Title: IT Security Incident Handling Policy

Purpose

The IT Security Incident Handling Policy identifies the steps necessary to adequately respond to suspected or known breaches surrounding Information Technology (IT).

Policy Statement

This policy requires that the University’s IT service provider establish a process for documenting, handling, and reporting IT security incidents.

Authority, Responsibility, and Duties

The Office of Information Technology (OIT) is required to protect University IT systems and data by preparing for and responding to IT security incident. At a minimum the following practices should be followed:

A. Designate an IT Security Incident Response team that includes the Information Security Officer (ISO), the Network Administrator, and designated IT Managers. Their responsibilities and roles include the following:

1. Maintain compliance with the University’s Incident Handling procedures to immediately investigate and respond to suspected or unknown breaches to the University’s IT security or network infrastructure.

2. Assess the incident categorization and prioritization based on the immediate and potential adverse effect of the incident and the sensitivity of the affected IT system and data.

3. Establish requirements for the University’s IT security incident reporting and reporting requirements to include reporting IT security incidents via email and/or online form.

4. Identify controls to deter and defend against cyber attacks to best minimize loss or theft of information and disruption of services.

5. Identify immediate mitigation procedures, including specific instructions, based on IT security incident categorization level, on whether or not to shut down or disconnect affected IT systems.

6. Use procedures for incident investigation, forensic analysis, and preservation of evidence.

B. Establish a process for reporting IT security incidents to the University’s Chief Information Officer (CIO) and Virginia Information Technology Agency (VITA) Chief Information Security Officer (CISO) in accordance with the § 2.2-603.(F) of the Code of Virginia.
Definitions

Information Security Officer (ISO) is responsible for overseeing the implementation of the University’s Information Technology (IT) Security program.

Information Security Event is an occurrence that has yet to be assessed but may affect the performance of an IT system.

Information Technology (IT) Security Breach is the violation of an explicit or implied security policy that compromises the integrity, availability, or confidentiality of an IT system.

Information Technology (IT) Security Incident is an adverse event or situation, whether intentional or accidental that poses a threat to integrity, availability, or confidentiality of an IT system.

Information Technology (IT) Security Incident Response Team is an organization within an agency constituted to monitor IT security threats and prepare for and respond to cyber attacks.

References

Virginia Information Technology Agency (VITA):
Information Technology Security Standard (ITRM Standard SEC501-01)

Virginia State University (VSU):
Policy 6520: Acceptable Use Policy
Policy 6630: Data Breach Policy

APPROVED BY:

President

Date