
# Information Technology Policy Manual

**Approved by the Board of Directors: February 13, 2019**

## ***Table of Contents***

**Purpose:**

Easter Seals NH and Subsidiaries (ESNH) has adopted this Information Technology Policy Manual to ensure uniform and appropriate use of its computer and telecommunication resources (the "Technology Resources," defined below). The rules, obligations, and standards described in this Policy apply to all employees, temporary workers, independent contractors, consultants, agents, and other computer or telecommunication users of ESNH Technology Resources (collectively, the "Users," as defined below), wherever they may be located.

It is every User's duty to use the Technology Resources responsibly and in a professional, ethical, and lawful manner. In addition, every User is responsible for ensuring the security of ESNH's Technology Resources and its valuable proprietary and confidential information.

Users who become aware of any violation of this policy must immediately report the incident to the Senior VP of Information Technology or his/her designated representative. Violations of this Policy may result in disciplinary action, including possible termination, and potential civil and criminal liability. Use of the Technology Resources is a privilege that may be limited or revoked at any time, with or without cause and without notice, in the sole discretion of ESNH.

This manual contains information about the policies and practices relating to the use of technology, including by employees. However, the provisions in this manual are not intended to create, and do not create, contractual obligations with respect to any matters covered in the manual or with regard to any employee's employment.

Users must also be attentive to the policies contained in the Compliance, Privacy & Security Policies and Procedures Manual if their use of technology involves Protected Health Information under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

**Scope:**

This policy applies to employees, contractors, consultants, temporary workers, agents, and other workers at ESNH, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by ESNH.

**Definitions:**

As used in this Policy, certain terms are defined as follows:

*"Confidential/Proprietary Information"* - includes all material, in any form, related to the operation of ESNH or a controlled subsidiary, including, but not limited to health information, financial information, employee information, customer or client information, proprietary products and product development, marketing and general business strategies, and any information that is not shared with the public or is designated as or treated as confidential or proprietary by ESNH. Access to Confidential/Proprietary Information is restricted according to this policy and applicable laws and regulations.

*"Computer Information*" - means all information and communications created, received, or stored on or passed through the Technology Resources. Computer Information includes all files and e-mail.

*"Copyrighted Publications"*- means materials that are subject to protection under the law of copyright. These materials include, but are not limited to, third party software, software manuals, trade articles, textbooks, newspaper and magazine articles, electronic databases, graphics, audio files, pictures, and material available on the Internet. While having a copyright notice and/or a "©" may provide the copyright owner with additional rights, they are not required for copyright protection to apply. Almost every document, whether written or electronic, is subject to copyright protection – whether or not it has a copyright notice. When in doubt, Users should always assume that a document is copyrighted.

*"Data/Telecom Network"*- means the hardware, software and all other components that are integral to the creation, transmission and storage of data, voice, or video signals within the data/telecom environment deployed and managed by ESNH.

*"E-mail*" - means electronic messages, including instant messages, text messages, etc., sent from one person to one or more individuals or groups (or addresses on a distribution list) via electronic media, either through an internal network or over an external network. Messages may consist of digitized text, graphics, video, voice and/or file attachments.

*"Firewall"* - means a hardware and/or software system placed between the Technology Resources and the Internet or to provide internal separation among Technology Resources. The primary function of a firewall is to limit unauthorized access to and use of the Technology Resources.

*"Malware"*- means any type of potentially unwanted program that can have a negative impact on the Technology Resources.

*"Policy"* - means this Information Technology Policy, including all attachments and amendments.

*"Server"* - means a computer or computer program that provides resources to connected Users and workstations.

*"Technology Resources"* - means ESNH's entire computer and telecommunications network, including, but not limited to, the following: servers, workstations, laptops, cell phones, other wireless technology, software, voice mail, data files, and all internal and external communications networks (e.g., Internet, e-mail systems) that may be accessed directly or indirectly from ESNH's network or telecommunications systems. Technology Resources include assets that are located on and off ESNH property so long as they are part of the ESNH serviced network or telecommunications systems.

*"Users"* - means all persons or entities that use the Technology Resources, wherever they are located. This includes Users who are not affiliated with ESNH, but who have authorized access to and permission to use computer and telecommunications systems maintained by ESNH.

*"Virus"* - means a program that infects computer files and systems, often with destructive results (e.g., loss of data, unreliable operation of infected software and systems).

*"Workstation"* - means the individual desktops or laptops assigned to one or more Users.

**Policy Statement:**

In using or accessing the Technology Resources, Users must comply with the following provisions:

***1. Use of Technology Resources - In General***

The Technology Resources constitute a valuable business asset of ESNH and may only be used for approved purposes. Users are permitted access to the Technology Resources to assist them in the performance of their jobs. Occasional, limited, appropriate personal use of the Technology Resources is permitted when the use does not: (1) interfere with the User's work performance; (2) interfere with any other User's work performance; (3) unduly impact the operation of the Technology Resources; (4) result in any material expense to ESNH; or (5) violate any other provision of this Policy or any other policy, guideline, or standard of ESNH.

***2. Standards***

The Senior VP of Information Technology may augment this Policy from time-to-time by publishing hardware, software, configuration, and practice standards. These are intended to ensure Technology Resources are secure, reliable, and can be economically maintained.

***3. No Expectation of Privacy***

Users understand and agree that:

a) ESNH retains the right, with or without cause or notice to the User, to access or monitor the Computer Information, including User e-mail and Internet usage. Please keep in mind that anything created or stored on the Technology Resources, including the Computer Information, may be reviewed by others and that even deleted files may be recovered;

b) Users have no expectation of personal privacy of any kind related to their use of the Technology Resources or any Computer Information;

c) Users expressly waive any right of privacy or similar right in their use of the Technology Resources or any Computer Information.

***4. Ownership of Computer Information and Technology Resources***

All of the Computer Information and the Technology Resources are the sole and exclusive property of ESNH. Any User files, e-mail, or other Computer Information created or stored on the Technology Resources will become the property of ESNH. ESNH is not responsible for non-agency files saved on Agency resources.

### *5. Prohibited Activities*

5.1 - Inappropriate or Unlawful Material - Content that is fraudulent, harassing, discriminatory, embarrassing to co-workers or clients, sexually explicit, profane, obscene, intimidating, defamatory, malicious, or otherwise unlawful or inappropriate, including any comments that would offend someone on the basis of race, color, religion, gender (including pregnancy, childbirth and related conditions), sexual orientation, citizenship status, creed, marital status, age, disability, ancestry, genetic information, gender identity or expression, military or veteran status, domestic violence victim status, national origin, or any other characteristic protected by law, must not be sent by e-mail or other form of electronic communication (e.g., bulletin board systems, newsgroups, chat groups), viewed on or downloaded from the Internet or other online service, or displayed on or stored on the Technology Resources. Users encountering or receiving such material must immediately report the incident to his/her supervisor.

5.2 - Prohibited Activities - Users may not use the Technology Resources for personal financial gain or the benefit of any third party (including the sale of any non-ESNH products or services), or to solicit others for activities unrelated to ESNH's business, or in connection with political campaigns or lobbying. The Technology Resources may also not be used to create, store, or distribute any form of malicious software (e.g., viruses, worms, or other destructive code). This policy will not be construed or applied in a manner that would interfere with an employee's right to discuss terms and conditions of employment under the National Labor Relations Act, but such communications should be on non-working time.

5.3 - Protection of ESNH Data/Telecom Network - Users, other than authorized Information Systems employees, may not do any of the following:

a) Access the Data/Telecom Network with a diagnostic or testing tool such as a protocol analyzer intended to monitor, decode, or filter packets of information.

b) Connect an unauthorized device to the Data/Telecom Network without prior coordination and approval of ESNH IT Department.

c) Enter a designated Data/Telecom Network equipment room without prior authorization from ESNH IT Department.

d) Attempt to physically or logically reconfigure, move, or disengage a Data/Telecom Network component.

e) Install computer software/services on the Data/Telecom Network.

5.4 - Waste of Technology Resources - Users may not deliberately perform acts that waste Technology Resources or unfairly monopolize resources to the exclusion of others. Examples of this are, but are not limited to, sending non-business related mass e-mails or chain e-mail, spending excessive time on the Internet, gaming sites, gambling sites, , engaging in non-business related online “chat groups,” streaming audio/video or otherwise creating unnecessary network traffic.

5.5 - Misuse of Licensed Software - Without prior written authorization from the Senior VP of Information Technology or his/her designated representative, Users other than authorized IT Department employees may not do any of the following:

a) Copy ESNH software for use on their home computers;

b) Upload or transmit any software licensed to ESNH;

c) Provide copies of ESNH software to any independent contractors or consultants of ESNH or to any third person;

d) Install software (including screen savers and games) or any updates to existing software on any of ESNH’s workstations or servers;

e) Download any software from the Internet or other online service to any of ESNH’s workstations or servers;

f) Modify, revise, transform, recast, or adapt any software; or

g) Reverse engineer, disassemble, or decompile any software.

Users who become aware of any misuse of software or violation of copyright law must immediately report the incident to the Senior VP of Information Technology or his/her designated representative.

5.6 - Online Agreements - Without prior written authorization from the Senior VP of Information Technology or his/her designated representative, Users may not accept or agree to be bound by any terms and conditions of use (other than standard terms and conditions of use for access to Web sites), license agreements, or other types of online agreements relating to use of Technology Resources.

5.7 - Resource Sharing - Use of software that allows computers located in ESNH to be shared as resources to the Internet is prohibited. For example, some P2P software allows a computer system to be accessed by non-ESNH systems. Desktop sharing/remote access applications that are required to enhance or enable third party support must be authorized by the IT Department prior to use.

### *6. Use of Copyrighted Information*

6.1 - In General - It is the policy of ESNH to prohibit copying or distribution of any Copyrighted Publications of third parties, except as:

a) Permitted by legal principles of “fair use” (as described in Section 6.3, below) or

b) Authorized by a contract or license that ESNH has obtained. Copies of all contracts and licenses for Copyrighted Publications should be retained by the office administrator at the location of use and by ESNH’s legal department. Copying may occur by using a photocopy machine, through retyping, faxing, and reprinting, as a result of storage, duplication or printing of electronic information, and through the posting of material on the Internet and other networks. Distribution may occur if Copyrighted Publications are sent through interoffice delivery, e-mail or Internet transmission (including newsgroups and other online discussion areas), client information services, etc.

6.2 - Limitations of Copyright - Copyright does not necessarily protect all forms of information or printed material, particularly raw data, facts, “ideas,” and “processes,” and works in the public domain (e.g., works that are very old or that are specifically dedicated to the public domain), so copyright law ordinarily should not preclude Users from extracting the base factual information they need to conduct normal business activities. If a User has any questions about what is permitted, please consult ESNH’s IT Department.

6.3 - Fair Use - “Fair use” is a legal principle that permits a limited amount of copying of Copyrighted Publications to occur, depending on the facts and circumstances. Based on the ordinary needs of ESNH, “fair use” will more likely occur if the following factors are present:

a) The purpose of the copying is for educational or research use;

b) The copying is a necessary step for extracting, understanding or using data or information (e.g., a necessary step in using a computer program is to copy the program into the memory of the computer);

c) The copying is to create a substantially different work, which conceptualizes, analyzes, expands upon or otherwise transforms the material being copied. This is a key element of fair use. It is one thing to simply copy an existing article and distribute it to twenty other people. It is quite another thing to take the ideas in an existing article and to expand upon them in a new article. In the first instance, there will likely be no fair use. In the later instance, the potential for fair use is higher;

d) The amount of material being copied is limited to small portions, excerpts, or abstracts (e.g., if a particular paragraph in an article is of interest, do not copy the entire article);

e) The copying is not “systematic” in the sense that copies of the same or similar works are not being made repetitively, continuously, and/or in multiple quantities under circumstances that could be seen to substitute for purchases or subscriptions. The classic example of “systematic” copying is the monthly copying of the entire contents of a trade journal for circulation to every member of a particular department. That kind of activity would almost certainly not be a fair use;

f) The copying is ad hoc and as needed, conducted within ESNH on a per-item basis, and not by commercial copy centers for large-scale distribution; and

g) Distribution of copies is strictly limited, and no fee or charge is collected for the copying or distribution.

The foregoing guidelines state some, but not all, applicable considerations, and do not preclude fair use from existing in other situations. Because every situation is judged separately, each User has final responsibility for exercising sound judgment and reasonable restraint. Each department of ESNH, depending on need, should consider establishing more particularized guidelines for limiting the amount of copying that occurs.

6.4 - Copyright Management Information - Users may not alter Copyrighted Publications in such a way as to change, obscure, or remove information relating to the copyright owner, copyright notice information, the author of the work, the terms and conditions of use of the work, or identifying numbers or symbols referring to the foregoing information or links to such information. To the extent possible, Users should use hyperlinks to reference copyrighted material instead of making copies of such material.

6.5 - Peer-to-Peer File Sharing - Users are prohibited from sharing digital audio music files, software or any other copyrighted material using ESNH Technology Resources without the written permission of the copyright holder, and ESNH’s IT Department.

### *7. Use of E-mail*

7.1 - In General - All User e-mail addresses assigned by ESNH shall remain the sole and exclusive property of ESNH. Users should endeavor to make each of their electronic communications truthful and accurate. Users should use the same care in drafting e-mail and other electronic documents as they would for any other written communication.

7.2 - Altering Attribution Information - Users may not alter the “From” line or other attributes of origin information in e-mail or other online postings.

7.3 - Forwarding E-mail - Users should use their good judgment in forwarding e-mail to any other person or entity. When in doubt, request the sender’s permission to forward the message. E-mail containing Confidential/Proprietary Information or attorney-client communications may never be forwarded without the permission of the sender or other authorized personnel. All messages written by others should be forwarded “as-is” and with no changes, except to the extent that the User clearly indicates where the User has edited

the original message (i.e., by using brackets [ ] or other characters to indicate changes to the text).

7.4 - Confidential/Proprietary Information - Each User must take all appropriate precautions to ensure that Confidential/Proprietary Information is not improperly disclosed or otherwise compromised by transmission via e-mail. If this information is transmitted via e-mail, the sender of the message is responsible for: (i) insuring that the e-mail is clearly labeled in the subject line and the body of the message as “Confidential”, “Proprietary,” “Confidential: Unauthorized Use or Disclosure is Strictly Prohibited” or “Privileged Attorney-Client Communication”; (ii) keeping the address list for the e-mail to a minimum; (iii) ensuring all recipients are aware of the obligation to maintain the confidentiality of the information contained in the e-mail; and (iv) assuring that the transmission of information is in accordance with this Policy and applicable law.

7.5 - Unauthorized Receipt of Confidential/Proprietary Information - In the event a User receives e-mail, whether designated as confidential or not, by mistake, the User should stop reading the message and immediately notify the sender or system administrator. It is a violation of this Policy to read e-mail intended for another person without the express prior consent of that person or other authorized ESNH personnel.

7.6 - Access to E-mail through Third Party Services - Users are provided Agency e-mail service access. This e-mail service is the only authorized Agency e-mail service, and as such Users should not send Agency information via non-ESNH provided e-mail services.

7.7 - Retention and Destruction of E-mail - Users should exercise good housekeeping practices with regard to their e-mail account. Attachments that have current business relevance should be stored on a file share on the network. Deleted email will, generally, not be recovered. Users are expected to use caution when deleting email as it may not be easily recoverable if permanent deletion has occurred.

7.8 - E-mail Forwarding - Automatic forwarding of email to a third party system is not permitted. It places an administrative burden on IT Department and can result in sensitive information being compromised in transit via the Internet. In exceptional cases, as approved by Senior VP of Information Technology, email forwarding may be done for temporary periods. Upon User termination, the e-mail account is forwarded to the direct supervisor of the User for a two week period at the end of which the e-mail account is deleted.

7.9 - E-mail Signature Standard – At a minimum each User’s signature line should contain:

a) Full name

b) Position title

c) Telephone number (for voicemail)

### *8. Internet Access and Use*

8.1 - Authorized Uses - Users are encouraged to use the Internet and intranets to assist them in the performance of their jobs. Authorized uses include, but are not limited to the following: a) Client services, human resources, education, and research; b) Electronic communication; c) Professional purposes and procurement of information from external sources.

8.2 - Internet Monitoring and Filtering - ESNH has software and systems in place that are capable of monitoring, filtering and recording Internet usage. These security measures may be capable of recording Web sites visited, chat, newsgroup, or e-mail messages, and each file transfer into and out of ESNH's networks. ESNH reserves the right to conduct such monitoring and recording at any time. As described in Section 3, Users have no expectation of privacy as to their Internet usage. ESNH may review Internet activity and analyze usage patterns, and may choose to publicize this data to ensure that the Technology Resources are used in accordance with the provisions of this Policy.

8.3 - Disclaimer of Liability for Internet Use - ESNH IS NOT RESPONSIBLE FOR MATERIAL VIEWED OR DOWNLOADED BY USERS FROM THE INTERNET. THE INTERNET IS A WORLDWIDE NETWORK OF COMPUTERS THAT CONTAINS MILLIONS OF PAGES OF INFORMATION. USERS ARE CAUTIONED THAT MANY OF THESE PAGES INCLUDE OFFENSIVE, SEXUALLY EXPLICIT, AND INAPPROPRIATE MATERIAL. IN GENERAL, IT IS DIFFICULT TO AVOID AT LEAST SOME CONTACT WITH THIS MATERIAL WHILE USING THE INTERNET. EVEN INNOCUOUS SEARCH REQUESTS MAY LEAD TO SITES WITH HIGHLY OFFENSIVE CONTENT. IN ADDITION, HAVING AN E-MAIL ADDRESS ON THE INTERNET MAY LEAD TO THE RECEIPT OF UNSOLICITED E-MAIL CONTAINING OFFENSIVE CONTENT. USERS ACCESSING THE INTERNET DO SO AT THEIR OWN RISK.

### *9. Passwords*

9.1 - Responsibility for Passwords - Users are responsible for safeguarding their passwords for access to the Technology Resources. Users should recognize that the combination of a user name and password is the equivalent of a signature. Individual passwords should not be printed, stored on-line, or given to others. Users are responsible for all activity occurring while using their user names and passwords. No User may access the computer system using another User's password or account.

9.2 - Password Guidelines – IT Department dictates the password guidelines that all Users must follow for network access. Passwords are subject to the following guidelines:

a) Each password will be not less than 8 characters in length

b) Passwords must comply with at least three of these four rules -

(1) English upper case letters – A, B, C, …Z
(2) English lower case letters – a, b, c, …z
(3) Westernized Arabic numerals – 0, 1, 2, …9
(4) Non-alphanumeric "special characters" - #, &, etc.

c) The password expires every 90 days

d) A password may not be reused in less than 36 months.

e) Passwords should not be associated with personal information (e.g., PIN used for bank cards, date of birth for self or family members, telephone numbers, first or last name of self or family members, passwords used for Internet accounts).

9.3 - Passwords Do Not Imply Privacy - Use of passwords to gain access to the Technology Resources or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on the Technology Resources.

***10. Security***

10.1 - Accessing Another User's Files - Users may not alter or copy a file belonging to another User without first obtaining permission from the owner of that file. The ability to read, alter, or copy a file belonging to another User does not imply permission to read, alter, or copy that file. Users may not use the computer system to "snoop" or pry into the affairs of others by unnecessarily reviewing their files and e-mail.

10.2 - Accessing Other Computers and Networks - A User's ability to connect to other computer systems using the Technology Resources does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems.

10.3 - Control of Media - Users having CDs, DVDs, USB drives and other removable media (collectively, "Removable Media") will establish procedures to label, account for, and control all media containing ESNH data or information, regardless of whether such data or information is current or obsolete. Removable Media in the possession of Users should never be left unattended. Removable Media must be disposed of in accordance with procedures provided by ESNH policy. If removable media contains PHI or ESNH sensitive information, the data must be secured at a minimum with a password. In all instances, the use of Removable Media should be considered a temporary storage solution. All data on Removable Media must be copied to the appropriate network storage location.

10.4 - Remote Access - ESNH provides several methods of remote access. When accessing hosts inside the ESNH firewall from external locations, no exception to these connection methods will be allowed unless approved by the IT Department.

10.5 - Use of Remote Access Software – For business to business connections, such as those used by outside vendors to provide remote maintenance support, the installation, set-up and use of software that provides remote control of an in-house desktop computer requires the prior approval of the IT Department (i.e. WebEx, GotoMyPC). Such installation, set-up and use, if approved, will be required to adhere to any additional procedures specified by the IT Department to restrict and control access.

10.6 - Network Admission - Before a device connects to the ESNH data network, it must comply with safe network admission practices. These ensure a device will not introduce security vulnerabilities, spread malicious software, or do other harmful actions that jeopardize business operations or sensitive information. Safe practices include having up-to-date software patches, activated and up-to-date antivirus software, and no unnecessary services running on the device. If the device is not under IT Department management, it must also have an able administrator assigned. Devices connected must be maintained as new security vulnerabilities arise and best practices change. Non-compliant systems will have their network port disabled.

10.7 - Outside Access Computer Security - Each User is responsible for ensuring that his or her use of outside computers and networks, like the Internet, will not compromise the security of the Technology Resources. This duty includes taking reasonable precautions to prevent intruders from accessing ESNH's network without authorization and to prevent the introduction and spread of viruses. When accessing ESNH computer resources from home or other off-site locations, users are expected to exercise reasonable precautions to ensure they are doing so in a safe manner. This includes keeping their local computer free of spyware, keystroke grabbers, and similar threats.

10.8 - Wireless Devices and Access – The IT Department provides access to the network via secure wireless access points in some office locations. This allows users with IT authorized wireless hardware to access the network when visiting these offices. All access and use of the wireless access points will be monitored by IT. IT procures both laptops and desktop pc's with wireless capabilities and maintains the settings required to use the wireless access points.

10.9 - Mobile Device Use - Users granted access to ESNH mobile computers for remote access to ESNH applications are responsible for insuring that unauthorized persons are prevented from using the device, accessing files stored on the device, or using the device to gain access to ESNH's network. In particular, a mobile device should never be left unattended in any uncontrolled environment (e.g., in a hotel room, at a vendor's facility, or at any other remote location). If need be and conditions permit, the device should be locked in a hotel safe or the trunk of a car or kept in the User's possession. Power-up and time-limited screensaver password protection must be enabled on mobile devices. If the User's device is lost or stolen,or if a User believes that a password has been

compromised, report the incident immediately to the Senior VP of Information Technology or his/her designated representative.

10.10 - HIPAA Security Regulations – Any device containing electronic patient health information, as defined by HIPAA and supplemented by ESNH privacy policies, shall comply with HIPAA security regulations. Additionally, User will comply with other ESNH privacy policies.

### *11. Viruses*

11.1 - Virus Detection - Viruses can cause substantial damage to computer systems. Each User is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into the Technology Resources and for timely reporting discovered viruses to the IT Department (603-621-3666). To that end, all material received on disk or other magnetic or optical media and all material downloaded from the Internet or from computers or networks that do not belong to ESNH will be scanned for viruses and other destructive programs before being placed onto the Technology Resources. Users should understand that their home computers and/or laptops might contain viruses. All files transferred from these computers to the Technology Resources will be scanned for viruses.

11.2 - Preventing the Spread of Viruses - To prevent the spread of viruses, every User must do the following:

a) Obtain prior approval of the IT Department before installing or loading any software or data, including demos, shareware, or freeware, on any of ESNH's workstations or laptops;

b) When accessing ESNH computer resources from off-site via a VPN or other trusted connection, ensure the device from which you are connecting has up-to-date software security patches and anti-virus software installed.

### *12. Encryption Software*

Use of Encryption Software - Users may not install or use encryption software on any of ESNH's computers without first obtaining written permission from the Senior VP of Information Technology or his/her designee.

### *13. Disclosures Regarding Security Issues*

Information relating to virus attacks, hacking incidents, and other breaches of security shall be treated as highly confidential. Unless specifically directed to do so by the Senior VP of Information Technology or his/her designee, Users may not discuss this information with their co-workers.

### *14. Third Party Access*

Access will be granted to Technology Resources based on the contracted work being performed. The IT Department will assign the User credentials, User permissions and access hours.

### *15. Video Surveillance*

After careful consideration, Easter Seals has determined that the use of audio and video devices is necessary to ensure the safety of employees, to provide added supervision, and to monitor the behavior of Agency clientele.

15.1 - Camera Locations - Easter Seals has installed video cameras in some of our Child Development Centers, Residential Facilities, Special Transit Service Vehicles and entrances to buildings. Each of these locations was chosen because they are areas where employee expectations of privacy are minimal. All areas subject to video monitoring will be identified by signs that are clearly posted.

15.2 - Use and Retention of Video- In the event of a reported or observed incident or potential crime, the recorded video may be used to assist in the investigation of the incident and may be turned over to law enforcement personnel, if appropriate. Any staff member disciplined as a result of the video shall have the opportunity to view the video which is the basis for the disciplinary action.

Only those portions of the recording relevant to the incident resulting in a complaint shall be reviewed, unless additional video may need to be reviewed to find the recording of the incident. At no time will persons other than those in a management position with Easter Seals or law enforcement, third parties pursuant to a subpoena, or persons who are the subject of the recording have access to the video made in the course of surveillance. Personal information contained on the video will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

Video from the surveillance cameras will generally be stored for no more than 30 days, unless required for the purposes outlined in this policy. Video from surveillance cameras located on Agency vehicles will be kept for no more than 30 days unless Easter Seals determines that the recording is relevant to a disciplinary proceeding or a court requires retention. However, if disciplinary action is taken as a result of conduct disclosed by the video, that video shall be retained until such a time as the disciplinary action is complete.

15.3 - Ownership of Recordings - Easter Seals shall own any images and/or sounds downloaded from the recording devices and shall treat recordings in accordance with all applicable federal and state laws governing privacy.

### *16. Employee Separation*

Upon the separation from employment of an employee for any reason the following will occur to ensure the security of the Technology Resources and enforce ESNH's ownership rights of the electronic data:

a) The User's network credentials are to be de-activated;

b) The User's email account is suspended and forwarded to the supervisor of record;

c) Reassign the home directory files to the supervisor of record;

d) Assign access rights to the supervisor of record for voicemail monitoring;

e) Return of any User assigned Technology Resources components.

f) Carry out any activities required to comply with potential civil or criminal proceedings.

### *17. Miscellaneous*

17.1 - Compliance with Applicable Laws and Licenses - In their use of the Technology Resources, Users must comply with all software licenses, copyrights, and all other state, federal, and international laws.

17.2 - Other Policies Applicable - In their use of the Technology Resources, Users must observe and comply with all other policies and guidelines of ESNH.

17.3 - Amendments and Revisions - This Policy may be amended or revised by ESNH from time-to-time as deemed necessary. This Policy will be available to all as requested inclusive of amendments and revisions.

17.4 - Hardware Protection – In an effort to protect end User Technology Resources, the following is required by all Users:

a) Workstations must be plugged into a surge protection device;
b) Workstation fans or vents must be clear of obstruction;
c) Magnets of all types are not allowed in close proximity to any Technology Resources;
d) No every day cleaning solvents should be used on any Technology Resource.

### *18. Personal Mobile Device Policy*

This policy governs the use of personally-owned smartphones, tablets and mobile devices (collectively referred to as “personal mobile devices”) by ESNH employees to access ESNH computer network resources or conduct ESNH business. Access to and continued use of ESNH’s computer network services through a personal mobile device is granted on the condition that the employee reads, signs, respects and follows ESNH’s policies concerning the use of these personal mobile devices and services.

ESNH reserves the right to change, audit or discontinue this policy at any time and in its discretion. ESNH reserves the right to select only certain employees to have access to the ESNH computer network through their personal mobile device; not all employees will be selected for participation. ESNH Employees who are permitted access to the ESNH computer system under this policy are hereinafter referred to as “Employee”.

18.1 - Using a personal mobile device to access ESNH computer network services requires compliance with all other applicable ESNH policies, including but not limited to ESNH’s Computer Use, Conduct, Client Confidentiality, Use of Cell Phones While Driving, Record Retention Policy, Litigation Hold Policy, and Telecommuting policies. ESNH expects compliance with this policy as it does with other policies.

An Employee who fails to comply with this policy will be subject to discipline.

Pursuant to ESNH policy, Employee has no expectation of privacy in any data or information stored on a personal mobile device that accesses ESNH computer network resources. Any data accessed by a personal mobile device is subject to inspection by ESNH. Any emails sent or received by a personal mobile device are subject to inspection by ESNH. ESNH will work with the employee to preserve the employee’s privacy to the extent possible or reasonable under the circumstances. However, if employees use a personal device to access ESNH’s computer network, they may wish to refrain from using that device for private purposes..

18.2 - Employee will not install or use any of the following apps or programs on an otherwise approved personal mobile device that accesses ESNH computer network resources:

***Network scanning applications.***

18.3 - Payment of Costs to Purchase and Maintain Approved Personal Mobile Devices - Employee will bear all costs to purchase and maintain the devices. Employee will bear all costs for any apps or programs used to access ESNH computer network resources.

Employee may select a cellular and data service provider or carrier of his or her choosing, but Employee will bear all costs for such services. ESNH is not responsible for any disruption in service or access. ESNH is not responsible for any costs incurred by Employee for exceeding monthly allowed data quantities.

For current reimbursement policies/guidelines regarding mobile phone or data services please contact the ESNH Accounts Payable Department.

18.4 - Confidential Information - Employee acknowledges that he/she may have access to ESNH sensitive and confidential information through his/her personal mobile device. Employee agrees to at all times comply with ESNH's Confidentiality Policies and to employ reasonable efforts to safeguard his/her personal mobile device. Employee shall employ pin numbers and security access codes to restrict access to his/her personal mobile device as available through the security settings on the personal mobile device. The pin codes or access codes used to access the personal mobile device shall not be the same pin codes or access codes used by the Employee to access the ESNH computer network services. Employee will not share the personal mobile device with anyone, including a member of the Employee's family.

Use of a personal mobile device is subject to ESNH's policies regarding confidentiality and any written non-disclosure agreements between Employee and ESNH.

18.5 - Storage of ESNH Information - ESNH data should not be stored locally on a personal mobile device without prior approval from ESNH. Accessing ESNH data should be accomplished through a Virtual Private Network ("VPN") connection established by ESNH. Any changes made to ESNH data should be saved on ESNH computer network resources and not on any hard drive or other storage media contained in or peripheral to the personal mobile device. Employee will not upload/transfer any ESNH data to a non-ESNH device or personal mobile device without prior authorization. To the extent any ESNH data is stored locally on a personal mobile device, it should be segregated from any personal data.

Employee agrees to comply with all directions from the IT Help Desk regarding syncing data to and from the personal mobile device and ESNH computer network resources. Employee will not use any third party data storage providers (including cloud providers such as Dropbox) to store or transfer ESNH data without the prior approval of an authorized representative of ESNH.

18.6 - Remote Disabling or Wiping of Personal Mobile Devices - By accessing the ESNH computer network and agreeing to the terms of this policy, Employee authorizes ESNH to remotely disable and/or wipe (erase) his/her personal mobile device as ESNH deems necessary. No additional approval is required from Employee. Without limiting the foregoing, Employee specifically authorizes ESNH to remotely wipe clean and/or disable the personal mobile device if ESNH believes it is lost or stolen, if Employee purchases a new personal mobile device to replace a current device, and at the conclusion of the Employee's employment with ESNH. Employee agrees that as part of the set-up of the personal mobile device to access ESNH computer network resources, ESNH can install any programs or record any information necessary to enable the remote disabling and/or wiping of the personal mobile device.

18.7 - Lost or Stolen Personal Mobile Devices - In the event Employee's personal mobile device is lost or stolen, he/she will immediately (and in no cases later than 24 hours after discovering the device was lost or stolen) notify IT Help Desk at 603-621-3666 or HelpDesk@eastersealsnh.org.

**19. Mobile Device Waiver**

In the event Employee's use of his/her personal mobile device ends for any reason, ESNH shall not be responsible for any service provider cancellation or any other costs or fees.

## ACKNOWLEDGMENT / RECEIPT

I have received a copy of the Easter Seals 2019 Information Technology Policy Manual and have either read it or have had it read to me carefully. I understand all of its rules, policies, terms and conditions and agree to abide by them. I realize that failure to do so may result in disciplinary action or termination. I understand and agree that my employment may be terminated at-will, so that both Easter Seals and I remain free to choose to end our work relationship at any time. I also understand that Easter Seals remains free to change, revise, or eliminate any or all of the policies contained in this manual at any time. I understand that nothing in this manual in any way creates an express or implied contract of employment between Easter Seals and me. I also understand that this manual is only intended to provide a better understanding of my use of WSNH's Technology Resources and to ensure compliance with legal requirements, for so long as the employee/employer relationship exists.

_____Date

_____ Employee's Signature

_____ Employee's Printed Name

_____ Date

_____Representative's Signature