

**ENI Information Technology**

**Infrastructure Overview, Risk Planning, and 2023 Technology Plan**

**Introduction**

Easterseals Northern Indiana (ENI) has made great strides over the last few years regarding Information Technology and plans to continue to improve in this area. The goal being, to make the necessary use of information systems be as minimal as possible to allow our front-line caregivers to focus more on the client.

Core systems have been streamlined and added redundancy and resiliency. Business continuity has been greatly improved and been given cloud redundancy.

**Infrastructure of main systems**

Virtualized servers in a redundant cluster

* Increased server density – One physical server (a host) that operates as a hypervisor can run many virtual machines (VM’s). Virtual machines may be any type of server, such as a web server or a database server.
* Virtual machines are easily able to be moved from one physical server to another. This is helpful in the case of a server failure as they will be moved automatically if one host fails
* Virtual machines support snapshotting – which allows changes to be rolled-back in a previous point in time. This is useful when making significant changes to a VM and the changes did not go as expected.
* Increased disaster resiliency – The guests can be backed up as a whole machine and restored quicker in the event of a disaster.

The backbone of our system is formed by using a high-performance Storage Attached Network (SAN) and a group of identical servers that are grouped into a cluster. The SAN takes care of the storage needs of the cluster by storing the data of all the virtual machines using high speed, high resiliency solid state drives. These drives are far faster and far more failure proof than standard hard drives as they make use of chips to store and rapidly retrieve data as opposed to spinning platens.

The SAN is attached to the server cluster by means of fiber optics and two redundant switches as well as two redundant controller modules and power supplies. This allows the SAN to be resilient to switch failure, controller failure as well as power supply failure

The cluster of 3 physical host machines that run our virtual machines connect to the network on multiple high speed 10Gb network cards connected to multiple switches to allow redundancy for both the network cards as well as the switches. This eliminates either as a single point of failure the servers network connections.

The cluster itself utilizes VMWare’s vSphere ESX with a vCenter acting as the central management point for all the hosts. The vCenter also handles the automatic migration or “failover” of the VMs from one host server to another should something happen to one host of the cluster. This process is seamless from the end users’ point of view. The VM can be moved without it ever shutting down or losing connectivity.

Another positive aspect of the cluster setup is that it is scalable. This means that as we expand and require more computing power to support more users and/or more functions, we can add another physical host to the cluster to spread the load across more physical hardware. We can add a nearly infinite number of additional hosts to the cluster to allow for growth in the future.

The cluster and VM setup also allow us to quickly create new virtual servers quickly and easily for any use case that may arise. It gives us the ability to create additional remote desktop servers very quickly as needed to support the ever-growing number of users.

This infrastructure allows us scalability, redundancy, and rapid deployment to support any growth or changes that the agency experiences in the future.

**End user machines and remote connectivity**

The current setup always for multiple options for remote connectivity to the network. The first being the use of a VPN client installed on the user’s mobile workstation. This method will allow for a direct encrypted tunnel from the machine to the network and allow the user to operate as if they are in the office from anywhere. The second method is the one being widely used by our DSPs both within the office as well as from the group homes. This is the Remote Desktop Server. This service always the users to remotely connect to the RDS (remote desktop server) and run a virtual desktop instance with everything they need to do their work. The bonus for this is that we can make use of small, inexpensive thin client devices that require no real setup or maintenance to operate.

**Wireless connectivity**

ENI has a widespread wireless network that spans all locations. Great care was taken in site planning and the vendor selection process. It is a fast and secure system that uses industry leading components to provide Wi-Fi to both our consumers and employees.

**Security Cameras**

Most locations and group homes currently have cameras recoding 24/7 and are accessible with software for QA purposes. There is currently a plan in place to replace all these cameras with a single unified system for all agencies and locations to allow a central management and access platform to access any camera anywhere. We are currently working with vendors to get quotes. Tentatively planning to begin the changeover process in the second half of the year.

**Redundancy of internet/firewall solution**

ENI currently has two separate 1Gb internet connections from two different vendors. This allows for redundancy on the provider as well as redundancy on our firewalls. The current firewalls are in the process of being replaced with upgraded firewalls with more functionality and increased security features. These will be in place within the next 1-2 months.

**Cloud based Software as a Service (SaaS)**

Currently, we are only making use of Microsoft 365 for email and some collaboration via Teams. However, we are working on or planning to, move several of the internal systems to the cloud.

Currently we are in the process of migrating shared files as well as the intranet page and all it contains to the Microsoft SharePoint Service. This will be completed in the next 2-3 months.

We are also vetting replacement vendors for the Acceltrax/Provide practice management systems. All the current front runners for that replacement are a SaaS cloud-based system.

**Document Storage**

Many of the forms currently in use have been converted into some form of electronic version. Some of these are in excel, some in Formstack and others as word documents. We are currently exploring options to move everything to a centralized platform that would allow any form to be created as well as digitally signed. This should streamline the process as well as eliminate most needs for a hardcopy of a form.

**Phone system**

Our current internal hosted and managed phone system is in the process of being replaced. The new system will be cloud based and hosted. This new system is being implemented at all agencies and all locations to all extension to extension dialing from any location to another. This will also allow us to add all group homes as internal extensions as well. It will also allow us to make use of “soft phone” apps on either the desktop or smart phone for any employee that wishes to do so or routinely works in different locations or remotely from home.

**Risk Planning**

As a healthcare related business, we maintain private information on clients in our system and need to protect that to the best of our ability. The risks associated with the storage of data are:

* Potential intrusions from the outside: Exposing any system (such as our email, or our client system such as Accel) is a potential source of a breach. The use of firewalls and encryption to limit these is currently being utilized. Implementing multifactor authentication for all access is another way we are and continuing to mitigate those risks.
* Critical loss of equipment: This includes such things as server failures or catastrophic conditions from fire, the weather, etc. The disaster recovery plan describes the steps required to return to a functional status. As a CARF accredited agency, we must also have a disaster recovery plan in place. We review this plan on a quarterly basis to update it for any changes. We also regularly test our cloud-based backups of the servers and data integrity.
* User or administrative error: Deletion of files, overwriting of files, etc., are an inevitable occurrence. To mitigate this, we are running incremental backups every hour and backing those up from the local appliance to the cloud every night. At any point we can restore a single file back to any given point in time or restore a complete server.
* We currently have a Cyber liability insurance policy to cover any issues that do make it past our rigorous security procedures. The policy we have covers security breaches, client privacy violations, and employee privacy violations.

**Backup & Disaster Recovery:**

**Overview:** ENI depends greatly on information technology resources to conduct business. In the event of a disaster such as theft or fire that would result in the loss of information, it is critical that these systems are restored in a timely fashion. This document describes the procedures in place to handle recovery operations.

**General Procedure**: ENI relies on a backup appliance for backup and recovery purposes. Due to cost considerations, there is no spare equipment stored at a separate location for replacement. Therefore, ENI has standardized on one brand of servers to ease the replacement process. The backup and restore policy includes the following:

• Datto backup agent runs an incremental backup of every server, once per hour throughout the day. These are appended to the server image for each server to allow for a full restore of the server to any of those backup points.

• Each of those backups is copied to the cloud storage every night. Those images are then powered up as a virtual server within the cloud system each night to verify that it is working and booting correctly.

• An email notification is sent out to the Tech Staff any time there is a discrepancy in the backup or verification process for any server.

**Precautionary Measures**:

• All servers have various levels of RAID and redundant power supplies to protect against drive failures and provide continuous operation in the event of a failure.

• Multiple domain controllers are present. If one fails, another one can authenticate users without interrupting operations.

• All servers are protected with a UPS system. At full load the UPS system is able to deliver 15 minutes of run time. We are exploring options to replace the current battery UPS system with a generator/battery system that would allow for continued operation for much longer if needed

• Servers and networking equipment are in limited access areas that always remain locked.

**Recovery Procedures:** To reduce the impact to users and configuration changes required, any server recovery will make no changes to the restored server. Server names and IP addresses will remain the same after the recovery.

* Single server failure
  + VMs automatically migrated to another host in the cluster.
  + The server will be assessed for either repair or replacement
  + New or repaired server will be merged into the cluster and begin hosting VMs
* Catastrophic loss such as fire, flooding, or theft
  + Begin procedures for backup image hosting by backup vendor Datto
  + Spin up all servers within Datto hosting
  + Open preconfigured access for users to hosted virtual network
  + Procure replacement hardware
  + Reinstall cluster host system
  + Reload server images from hosted cloud to cluster
  + Estimated down time 1-2 hours

**Hardware-Software Replacement/Upgrades:**

**Hardware:** Hardware is reviewed on an on-going three to five year cycle depending upon the equipment, need, and/or usage. Lifespan of the equipment is also taken into consideration.

Personal computers are evaluated over a three to five year period. Depending upon need, replacement cost, or upgrade feasibility; the appropriate plan of action to proceed is decided upon. A detailed inventory of equipment is kept and reviewed quarterly.

**Software:** Application software purchases are made when warranted by a particular need. End-user application and operating software are kept up-to-date with centralized servers that deliver updates out to all systems.

Vendor packages are reviewed by key staff to assess their usefulness to the agency prior to purchase and implementation. Maintenance and upgrade protection are also evaluated and taken into consideration.

Networking and server software is evaluated and usually updated to the newest release when deemed to be mostly bug-free as to keep in tune with the latest technology. Compatibility with older applications is also taken into consideration prior to updating.

Software assurance and upgrade protection are purchased to lessen the financial impact of upgrading to newer versions. Software licensing contracts are purchased and updated as necessary. This is monitored closely and reviewed at budget preparation time each year for renewal purposes.

Downloading and installing applications or other unauthorized software from the Internet is strictly prohibited except when approved by the Tech department.

**Security:**

**Overview:** ENI utilizes information technology for nearly every aspect of administrative and program service delivery. Given the nature of the confidential information stored and accessed, it is imperative that strict controls are in place to maintain the integrity and security of the information collected. This document describes the security policies in place to address these concerns.

**Network Access**: There are three methods to access ENI’s network:

• Locally, through the local area network

• Remotely, through virtual private networking (VPN)

• Wirelessly, through various wireless access points within the main buildings

The following policies apply to all the above connection types:

• A username and password in required for access. The password must not be  
 disclosed. Multifactor is required to access some systems

• Requests for new accounts must be arranged through the IT department.

• Managers and supervisors must notify the IT department in a timely manner when a job termination occurs, so that network account access can be restricted or eliminated.

• Manager and supervisors must notify the IT department when job transfers occur. The IT department will then make the necessary modifications to user security levels depending on the new job role.

• User accounts have the following settings:

* + Minimum length of 8 characters
  + Combination of letters and numbers is required
  + Passwords are forced to change every 90 days
  + Accounts are locked after five incorrect login attempts
  + Passwords cannot be repeated

The following applies to VPN connections:

• The default setting is to disallow VPN access to ENI’s network.

• Users requesting remote access will have their needs reviewed and if approved will be granted VPN access.

The following applies to wireless connections:

• The wireless network is password protected using WPA2 security.

• The passkey is not given out; the IT department sets up access to the wireless network for the user.

**Internet and Email Security:**

ENI’s internet service is provided on two separate 1Gb Fiberoptic lines from two separate vendors. In the event of a failure of circuit, the connection remains operational at a reduced throughput until the downed circuit for that vendor is repaired. This provides a level of fault tolerance for internet connectivity.

A Cisco Firewall is utilized in granting and denying access to internet resources.

• All internet connection traffic and web sites visited are logged. Web sites are not actively filtered or blocked at this time, however we have the ability to do so if deemed necessary.

**PC and Laptop Security:**

To reduce downtime, ease manageability, and provide a productive environment requires policies that balance the needs of the users with potential security concerns. All computers have the following baseline of features:

• Password protected screensavers are set to activate after 15 minutes of inactivity.

• All users are given lowest level of access when possible. Certain software applications require elevated user rights which are reviewed before being granted.

• Group security policies are enforced agency wide to restrict users from making changes in the configuration of the computer.

• A centrally managed antivirus solution is installed on every computer. The antivirus client is password protected and cannot be disabled or removed. We will be adding an extra level of security via an Endpoint Detection and Response agent. We expect to have that in place in the next 1-2 months

• A remote management and monitoring and asset management system keeps detailed records of every device on the network. This also will push patches, security updates and software install to any and all workstations.

• A home drive is provided for file storage for all users. This is backed up on the same schedule as the servers. However, we will be migrating this to the Microsoft SharePoint/OneDrive cloud system. We expect to have the project complete before the end of 2023

In addition, the user has the responsibilities of:

• Notebooks must be stored in a physically secure environment.

• The use of USB thumb drives to store client records is forbidden.

• Any damage incurred to the equipment must be reported to the IT department.

ENI also makes extensive use of thin clients and Chromebooks. These accounts are provided a customized desktop and have a very high level of security.

**Systems Security:**

All of ENI servers are located in a locked and climate controlled room for security and increased life. Only during maintenance are the console screens unlocked for access. Additionally, only select IT staff has access to administrative passwords.

Servers are constantly monitored for performance and other related security threats. Audits are performed regularly to determine if directories and files have necessary rights in place. The disaster recovery plan discusses policies and procedures for the protection of agency data.

Servers are regularly patched when security/product updates are released by vendors.

**Virus Malware Protection:**

**Overview**: ENI relies on Bitdefender for virus protection. A support agreement provides continual updates to virus signatures on a daily basis. These updates are then pushed and installed to all agency computers and servers. All incoming emails are also scanned by both the Microsoft 365 system as well as the Bitdefender agent on the endpoint.

**Actions**: Policies are enforced to perform the following on each computer:

1. Delete an infected file if found
2. If delete fails then quarantine the file
3. Computer virus signatures are continually updated and managed via a centralized server
4. Users are unable to inactivate, uninstall, or change settings of the virus software
5. Workstation drives are encrypted

**Deployment:** The antivirus software is installed on every computer and server under agency control.

**Notification:** Whenever a threat or virus is detected, the IT staff is automatically emailed the details of the infection and the actions performed by the virus software.  
  
**Automatic scanning:** The antivirus software performs a full scan on a daily basis on every computer within the agency.

**Projects for 2023**

* Move to new remote management and monitoring system, helpdesk and asset manager
  + Kaseya VSA asset management and RMM - March
  + Autotask PSA Helpdesk – March
  + IT Glue self service portal for documentation – March
* Migrate from Cisco firewall to Fortigate Firewall -- March
* Move to unified phone system
  + Cardinal – February
  + Coldwater/PDG – March-April
  + Rise – March-April
  + Passages – March-April
* Migration of shared file storage from internal server to SharePoint/OneDrive -- April
* Migrate from Dynamics GP to Sage Intact – April-May
* Complete implementation of multifactor authentication – June
* Migrate to new Practice management software – May-December