FORT HAYS STATE UNIVERSITY

University Policies
www.fhsu.edu/policies/

POLICY TITLE: Information Security Policy

POLICY PURPOSE:

This Information Security Policy defines the security requirements that everyone with access to information technology services at FHSU is expected to be familiar with and consistently follow. These security measures are set forth to avoid problems that affect the Confidentiality, Integrity, and Availability of information and systems at the University.

The Policy is an important part of the University's efforts to create a secure environment in which to carry out the mission of the University. Security requires the participation of each constituent who comes into contact with University information or systems.

BACKGROUND:

KITEC Information Technology Policy 7230 requires that all State of Kansas agencies, including Regents' institutions, implement an Information Technology Security Policy.

KITEC Information Technology Policy 7230A establishes minimum security standards and procedures for all State of Kansas agencies, including Regents' institutions.

The Safeguards Rule of the Gramm-Leach-Bliley Act of 1999 (GLBA) requires financial institutions, which the Federal Trade Commission (FTC) explicitly indicated includes higher education institutions, to have an information security program to protect the confidentiality and integrity of personal information.

Payment Card Industries (PCI) Data Security Standard (DSS) requires organizations that handle branded credit cards from the major card schemes to institute and implement an Information Security Policy.

APPLIES TO:

This policy applies to all individuals who are issued a user account on any FHSU information technology system.

This policy applies to any information technology device owned by the University or any information technology device used for University business by faculty, staff, students, and affiliates.

This policy applies to any device that obtains an Internet Protocol (IP) address from the University.

DEFINITIONS:

Affiliated Organization (or "Affiliates") Any organization associated with the University that uses university information technology resources to create, access, store, or manage University Data to perform their business functions.

KITEC: Kansas Information Technology Executive Council

System users: Faculty, staff, students, official university affiliates, and any other individuals who use FHSU computing resources.

TigerNetID: Username assigned to System Users upon employment, acceptance to, or the beginning of a business relationship with FHSU.

University data: Electronic information providing support to and meeting needs of the University community. Data includes, but is not limited to:

- Elements supporting financial management;
- Student records;
- Payroll;
- Personnel records;
- Capital equipment inventory; and,
- Any electronic information:
    - Used for planning, managing, reporting, or auditing a major administrative function;
    - Referenced or used by a Department(s) or College(s) to conduct University business;
    - Included in a University administrative report; or,
    - Used to derive a data element meeting any of the criteria above.

CONTENTS:

Contents

POLICY STATEMENT:

Overall Security Statement

Security requirements will be in place for the protection of the privacy of information, protection against unauthorized modification of information, protection of systems against the denial of service, and protection of systems against unauthorized access. System Users are reminded that all usage of

FHSU's information technology resources is subject to all University policies including the Acceptable Use of Computing Resources Policy.

This policy directs that FHSU meet the requirements as stipulated by KITEC Information Technology Security Standards (policy 7230A). This policy will be supported by procedures that set forth the detailed requirements that apply to individuals, devices, and systems.

Responsibilities

Computer Security Incident Response Team (CSIRT)

The CSIRT team will consist of the Information Security Officer (ISO), a Windows System Administrator, a Linux System Administrator, a Network Administrator, a TigerTech Tier 2 full-time employee, Asst VP of Tech Services and a member of the application development team.

Responsibilities include coordinating the campus-wide response to major security incidents; coordinating implementation of preventative measures; communicating threats and best practices to University colleges/units; approving requests for restoring network access to vulnerable or compromised computers; participating in the development of IT security policies, standards, guidelines, and procedures; and assisting with IT security training and awareness efforts. CSIRT duties should constitute no more than 30% of an individual's job responsibilities, with the exception of the ISO.

The CSIRT is authorized to evaluate the seriousness and immediacy of any threat to information resources and to take action to mitigate that threat, including disconnection of information resources. The CSIRT will evaluate the impact of disrupting service when devising an action plan that mitigates any threat.

Risk Management Committee

The Risk Management Committee will consist of the ISO, University General Counsel, Internal Auditor, and line of business representatives.

Responsibilities include ensuring that risks are assessed; directing the investigation, mitigation, and acceptance of risks on behalf of FHSU; approving variances to KSIRT 7230A at FHSU; and approving exclusions or special circumstances to FHSU's Information Security Policy and all related policies and procedures.

FHSU Information Security Officer

The ISO will investigate Security Events and respond to Security Incidents in accordance with established procedures. The ISO will lead the Computer Security Incident Response Team (CSIRT).

ISO will cultivate awareness of security issues and vulnerabilities within the University.

ISO will assess risks to University systems as defined by this policy in accordance with established procedures. Findings will be presented to the Risk Management Committee.

Technology Services Staff

All Technology Services staff must abide by all Technology Services and University policies and make security a priority when designing, building, implementing, upgrading, decommissioning, or otherwise working with information technology resources.

Deans, Vice Presidents and Department Heads

Deans, and Vice Presidents and department heads are responsible for authorizing access to computer systems in their units, ensuring that System Users understand and agree to comply with FHSU policies, and ensuring that the technical and procedural means and resources are in place to assist in maintaining security policies and procedures.

Authorized Users of Information Technology

System Users must follow the Acceptable Use of Computing Resources Policy, as well as all other FHSU policies and procedures.

System Users share in responsibility for information security by following all applicable security policies and procedures. Responsibilities include agreeing to and complying with all applicable FHSU policies and procedures; taking appropriate precautions to prevent unauthorized use of their accounts, software, and computers; protecting University Data from unauthorized access, alteration, or destruction; representing themselves truthfully in all forms of electronic communication; and respecting the privacy of electronic communication.

System Users must report any discovered unauthorized access attempts or other improper usage of FHSU information resources. Report observed or suspected violations to TigerTech (www.fhsu.edu/tigertech).

End Point Protection and Configuration

Desktops, laptops, servers, and all other end points must be configured in accordance with the “End Point Protection and Configuration Policy,” and all related procedures.

Protection of University Data

Technology Services will perform regular backups of University Data that resides on servers owned by FHSU, as detailed by the “End Point Protection and Configuration Policy.”

In the event that a department outside of Technology Services or an affiliated organization is responsible for storing or maintaining University Data, that entity must comply with the "End Point Protection and Configuration Policy."

The "Media Sanitization and Disposal Policy" must be followed when disposing of media that contains or may contain University Data.

Servers owned by FHSU that contain University Data must be housed in the Data Center and protected according to the "Physical Security of Data Center and University Data Policy."

Account Management

System Users must be identified by a unique system identifier (username).

All information system accounts will provide the most restrictive set of privileges required. Separation of duties will be enforced through account privileges; no single user will have privileges to authorize, perform, review, and audit a single transaction.

User access to FHSU information systems will be authorized by an appropriate FHSU official and accounts will be provisioned according to the "Access Control Procedures."

Access may be granted to persons who are not FHSU employees or students according to the "Third-Party Access to FHSU Information Systems Procedure."

Upon termination of employment or relationship with FHSU, an individual's user accounts will be disabled, removed, or reverted to a student account in accordance with the "Account Termination Procedure."

In cases where a multi-user or generic account is necessary, such as for a kiosk or public-use computer, the account must be restricted so it can only logon to a limited number of computers. All multi-user or generic accounts must be approved and created according to the "Generic Account Procedure."

Passwords

Default account passwords that are included in many applications and systems must be changed immediately.

All FHSU systems and services must be configured to meet the following minimum guidelines:

- Passwords must be at least 12 characters in length;
- Passwords must be made using at least 3 of the following 4 groups of characters:
  - Uppercase alphabetic characters (A-Z)
  - Lowercase alphabetic characters (a-z)
  - Numbers (0-9)
  - Special characters (i.e., #, &, *...)
- Passwords must be changed immediately upon first log-in, and at least every 360 days;

- Passwords must be different than the username, first name, or last name of the account holder;
- Passwords must be different from the previous 24 passwords.
- Passwords must never be transmitted over the network in clear text (e.g., it must always be encrypted in transit).
- Accounts will be restricted to a maximum of thirty (30) consecutive failed attempts before being locked out.
- Accounts will remain locked out for a minimum of thirty (30) minutes without administrator intervention.

System Users are expected to meet the following additional requirements when creating and handling passwords for an FHSU system or service:

- Passwords must not consist solely of a single word found in a dictionary;
- Passwords must not consist solely of a familiar name (e.g., relatives, pets);
- The password used to access FHSU systems (e.g., your TigerNetID password) must not be used for non-FHSU systems or applications such as online shopping, banking, etc.
- Passwords must never be communicated via clear text, including unencrypted email.
- Passwords must never be shared with other System Users or any other individual.

Contracts with Third Parties

Contracts between the University and third parties involving University Data must include language requiring compliance with all applicable laws, regulations, and University policies related to data and information security. Contracts must stipulate immediate notification of the University if University Data is used or disclosed in any manner other than allowed by the contract and, to the extent practicable, require the third party to mitigate any harmful effect of such use or disclosure.

Enforcement

Enforcement of this policy and associated policies and procedures is the responsibility of the Asst VP of Technology Services or designee. Any system that does not comply with security policies and standards, is susceptible to a known vulnerability, or is compromised may have its network access blocked immediately and without prior notification to protect the integrity of other systems and data.

Any device directly connected to the campus network (e.g., with a direct wired or wireless connection, remote access software like Windows Remote Desktop, use of a Virtual Private Network (VPN), and the like) may be scanned and assessed by designated information technology staff at any time to determine compliance with security policies and standards, or detect anomalous activities, vulnerabilities, and security compromises. Firewalls must be configured to permit this remote scanning function. Scanning may only be performed to the extent necessary to detect and assess the risk.

Consequences

Faculty, staff, and student employees who violate this policy may be subject to disciplinary action for misconduct and/or performance based on the administrative process appropriate to their employment.

Students who violate this policy may be subject to proceedings for non-academic misconduct based on their student status.

Faculty, staff, student employees, and students may also be subject to the discontinuance of specified information technology services based on the policy violation.

EXCLUSIONS OR SPECIAL CIRCUMSTANCES:

Variances to this Policy will only be allowed if previously approved by the FHSU Risk Management Committee, as documented in the Information Security Exception Procedure.

RELATED DOCUMENTS:

Policies:

Acceptable Use of Computing Resources Policy

Data Classification Policy

Email Policy

Endpoint Protection and Configuration Policy

Media Sanitization and Disposal Policy

Physical Security of Data Center and University Data Policy

Security Awareness Training Policy

Forms:

Other:

Access Control Procedure

Account Termination Procedure

Generic Account Procedure

Information Security Exception Procedure

Third-Party Access to FHSU Information Systems Procedure

KEYWORDS:

Information technology, information security, passwords

RESPONSIBLE OFFICE:

Division of Technology Services

RESPONSIBLE UNIVERSITY OFFICIAL:	Asst VP of Technology Services
ORIGINATION DATE:	Adopted by President's Cabinet 12/02/09
CHANGE HISTORY:	Adopted by President's Cabinet 12/02/2009 Adopted by ELT 3/31/2017 Adopted by ELT 6/19/2017