

# Patch Management Policy

## 1.0 Overview

Thiel College is responsible for ensuring the confidentiality, integrity, and availability its data and that of customer data stored on its systems. Thiel College has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the system or its data entrusted on the system. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within this scope.

## 2.0 Purpose

This document describes the Director of Computer Information Services (CIS) requirements for maintaining up-to-date operating system security patches on all Thiel College owned and managed workstations and servers.

## 3.0 Scope

This policy applies to workstations or servers owned or managed by Thiel College. This includes systems that contain college data owned or managed by Thiel College regardless of location. The following systems have been categorized according to management:

- Unix/Linux servers managed by CIS
- Microsoft Windows servers managed by CIS
- Workstations (desktops and laptops) managed by CIS

## 4.0 Policy

Workstations and servers owned by Thiel College must have up-to-date (as defined by Director of CIS minimum baseline standards) operating system security patches installed to protect the asset from known vulnerabilities. This includes all laptops, desktops, and servers owned and managed by Thiel College.

### 4.1 Workstations

Desktops and laptops must have automatic updates enabled for operating system patches. This is the default configuration for all workstations built by Thiel College. Any exception to the policy must be documented and forwarded to the Director of CIS for review. *See Section 8.0 on Exceptions.*

### 4.2 Servers

Servers must comply with the minimum baseline requirements that have been approved by the Director of CIS. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the Thiel College asset and the data that resides on the system. Any exception to the policy must be documented and forwarded to the Director of CIS for review. *See Section 8.0 on Exceptions.*

## 5.0 Roles and Responsibilities

- **CIS** will manage the patching needs for the Servers including Linux, Unix, Windows, and all workstations including all Domain based desktops and laptops on the network
- **CIS** is responsible for routinely assessing compliance with the patching policy and will provide guidance to all groups in issues of security and patch management.

## 6.0 Monitoring and Reporting

Active patching teams noted in the Roles and Responsibility section (5.0) are required to compile and maintain reporting metrics that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk.

## 7.0 Enforcement

Implementation and enforcement of this policy is ultimately the responsibility of all employees at Thiel College. Information Security and Internal Audit may conduct random assessments to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the Thiel College issue tracking system and support teams shall be dispatched to remediate the issue. Repeated failures to follow policy may lead to disciplinary action.

## 8.0 Exceptions

Exceptions to the patch management policy require formal documented approval from the Director of CIS. Any servers or workstations that do not comply with policy must have an approved exception on file with the Director of CIS.

## 9.0 Definitions

<b>Term</b>	<b>Definition</b>
Patch	A piece of software designed to fix problems with or update a computer program or its supporting data
Trojan	A class of computer threats (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the owner.
Worm	A self-replicating computer program that uses a network to send copies of itself to other nodes. May cause harm by consuming bandwidth.