FORT HAYS STATE UNIVERSITY

University Policies
www.fhsu.edu/policies/

POLICY TITLE: Endpoint Protection and Configuration Policy

POLICY PURPOSE: The purpose of this policy is to outline the minimum security protections to be employed on all endpoints.

BACKGROUND: KITEC Information Technology Policy 7230 instructs all State of Kansas agencies to implement policies for configuration management, system and communication protection, and system and information integrity.

Payment Card Industries (PCI) Data Security Standard (DSS) requires organizations that handle branded credit cards from the major card schemes to develop and maintain secure systems and applications, protect all systems against malware, and regularly update anti-virus software.

APPLIES TO: This policy applies to all server and workstation computers owned or controlled by FHSU, including but not limited to: desktops, laptops, tablets, and servers (hereinafter "endpoints").

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.

Endpoint: all server and workstation computers owned or controlled by FHSU, including but not limited to: desktops, laptops, tablets, and servers.

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:

Asset Inventory

Technology Services shall maintain an asset inventory of information systems components and update it as changes are made. The inventory shall be reviewed annually.

The asset inventory shall also identify and document the relationships between each of the information system components and the ownership of each component.

Configuration Management

All systems will be built from a standard configuration baseline, in accordance with the System Configuration Procedure.

Change Control

Technology Services shall adhere to the Change Control Procedure when making changes to production servers and infrastructure systems.

Virus Protection

All university-owned computers must use the university-supplied antivirus software configured in a managed mode (managed mode allows a server to monitor and configure the antivirus protection on the client computer and push updates to the client on demand).

All other computers accessing the FHSU campus network must be running active, up-to-date virus protection software.

Antivirus software must be activated when the computer boots up and remain active at all times during its operation.

On-access file scanning must be enabled where files are scanned for malicious anomalies as they are read or written.

The version of the antivirus software (e.g., the antivirus program or engine) must be no more than one version behind the current version offered by the vendor.

Virus definition files (e.g., the database in the antivirus software that identifies known malware) must be up-to-date with the most current version available from the vendor.

Checking for and installing updates to virus definition files and antivirus software must be automated and performed at least daily.

Comprehensive virus scans of all local hard drives must be performed at least weekly.

Spyware/Adware Protection

All computers connected to the campus network must run active spyware/adware protection software.

Spyware/adware definition/detection rules must be up-to-date with the most current version available from the vendor.

Scans of all local hard drives for spyware/adware must be performed at least weekly.

Personal Firewall Protection

All university-owned computers must have the firewall enabled.

Any other computer connected to the campus network must run a personal firewall. Microsoft Windows Firewall is an acceptable personal firewall.

Backups

Servers owned by FHSU and containing University Data must be backed up according to the Backup Procedure.

Technology Services will conduct an annual test of the backup system as detailed in the Backup Procedure.

System Patching

All systems connected to the campus network and the applications running on those systems must have the latest security patches available from the

respective vendors applied. Any system or application with known vulnerabilities for which a patch is not available must take appropriate measures to mitigate the risk, such as placing the system behind a firewall. FHSU may block access to the network for systems that have not been patched. Mitigating factors must be approved by the Risk Management Committee with advice from the Computer Security Incident Response Team.

Technology Services will monitor vendor's websites as well as other resources for information about updates to all FHSU owned or controlled systems and applications.

Patches will be distributed and applied per the System Patching Guidelines and Standards.

Owners will be responsible for applying system patches to personally owned devices connecting to the FHSU network.

Technology Services will periodically perform a vulnerability scan on the systems attached to the network. Systems not having the proper patch level will be reported to the Information Security Officer (ISO) for further action.

End-of-Life Operating Systems and Software

The "End-of-Life" (EOL) process is a series of technical and business milestones and activities that, once completed, make a product or service obsolete. Once obsolete, the product or service is no longer sold, manufactured, improved, repaired, maintained, or supported. Endpoints running EOL operating systems or software must be retired according to the Unsupported Operating Systems and Software Procedure.

System use Notification Banner

Every login process for FHSU systems, multi-user computers, and infrastructure devices must include a standard system use notification banner.

System Users shall acknowledge the system use notification banner before gaining access to the information system.

The Risk Management Committee will develop standard language to be used in all logon banners. This language will reflect the Acceptable Use Policy.

Technology Services staff will be responsible for applying the banner to University systems.

For those devices that allow multiple avenues for logging in, this banner must be present at each avenue (e.g. server that allows desktop access as well as FTP access).

Digital kiosks and other devices that login automatically and are only used to display information may be exempt from the system use notification banner. The ISO is responsible for approving exclusions.

Unattended Computers

All university computers must require a password for re-entry after they have been inactive for a maximum of 30 minutes.

Remote access to systems that house Restricted-Use Information must be automatically disconnected after a maximum of 30 minutes of inactivity.

System Users are advised to never leave a computer unattended and unprotected. Before leaving a computer, System Users must lock the display or log out in a manner that requires a password to gain access.

Special-purpose computers designed for public access or digital signage are exempt from the requirements in this section.

Time Synchronization

All production information systems shall be configured to have time synchronized with authoritative time sources.

Server Redundancy and Virtualization

Virtual servers are preferred over physical servers due to enhanced fault tolerance and ease of management. Physical servers may only be used when vendor specifications or specialized hardware prevent the use of a virtual server. Physical servers must be configured with dual power supplies and use RAID configured in such a manner that data will not be lost if a single disks fails.

Enforcement

Systems found to be out of compliance with this policy and related procedures may have network access revoked until the problem is corrected.

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 Policy

Data Classification Policy

Email Policy

Information Security Policy

Media Sanitization and Disposal Policy

Physical Security of Data Center and University Data Policy

Security Awareness Training Policy

Forms:

Other:

Change Control Procedure

Unsupported Operating Systems and Software Procedure

Information Security Exception Procedure

KEYWORDS:	configuration management, change control, virus scan, firewalls, backups, system patching, unattended computers, information technology
RESPONSIBLE OFFICE:	Division of Technology Services
RESPONSIBLE UNIVERSITY OFFICIAL:	Director of Technology Services
ORIGINATION DATE:	3/2017
CHANGE HISTORY:	Adopted by ELT 3/31/2017