Security Monitoring Policy

Introduction
Security Monitoring is a method used to confirm that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as the review of:

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- Application logs
- Data backup recovery logs
- Help desk logs
- Other log and error files
- Vulnerability Scanning

1. Purpose
The purpose of the Security Monitoring Policy is to ensure that Information Resource (IR) security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing, new security vulnerabilities, or new unforeseen threats to IR assets. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact. Other benefits include Audit Compliance, Service Level Monitoring, Performance Measuring, Limiting Liability, and Capacity Planning. Security monitoring must have the capability to trigger alerts and send them to authorized CIS staff.

2. Audience
The Texas A&M University-Kingsville Security Monitoring Policy applies to all individuals that are responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resource Security.

3. Security Monitoring Policy
3.1. Automated tools will provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:

- Internet traffic
- Electronic mail traffic
- LAN traffic, protocols, and device inventory
- Operating system security parameters
- Operating System Vulnerabilities

3.2. The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- System error logs
- Application logs
- Data backup and recovery logs
- Help desk trouble tickets
- Telephone activity – Call Detail Reports
- Network printer and fax logs

3.3. The following checks will be performed at least annually by assigned individuals:
3.4. Any security issues discovered will be reported to the Information Security Officer (ISO) for follow-up investigation.

3.5. The ISO is responsible for returning the IR to a preset level of security control.

**Disciplinary Actions**

Violation of this policy may result in disciplinary action up to and including termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Texas A&M University-Kingsville Information Resources access privileges, civil, and criminal prosecution.