NATIONAL HEMOPHILIA FOUNDATION
for all bleeding disorders

Information and Technology Policy & Procedure

Revision Date June 2018

RELATED POLICIES/PROCEDURES AND REFERENCES:

Information and Technology Policy

PURPOSE

NHF's Information and Technology Policy (I.T. Policy) is set in place to outline the acceptable use of Electronic Communications created sent, received, used, transmitted or stored using NHF's systems or equipment and employee provided systems or equipment used either in the workplace, during working time or to accomplish work tasks. This policy applies to the use of NHF's Systems to conduct NHF business or interact with internal or external networks and business systems, whether owned or leased by NHF, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at NHF and its chapters are responsible for exercising good judgment regarding appropriate use of NHF's Systems in accordance with NHF policies and standards, and local laws and regulation.

DEFINITIONS

For purposes of this procedure, the following terms shall be defined as follows:

Electronic Communications includes, but not limited to, images, emails, instant messages, text messages, voice mail, or faxes. I.T. Resources includes, but is not limited to computers, mobile devices (including, but not limited to, smart phones, smart watches, tablets, laptops, or similar devices), network server storage, cloud storage, external storage devices (including, but not limited to, memory card, flash or jump drive, and any other type of internal or external removable storage drives), Intranet, and Internet. All content contained, stored, or transmitted is collectively called "Data." The Electronic Communications, I.T. Resources, and Data will be collectively called "Systems."

PROCEDURE(s)

Acceptable use Procedure

This procedure outlines the acceptable use of computer equipment at NHF. These rules are in place to protect the employee and NHF. Inappropriate use exposes NHF to risks including virus attacks, compromise of network systems and services, and legal issues.

1. General Use and Ownership

    a. NHF proprietary information stored on electronic and computing devices whether owned or leased by NHF, the employee or a third party, remains the sole property of NHF. You must ensure through legal or technical means that proprietary information is protected and backed-up.

    b. All NHF proprietary data should be stored on the server or OneDrive Cloud storage.

    c. You have a responsibility to promptly report the theft, loss or unauthorized disclosure of NHF proprietary information.

    d. You may access, use or share NHF proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

    e. Employees are responsible for exercising good judgment regarding the reasonableness use NHF systems for personal use.

    f. For security and network maintenance purposes, authorized individuals within NHF may monitor equipment, systems and network traffic at any time.

    g. NHF reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

    h. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

    i. Employees handling PHI (Protected Health Information) data. See HIPAA policy.

Unacceptable use Procedure

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of NHF authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing NHF owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

1. System and Network Activities

    a. Violations of the rights of any person or NHF protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by NHF.

b. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which NHF or the end user does not have an active license is strictly prohibited.

c. Accessing data, a server or an account for any purpose other than conducting NHF business, even if you have authorized access, is prohibited.

d. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

e. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

f. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

g. Using a NHF computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

h. Making fraudulent offers of products, items, or services originating from any NHF account.

i. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

j. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

k. Port scanning or security scanning is expressly prohibited unless prior notification to NHF is made.

l. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

m. Circumventing user authentication or security of any host, network or account.

n. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

o. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

p. Providing information about, or lists of, NHF employees to parties outside NHF.

1. Email and Communication Activities

When using NHF resources to access and use the Internet, users must realize they represent the NHF. Whenever employees state an affiliation to the NHF, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the NHF". Questions may be addressed to the IT Department

a. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

b. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

c. Unauthorized use, or forging, of email header information.

d. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

e. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

f. Use of unsolicited email originating from within NHF's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by NHF or connected via NHF's network.

Email Procedure

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it’s important for users to understand the appropriate use of electronic communications.

The purpose of the NHF email system is to facilitate our day-to-day business operations. The purpose of this email policy is to ensure the proper use of NHF’s email system and make users aware of what NHF deems as acceptable and unacceptable use of its email system. This procedure outlines the minimum requirements for use of the email within NHF network.
It covers appropriate use of any email sent from a NHF email address and applies to all employees, vendors, and agents operating on behalf of NHF.

1. All use of email must be consistent with NHF policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

2. NHF email account should be used primarily for NHF business-related purposes;

personal communication is permitted on a limited basis, but non NHF related commercial uses are prohibited.

3. Email should be retained only if it qualifies as a NHF business record. Email is a NHF business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
4. Email that is identified as a NHF business record shall be retained per NHF Retention Policy.
5. The NHF email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any NHF employee should report the matter to their supervisor immediately.
6. Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct NHF business, to create or memorialize any binding transactions, or to store or retain email on behalf of NHF.
7. Using a reasonable amount of NHF resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a NHF email account is prohibited.
8. User sending PHI (Protected Health Information) via email. See HIPAA Policy.

Internet Usage Procedure

The Internet usage procedures covers all Internet users (individuals working for NHF, including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners, and vendors) who access the Internet through the computing or networking resources. NHF's Internet users are expected to be familiar with and to comply with this policy, are required to use their common sense, and exercise good judgment while using Internet services.

Internet Services Allowed

Internet access is to be used for business purposes only. Capabilities for the following standard Internet services will be provided to users as needed:

- E-mail -- Send/receive E-mail messages to/from the Internet (with or without document attachments).
- Navigation -- WWW services as necessary for business purposes, using a hypertext transfer protocol (HTTP) browser tool. Full access to the Internet.
- File Transfer Protocol (FTP) -- Send data/files and receive in-bound data/files, as necessary for business purposes.
- Streaming services video & audio (e.g. YouTube, Netflix, iTunes) for business purposes.

Internet access will be provided to users to support business activities. Users are responsible for making sure they use this access correctly and wisely. Users should not allow Internet use to interfere with their job duties.

1. Allowed Usage
   a) Access to and distribution of information that is in direct support of the business-related activities.

   b) NHF Internet connection may be used for educational and research purposes.

   c) If any user has a question of what constitutes acceptable use, they should check with I.T. department.

2. Inappropriate Use
   a) NHF, Internet access shall not be used for any illegal or unlawful purposes. Examples of this would be the transmission of violent, threatening, defrauding, pornographic, obscene or otherwise illegal or unlawful materials.

   b) Use of NHF electronic mail or messaging services shall be used for the conduct of NHF, business only. These services shall not be used to harass, intimidate or otherwise annoy another person.

   c) NHF Internet connection shall not be used for commercial or political purposes.

   d) Internet access shall not be used for personal gain such as selling access of a NHF user login. Internet access shall not be used for or by performing work for profit with NHF resources in a manner not authorized by NHF.

   e) Users shall not attempt to circumvent or subvert security measures on the NHF's network resources or any other system connected to or accessible through the Internet.

   f) Unauthorized downloading of any shareware programs or files for use without authorization in advance from the IT Department and the user's manager.

Remote Access Procedure

The purpose of this procedure is to define rules and requirements for connecting to NHF's network from any host. These rules and requirements are designed to minimize the potential exposure to NHF from damages which may result from unauthorized use of NHF resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical NHF internal systems, and fines or other financial liabilities incurred as a result of those losses.

General access to the Internet for recreational use through the NHF network is strictly limited to NHF employees, temp employees, contractors, and interns (hereafter referred to as "Authorized Users"). When accessing the NHF network, Authorized Users are responsible for preventing access to any NHF computer resources or data by non-Authorized Users. Performance of illegal activities through the NHF network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of

misuse of the Authorized User's access. For further information and definitions, see the *Acceptable Use Procedure*.

This procedure covers to all Authorized Users with a NHF-owned computer or workstation used to connect to the NHF network and remote access connections used to do work on behalf of NHF, including reading or sending email, accessing network resources, and viewing intranet web resources as well as all technical implementations of remote access used to connect to NHF networks.

It is the responsibility of Authorized Users with remote access privileges to NHF's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to NHF.

1. Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong password from NHF provided devices.

2. Authorized Users shall protect their login and password, even from family members.

3. While using a NHF-owned computer to remotely connect to NHF's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

4. All hosts that are connected to NHF internal networks via remote access must use the most up-to-date anti-virus software.

5. Personal equipment will be restricted from accessing the NHF network and server resources.

Workstation Security Procedure

The purpose of this procedure is to provide guidance for workstation security for NHF workstations in order to ensure the security of information on the workstation and information the workstation may have access to. Additionally, this provides guidance to ensure the requirements of HIPAA Security are met, *see HIPAA Procedure.*

This procedure applies to all NHF Authorized users with NHF owned or personal devices connected to NHF network. Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access to sensitive information is restricted to authorized users.

1. Authorized users accessing workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.

2. NHF will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users, *see HIPAA Procedure.*

3. Appropriate measures include:

a) Restricting physical access to workstations to only authorized personnel.

b) Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.

c) Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password must comply with NHF Password Policy.

d) Ensuring workstations are used for authorized business purposes only.

e) Never installing unauthorized software on workstations.

f) Storing all sensitive information, including protected health information (PHI) on network servers.

g) Keeping food and drink away from workstations in order to avoid accidental spills.

h) Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.

i) Installing privacy screen filters or using other physical barriers to alleviate exposing data.

j) Ensuring workstations are left on but logged off in order to facilitate after-hours updates.

k) Exit running applications and close open documents.

Password Procedure

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of NHF's resources. All Authorized users with access to NHF systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The scope of this procedure includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any NHF facility, has access to the NHF network, and email.

1. Password Creation
    a) All user-level and system-level passwords must conform to:
        - Contain at least 8 alphanumeric characters.
        - Contain both upper and lower case letters.
        - Contain at least one number or at least one special character.

    b) Users must not use the same password for NHF accounts as for other non NHF access (for example, personal ISP & email accounts, bank, and so on).

c) Where possible, users must not use the same password for various NHF access needs.

2. Password Change
    a) All system-level passwords (for example, root, enable, admin, application administration accounts, and so on) must be changed annually.

    b) All user-level passwords (for example, email, database, web apps, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.

3. Password Protection
    a) Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential NHF information.

    b) Passwords must not be inserted into email messages, text messages or other forms of electronic communication.

    c) Passwords must not be revealed over the phone to anyone.

    d) Do not reveal a password on questionnaires or security forms.

    e) Do not hint at the format of a password (for example, "my family name").

    f) Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices without encryption.

    g) Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

Mobile Device Procedure

This procedure is to define standards, procedures, security and safety for end users who have legitimate business uses for connecting mobile devices to NHF corporate network and data. This mobile device policy applies, but is not limited to, all devices and accompanying media that fit the following classifications:

- Smartphones
- Tablets
- E-readers
- Portable media devices
- Portable gaming devices
- Laptop/notebook/ultrabook computers

- Wearable computing devices
- Any other mobile device capable of storing corporate data and connecting to a network

The procedure covers any mobile hardware that is used to access NHF resources, whether the device is owned by the user or by NHF.

The goal of this procedure is to protect the integrity of the confidential business data that resides within NHF technology infrastructure, including internal and external cloud services. It intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it could potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to the NHF's public image. Therefore, all users employing a mobile device connected to NHF network, and/or capable of backing up, storing, or otherwise accessing corporate data of any type, must adhere to company-defined processes for doing so.

Connectivity of all mobile devices will be centrally managed by NHF IT department and will use authentication and strong encryption measures. Although IT will not directly manage personal devices purchased by employees, end users are expected to adhere to the same security protocols when connected to non-NHF equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the NHF's infrastructure.

1. Access Control

    a) IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to NHF and NHF-connected infrastructure. IT will engage in such action if such equipment is being used in a way that puts the NHF's systems, data, and users at risk.

    b) Users who wish to connect such devices to non-corporate network infrastructure to gain access to enterprise data must employ, for their devices and related infrastructure, security measures deemed necessary by the IT department. Enterprise data is not to be accessed on any hardware that fails to meet NHF's established enterprise IT security standards.

    c) All personal mobile devices attempting to connect to the Internet within NHF office must use NHF-Guest network.

2. Security

    a) Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password. Employees agree never to disclose their passwords to anyone.

    b) All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices against being lost or stolen, whether or not they are actually in use and/or being carried.

    c) Any non-corporate computers used to synchronize or back up data on mobile devices will be password protected and have installed up-to-date anti-virus.

d) Passwords and other confidential data, as defined by IT department, are not to be stored unencrypted on mobile devices.

3. User Requirements

a) Users must only load data essential to their role onto their mobile device(s).

b) Users must report all lost or stolen devices to IT department immediately.

c) Users must not load pirated software, illegal content, or jailbreak their devices.

d) Users may must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the NHF email system.

e) Users must not use mobile devices while operating motor vehicle.

Hardware and Software Standard:

Desktop and laptop Operating System: Windows 7 & Windows 10
Desktop: Dell Optiplex
Laptop: Microsoft Surface Pro 4 with Windows 10
Laptop: Lenovo ThinkPad with Windows 10
MS Office: Office 2016
Email platform: Office 365 Exchange
Cloud Storage: OneDrive for Business
Antivirus: Symantec
PDF: Adobe Acrobat
Verizon cell phone – will depend on free device offering from Verizon. Anything outside of free offering will be available at personal out of pocket cost.