Purpose

The purpose of the Facility Security policy is to ensure that VSU implements sound business practices to safeguard the physical facilities that house all University Information Technology (IT) systems, equipment, services, and personnel. The intent is to design safeguards, commensurate with risk, to protect human life and the University IT Infrastructure from natural, and environmental threats.

Authority, Responsibility, and Duties

The IT Security Program 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. Refer to Information Security Policy 6110 for IT Security Program roles and responsibilities.

A. Information Security Officer (ISO)

B. The VSU Information Security Officer or designee is required to periodically review the list of personnel in the VSU Data Centers and/or University network closets who have access to sensitive IT systems. The ISO or ISO designee is permitted to request the removal of individuals from the facility access list when access is no longer required.

C. Enterprise Systems Manger

The Enterprise Systems Manager, shall perform periodic review of access to Data Center to enable the following.

A. Temporarily disables physical access rights when personnel do not need such access for prolonged period in excess of 30 days because they are not working due to leave, disability, or authorized purpose.

B. Disable physical rights upon suspension of personnel for greater than I day for disciplinary purposes.

D. University Staff and Employees

Employees are expected to report any unauthorized access, entry, suspicious activity, lost or stolen IT equipment to supervisors, IT Help Desk (x5210), Department of Police & Public Safety (DPPS), VP of Administration and ISO.

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

1. This policy applies to all University employees (permanent, temporary, contractual, faculty, administrators and students) who are responsible for the development, coordination, and execution and use of VSU information technology resources to conduct University business and to transmit sensitive data in the performance of their jobs.
2. Safeguard University 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).
    a. The VSU Trojan Card is the official identification card for all University employees, students, and contractors. It is used as a controlled access card entry system for computer rooms, data center, residence halls, class rooms, and buildings.
    b. Faculty, staff, students, visitors and vendor maintenance personnel are required to sign an access log, show government issued identification (photo ID), and be escorted by University employees or Information Technology (IT) Services Provider in the data center.
    c. Surveillance cameras and alarm systems are located throughout campus to ensure public safety.
    d. Mobile computing (i.e. laptops, tablets, Personal Digital Assistants (PDAs), USB flash drives, smart phones, and handheld devices) should be properly secured and locked to reduce the occurrence of theft.
3. Safeguards are designed to protect against human, natural, and environmental risks, e.g., the evacuation plan emphasizes human safety and is posted near the entrance and exit doors within the Data Center.
4. Require appropriate environmental controls such as electrical power, heating, fire suppression, ventilation, air conditioning and air purification, as required by the IT system and data.
    a. Business critical desktop computers should be connected to surge protectors or Uuninterruptible Power Supply (UPS) to prevent power spikes and subsequent damage to data and hardware.
    b. Environmental controls such as fire extinguishers, manual fire alarms, smoke detectors, fire-proof walls, sprinkler systems, emergency power-off switch, humidity and temperature control unit, and raised floors are located in the data center.
    c. Uninterruptible Power Supply (UPS) and a generator(s) support mission critical IT systems.
    d. Adequate air conditioning should be operational in office environments that house desktop computing and high technology resources to prevent long-term heat damage and equipment failure.
5. Protect against physical access by unauthorized personnel.
    a. Desktop computers should be locked when not occupied by employees to reduce the

Occurrence of unauthorized entry or access. Password protected screensavers should be enabled for inactivity.

b. Desktop computers in public access areas and computer labs should be properly secured to workstations, counters, or piece of furniture using security/theft inhibiting devices.

c. Offices that are controlled by lock and key should be locked by the employee when not occupied.

6. Control access to essential computer hardware, wiring, displays, and networks by the principle of least privilege.

7. Provide a system of monitoring and auditing physical access to sensitive IT systems.

a. All computing equipment should have serial numbers and VSU property tags recorded in the University's Fixed Asset Accounting Control System (FAACS) for identification purposes.

b. University computer equipment located off campus, particularly in the home of faculty and staff members, must submit, sign, and date a FAACS Equipment Release forms with appropriate signatures. Notify the FAACS Office in writing when the equipment is returned to campus and its condition.

c. University Data Centers shall have surveillance cameras, steel bars on windows, alarm systems, and access control card readers to monitor physical access to sensitive IT systems.

References

Virginia Information Technology Agency (VITA):
Information Security Standard (SEC 501-09) (02/20/2015)

Approval By: _____ Date: 5/10/16
President