Security Monitoring and Scanning

Approved June 11, 2007
Reviewed March 19, 2012
Supplements University Rule 29.01.03.C2

1. GENERAL

Security monitoring and network scanning are common methods used to ensure that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as the review of: user account logs, application logs, data backup and recovery logs, automated intrusion detection system logs, etc. Network scanning consists of activities such as network, host, and application enumeration and vulnerability detection.

The purpose of the Security Monitoring and Scanning procedure is to ensure that information resource security controls are in place, are effective, and are not being bypassed. Some of the benefits of this procedure include the early identification of wrongdoing and the identification of avoidable security vulnerabilities.

2. APPLICABILITY

This university procedure applies to all university-managed information resources containing mission critical information, confidential information, and other information resources as may be managed by the university.

The purpose of the implementation of this university procedure is to provide a set of measures that will mitigate information security risks associated with Security Monitoring and Scanning. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee.

Please also refer to Procedure 29.01.03.C2.25 “Exceptions from Risk Mitigation Measures.”

The intended audience is all individuals that are responsible for the installation of new information resources, the operations of existing information resources, and individuals charged with information resources security.

3. DEFINITIONS

Please refer to University Procedure 29.01.03.C2.01 Definitions.

4. PROCEDURES
4.1. Network monitoring for maintenance and anomaly detection purposes shall be conducted by Media and Computer Services on any network segment connected to the university network environment.

4.2. Departments may only conduct network monitoring for maintenance purposes on information resources maintained by the department’s resource custodians. Anomaly detection monitoring can only be performed by the department’s resource custodians with prior approval from and coordination with the Information Resources Manager.

4.3. Suspicious or malicious activity shall be immediately reported according to procedures outlined in University Procedure 29.01.03.C2.08 Incident Response.

4.4. Audit logs, reports, and any additional, related, information shall be furnished to representatives of the Information Resources Manager immediately upon request.

4.5. Resource custodians of systems and networks involved with the storage or transmission of Sensitive Information shall develop a network, host, and application security baseline and monitor it for security related exceptions.

4.6. An annual, at a minimum, risk assessment shall be performed for each information resource connected to the university network. This risk assessment shall be conducted by the resource custodian, department head, and any other critical personnel associated with the information resource. Where applicable the following checks shall be performed:

1. verification of password strength,
2. detection of unauthorized hosts, servers, and applications,
3. integrity and appropriateness of access controls, and
4. information resource and Sensitive Information inventory.

4.7. The Media and Computer Services network group shall conduct periodic network and vulnerability scans of devices attached to the university network. Information gathered shall be used for network management, including notifying owners of vulnerabilities, determining incorrectly configured systems, validating firewall access requests, and gathering network census data.

4.8. Except as provided in section 4.7, no network or vulnerability scans may be conducted except by the owner of the information resource being scanned. In no case may network scanning traffic transit a router maintained by the Media and Computer Services network group. All scans of this type must be coordinated
with the Media and Computer Services network group to distinguish it from malicious activity.

4.9. Except as provided in section 4.7, network and vulnerability scans may only be conducted by university employees designated by the organizational unit head responsible for the information resource. Network and vulnerability scans may not be conducted by student systems in the housing/dormitories or on the university network.

4.10. Education based network and vulnerability scans or any other security related training (as interpreted by the Information Resources Manager) may only be conducted by students supervised by university faculty. These activities shall also be limited to networks that have been completely isolated from the university wired and wireless networks and approved by the Information Resources Manager.

5. CONSEQUENCES FOR VIOLATIONS

All university employees to include staff, tenured and non-tenured faculty, graduate assistants, student workers, interns, guests, volunteers, and probationary, temporary, or wage employees as well as contractors, consultants, and vendors required to adhere to this university procedure may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and university rules.

Individuals found in violation of this university procedure are subject to loss of access privileges to university information resources (e.g. servers, workstations, email, etc). In addition, contracts associated with contractors, consultants, or vendors are subject to review and possible termination. Any device, system, or software found in violation of this procedure may be confiscated and temporarily stored by the Information Resources Manager or a representative of the office.

Additional guidance may be found, but is not limited to, the following policies and rules.

- Texas A&M System Policy
  - 01.03 Appointing Power and Terms and Conditions of Employment
  - 07.01 Ethics Policy, TAMUS Employees
  - 32.02 Discipline and Dismissal of Employees
  - 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees
  - 33 Employment, Standards of Conduct

- Texas A&M University-Corpus Christi Rule
  - 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments
  - 13.02.99.C1 Student Disciplinary Proceedings