Security Monitoring Policy

1. Overview

A regular monitoring program is key to managing risk in an organization. Security monitoring occurs on both physical areas as well as logical components in many different information system areas. Information security monitoring confirms that appropriate mechanisms and controls are in place to secure systems and applications, that they are effective, and are not being bypassed in any way.

2. Purpose

One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. Early identification can help block wrongdoing or vulnerabilities before harm can be done. Other benefits include audit compliance, service level monitoring, performance measuring, limiting liability, and capacity planning. This policy establishes Thiel College security monitoring processes and procedures.

3. Scope

This policy applies to support staff charged with security responsibility for installation and operation of application and computing resources.

4. Policy

Automated tools provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible, staff shall develop security baselines and tools to report exceptions. Baselines and tools shall be deployed to monitor:

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

The following files shall be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by the Director Of Information Systems or their designee:

- 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 (e.g. call detail reports)
- Network printer and fax logs

An evaluation of the efficacy of the current program and practices shall be conducted and documented by the Director of Information Systems on an annual basis. Such evaluations shall minimally include review of:

- Password strength
- Unauthorized network devices
- Unauthorized personal web servers or devices
- Unsecured sharing of devices
- Unauthorized remote connectivity
- Unauthorized operating systems
- Unauthorized software licenses

Any security issues discovered will be reported to the Director Of Information Systems for follow-up investigation and remediation. As part of the review, procedures shall be developed to review and record growth and traffic patterns, bandwidth issues, etc. Appropriate reporting shall be in place to allow the IT Department to anticipate performance issues and delays and react in a timely and proactive manner.

5. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the Thiel College. Satisfactory examples of evidence and compliance include:

- Spot user checks for appropriate security monitoring logs
- Archival documentation of annual reviews
- Historical communications on reviews and continuous improvement enhancements

6. Enforcement

Staff or Faculty members found in policy violation may be subject to disciplinary action, up to and including termination.

7. Distribution

This policy is to be distributed to all Thiel College staff conducting security audits and reviews.