ST. JOSEPH'S HEALTH

A Member of Trinity Health

INFORMATION SECURITY: INFORMATION SECURITY ASSET MANAGEMENT
PROCEDURE NO. ISP.4

PROCEDURE

The purpose of this Procedure is to implement the Information Services Policy on information security describing the requirements for Asset Management.

Inventory of Assets

A. All Information Systems shall be inventoried and maintained in the system of record approved by Trinity Health. At a minimum, each asset record shall have the following information:

1. Name;
2. Status;
3. Class and Subclass;
4. Environment;
5. Location;
6. Business/Application Owner;
7. Software License Status;
8. Internet Accessible;
9. TIS (Trinity Information Services) Managed Device;
10. Whether the Information System contains PHI Data.

B. Trinity Information Services (TIS) requirements

1. All Trinity Health System Owners shall be responsible for ensuring that TIS hardware and enterprise software tools are inventoried in the Configuration Management Database (CMDB).

2. All Trinity Health Application Owners shall be responsible for ensuring that applications supporting a business or clinical process are inventoried in the Application Portfolio Management (APM) system.

Equipment Maintenance

A. All Trinity Health Information Systems shall be maintained in accordance with the supplier's recommended service intervals and specifications. Only authorized maintenance personnel shall carry out repairs and service equipment. Appropriate controls shall be implemented when equipment is scheduled for maintenance (e.g., authorization levels) taking into account whether this maintenance is performed by personnel on site or external to the organization.

B. TIS shall be responsible for obtaining maintenance support and/or spare parts for defined key information system components within the applicable Recovery Time Objective (RTO) specified in the TIS Business Continuity Plan and Recovery Plan.

Clock Synchronization

The clocks of all Trinity Health systems shall be synchronized with an agreed accurate time source to support tracing and reconstitution of activity timelines.

Ownership of Assets

All Trinity Health Information Systems shall be documented in the asset management system with an assigned owner of responsibility, contact information and purpose.

Trinity Health Information Classification

A. All Trinity Health Information shall be classified based on the following:

1. Unclassified Data is information that has been made available for public distribution through authorized Trinity Health channels. Unclassified Data is not proprietary in context or content.

2. Internal Data is information intended to conduct business and is proprietary in nature. This information, if released or disclosed, could have competitive value to others and/or could adversely affect Trinity Health in other ways; but the likelihood of serious harm is low. Access, use, and distribution of Internal Data is limited to Trinity Health Users with Authorized Access.

    a. All information that is not labeled or otherwise identified as PHI Confidential, Confidential or Unclassified is considered Internal.

3. Confidential Data is information that is highly sensitive information to Trinity Health that if released or disclosed, could have competitive value to others and/or would adversely affect Trinity Health.

    a. Access to Confidential Data is restricted to Users on a need to know basis when performing their job duties.

    b. Confidential Data will possess one or more of the following attributes:

        (i) If disclosed, could violate the privacy of others (including patient information, employee information, personnel matters, etc.);

        (ii) Would cause reputational, financial, or other damage to Trinity Health if released;

        (iii) Provides Trinity Health a competitive advantage (strategic plans, medical research, etc.);

        (iv) Is necessary for the continuation of a critical business function; and/or

        (v) Regulatory or legal requirements for Trinity Health to protect.

4. PHI Confidential is established as a separate category due to the significance in regulatory requirements and due to the volume and importance of the information within Trinity Health. PHI Confidential is any information that:

    a. Is held, created or received by a health care provider, health plan, or health care clearinghouse; and

        - Relates to the past, present or future physical or mental health or condition of an individual; or

        - The provision of health care to an individual; or

- Relates to the past, present or future payment for the provision of health care to an individual; and

e. Identifies the individual (or for which there is a reasonable basis for believing that the information can be used to identify the individual).

Managed Mobile Device Security

A. Trinity Health Managed Mobile Devices including smartphones and tablets shall adhere to the Information Security Standard - Mobile Device/Platform Security Standard.

B. Trinity Health Managed Mobile Devices shall require:

1. Enrollment in the Mobile Device Management (MDM) system;

2. Minimum personal identification number (PIN) or passcode length of six (6) characters OR biometric protection such as a fingerprint or facial recognition;

3. Device auto-lock time not to exceed fifteen (15) minutes;

4. Auto device-wipe after five (5) failed Authentication attempts;

5. Remote device-wipe enabled; and

6. Device Encryption.

C. Lost or stolen mobile devices shall be immediately reported to the TIS Service Desk and assigned the Security Incident Response Team.

Change Management

All changes to Information Systems shall follow the established Enterprise Change Management process and must be tracked in the change management system. All changes to Information Systems, including changes performed by Third Party Users, are required to follow a formal change management process that ensures changes are documented, scheduled, approved, and communicated prior to implementation and implemented under the control of change management.

A. All new Trinity Health Information Systems, upgrades, and version changes shall meet the following criteria prior to being moved to production:

1. Documented evidence of successful testing;

2. Completed Enterprise Information Security Risk Assessment;

3. Formal approval from the Trinity Health Change Management Approval Board when prescribed by the Enterprise Change Management process; and

4. To avoid segregation of duties conflicts, developers shall be restricted from implementing changes in production systems.

B. Information Systems shall be separated into distinct environments for development, testing, and production.

C. Trinity Health Application Owners shall minimize any testing in production systems.

D. Trinity Health Application Owners shall retain evidence of successful unit, system, and User acceptance testing in an environment segregated from development and production.

E. The use of production data for testing purposes shall be De-Identified prior to testing to ensure all sensitive information is removed or modified beyond recognition.

1. If production data cannot be De-Identified prior to testing, all testing and development environments shall adhere to all security controls and Information Security Procedures.

F. A contingency plan shall document all changes to the system and the procedures for reverting any changes made to the system (e.g., removing test accounts).

Capacity Management

Information Systems shall be monitored to ensure the availability of adequate capacity and resources are managed to deliver the required system performance. Projections of future capacity requirements shall be made to mitigate the risk of system overload.

Disposal of TIS Hardware

All Managed Devices shall be securely disposed of or sanitized when no longer required. To ensure that any hardware is properly disposed of, all disposals shall have an official Hardware Disposal Request assigned to the TIS Service Management Team.

Lost or Stolen Managed Devices

Lost or stolen Managed Devices shall be immediately reported to the TIS Service Desk and assigned the Security Incident Response Team.

Return of Assets

All Trinity Health Managers shall be responsible for ensuring any Managed Workstation or Managed Mobile Device is returned upon a User's separation.

Information Labeling and Handling

A. All Trinity Health Information shall be:

1. Shared only with Users with a business need to know;

2. Shared outside Trinity Health only when a business need exists;

3. Safeguarded with logical and physical controls

4. Labeled with the proper data classification; and

5. Handled in accordance with the TIS Information Handling Standard.

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.

Application Owners means an employee or group with the responsibility to ensure that the application accomplishes the specified objectives and requirements for that application, including appropriate security safeguards.

Application Portfolio Management (APM) means a Clarity database that contains all relevant information about the applications used by Trinity Health Ministries.

Authentication means the process of determining whether a User or account is in fact who or what it is declared to be. Authentication may be performed through (i) something you know (e.g., password/PIN); (ii) something you have (e.g., token, FOB, mobile device); or (iii) something you are (e.g., fingerprint or biometric).

Authorized Access means access to Trinity Health Information, Information Systems, or facility by an individual that has been granted explicit Permission to do so.

Business Continuity Plan means the plan that provides departmental direction and procedures to continue critical business services while recovery and restoration efforts are underway.

Change Management Approval Board means the group of Trinity Health employees responsible for reviewing and approving changes as part of the Enterprise Change Management process prior to the changes being moved to production.

Confidential Data Information means data 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.

Configuration Management Database (CMDB) means a database that contains all relevant information about the Information Systems used in an organization and the relationships between those components.

De-Identified means the process used to prevent a person's identity from being connected with information. For PHI Confidential Data, there are two methods to de-identify data in accordance with HIPAA: Expert Determination (apply statistical principles) and Safe Harbor (remove the 18 PHI identifiers).

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

Enterprise Change Management means the formal TIS-approved process for making changes to Information Systems, which includes documentation of the change, testing, approval, and communication.

Information System 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.

Internal Data means information used to conduct business, and is proprietary in nature. If data is released or disclosed, it could have competitive value to others and/or could adversely affect Trinity Health in other ways; but the likelihood of serious harm is low.

Manager means an employee who oversee the work of other employees and provides direction on their work.

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; and
7. Supported via a TIS Assignment Group or Team.

Managed Mobile Devices means a subset of Managed Devices that include mobile phones, smartphones, tablets, and mobile hot spots.

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.

Mobile Device Management (MDM) means software that allows System Administrators to control, secure and enforce policies on smartphones, tablets and other endpoints.

Permissions means the rights granted to a User Account that determine the tasks that can be performed and the features or Trinity Health Information that can be accessed.

PHI Confidential Data 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).

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.

Recovery Plan (Playbook) means the Information Technology plan that defines recovery roles/responsibilities, resources, actions, and data required to restore system service.

Recovery Time Objective (RTO) means the maximum tolerable length of time systems, applications, or services must be recovered after a failure or disaster.

Risk Assessment means the process of identifying the risks to Information System security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Also known as risk analysis.

System Administrator means an individual who is responsible for the upkeep, configuration, and reliable operation of Information Systems; especially servers. The System Administrator seeks to ensure that the uptime, performance, resources, and security of the computers they manage meet the needs of the users.

System Owners means an employee or group with the responsibility to ensure that the system accomplishes the specified objectives and requirements, including appropriate security safeguards.

Third Party means an external entity with whom Trinity Health has a relationship. External entities may include, for example, service providers, vendors, supply-side partners, demand-side partners, alliances, consortiums, and investors, and may include both contractual and non-contractual parties.

Third Party User means a non-employee individual who has been granted explicit Authorization to access, modify, delete, and/or utilize Trinity Health Information. May include contractors, vendors, non-credentialed Physicians, business partners, consultants, etc.

Trinity Information Services (TIS) means the Trinity Health Information Technology department.

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

Trinity Health Information means any record in paper or electronic format that contains information classified as Unclassified, Internal, Confidential, or PHI Confidential. *See* Data Classification in Information Services Procedure No. 1.4 - Asset Management Procedure.

Trinity Information Services (TIS) means the Trinity Health IT department.

Unclassified Data means information that has been made available for public distribution through authorized Trinity Health channels. Unclassified information is not proprietary in context or content.

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

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.5 – Access Control
- Control Alignment Matrix
- Enterprise Change Management Reference Documentation
- Configuration Management Database (CMDB) Job Aid
- Application Portfolio Management (APM) Job Aid
- Information Handling Standard
- Information Security Standard - Mobile Application Security Standard
- Information Security Standard - Mobile Device/Platform Security Standard

APPROVALS

Initial Approval: October 19, 2019
Subsequent Review/Revision(s): N/A

DOCUMENT CONTROL TRACKING FILE

Title: Information Security: Information Security Asset Management (IS Procedure ISP.4)	
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: