A Member of Trinity Health

ACCEPTABLE USE
INFORMATION SECURITY PROCEDURE NO. ISP.1

PROCEDURE

The purpose of this Procedure is to implement the Information Services Policy on information security describing the requirements for Information Security Acceptable Use.

Acceptable Use of Email, Network and Internet

Trinity Health reserves the right to access, monitor, or disclose, as it deems necessary, the contents and history of each User's email messages and network activity for any purpose. Trinity Health may also disclose a User's activity and its content to law enforcement officials and Trinity Health management without the User's consent or prior notice to the User.

Confidential or PHI Confidential Information shall be Encrypted when transmitted over the internet or other public networks.

Users are accountable for the content of their email and internet use. The User shall consider whether Trinity Health would be comfortable if the communication was publicly circulated.

Trinity Health Network Services shall be used to perform approved job functions. Trinity Health recognizes the use of email and Network Services for the following functions as appropriate to fulfill job functions:

A. providing patient care;

B. communicating for the purpose of conducting business;

C. reviewing web sites for product information and services; and

D. researching medical, regulatory or technical information that is appropriate to fulfill job functions.

Users shall adhere to Trinity Health's Communications Policy 1 – Social Media Use.

Inappropriate and Prohibited Use

Users of Trinity Health Information Systems shall not misuse or attempt to alter Information Systems in any inappropriate way. Inappropriate use of an Information System is strictly prohibited.

Users of Trinity Health Information Systems must use the systems in an appropriate manner and protect the information on them. Users of Trinity Health Information have the responsibility to protect that information in a responsible manner consistent with the best interests of Trinity Health.

A. Inappropriate Use

1. Personal use that inhibits or interferes with the productivity of Users or others associated with Trinity Health;

2. Transmission of information that is disparaging to others based on race, national origin, sex, sexual orientation, age, disability or religion, or which is otherwise offensive, or in violation of the Mission and Values of Trinity Health;

3. Disclosure of Trinity Health Information to any individual, inside or outside the organization, who does not have a legitimate, business-related need to know;

4. The unauthorized reproduction of Trinity Health Information or Information System;

5. Engaging in any activity that is illegal under local, state, federal or international law when utilizing Information Systems;

B. Prohibited Use

The use of Network Services for a function that could harm Trinity Health, inappropriately expose Trinity Health Information, or create legal liabilities is prohibited. The following are examples of prohibited uses of the Trinity Health Information Systems:

1. Fraud and Unethical Use

   a. Misrepresenting oneself, or inappropriately representing Trinity Health;

   b. Any misrepresentation/fraud to gain Unauthorized Access to an Information System;

   c. Unauthorized decrypting or attempted decrypting of any system or User passwords or any other User's Encrypted files;

   d. Using the e-mail account of another User without that User's express permission or proxy;

   e. Solicitations that are not specifically approved by Trinity Health Leadership;

   f. Participating in non-Trinity Health sponsored contests and games, or on-line gambling;

2. Service-Impacting

   a. Carelessly utilizing internet capabilities that negatively affect network performance or unduly jeopardize Network Services;

   b. Scanning of the network is prohibited when not within the scope of the User's job function;

   c. Any unauthorized or deliberate action that damages or disrupts Information Systems, alters their normal performance, or causes them to malfunction regardless of location or duration;

   d. Willfully introducing a computer Virus, Malware, or other destructive program into the Trinity Health Network, systems or into external systems or networks;

   e. Connecting to internet services (including email) or utilizing the Network Services for unauthorized purposes;

f. Automatically forwarding email from a Trinity Health email account to an external destination not specifically approved by Trinity Health Leadership;

g. Using the Trinity Health Network Services for Phishing, Spam, or other non-Trinity Health commercial endeavors not specifically approved by Trinity Health Policy, administration, or department management;

3 Offensive / Discriminating Behavior

a. Communications that are demeaning, defaming, harassing, or discriminatory against any person;

b. Accessing, displaying, storing, or distributing offensive, discriminatory, or pornographic materials inconsistent with, or in violation of, the mission or values of Trinity Health; or material that contributes to an intimidating or hostile work environment;

4. Inappropriate Access to, or Disclosure of, Confidential Information

a. Accessing Confidential and PHI Confidential Information that is not within the scope of a User's job function;

b. Dissemination of proprietary, strategic, confidential, private or otherwise restricted information without appropriate approvals and proper security controls;

c. Unauthorized reproductions of Confidential Data; and

d. Any violation of copyright or intellectual property rights laws.

Password Use and Security

A. All Users of Trinity Health Information Systems shall be required to:

1. Keep passwords confidential;

2. Avoid keeping a record (e.g., paper, software file or hand-held device) of passwords, unless this can be stored securely using a solution that has been approved by Enterprise Information Security;

3. Not store together User names and passwords in an unencrypted format;

4. Change passwords whenever there is any indication of possible system or password compromise;

5. Not share individual User accounts or passwords;

6. Not provide their password to anyone for any reason;

7. Not use the same password for business and non-business purposes; and

8. Create passwords according to Information Security Procedure 1.5 - Access Control.

Use and Security of Trinity Health Managed Devices

The User of a Trinity Health Managed Device shall be responsible for the following:

A. Users of Managed Devices must read, sign, and agree to the Trinity Health Confidentiality and Network Access Agreement prior to being assigned to a workstation.

B. All Users are required to complete mandatory security awareness training upon hire and annually thereafter.

C. Users are responsible for managing the care and use of the Managed Device, including its physical security.

1. Users are required to report lost or stolen Managed Devices to the TIS Service Desk and assigned Security Incident Response Team.

2. Users must not misuse Managed Devices in any way.

3. Users must not engage in activities that attempt to circumvent or subvert security controls. Users must not acquire, possess, trade, or use hardware or software that could be employed to evaluate or compromise Information System security.

4. Users may not alter or change in any way Managed Devices (e.g., upgraded processor, expanded memory, or extra circuit boards).

5. Users shall not attempt to disable or modify anti-malware or any other security capabilities on Managed Devices.

6. Users are required to actively protect Managed Devices during and after each session and are responsible for ensuring the security and confidentiality of the device. Users are responsible to:

    a. Ensure the physical security of the Workstation.

    b. Protect the application session.

    c. When using a Clinical Workstation, the User must log out of the application when finished or when leaving the workstation.

    d. When using a Dedicated Workstation, the User must initiate a password protected screen saver or physically protect the workstation when leaving the workstation.

    e. When using a Shared Workstation, the User must initiate the operating system session protection feature, initiate a password protected screen saver, or physically protect the workstation when leaving the workstation.

7. Users are required to actively protect Workstations during and after each computing session and are responsible for ensuring the security and confidentiality of Trinity Health Information residing on the Workstation.

8. Storage or processing of Confidential or PHI Confidential information shall be limited to appropriate business need only.

9. Users shall remove or delete Confidential Data when it is no longer needed, including from the Windows recycle bin.

10. Users shall discuss and receive permission from their supervisor before removing Confidential and/or PHI Confidential Information outside of the workplace.

11. Users shall ensure the integrity and availability of Confidential and PHI Confidential Information.

12. Users shall follow the Data Backup requirements for all data stored on the local drive of the Workstation.

D. Non-Trinity Heath Licensed Software:

1. Users must not install software packages on their Workstation without obtaining advance permission from the local IS Manager. Unapproved software may be removed without User advance notice.

2. If permission to install software packages has been granted, the User must comply with the following:

a. Users must ensure that all non-Trinity Health software running on the Workstation have valid software licenses. Strict adherence to software vendor license agreements and copyrights must be followed.

b. Public domain software, freeware, or shareware must not be downloaded to Trinity Health Workstations.

Security of Trinity Health Managed Devices when Off-Site or Traveling

A. Users must adhere to the following additional security requirements for Managed Devices when taking the Managed Devices offsite or traveling:

1, Only Managed Devices specifically designed for portability (laptops, smartphones, and tablets) shall be removed from Trinity Health facilities.

2. Users shall log off and turn off Managed Devices (except smartphones) when transporting.

3. Users who work from home, remote locations or frequently travel must have updated security patches and virus protection installed.

4. Users must not leave Managed Devices unattended in public places.

5. Users must not place Managed Devices in checked luggage. If necessary, remove the Managed Device from the case and personally carry the Device.

6. Users must lock Managed Devices in the trunk if leaving the vehicle unattended. Users must keep Managed Devices secure and out of plain view if a trunk is unavailable.

7. If a cable lock has been provided to the User, it must be used whenever possible.

8. Managed Devices left unattended in hotel rooms must be logged out, turned off and hidden from plain view. Users should store Managed Devices in a hotel safe; lock them in a piece of luggage or cable lock to an immobile piece of furniture.

9. Unauthorized Access by family members is prohibited, and other non-Trinity Health individuals are prohibited from using any Managed Device. It is the User's responsibility to ensure that family members and others cannot access Trinity Health Information.

Unmanaged Device Security (laptops, desktops, tablets, smartphones)

A. Guest Internet Access for Temporary Service – Guest internet access is provided for Users who bring personal devices into Trinity Health.

B. Wired Connection for Long Term Services - Personal devices that require wired connections for services like printing shall meet the following controls:

1. Require TIS approval - Workstations not owned or managed by Trinity Health must be approved by TIS management prior to connection to Trinity Health Networks and/or connection to, access to, or storage of Trinity Health Data (or Confidential Information).

2. Controls Agreement - Both parties must agree to the following:

a. The degree of protection required for information stored on the equipment, including current anti-virus software and operating system (OS) patches.

b. Storage of limited Business Confidential or PHI Confidential Information on a Workstation.

c. Trinity Health is not responsible for loss or theft for Unmanaged Devices.

d. The Unmanaged Device shall follow the same Policies, Standards, and Guidelines as a Trinity Health Managed Device.

C. Device Security for Personal Mobile Devices

1. Users shall not knowingly download or store Trinity Health Confidential or PHI Confidential Data to their personal mobile devices such as smartphones or tablets.

2. Users that use their Personal Mobile Devices to access Trinity Health Information shall ensure that the device is secure by validating that:

a. Devices are kept up to date with the most recent operating system and software.

b. At a minimum Personal Mobile Devices are protected with a six (6) character device PIN. If capable, enhanced security using biometric protection such as a fingerprint or facial recognition shall be used.

c. Any lost or stolen device used to access or store Trinity Health Information shall be immediately reported to the TIS Service Desk.

Unattended User Equipment

All Trinity Health Users shall be responsible for ensuring the security of Trinity Health Workstations. All Users are required to:

A. Terminate active sessions when finished unless they can be secured by an appropriate locking mechanism (e.g., a password protected screen saver).

B. Log-off Workstations when the session is finished (e.g., do not just turn off the PC screen or terminal).

Clear Desk Requirements

Physical documents with information classified as Trinity Health Confidential or PHI Confidential shall be secured in a locked location such as a safe or cabinet when not in use.

SCOPE/APPLICABILITY

This Procedure is intended to apply to Trinity Health, its Ministries and Subsidiaries.

DEFINITIONS

Account or User Account means the combination of a username and password a User uses to perform functions or interact with Information Systems.

Active Directory means the Microsoft object-based system used to manage Permissions and access to networked resources such as a user, group, application, or device.

Clinical Workstation means a Workstation that is used in the direct delivery of patient care and is intended to be shared by hospital staff including nurses, doctors, and other caregivers. Clinical Workstations are not associated with an individual User.

Confidential Information or Data means information with the highest sensitivity; information that, if released or disclosed, could have competitive value to others and/or would adversely affect Trinity Health, employees or patients.

Dedicated Workstation means a workstation typically assigned to and configured for a specific User. Typically located and used in a desk, cubicle, or office environment. The Workstation may be a laptop or desktop.

Encryption means the conversion of plain text to cipher text through the use of a cryptographic algorithm.

Executive Leadership Team ("ELT") means the group that is composed of the highest level of management at Trinity Health.

Information Systems means an electronic device managed by Trinity Health used to store, transmit, or process Trinity Health Information including but not limited to workstations, servers, networks, network devices, and mobile devices.

Malware means a malicious computer code that performs an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. Examples of malware include a Virus, worm, T+ BNROJAN horse, spyware, some forms of adware, etc.

Managed Device means assets or devices managed by Trinity Information Services (TIS) that satisfy the following seven criteria:

1. Provisioned via TIS standard build and configuration standards
2. Maintained centrally using TIS management tools
3. Member of a TIS Windows Active Directory domain if applicable technically
4. Enforce endpoint security controls via TIS standard tools
5. Inventoried and maintained in Configuration Management Database (CMDB)
6. Infrastructure patched and application upgraded as part of TIS procedures
7. Supported via a TIS Assignment Group or Team

Ministry means a first tier (direct) subsidiary, affiliate, or operating division of Trinity Health that maintains a governing body that has day-to-day management oversight of a designated portion of Trinity Health System operations. A ministry may be based on a geographic market or dedication to a service line or business. Ministries include Mission Health Ministries, National Health Ministries, and Regional Health Ministries.

Network means a group of Information Systems, Workstations, and other hardware devices that are linked together through communication channels to facilitate communication and resource-sharing.

Network Services means applications or tools provided to Users for the purpose of communication over the Trinity Health Network. Includes email, VoIP calling, instant messaging, team collaboration tools, official Trinity Health social media accounts, file transfer services, and file storage services.

PHI Confidential Information or Data ("PHI") means information that: (i) is created or received by a Health Care Provider, Health Plan, or Health Care Clearinghouse; (ii) relates to the past, present or future physical or mental health or condition of an individual; the provision of Health Care to an individual, or the past, present or future Payment for the provision of Health Care to an individual; and (iii) identifies the individual (or for which there is a reasonable basis for believing that the information can be used to identify the Individual).

Phishing means a technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.

Policy means a statement of high-level direction on matters of strategic importance to Trinity Health or a statement that further interprets Trinity Health's governing documents. System Policies may be either stand alone or Mirror Policies designated by the approving body.

Procedure means a document designed to implement a policy or a description of specific required actions or processes.

Shared Workstation means a workstation that is shared by multiple Users for non-clinical purposes.

Spam means electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

TIS Service Desk means the Trinity Health Information Services (TIS) team responsible for Level 1 or first call User support.

Trinity Health Information means a record in paper or electronic format that contains information classified as Unclassified, Internal, Confidential, or PHI Confidential. See data classification in ISP 1.4 Asset Management.

Trinity Health Leadership means employees that are in an official management position.

Trinity Health Network means a group of Information Systems, Workstations, and other hardware devices that are linked together through communication channels to facilitate communication and resource-sharing

Unauthorized Access means access to Trinity Health Information, Information Systems, or facility by an individual that has not been granted explicit permission to do so.

Unmanaged Devices means assets or devices not under the direct control of Trinity Information Services (TIS).

User means an individual who has been granted explicit permissions to access, modify, delete, and/or utilize Trinity Health information.

Virus means a hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting (i.e., inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

Workstation means a Trinity Health Managed Device used to conduct business on behalf of Trinity Health.

RESPONSIBLE DEPARTMENT

Further guidance concerning this Procedure may be obtained from Enterprise Information Security.

RELATED PROCEDURES AND OTHER MATERIALS

- Information Services Policy No. 1 – Information Security
- Information Security Procedure ISP.4 - Asset Management
- Information Security Procedure ISP.5 - Access Control
- Information Security Procedure ISP.9 – Business Continuity Management
- Communications Policy No. 1 – Social Media Use
- Confidentiality and Network Access Agreement
- Functional Records Management Guidelines
- Control Alignment Matrix

APPROVALS

Initial Approval: October 19, 2019

Subsequent Review/Revision(s): N/A

DOCUMENT CONTROL TRACKING FILE

Title: Acceptable Use (IS Procedure ISP.1)	
Standard: NIAHO:_____ CMS_____ ISO_____	
Document Owner: Director of Information Services	Forms #:
Reviewed by the following:	
Regional Information Security Officer	Date: 1/20
Director of Information Services	Date: 1/20
	Date:
	Date:
	Date:
	Date:

Administrative Approvals:

Joseph W. Spinale, D.O.
Chief Medical Officer

AnneMarie Walker-Czyz, RN, Ed.D
Chief Nursing Officer

Additional Approvals:

Education:

Monthly policy/procedure update: 2/20

Additional:

Revisions: 1/20 Mirror policy from Trinity

References:

Original Date: 1/20	Reviewed/Revision Dates: