FORT HAYS STATE UNIVERSITY
Forward thinking. World ready.

University Policies
www.fhsu.edu/policies/

POLICY TITLE: Security Awareness and Training Policy

POLICY PURPOSE: To help reduce the risk of human error, theft, fraud, or misuse of Fort Hays State University's information assets, all persons having access to those assets should be aware of the role they play in helping maintain the security of those assets. This policy sets out to ensure that everyone is aware of their role and is also intended to help foster an understanding of how the Information Security Policy protects FHSU, its employees, and its students.

BACKGROUND: KITEC Information Technology Policy 7230 instructs all State of Kansas agencies to implement Security Awareness Training.

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 and train employees on that policy.

APPLIES TO: FHSU employees, student employees, and any other person who has access to FHSU's internal network.

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.

ISO: Information Security Officer within the Division of Technology Services

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 and password 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:

Required Training

FHSU will provide and conduct security awareness training in accordance with the KITEC Information Technology Security Standards (policy 7230A).

Security awareness training is required for System Users. This includes visiting faculty, emeritus or retired faculty, contractors, or business partners with access to student or personnel data, the internal FHSU network, or the FHSU VPN.

Responsibilities

The ISO will oversee FHSU's Security Awareness and Training program, including development, implementation, testing, and annual review of content.

The ISO or designee will coordinate, monitor and track the completion of the Security Awareness Training for all System Users and report incomplete training to the respective manager or responsible party.

The ISO or designee will ensure that current versions of the FHSU security policies and procedures are included in the Security Awareness Training.

The Risk Management Committee will determine which training modules to assign. Security Awareness and Training will include, at a minimum, contents described in the Kansas information Technology Executive Council's Information Technology Security Standards (policy 7230A), section 8.5.

Each manager, department chair, or director is responsible for ensuring that his or her respective employees and student employees complete mandatory Security Awareness Training. Each manager, department chair, or director is also responsible for visiting faculty, retired or emeritus faculty, contractors, or business partners who gain access to the internal FHSU network at the request of a department.

All new System Users will complete the Security Awareness Training course within the first 30 days of commencing work and repeat the training at least on an annual basis afterward.

All System Users will acknowledge that they have read, understand, and accept the FHSU Information Security policies and procedures included in the training.

Consequences

The ISO or designee may revoke information technology access until mandatory Security Awareness Training is completed.

EXCLUSIONS OR SPECIAL CIRCUMSTANCES:

RELATED DOCUMENTS:

Policies:

Acceptable Use Policy

Data Classification Policy

Email Policy

Endpoint Protection and Configuration Policy

Information Security Policy

Media Sanitization and Disposal Policy

Physical Security of Data Center and University Data Policy

Forms:

Other: FHSU Security Awareness and Training Procedure

KEYWORDS: Security, information technology, training

RESPONSIBLE OFFICE: Division of Technology Services

RESPONSIBLE UNIVERSITY OFFICIAL: Director of Technology Services

ORIGINATION DATE: 3/2017

REVIEW CYCLE: Every 3 years

POLICY ADDRESS:	
LAST APPROVED ON:	Adopted by ELT 3/31/2017
REVIEW/CHANGE HISTORY:	
NEXT REVIEW DATE:	3/2020