leave the device, application, or website session in the middle of a transaction.

4. Passwords

Employees using approved POS devices, applications or websites must have unique passwords that meet Pathfinder's password requirements. Passwords should never be written down, always kept confidential, and never sent through any type of written communication.

5. Cardholder Data Retention and Security

Strict control is to be maintained over the storage, accessibility and internal or external distribution of any kind of media that contains cardholder data. Data will only be retained in the minimum amount and for the minimum periods required for legal, regulatory or business purposes, generally described below.

- No cardholder data will ever be stored electronically.
- Strong cryptography and security protocols, such as SSL, TLS or IPSEC, are to be used to safeguard sensitive cardholder data during transmission over open, public networks.
- Wireless devices must be set up securely by establishing secure accounts/passwords, disabling SSID broadcasts, and using the highest available encryption for the device.

PATHFINDER POLICY

Owner: IT Services
Subject: Payment Card Security
Revision Date: April 14, 2023



- All sending of unencrypted Primary Account Numbers (PAN) by end-user messaging technologies (i.e., email, instant messaging, and chat) is strictly prohibited.
- PANs must be truncated to the last four digits on paper cardholder receipts.
- The 3-4 digit authorization code on the back of the card must not be permanently recorded and any record of it should be blacked out or destroyed immediately after the transaction.
- Any written PAN temporarily noted while assisting a cardholder must be immediately destroyed after the transaction.
- All paper receipts must be stored in a locked drawer or other secure physical storage until moved to a locked storage area at the end of each fiscal year where they remain with the cash logs for a period of 7 years, after which period they are destroyed.
- Paper receipts are to be shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. Electronic media must be physically destroyed, degaussed or reformatted.
- No employee is to have access to paper receipts without prior written permission of management.

6. Incident Response

Immediately report any suspected theft, loss or other breach of cardholder data of any kind to the supervisor and Information Security Officer (IT Director) per the [Incident Response Plan](#) and email details of suspected incident to itservices@pathfinderservices.org with subject: Urgent –Suspected Security Event.

It is extremely important that all employees adhere to every aspect of this policy. Violation of these guidelines may result in disciplinary action, which could include termination of employment. Theft of cardholder data is punishable by law.

7. Device, Application and Vendor Requirements

All vendors providing any service or technology in the processing of payment cards must have a current contract that insists they are PCI compliant and understand their responsibilities for safeguarding cardholder data. Such compliance must be evidenced by an official PCI Security Council Attestation of Compliance (AoC) or other third-party proof. Each vendor's AoC must be collected and reviewed for continued compliance annually.

All contracts and in scope devices, applications and payment card processors must be approved by Pathfinder's Chief Information Officer prior to use. All vendor contracts must be logged in our digital legal file. A list of each vendor service with its described use must also be maintained.

No unauthorized equipment can be joined to the Pathfinder network or used in the processing of payment card transactions. This includes, but is not limited to POS devices, applications, web sites, modems, computers, or wireless devices. All in scope devices must be inventoried and

PATHFINDER
POLICY

Owner: IT Services
Subject: Payment Card Security
Revision Date: April 14, 2023



periodically inspected for tampering or substitution. Inventory must remain current and include make and model, location, serial number, or other unique identification.

8. Referenced Standards

PCI DSS: 2.3, 3.1, 3.2, 3.3, 3.4, 3.5, 3.7, 4.1, 4.2, 4.3, 7.1, 7.3, 8.1, 8.2, 8.4, 8.5, 8.6, 8.8, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 9.9, 9.10

GLBA: Safeguards Rule

HIPAA: A-§164.530(c), R-§164.308(a)(3)(i), A-§164.308(a)(5)(ii)(D), A-§164.512(i)(2), R-§164.312(c)(1)

PATHFINDER POLICY

Owner: IT Services
Subject: Physical Security
Revision Date: April 14, 2023



1. Policy Overview

Pathfinder has an important responsibility to protect our people, workplaces, and the confidentiality of private information and the continuity of our business. This policy outlines the basic security and protection measures that shall be implemented at every Pathfinder location, with the exception of residential settings managed by Pathfinder, which have their own Physical Security practices appropriate for a typical residence.

2. Training

Employees will receive training regarding this policy and employee responsibilities during the new hire training process and periodically thereafter as deemed necessary.

3. Facility Access Policy

Doors equipped with card readers or other electronic access control security systems require each person authorized to enter the location to have a valid access badge or fob. Employees are always to visibly display their badge while on premises. Employees must make sure that no unauthorized persons, i.e., anyone without a Pathfinder ID card, follow them through the building's entrance doors. While the card reader system used at the entrance doors is an effective control device, it cannot prevent entry to unauthorized persons following employees through the doors while they are open - "tailgating." Instances of unauthorized entry are to be reported immediately to the front desk.

Unescorted access within Pathfinder buildings, facilities, and offices is restricted to employees, approved contract staff, authorized service providers who are permanently assigned to work at the facility, and those service providers or vendors who regularly provide service at the facility. Scheduled visitors, who are properly registered to enter a facility and assigned to an employee host may walk the general access areas within reason (e.g. to visit a rest room or take a cell phone break from a business meeting).

- Each door, entrance, and exit that provides exterior access to a building or office space from the outside or from shared or common tenant spaces must be physically controlled to prevent unauthorized access.
- Emergency exits must always remain closed. Emergency exits are not to be used for nonemergency exiting or entrance to the building.
- Secured entrances and doors equipped with access control devices, such as manual locks or electronic card readers, should never be propped or left open.
- All keys or security badges that have been issued or assigned must be immediately surrendered to management or security staff when asked or be returned upon transfer or termination of employment.
- The loss of any key or badge, or suspected compromise of any lock code must be promptly reported.

PHYSICAL SECURITY POLICY

Any exceptions to this policy must be authorized and conform to the Security Exceptions Policy.

PATHFINDER POLICY

Owner: IT Services
Subject: Physical Security
Revision Date: April 14, 2023



- IT Services must be immediately notified any time an employee goes on any type of Leave of Absence, has resigned employment, or has been terminated so that his or her access can be either suspended or cancelled.
- Network jacks that are in public areas and areas accessible to visitors should be disabled and only enabled when network access is authorized by the IT Director.

4. Visitor Access

Any person that is not an employee, contractor, consultant, or other service provider permanently assigned to work at the business location (guests and visitors) entering a Pathfinder facility must sign in to ensure that a record of the visit is established. A Visitor Log is used to record all visitors. All visitors must be assigned a badge to wear during the visit and must return the badge before leaving the facility.

Unless on official company business, guests and visitors are limited to non-restricted and non-hazardous areas of the facility. In those rare instances where a visitor is to be shown or taken into a secure or restricted area, the guest must be escorted by a Pathfinder employee, the identity of each guest confirmed, and appropriate precautions taken to safeguard information assets.

5. Server Room/IT Equipment Room Access

- Access to server rooms and IT equipment rooms are restricted to only those whose job responsibilities require that they maintain the equipment or infrastructure of the room.
- Server rooms and IT equipment rooms do not double as office space or storage space or serve any other shared purpose.
- Doors to server rooms and IT equipment rooms are fireproof and secured with deadbolt type locks that can't be easily picked.
- Access to server rooms and IT equipment rooms is controlled by a strong authentication method, such as an electronic combination lock or badge reader.
- Server rooms and IT equipment rooms should not have windows through which a person could gain access. If there are windows, they should be bulletproof/shatterproof, and/or protected by metal grates to prevent access if broken.

6. Maintenance

Pathfinder will retain records to document and manage repairs and modifications to the physical security components of the facility related to security controls. This includes maintenance records relating to hardware, walls, doors, locks, and security alarms.

7. Referenced Standards

PCI DSS: 9.1, 9.2, 9.3, 9.4, 9.5, 9.10

HIPAA: R-§164.310(a)(1), A-§164.310(a)(2)(ii), A-§164.310(a)(2)(iii), A-§164.310(a)(2)(iv)

GLBA: Safeguards Rule

PHYSICAL SECURITY POLICY

Any exceptions to this policy must be authorized and conform to the Security Exceptions Policy.

PATHFINDER POLICY

Owner: IT Services
Subject: Physical Security
Revision Date: April 14, 2023



PHYSICAL SECURITY POLICY

Any exceptions to this policy must be authorized and conform to the Security Exceptions Policy.

PATHFINDER POLICY

Owner: IT Services
Subject: Sanctions
Revision Date: April 14, 2023



1. Policy Overview

Appropriate sanctions will be applied against workforce members or third-parties who fail to comply with Pathfinder's Written Information Security Program, General Health Information Privacy Policy, or any underlying policies.

2. Reporting Requirements

All workforce members are responsible for promptly reporting to their immediate supervisor any known or suspected action or practice that is inconsistent with Pathfinder Services, Inc.'s Privacy and Information Security Program or any underlying policies, including any breach of confidentiality or privacy. The supervisor must report the event to the Privacy Officer (Chief Strategy Officer) or the Information Security Officer (IT Director).

If the supervisor is not deemed to be the appropriate contact, or if the supervisor fails to respond appropriately, then reports may be made to Pathfinder Services, Inc.'s Compliance Officer who will maintain confidentiality, at 1-260-200-1271, email at cco@pathfinderservices.org, or by US Postal Mail to:

Corporate Compliance Officer, Pathfinder
PO Box 1001
Huntington, IN 46750

Individuals who accidentally violate any policy are expected to immediately self-report the incident. Failure to report a known or suspected breach will result in appropriate disciplinary action. Reporting of a potential breach out of malice will also result in appropriate disciplinary action.

3. Investigation

The Privacy Officer is responsible for investigating and evaluating the specific facts and circumstances of each incident to determine if a violation has occurred. In the event the incident involves private information or any Pathfinder electronic systems, the Information Security Officer will assist the Privacy Officer in investigating the matter. The Privacy Officer will consult with members of management and legal counsel as necessary.

4. Corrective and Disciplinary Action

Pathfinder will take appropriate corrective and disciplinary action against members of its workforce who fail to comply with its Written Information Security Program. Action taken may include additional training, the disabling of access to Pathfinder information systems, suspension, or any other action Pathfinder deems appropriate, up to and including termination. Pathfinder will report incidents involving the improper use or disclosure of private information to authorities as required by law. Violators may also be subject to legal penalties. All documentation relating to a report will be retained by the Privacy Officer and Human Resources.

5. Referenced Standards

SANCTIONS POLICY

Any exceptions to this policy must be authorized and conform to the Security Exceptions Policy.

PATHFINDER POLICY

Owner: IT Services
Subject: Sanctions
Revision Date: April 14, 2023



HIPAA: R-§164.308(a)(1)(ii)(C), R-§164.530(d), R-§164.530(e), R-§164.530(g), R-§164.530(h)

SANCTIONS POLICY

Any exceptions to this policy must be authorized and conform to the Security Exceptions Policy.

PATHFINDER POLICY

Owner: IT Services
Subject: Security and Privacy Awareness Training
Revision Date: April 14, 2023



1. Policy Overview

Security and privacy awareness training provides an overview of information security and privacy guidelines for Pathfinder employees, contractors, temporary staff, and others who access, use, transmit and/or process private information. Properly educating users aids in protecting the confidentiality and integrity of Pathfinder systems and information by helping to ensure users have a solid understanding of company security and privacy policies, procedures, and best practices. Content is designed to help employees fulfill their security and privacy responsibilities.

2. New Hire Training

Each workforce member whose job responsibilities involve accessing, using, disclosing, or requesting private information will receive privacy and security awareness training. The Human Resources department schedules privacy and security training for each new hire. New hires are required to complete this training within two weeks of being provided access to Pathfinder systems containing private health information. The IT Director, in consultation with the workforce member's supervisor, are responsible for determining the training content necessary and appropriate for the trainee to carry out their job responsibilities and functions.

Pathfinder will document and provide evidence of the completion of training and ensure it is retained for six (6) years where Pathfinder can access it.

3. Refresher Training

All workforce members will receive privacy and security refresher training annually or as otherwise appropriate. When Pathfinder makes a material change in policies or procedures, Pathfinder will provide additional training for those workforce members affected by the change within a reasonable time.

Pathfinder will document and provide evidence of the completion of training and ensure it is retained for six (6) years where Pathfinder can access it.

4. Security Reminders

Workforce members will be notified of periodic updates or changes in security policies and procedures via e-mail updates, posters, or during staff meetings.

5. Referenced Standards

PCI DSS: 9.9, 12.6

HIPAA: R-§164.530(b), R-§164.308(a)(5)(i), A-§164.308(a)(5)(ii)(A), A-§164.308(a)(5)(ii)(D), R-§164.530(b)

GLBA: Safeguards Rule

PATHFINDER POLICY

Owner: IT Services
Subject: Security Exception
Revision Date: April 14, 2023



1. Policy Overview

During the course of business, there may be instances when a process or technology must be implemented in a manner that may not comply with Pathfinder policy because compliance is either impractical or not possible. All reasonable efforts must be made to comply with all applicable regulatory requirements. Security Exception requests are only to be pursued as a last resort.

2. Request and Approval Process

The Pathfinder employee who is requesting the exception will be deemed the owner of the exception. The Owner must contact the IT Director to submit the exception request. The IT Director will hold discussions to obtain the following information:

- System or application impacted
- Policy to which the exception relates
- Business justification for the exception, including consequences if exception is not approved
- Compensating controls in place
- Is this a permanent or temporary exception; if temporary, the remediation timeline
- What processes/tasks/business areas the exception will affect

The IT Director will evaluate the risk for each requested security exception. Four factors are considered in each exception review:

- The impact of potential losses (financial, regulatory, information technology, data)
- The probability of a threat occurring
- Compensating controls
- Regulations or compliance requirements affected

After reviewing this information and holding any additional information gathering meetings/discussions with the requestor, IT services, or other relevant parties, the CSO determines if the security exception can be approved, or if other alternatives must be found, and documents this decision within the IT Risk Assessment.

Granting of a security exception does not imply that the CSO or IT services is assuming the risk for a requested exception. Approval of a security exception means that the CSO and IT services will allow the business area requesting the exception to assume the risk to their system(s).

3. Security Exception Durations

Security exceptions may be granted for a maximum of 12 months. The IT Director will monitor the expiration dates for approved security exceptions. When an exception is up for expiration, the IT

PATHFINDER POLICY

Owner: IT Services
Subject: Security Exception
Revision Date: April 14, 2023



Director will contact the requestor to obtain the following updated information:

- Compensating controls, including effectiveness
- System or application impacted
- Is this a permanent or temporary exception; if temporary, the remediation timeline
- What processes/tasks/business areas the exception will affect

The IT Director will follow the Request and Approval Process to ensure the security exception remains appropriate. If IT Director approval is obtained, the IT Director will update the expiration date for the exception.

4. Referenced Standards

PCI DSS: 12.1

HIPAA: R - §164.316(b)(1)

GLBA: Safeguards Rule

PATHFINDER POLICY

Owner: IT Services
Subject: User Identification
Revision Date: April 13, 2023



1. Overview

The ability to access a Pathfinder computer system requires the use of a User Identification Account, also known as a User ID. A User ID is a unique string of letters or characters that is used for identification purposes during the log-on process to a computer system or software application. The User ID is used to help determine whether a person is authorized to access a specific computer, application, database record or file. Various audit records exist that record the User ID information so that the person who accessed a computer or performed an action may be later identified if necessary.

The IT Director is responsible for determining the format for User IDs that will be created, issued, and used to access computer systems and applications. Format must meet applicable compliancy standards and industry best practices

2. General Requirements

The following requirements exist for all personal User IDs:

- All users will be assigned a unique personal User ID that allows access to the computer systems and applications that they have been authorized to use.
- Whenever possible, a user will only be assigned a single User ID that is common to all computer systems and applications requiring a log-on. Some users may be required to have more than one personal User ID for security reasons or because of incompatibilities between computer operating systems. The number of users requiring multiple User IDs will be kept to a minimum as will the number of User IDs assigned to any one person.
- The specific level of access granted to a user for any system, application or information resource should be approved by the user's management and if applicable, the IT Director. This access will be commensurate with the duties and job responsibilities of the individual needing access.
- The individual to whom a User ID has been assigned will be accountable for any use of the User ID.
- All User IDs that are assigned to clients, consultants, contractors, temporary staff, and other non-employees will only be authorized to access computer systems for a period of 120 days from the date of issue unless a longer activation period has been specified by the requesting manager. Regardless of the contract length or business relationship, all non-employee User IDs will be set to automatically expire annually and will require validation and re-verification by management.
- All User IDs assigned to a person who has left the organization will be immediately disabled and staged for deletion from all computer systems. User IDs will not be kept or maintained on the systems for the purpose of allowing others to use the User ID or access files, datasets, jobs, objects, or other resources associated with the User ID. All resources associated with a disabled User ID should be transferred to a new owner if the resources are needed.
- Employees who are placed on Leave of Absence (LOA) must have their personal User IDs disabled on core security authentication systems and mechanisms to prevent unauthorized use.

USER IDENTIFICATION (User ID) POLICY

Any exceptions to this policy must be authorized and conform to the Security Exceptions Policy.

PATHFINDER POLICY

Owner: IT Services
Subject: User Identification
Revision Date: April 13, 2023



-

3. Privileged Users

The following additional requirements exist for all User IDs that grant privileged access, which is defined as platform-, system-, or administrative-level access that allows the use of system control programs or features, ability to configure functional parameters for a system or application or other special purpose functionality.

- Access to privileged functions is based upon the user's job function and responsibilities.
- All users who require privileged access must be approved by the user's management and authorized by the IT Director.
- Users who are granted privileged access are assigned an additional User ID, which is different from the User ID they use for normal business purposes.
- Users who have been granted privileged access must be revalidated on a regular basis by their management to ensure the privileged access is still required.

4. Referenced Standards

PCI DSS: 8.1

HIPAA: R-§164.312(a)(2)(i)

GLBA: Safeguards Rule

PATHFINDER SERVICES, INC.

POLICY/PROCEDURE



Number: 128

Sponsor: Senior Leadership Team

Subject: **Using Electronic Signatures**

Original Date: February 14, 2003

Revised/Reviewed Date: September 25, 2019

Outlines the process and procedure for using electronic signatures.

Summary

Secure procedures shall be used to assure that an electronic signature on a client or employee electronic record verifies that the information or any changes in this documentation is attributable to the employee and an act of the employee. All of these records shall be contained in a secure computer database. In order to create or modify a record in this database an employee must authenticate to the database. This is done via a logon process where the employee provides his/her name and password. Therefore, any record that contains the employee's name is assured to have been created or modified by that employee.

Process

When a Pathfinder Services, Inc. employee electronically documents client service or employee information, the employee's signature is automatically computed based upon the employee's ID. ID files allow the creation of verifiable digital signatures on documents. These signatures assure readers of the identity of the document author.

When an employee documents a client service or employee information, a digital signature, which is a unique block of text verifying the employee's identity, is placed on this entry. The private key in a user ID file will generate this signature.

Every employee who possesses an electronic ID shall maintain a secure, unique and private electronic password for this ID.

Technical Description of the Authentication Process

The employee ID authenticates the employee and contains all the information needed for an employee to be securely identified to the Pathfinder Services, Inc. database server(s). This ID includes the employee name, password, and appropriate server certificates. Before connecting to the server, the employee must enter his/her individual password correctly. Then, to establish a connection with the server, all certificates stored in the ID are sent to the server. The server validates the certificates stored in the ID (private key) with the corresponding certificates in the Server Directory (public key) and assures that the employee is valid, otherwise access is denied. After the employee is validated (that is, the certificates are trusted), the authentication process proves that the employee really is who the employee claims to be by establishing a challenge/response dialog between the computer workstation and server.

DEFINITIONS

Electronic means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

Electronic signature means a digital symbol that is associated with an electronic record that is used with the intent to sign the record.

Employee ID is a unique binary file that identifies a legal Lotus Notes Domino server and Lotus Notes user. IDs are created at the time of employee database registration. An ID file contains the name of its owner and a public key, a private key and at least one certificate from a certifier ID. Each ID has a unique public key used for server authentication and mail encryption. The public key is stored in an ID file and in the Person or Server document for that ID in the Public Address Book. Notes client ID files contain a private key that is mathematically related to the public key stored in the Public Address Book. Information encrypted with one key can be decrypted with the other.

Certificate is an electronic stamp added to a user ID or server ID. This stamp is generated using the private key of a certifier ID that verifies that the name of the owner of the ID is correctly associated with a specific public key.

Client is an individual receiving a service provided by a Pathfinder Services employee.

Electronic Employee Information or Documentation is any electronic document that requires a digital signature, such as a Time Sheet, Performance Evaluation, or Request for Absence to validate the employee's identity.