Information Technology Security Incident Handling Policy

Date: 06/12/06	**Policy ID:** UVAW - 13	**Status:** Approved

Contact Office: Office of Information Technology

Oversight Executive: Director of Information Technology

Applies to: The University of Virginia's College at Wise

Reason for Policy: To establish guidelines and procedures for handling all incidents involving Information Technology Resources including but not limited to data, equipment, access, and infrastructure.

Definitions: Incident – is defined as any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. Examples include penetration of a computer system, exploitation of technical vulnerabilities, or introduction of computer viruses or other forms of malicious software.

Policy Statement: Providing access to resources in support of the mission of UVa-Wise is the primary goal of the Information Technology Office, ensuring the confidentiality, integrity and availability of those resources includes the prompt handling of any and all information security incidents.

Procedures:

1.0 All potential security incidents shall be handled per the incident response plan.

2.0 Incident response plan

- 2.1 The appropriate server administrator and the Incident Response Team (abuse@uvawise.edu, Susan Herron – Coordinator, (276) 376-4641) should be notified immediately.
- 2.2 No actions should be done to the server/system until the Incident Response Team arrives.
  - 2.2.1 Incident Response Team members will include: Server/Network Administrator, Security and Policy Coordinator, Network Security Specialist, and the Information Security Officer
    - 2.2.1.1 This portion of the team will determine what immediate necessary actions to take.
  - 2.2.2 Other members (depending on the criticality of the incident) may include any or all of the following:

Director of Network Services, Director of User Support Services, Director of Information Technology, Public Relations, Campus Police, Vice Chancellor (affected area), Chancellor, and Provost

2.3 Once the immediate threat has been contained the IRT will decide on a further plan of action. This includes notifying any other responsible parties and beginning the documentation by filing an Incident Report.

2.3.1 The Incident Report shall include the date, time, parties involved, system(s) involved, a complete description of the incident, who was notified and what further action is planned.

2.3.2 Each action toward resolution of the incident shall be documented in complete detail.

2.3.3 At the conclusion/resolution of the incident a "Lessons Learned" meeting shall take place and will also be documented.

Related Information:

Background: Approved by Brian Ward, CIO – UVa-Wise, June 13, 2006
