



OIT 62.904: Information Security Incident Handling

Responsible Executive: Information Security Officer
Responsible Office: Office of Information Technology
Related Policy:
Approved-On Date: 2/28/2011
Effective Date: 7/1/2011
Revision Date: 2/1/2011

I. Policy Statement

Information Security Incident Handling addresses protection of IT systems and information by preparing for and responding to information security incidents.

II. Purpose

Information Security Incident Handling policy identify the steps necessary to respond to suspected or known breaches to information security safeguards.

III. Scope

This policy applies to all Commonwealth of Virginia (COV) systems and to the University IT network infrastructure.

IV. Requirements

The University shall document information security incident handling practices and where appropriate the University shall incorporate its service provider's procedures for incident handling practices that include the following, at a minimum:

1. Designate an Information Security Incident Response Team that includes personnel with appropriate expertise for responding to cyber-attacks.
2. Identify controls to deter and defend against cyber-attacks to best minimize loss or theft of information and disruption of services.
3. Implement proactive measures to defend against new forms of cyber-attacks and zero-day exploits.
4. Establish information security incident categorization and prioritization based on the immediate and potential adverse effect of the information security incident and the sensitivity of affected IT systems and data.

5. Identify immediate mitigation procedures, including specific instructions, based on information security incident categorization level, on whether or not to shut down or disconnect affected IT systems.
6. Establish a process for reporting information security incidents to the ISO. Users must report security incidents within 24 hours from when they are discovered.
7. Establish requirements for internal University information security incident recording and reporting requirements, including a template for the incident report.
8. Establish procedures for information security incident investigation, preservation of evidence, and forensic analysis.
9. Report information security incidents only through channels that have not been compromised.

Note: The ISO or other Administration authorities as necessitated by circumstances, may authorize the confiscation and removal of any IT resource suspected to be the object of inappropriate use or violation of laws, regulations, policies or standards in order to preserve evidence that might be utilized in forensic analysis of a security incident.

V. Violations

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

VI. Interpretation

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.