Sensitive Data Access Tracking and Monitoring

Date: 06/12/06	**Policy ID:** UVAW – 9	**Status:** Approved

Contact Office: Office of Information Technology

Oversight Executive: Director of Information Technology

Applies to: University of Virginia's College at Wise networks and systems

Reason for Policy: The purpose of this policy is to establish guidelines and procedures for monitoring access, tracking changes, and establishing audit trails.

Definitions:

Policy Statement: Those responsible for devices containing sensitive data connected to the University of Virginia's College at Wise networks and systems must ensure that critical modifications and access to information is valid and legitimate. Intrusion detection/prevention is one of the methods that is used to help accomplish this task, by making use of audit and log features to identify intrusions or attempted intrusions by any unauthorized person(s).

Procedures:

1.0 Tracking and monitoring access to networks and systems housing sensitive data
- 1.1 Link access through administrative privileges to individual user accounts rather than generic administrator accounts when possible.
- 1.2 Implement automated audit trails for all system components: system modifications, logon success, logon failure, object access, object creation, object deletion.
- 1.3 Record entries for each event including the following information: User identification, type of event, date and time stamp, success or failure, origination of event, identity or name of affected data, system component, or resources.
- 1.4 Synchronize all critical system clocks and times.
- 1.5 Secure audit trails so that they cannot be altered and maintain restricted access.
- 1.6 Review logs for all system components on sensitive servers regularly.
- 1.7 Retain audit trails for a year.

Related Information: See also Logging/Auditing of PCI Data Access Policy PCI – 10

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