Purpose

The University recognizes its responsibility to protect its information technology resources and environment whether information is on site, in-transit or hosted off-site. As such, this policy provides the overarching methodology to safeguard university systems and data internally and externally hosted.

Authority, Responsibilities, Duties and Scope

This policy applies to all University employees (permanent, temporary, contractual, faculty, administrators and students) who use VSU information technology resources to conduct University business.

These roles and responsibilities are assigned to individuals, and may differ from the actual role title or working title of the individual's position. Individuals may be assigned multiple roles, as long as the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests.

A. Chief Information Officer (CIO)

The CIO will give the Technology Service Team direction to ensure the criteria and methodology to protect university systems and data are both valid and financially feasible.

B. Information Security Officer (ISO)

The ISO will identify all information technology processes designed to protect systems and data and ensure that procedures maintain appropriate levels of security to maintain system and data integrity.

C. Enterprise Manager

The Enterprise Manager is responsible for ensuring that the enterprise management team is trained and educated on the details of the Physical and Environmental Protection Policy and Procedure to ensure that the process is fully understood and implemented.

Definitions

The IT security definitions and terms can be found in the Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Glossary. It is referenced on the ITRM Policies, Standards, and Guidelines web page on www.vita.virginia.gov/library.

Policy Statements

A. Physical Access Authorizations

When safeguarding IT systems and data assets the Enterprise Management Team, Security Team and the ISO (Technology Services Team) will:

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the information system resides;
b. Issue authorization credentials for facility access;
c. Review the access list detailing authorized facility access by individuals on an annual basis or more frequently if required to address an environmental change; and
d. Remove individuals from the facility access list when access is no longer required
e. Temporarily disables physical access rights when personnel do not need such access for a prolonged period in excess of 30 days because they are not working due to leave, disability or other authorized purpose.
f. Disables physical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes.

B. Physical Access Control

When controlling physical access to systems and data the Enterprise Management Team, Security Team and the ISO (Technology Services Team) will:

a. Enforce physical access authorizations for all physical access points including organization-defined entry/exit points to the facility where the information system resides by;
    1) Verifying individual access authorizations before granting access to the facility; and
    2) Controlling ingress/egress to the facility using organization-defined physical access control systems/devices; guards;
b. Maintain physical access audit logs for all organization-defined entry/exit points;
c. Provide organization-defined security safeguards to control access to areas within the facility officially designated as publicly accessible;
d. Escort visitors and monitors visitor activity for organization-defined circumstances requiring visitor escorts and monitoring;
e. Secure keys, combinations, and other physical access devices;
f. Inventory organization-defined physical access devices every on an annual basis or more frequently if required to address an environmental change; and
g. Safeguard IT systems and data residing in static facilities (such as buildings), mobile facilities (such as computers mounted in vehicles), and portable facilities (such as mobile command centers).

C. Access Control for Transmission Medium and Control Output Devices

When controlling access to transmission medium or output devices the Technology Services Network Team and the ISO will:

a. Provide protection methods to control physical access to organization-defined information system distribution and transmission lines within organizational facilities using the appropriate organization-defined security safeguards. For example:
    i. Locked wiring closets;
    ii. Disconnected or locked spare jacks; and/or
    iii. Protection of cabling by conduit or cable trays.
b. Safeguard physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

D. Monitoring Physical Access

Enterprise Management staff will:

a. Monitor physical access to the facility where the information system resides to detect and respond to physical security incidents;
b. Review physical access logs at least once every 30-days and upon occurrence of organization-defined events or potential indications of events; and
c. Coordinate results of reviews and investigations with the organizational incident response capability.

E. Access Records

Enterprise Management staff will:

a. Maintain visitor access records to the facility where the information system resides for a minimum period of one year; and
b. Review visitor access records at least once every 30-days.

F. Power Equipment & Power Cabling

The power equipment and power cabling will be in place to protect information systems from damage and destruction. (This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.)

G. Emergency Shut off

The technology management responsible for the emergency shut-off system will:

a. Provide the capability of shutting off power to the information system or individual system components in emergency situations;
b. Place emergency shutoff switches or devices in organization-defined location by information system or system component to facilitate safe and easy access for personnel; and
c. Protect emergency power shutoff capability from unauthorized activation.

H. Emergency Power

Information technology support will provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system; in the event of a primary power source loss.

I. Emergency Lighting

Information technology resources will include the employment and maintenance of automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

J. Fire Protection

Fire protection procedures in the data center will include employment and maintenance of fire suppression and detection devices/systems for the information systems that are supported by an independent energy source.

K. Temperature and Humidity Controls

The Data Center and any other area that houses the university's servers will:

a. Maintain temperature and humidity levels within the facility where the information system resides at organization-defined acceptable levels; and

b. Monitor temperature and humidity levels on a daily basis.

L. Water Damage Protection

Strategies will in place and implemented to protect the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

M. Delivery and Removal

Delivery and removal of devices will require technology staff and or management to authorize, monitor, and control organization-defined types of information system components entering and exiting the facility and maintains records of those items. (Including devices like copy machines, other devices that may contain data.)

N. Alternate Work Site

Alternate work sites approved by the university will:

a. Employ organization-defined security controls at alternate work sites;
b. Assesse as feasible, the effectiveness of security controls at alternate work sites; and
c. Provide a means for employees to communicate with information security personnel in case of security incidents or problems.

O. Location of Information System Components

Locations housing university information system components will:

a. Position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access, when feasible;
b. Ensure that all information system components and services remain within the continental United States *unless the COV CISO has granted an exception*;
c. Ensure that all data and system information associated with the information system components and services remain within the continental Unites States;
d. Ensure that all physical components associated with an information system or service classified as sensitive with respect to confidentiality or integrity must be housed within the same storage location dedicated for the exclusive use of the organization and are clearly marked;
e. Ensure that all virtual components associated with an information system or service classified as sensitive with respect to confidentiality or integrity must reside in hypervisors dedicated to the exclusive use of the organization; and
f. Ensure that each hypervisor can only host one tier of the application architecture and no hypervisor may host the application interface and the data storage component for any information system, even if the components in question do not interact within the same information system.

References

Virginia Information Technology Agency (VITA):
Information Security Standards (SEC501-09.1) (12/08/2016)
Hosted Environment Information Security Standard (SEC525-02) (12/08/2016)

Approval By: _____ **Date:** 10/4/17

President