Policy Title: Information System Monitoring

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 1704 Information System Monitoring (2014)

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Information system monitoring addresses the continued observance of network traffic within the University’s information system for the purpose of detecting threats to the system and/or violations of University policy and establishing the necessary controls to mitigate these threats and violations.

TABLE OF CONTENTS

Contacts ........................................................................................................................................... 1
Stakeholder(s) ................................................................................................................................. 2
Purpose ........................................................................................................................................... 2
Requirements ................................................................................................................................. 2
Violations ......................................................................................................................................... 3
Interpretation ................................................................................................................................. 3
Publication ....................................................................................................................................... 3
Review Schedule ............................................................................................................................ 4
Related Documents ......................................................................................................................... 4

CONTACT(S)

Office of Information Technology – (757)823-2869
STAKEHOLDER(S)

University Faculty & Staff
Office of Information Technology

PURPOSE

This policy is intended to establish the policy and procedures for the monitoring of the University’s information system.

REQUIREMENTS

NSU:

1. Monitors events on the information system in accordance with University defined monitoring objectives and detects information system attacks;

2. Identifies unauthorized use of the information system;

Supplemental Guidance: Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal University networks and system components). Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, at selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls 62.8.1607 and 62.8.117. The Einstein network monitoring device from the Department of Homeland Security is an example of a system monitoring device. The granularity of the information collected is determined by the University based on its monitoring objectives and the capability of the information system to support such activities. An example of a specific type of transaction of interest to the University with regard to monitoring is Hyper Text Transfer Protocol (HTTP) traffic that bypasses University HTTP proxies, when use of such proxies is required.

Control Enhancements for Sensitive Systems:

1. The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.

   Enhancement Supplemental Guidance: Unusual/unauthorized activities or conditions include, for example, internal traffic that indicates the presence of malicious code within an information system or propagating among system components, the unauthorized export of information, or signaling to an external information system. Evidence of malicious code
is used to identify potentially compromised information systems or information system components.

2. The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.

3. NSU employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

4. NSU employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wired networks.

VIOLATIONS

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 32-01 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.

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.

PUBLICATION

This policy shall be widely published and distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

1. Communicate the policy in writing, electronic or otherwise, to the University community within 14 days of approval;

2. Submit the policy for inclusion in the online Policy Library within 14 days of approval;

3. Post the policy on the appropriate SharePoint Site and/or Website; and

4. Educate and train all stakeholders and appropriate audiences on the policy’s content, as necessary. Failure to meet the publication requirements does not invalidate this policy.
ADMINISTRATIVE POLICY # 32 – 8 – 1704 Information System Monitoring (2014)

REVIEW SCHEDULE

- Next Scheduled Review: 05/28/2015
- Approval by, date: Office of Information Technology and 05/28/2014
- Revision History:
  - Supersedes (previous policy): OIT 62.8.1704 Information System Monitoring

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard