Title: Threat Management Policy: 6600

Purpose

This Threat Management policy reflects the University's commitment to protect IT systems and data by preparing for and responding to information security incidents. This policy is to also ensure that the University identifies the practices for implementing components to prepare, detect and analyze, contain, eradicate, and recover from information security threats by implementing the Computer Information Security Incident Response Program (CSIRP).

Authority, Responsibility, and Duties

The IT Security program roles and responsibilities are assigned to individuals, and roles and responsibilities 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 prevent conflict of interests. Refer to Information Security Policy 6110 for roles and responsibilities.

A. Information Security Office

The Information Security Office Security Incident Coordinator and Information Security Officer (ISO) will provide a central point for collaboration and decision making during an incident. They will also work with the CSIRT members in overall information security threat management for the University.

B. Computer Security Incident Response Team (CSIRT)

The CSIRT is responsible for providing necessary services for responding to information security incidents to support the resolution and work to prevent future information security incidents within the University. Designated members of the VSU CSIRT may be called upon to pm1icipate in the detection, response, and remediation of threats. Refer to the VSU Computer Security Incident Response Program (CSIRP) Manual for additional information and procedures.

C. VSU Technology Services

1. Implement Intrusion Decision (IDS) and Intrusion Prevention System (IPS).
2. Conduct IDS and IPS log reviews to detect new attack patterns as quickly as possible.
3. Develop and implement required mitigation measures based on the results of the IDS and IPS log reviews.
4. Prohibit the installation or use of unauthorized monitoring devices.
5. Implement proactive measures based on cyber-attacks to defend against new forms of cyber-attacks and zero-day exploits.
6. Technical Members of CSIRT (ISO, Security Analyst and selected Network Team members) who work in VSU Technology Services have been assigned responsibilities for detection, response and remediation of information security threats to the University

computing resources. Parts of their daily routines include proactive monitoring for threats and deployment of tools to minimize the risk of threats.

7. CSIRT interaction with other staff of VSU Technology Services is important during response to an incident. Specific actions carried out by VSU Technology Services staff and specific actions carried out by CSIRT members during response operations must be documented and reviewed. Members of the CSIRT will have access to security and network monitoring logs and system logs for analysis purposes. The CSIRT team membership includes Senior Executives (i.e. Vice Presidents and Chief of Staff), University Council, University Relations, Human Resources, Department of Police & Public Safety (DPPS), Information Security Officer (ISO), and Technology Services.

D. University Council

Legal advice may be required to develop or review contract terms for non-disclosure agreements and determine liability for information security incidents.

E. VSU Human Resources (HR)

Human Resources will assist with job descriptions for CSIRT staff. Also, HR may need to develop policies and procedures for removing internal employees found engaging in unauthorized or illegal computer activity.

F. University Relations

University Relations will manage media relations and inquiries and assist m developing information-disclosure policies and practices.

G. VSU Department of Police and Public Safety (DPPS)

Physical security entities may share responsibility and exchange information with the CSIRT concerning information security incidents related to computer or data theft.

Definitions

The IT security definitions and terms can be found in the COV ITRM IT 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 develop and use VSU information technology resources to conduct University business and to transmit sensitive data or personally identifiable information (PIT) in the performance of their jobs, and all VSU information systems that store or process PIT or other sensitive data.

2. This policy expressly prohibits the installation or use of unauthorized monitoring devices and keystroke logging, except when required for security investigations and a documented business case outlining the need and residual risk has been approved in writing by the ISO.
3. The Computer Security Incident Response Program (CSIRP) and manual defines standard methods for detection and analysis, containment, eradication and recovery, evidence gathering, and documentation of information security incidents. The program consists of this policy and subsequent Program manual, staff development, and ongoing review.
4. The VSU Computer Security Incident Response Team (CSIRT) will hold quarterly meetings to review threat management activities such as Intrusion Detection/Prevention (IDS/IPS) logs and settings, Firewall logs and rules, as well as, other logging and monitoring activities, discuss security alerts and information from outside resources such as US CERT, and follow up on activities from previous information security incidents.
5. At least once per year, the CSIRT will hold a formal tabletop exercise to incorporate simulated events to facilitate effective response by personnel in crisis situations.
6. Information Security Officer (ISO) is required to provide quarterly summary reports of IDS and IPS events to Commonwealth Security and Risk Management at VITA.

7. Information Security Incidents

An incident is the occurrence of an event. An information security incident is a violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices. Most incidents can be categorized as follows:

a. Inappropriate Use
b. Unauthorized Access
c. Malicious Code
d. Denial of Service
e. Multiple-Component Incident

8. Reporting Information Security Incidents

Incidents that involve information security, along with initial assessments of vulnerability and risk, must immediately be reported to the Service Desk by dialing: 804-524-5210, or sending email to secureiT@vsu.edu. Timely reporting enables prompt corrective action and allows for thorough information gathering and reporting.

a. The ISO shall escalate and notify as per the process outlined in the CSIRP Manual and work with the Computer Security Incident Response Team (CSIRT) to coordinate, investigate, and respond to the incident as appropriate.

b. If a reportable incident, the ISO shall report the incident to the VITA Commonwealth Security and Risk Management team within 24 hours of the incident occurring.

9. Modifications and Adjustment

a. VSU Technology Services management has developed a Computer Security Incident Response Program (CSIRP) Manual to respond to University incidents. The Program includes roles, responsibilities, processes, and procedures for handling computer security incidents.

b. The ISO will maintain the official copy of this document. This policy and the program manual will be reviewed at least annually and immediately following an incident to adjust processes, identify new risks, and remediation.

10. Special Situations

Any personally-owned devices or VSU-owned devices such as PDAs, mobile phones, phones, wireless devices, laptops, or other electronic transmitters which have been used to store University data, and are determined to contribute to an incident, may be seized and retained by the CSIRT for investigation and chain of custody until the incident has been remediated, unless the custody of these devices is required as evidence in the commission of a crime. All these devices used within the University network for business purposes, are subject to the University's policies.

References

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

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