|  |  |
| --- | --- |
|  | |
| **Document Title:** Information Technology Procedures | **Document Number:** PBO-051 |

**PURPOSE:** To support and enhance business processes and practices, privacy and security of protected information, service delivery, performance management and improvement and satisfaction of person served, personnel and other stakeholders. This procedure works to combat threats and manage risk while also ensuring efficient, effective, and consistent operations.

**SCOPE:** This procedure applies to all organizations within the Easterseals Northern Indiana Inc. network.

**RESPONSIBILITIES:**

Network Information Technology Director: To ensure this policy is updated and reflects the ongoing needs of the network.

**REFERENCES:**

**DEFINITIONS:**

**Endpoint Devices**: A computer hardware device on a network such as, but not limited to workstations (desktop computers, laptops, and then clients), servers, smartphones, tablets, printers, or other specialized hardware.

**Endpoint Security**: Approach to network security that requires endpoint devices to comply with specific criteria before they are granted access to network resources.

**Security Information and Event Management (SIEM):** Application that supplies the ability to gather security data from information system components and present that data as actionable information via a single interface.

**ENI**-Easterseals Northern Indiana Inc.

**Sensitive date**: Data that is encrypted or in plain text that contains PII or PHI data.

**Encryption**: The process of converting information or data into a code, especially to prevent unauthorized access.

**Information**: Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, verbal, or audio/visual.

**Risk of harm**: Risk to the Agency’s mission, state of compliance, finances, operations and/or reputation.

**Agency Information**: Agency-owned information or information made or received in connection with the transaction of Agency business by an Affiliate of ENI. Data, information, or records maintained by the Agency in any medium or form.

**External Network**: A network not controlled by the Agency.

**Protected Health Information:** Tier 3 information covered by the Health Insurance Portability and Accountability Act (HIPAA).

**Sensitive Information**: Sensitive information is defined as Tier 2 or Tier 3 information as defined in the Information Classification Policy that is protected against unwarranted disclosure. See the reference links below for assistance in recognizing and managing sensitive information at the Agency.

**Unsecure Medium**: A transmission method, or storage, networking and/or computing device, which does not meet the requirements of a Secure Communication Protocol.

**Users:** All Agency affiliates/constituents including, but not limited to, faculty, students, staff, temporary employees, contractors, outside vendors, and visitors to campus who access Agency-owned or Agency-managed digital information

**PROCEDURE:**

**Configuration Management**

Endpoint security management is an approach to network security that requires, and ensures, endpoint devices comply with specific criteria before being granted access to the network. Endpoint security is an important aspect of maintaining the confidentiality, integrity, and availability of information. The increasing ease and prevalence of a mobile-enabled workforce makes it more important than ever to protect endpoint devices and the security posture of IT systems. ENI Information Technology Services will use baseline controls and standards established by NIST SP 800-53R4. All Agency owned devices will be installed with Kaseya RMM for bulk and remote management.

**Data Breach:**

ENI’s intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how ENI established culture of openness, trust and integrity should respond to such activity. ENI is committed to protecting its employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

This policy mandates that any individual who suspects that a theft, breach, or exposure of ENI Protected data or ENI Sensitive data has occurred must immediately provide a description of what occurred via e-mail to [Helpdesk@esarc.org](mailto:Helpdesk@esarc.org) or using the End User Service Portal. This e-mail address, phone number, and Service Portal are monitored by the ENI IT department. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach, or exposure has occurred. If a theft, breach, or exposure has occurred, the Information Security Administrator will follow the proper procedure in place.

**Theft, data breach or exposure:**

As soon as a suspected theft, data breach or exposure containing ENI protected data or ENI sensitive data is identified, the process of removing all access to that resource will begin.

The network IT director will chair an incident response team to manage the breach or exposure. The team will include members from the following areas:

* Executive Management
* IT
* Finance
* Legal
* Human Resources
* Communications
* The affected unit or department that uses the involved system or output or whose data may have been breached or exposed.
* More departments based on the data type involved, Additional individuals as thought necessary by the Executive Director

The president of operations will be notified of the theft, breach, and or exposure. IT along with the designated forensic team will analyze the breach or exposure to determine the root cause. ENI will work with cyber insurance to access forensic investigators and experts that will determine how the breach or exposure occurred; the type of data involved; number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

**Develop a communication Plan:**

ENI executive management will decide how to communicate the breach to a) internal employees, b) the public, and c) those directly affected.

* **Sponsors** - Sponsors are those members of the ENI that have primary responsibility for maintaining information resources. Sponsors may be designated by any ENI Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
* **Information Security Administrator** member of the ENI team, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
* Users include virtually all members of the ENI community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees, and volunteers.
* The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure; Communications; Legal; Management; Financial Services, Programs; Human Resources, and Executive Management.

**Disaster Recovery:**

To ensure business continuity, IT will maintain a standardized backup system for all servers containing critical systems or data. This system will be configured to create differential backups of all server systems hourly from 6:00am to 6:00pm that are stored on a local appliance on-site. Each evening those backups are synchronized out to a cloud provider for long term storage. All backup images should be encrypted fully both on the local appliance as well as the cloud provider.

In the event of data loss, one or more of the following options can be used depending on the severity.

* Individual files or folders: If a user notifies IT of a small-scale loss such as this, an image of the drive in question will be mounted with network accessibility to copy the lost files/folders back to their original location.
* Full server loss: A virtual image of the full server can be brought up in the local appliance and continue being used by the staff as the server itself is restored back to its original location or to new hardware. Once the restoration is complete, any differential changes made to the temporary VM will be merged into the restored version.
* Full site loss: In the event of a full loss of the building and all equipment, every server will be spun up in the cloud provider and made available for all staff to access from a temporary worksite until new equipment can be sourced and deployed. Once new hardware is available, all servers will then be restored to said hardware with all changes merged.

**Data Disposal:**

To support proper cleaning or destruction of sensitive/confidential data and licensed software on all computer systems, electronic devices and electronic media being disposed, recycled, or transferred either as surplus property or to another user.

ENI requires that before any computer system, electronic device or electronic media is disposed, recycled or, transferred either as surplus property or to another user, the system media, or device must be either:

* Properly sanitized of agency sensitive/confidential data and software, or properly destroyed.
* Any official agency records must be appropriately kept / disposed of based on the agency’s records retention policy prior to erasure or destruction of the system, device, or media.

Electronic media must be sanitized following the guidelines in [NIST Special Publication 800-88, “Guidelines for Media Sanitization”](http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=917935) . The specific procedures and requirements to be followed when cleaning or destroying computer systems, electronic devices and electronic media are found in the Electronic Data Disposal Procedure document.

**Electronic Equipment Disposal:**

As of January 1, 2011, the State of Indiana prohibit the discarding of electronic waste (computer monitors, laptops, desktops, printers, etc.) in general waste receptacles. All electronic waste must be disposed of at an approved electronic waste collection facility.

Electronic waste not containing ePHI (motherboards, processors, etc.) is packaged and stored in the IT department’s storage area. Once there is enough in storage, we call for a pickup from the recycling company.

**Data Encryption:**

All agency owned devices should be encrypted at the drive level by default, storing the decryption keys via the central management system within the endpoint security system.

**Endpoint Security**

Endpoint security management is an approach to network security that requires, and ensures, endpoint devices comply with specific criteria before being granted access to the network.

Endpoint protection is an important aspect of maintaining the confidentiality, integrity, and availability of information. The increasing ease and prevalence of a mobile-enabled workforce makes it more important than ever to protect endpoint devices and the security posture of IT systems. The ENI Information Technology Services will utilize baseline controls and standards established by NIST SP 800-53R4. All agency owned devices will be installed with Bitdefender for security management. Any attempt by personnel to circumvent or otherwise bypass this endpoint protection policy will be treated as a security violation and subject to investigation. The results of the investigation may entail written notice, suspension, termination, or possibly criminal and/or civil penalties.

**Purchasing Assignment and Usage:**

1. **Introduction**
2. All technology at ENI valued over $499.99 must be purchased by the IT department, all technology equipment purchased is owned by ENI and is the property of the original purchasing department. Equipment may be provided to a staff member while he/she is employed by the company. As such, the supervisor or department head handles maintaining knowledge of the location of the equipment.
3. When equipment is distributed to a department, the user will be required to sign for responsibility for maintaining location of the equipment.
4. Each year IT conducts a “Technology Refresh.” At that time, aging equipment is replaced with new, and the cost is budgeted to the department it is being issued to. For depreciation purposes, the new equipment is assigned and becomes the property of the department with the replaced equipment.
5. When technology equipment is replaced or reassigned, the equipment in question must be returned to IT. The equipment cannot be passed from one user to the next, even within the same department, without being formally reassigned.
6. IT will evaluate returned technology equipment to determine it’s remaining life and appropriateness for reassignment. Technology equipment that does not meet reassignment standards will be disposed of in compliance with the Technology Disposal Policy.
7. Technology equipment that is considered appropriate for reassignment may be reassigned (also known as trickle down) to an individual within the department that funded the original purchase. Or to another department where it may be needed.
8. When a staff member leaves a department, his/her technology should remain in the former department unless the two department heads have negotiated that the person will bring their old technology with them to the new department. If this happens, the former department head must inform IT, and remove inappropriate data from the hard drive of the equipment.
9. When a staff leaves a department, If the equipment is of the mobile nature, it must be returned at once to the IT. If the equipment has reached IT depreciated value, that equipment will go into a pool for potential redistribution. Equipment that has not been fully depreciated, will be held for the department awaiting new hired staff.
10. IT keeps an inventory database of the location of every piece of technological equipment. It is essential that technology is not moved to a new department without the knowledge of IT.

## **Pool of Reassigned Technology Equipment**

1. Technology equipment that is determined to have remaining life and will not be trickled down to an individual within the department that originally purchased it, will be placed in an inventory pool for reassignment elsewhere at ENI.
2. IT will re-format the equipment with a clean operating system (appropriate for the processing ability of the equipment) and a standard software image.
3. Technology equipment that is placed into the reassignment pool does not carry a manufacturer’s warranty. IT does not provide any operating guarantee on the reassigned technology equipment. Additionally, this equipment may or may not appropriately support new or upgraded software applications.
4. Departments that want to upgrade memory, hard drives or other aspects of the reassigned technology equipment will handle the associated costs. Upgrades may not result in extending the life of reassigned technology equipment.
5. Reassigned technology equipment is older technology that has been heavily used by an earlier user. As equipment ages, it is more likely to have operating problems and failures. Reassigned technology equipment will be slower than new equipment. There may be situations in which IT will recommend newly hired staff in a department purchase a new computer rather than using a reassigned machine.
6. **Eligibility to receive reassigned technology equipment from the inventory pool.**
7. Priority is:
   * 1. Break-Fix/No Machine
     2. Primary Computer –individual staff, group home or community living site
     3. Used for Instructional Support or computer lab.
     4. Secondary Computer

1. **Process for technology to be Recycled.**
   1. Departments that originally funded the purchase of technology equipment may want the equipment to be reassigned within their department. Requests to trickle down technology within the department that originally funded should be made with the Trickle-down Technology Equipment form located on the Information Technology Services website.
   2. IT will pick up the equipment to conduct an evaluation. Technology equipment that does not meet reassignment standards will be disposed of in compliance with the Technology Disposal Policy.
   3. Technology equipment that is deemed appropriate for reassignment may be trickled down to an individual within the department that funded the original purchase. However, the technological equipment must first be returned to IT for evaluation and optionally for the hard drive to be wiped and re-formatted. Departments wishing to retain any data should copy it and then restore it after the technology has been returned to them.
   4. Prior to distribution of the reassigned technology equipment, IT will wipe clean all data including all files and licensed software from the equipment.
   5. IT is not responsible for any loss of data stored on computer devices that have been returned for reassignment. Per policy, data is to be stored only on department SharePoint group drives or Individual OneDrive.

**Hardware and Software Maintenance:**

Hardware and software maintenance and support arrangements shall be required for all standard and non-standard, servers, network infrastructure equipment, peripherals, and related software. This shall include applications and systems that are subject to their own proprietary maintenance and upgrade policies.

## Server and Network Hardware

Director and staff shall ensure:

All infrastructure desktop, servers, peripherals, and network hardware (switches, routers, firewalls) are covered by on-site warranty agreements with appropriate response times to meet business continuity needs.

Defective items under warranty are repaired in a timely fashion.

Repairs or surplus of equipment not covered under current warranty meet all protocols and procedures under the direction of Director shall centrally procure and install all network and departmental computer hardware including but not limited to desktops, servers, audio-visual, security, laptops, printers, scanners, monitors, keyboards, and mice. This shall ensure:

* The equipment is compatible with existing hardware standards and current software.
* Hardware and software standards are enforced.
* Equipment is covered under appropriate warranty and maintenance support agreements.
* Configuration management and security policy implementation are consistent and minimize organizational risks.
* The equipment is properly configured and has appropriate security controls/software.

IT staff shall be responsible for the installation and maintenance of all ENI agency software as well as the following:

* Adhere to configuration standards for all system components that address all known security vulnerabilities and are consistent with industry accepted definitions.
* Periodically update system configuration standards as new vulnerabilities are identified.
* Install and maintain system and end-user software.
* Maintain appropriate software license records for compliance purposes.
* Fully test applications to ensure they are compatible with and run on standard agency hardware.
* Subscribe to vendor software maintenance programs where appropriate and applicable.
* Tune and analyze operational software configurations for optimum performance.
* Ensure software and user data are fully backed in accordance with the Data Backup Policy
* Update critical Security system patches within 7 days of release.
* Update manufacturer recommended feature patches within 30 days of release.
* Update feature patches on an as needed basis
* Patches shall be tested before deployment to production environments.
* Ensure third party vendors and contractors work in conjunction with the infrastructure and uphold all policies and procedures.

Individuals seeking exceptions to this policy must seek approval from Director and the System Administrator PRIOR to purchasing any specialized, non-standard hardware, software, or equipment. Support for non-standard hardware, software, or other equipment shall be assessed and agreed upon on a case-by case basis by Director and if needed the Easter Seals Steering Committee.

**Remote Access:**

All remote access tools used to communicate between ENI assets and other systems must comply with the following policy requirements.

**Determining eligible users**

Only users with a demonstrable business need to connect to company resources shall be provided with remote access capabilities. This will obviously apply to offsite workers by default, but onsite workers should be screened accordingly. Users with access to credit card data, for instance, may be ineligible for remote access capability if this would pose a security or financial risk. Users whose job responsibilities involve hands-on or face-to-face interaction may also be restricted from remote access privileges.

Employee eligibility to remotely access the organization’s computer network will be determined by their respective managers. The IT department must also approve each staff member’s remote access use.

**Determining appropriate remote access software**

The IT department should utilize standard remote access software (Forticlient VPN, for instance) and maintain a standard set of documentation to assist users in installing and using these products. The software should match the operating system environments in use at the organization (or upon employee-owned devices, if applicable); common examples are Windows, Linux. and Apple OS X. It may also be necessary to utilize remote access software on Android and iOS operating systems used by mobile devices.

Remote access software should prohibit split tunneling (accessing two networks at once), but instead should limit connecting devices to work upon company networks only.

**Remote access standards**

The use of equipment and software provided by the organization for remotely accessing the organization’s computer systems, network, and data is limited to authorized persons and only for purposes relating to fulfilling organization business and operations.

Remote access user accounts should be configured with complex passwords and set to lock out upon a set number of authentication failures (five, for example). Screen saver passwords should also be employed.

The IT department should ensure that all devices that will connect to the company’s networks or resources via remote access do not have third-party software or applications that pose a threat to the organization’s systems and networks or that could introduce application incompatibilities. If possible, periodic monitoring of these devices should be conducted to ensure they continue to meet compliance standards.

The IT department must ensure that all devices used for remote access have appropriate anti-malware and security software with the appropriate controls and that no existing infections are present. Anti-malware, application, and operating system updates should also be applied to the device(s) regularly (this will be the employee’s responsibility if they are the device owners) and where possible the IT department should monitor to ensure compliance.

The IT department must ensure that all remote access devices are properly encrypted if the potential exists for the device to save, cache, or temporarily store organization data.

The IT department must log all activity of any devices configured for remote access and maintain these logs for at least 90 days (about 3 months). These will be provided to the security department upon request if needed.

Where possible, two-factor authentication should be utilized to increase the security of remote access connections. Passwords, tokens, and other authentication elements should rotate frequently. These should never be saved on any devices but reentered each time remote access is established.

## Personal computer and equipment use

At no time will a user be allowed to use a personal computer, or any computer not owned and managed by the agency, to access the agency network or servers remotely or locally.

**Remote access authorization and implementation process**

* Whenever any organization user—whether a full-time employee, executive, contractor, consultant, or volunteer—wants to use an organization-owned/provided device to connect to the organization’s networks, systems, and resources, the following steps must be completed:
* The user must get approval from their manager for remote access.
* If the manager approves the request, it should then be sent to the IT department. No individual, staff member, or user other than the organization’s IT director may authorize software or hardware for remote use within the organization.
* The IT department will provide the user with the necessary documentation and/or support for getting remote access software running and confirmed functional.

**Remote access user responsibilities**

Only authorized company personnel are to use company-provided equipment or to access company systems and networks.

If a user believes equipment used to remotely access ENI’s resources, systems, and networks might be infected with a virus, spyware infection, or other malware threat or that it might be somehow compromised, they must immediately notify the IT department of the potential security risk and make the equipment available for analysis and remediation.

If a user loses or misplaces equipment authorized to remotely connect to the organization’s resources, systems, and networks, they must immediately notify the IT department of the potential security risk. It will then be the responsibility of the IT department to remotely wipe the device(s), change passwords, or lock the user’s account as needed.

If the device(s) involved are employee-owned, it will be the responsibility of the employee to seek and fund replacement items.

**Monitoring**

The IT department and managers will monitor for adherence to this policy through both electronic and hands-on means where applicable.

## Compliance Measurement

The IT Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audit, and inspection, and will provide feedback to the policy owner and appropriate business unit manager.

**Exceptions**

Any exception to the policy must be approved by Remote Access Services and the IT Team in advance.

Failure to comply with this standard may put ENI’ information assets at risk and may have disciplinary consequences for employees, up to and including termination of employment. Contractors, vendors, and others who fail to adhere to this standard may face termination of their business relationships with ENI.

**Hardware and Software Maintenance:**

Protected Health Information (PHI) and other Sensitive Information (SI) (data classified as Tier 3 or Tier 4 in the ENI Information Classification) that is transmitted or received by ENI (the Agency’s) computer systems, including mobile devices, must be encrypted in accordance with the ENI Standard for the Transmission of Protected Health Information and Sensitive Information when transmitted over external networks or an unsecured medium.

Sensitive Information, as defined below, in all IT forms – written, spoken, electronically recorded, or printed – must be protected from accidental or intentional unauthorized modification, destruction, or disclosure. This policy statement addresses specifically the risks to privacy inherent in digital technologies.

ENI requires all Users to protect the Agency’s Sensitive Information by adhering to the attached Procedures and Standards.

Users who are third-party contractors and vendors must be made aware of this policy and their responsibilities for safeguarding the Agency’s Sensitive Information.

**Sensitive Information:** Sensitive Information includes all data, in IT original and duplicate form, which contains:

* “Personal Identifying Information,” as defined by the North Carolina Identity Theft Protection Act of 2005. This includes employer tax ID numbers, driver’s license numbers, passport numbers, SSNs, state identification card numbers, credit/debit card numbers, banking account numbers, PIN codes, digital signatures, biometric data, fingerprints, passwords, and any other numbers or information that can be used to access a person’s financial resources.
* “Protected Health Information” as defined by the Health Insurance Portability and Accountability Act (HIPAA).
* “Customer record information,” as defined by the Gramm Leach Bliley Act (GLBA).
* “Card holder data,” as defined by the Payment Card Industry (PCI) Data Security Standard.
* Information classified at tier 3 or tier 4 of the Agency Information Classification Policy.

Sensitive Information also includes any other information that is protected by IT policy or federal or state law from unauthorized access. Sensitive Information must be restricted to those with a legitimate business need for access. Examples of Sensitive Information may include, but are not limited to, Social Security numbers, system access passwords, some types of research data (such as research data that is personally identifiable or proprietary), public safety information, information concerning select agents, information security records, and information file encryption keys.

**Wireless Communication:**

**General Requirements**

All wireless infrastructure devices that reside at an ENI site and connect to a ENI network, or provide access to information classified as ENI Confidential, or above must:

* Abide by the standards specified in the Wireless Communication Standard.
* Be installed, supported, and maintained by an approved support team.
* Use ENI approved authentication protocols and infrastructure.
* Use ENI approved encryption protocols.
* Maintain a hardware address (MAC address) that can be registered and tracked.
* Not interfere with wireless access deployments maintained by other support organizations.

**Public Wireless Device Requirements**

There are a several problems with using a public Wi-Fi network. The open nature of the network allows for snooping, the network could be full of compromised machines, or the hotspot Itself could be malicious.

* Connection to unsecure public wireless infrastructure is prohibited when interacting with ENI Service’s resources.
* Transmission of any Agency related information must be done over a secure network infrastructure only.

**Home Wireless Device Requirements**

1. Wireless infrastructure devices that provide direct access to the ENI corporate network, must conform to the Home Wireless Device Requirements as detailed in the Wireless Communication Standard.
2. Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibit direct access to the ENI corporate network. Access to the ENI corporate network through this device must use standard remote access authentication.
   1. All home wireless infrastructure devices that provide direct access to a ENI network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:
   2. Enable WIFI Protected Access Pre-Shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
   3. When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point.
   4. Disable broadcast of SSID
   5. Change the default SSID name.
   6. Change the default login and password.