Saint Mary's College of California
Information Technology Policy

Information
Technology Services

Patch Management Policy

Policy:	No: 1.0
Responsible Officer:	Chief Information Officer, James Johnson
Effective Date:	April 25, 2024
Updated:	April 25, 2024
Issued By:	ITS - Information Technology Services

CONTENTS

Overview

Saint Mary's College of California (SMC) recognizes the importance of effective patch management in maintaining the security of the network and the information technology infrastructure. Saint Mary's College Patch Management Policy establishes a framework for systematically identifying, testing, and deploying software and system updates. It underscores our commitment to a structured approach to patch management, ensuring the integrity and reliability of our IT environment.

Purpose

Saint Mary's College has established the Patch Management Policy to achieve the following objectives:

- **Mitigate security risks:** Address vulnerabilities and reduce the risk of security breaches, data loss, and unauthorized access.
- **Ensure system stability:** Minimize operational disruptions and system failures.
- **Maintain compliance and accountability:** Emphasize our commitment to responsible IT management and compliance with relevant laws, regulations, and industry standards.
- **Enhance user trust:** Foster trust among faculty, staff, students, and partners who rely on the security and reliability of our systems.

Scope

The scope of this policy pertains to the following IT resources directly related to patch management:

- **Hardware assets**: All hardware resources involved in the organization's IT infrastructure and operations, including servers, workstations, and network equipment.
- **Software assets**: All software applications and systems, including operating systems, software applications, and software licenses.
- **User accounts and access**: User accounts and access permissions associated with IT resources.
- **Licensing and compliance**: Software licenses, compliance documentation related to patching, and software usage records that impact patch management activities.

Audience

This policy applies to the following key stakeholders and groups:

- **All employees:** Who interact with or have access to our IT infrastructure and systems.
- **IT department:** Responsible for executing the patch management procedures, such as identification, testing, deployment, and documentation.
- **Third-party vendors:** Expected to provide patches and updates for their software or services used within the organization promptly.
- **Contractors:** Who work within the SMC's IT environment.

Patch Management Policy Details

a. Roles and Responsibilities

Saint Mary's College **IT Department** is responsible for:

- Identifying, testing, and deploying patches in a timely manner.
- Documenting patch management activities.
- Maintaining a rollback plan for unforeseen issues during patch deployment.
- Ensuring compliance with this policy and relevant regulations.

End users must:

- Report vulnerabilities and issues promptly to the IT department.
- Adhere to security best practices and user awareness guidelines provided by the IT department.
- Colleague Software Update Approvers are responsible for testing Ellucian patches once released in the TEST environment and updating the official patch tracking document with approvals and concerns.

Third-party vendors should:

- Promptly provide patches and updates for their software used within the organization, in accordance with service-level agreements (SLAs) or contractual agreements.

b. Patch Identification

Saint Mary's College places critical importance on the effective identification of patches to ensure staying informed about vulnerabilities and available fixes. The following responsibilities pertain to patch identification:

- **Regular scanning** using automated tools to detect missing patches.
- Promptly receiving and assessing **vendor notifications** for relevant patches.

c. Patching Priority

Responsibilities related to patching priority include:

- **Risk Assessment:** The IT Department systematically prioritizes patches based on the severity of vulnerabilities and their potential impact on the organization.
- **Critical Systems:** Critical systems and applications within our organization will receive top priority for patching.

d. Patch Testing

Patches will be tested in a controlled environment before deployment to minimize the risk of unforeseen issues. During patch testing:

- **Test environment:** The network administrators will set up and maintain a controlled test environment to evaluate patches for their impact on system functionality and stability before deployment in the production environment.

e. Patch Deployment

The following guidelines should be followed during patch deployment:

- **Maintenance windows:** Saint Mary's College Network administrators, desktops administrators, and server administrators have regular maintenance windows for patch deployment to minimize operational disruptions. The schedule is listed in the table below.

Category	Patch Asset	Patch Window	Related Notes
Windows Operating System	Devices running supported Windows versions	IT Department Early Adopters – Thursday after Microsoft's Patch Tuesday. Patch Tuesday occurs on the 2nd Tuesday of every month. Campus-Wide and Remote Devices – The following Tuesday	You will be able to postpone the reboot of your Windows machine after patching 2 times. You will not be able to postpone the reboot a 3rd time as the updates / patches will be applied to computers upon the 3rd warning.
Windows Server Operating System	Servers running supported Windows Server operating system versions	Servers are manually patched to be able to control the reboots better before taking a server down.	
Mac Operating System - macOS	Devices running supported macOS versions	Varies for new operating system releases	New operating system versions are blocked until it is approved by IT
Linux/Unix Operating Systems	Racktables running on Ubuntu.	Server is manually patched to be able to control the reboots better before taking a server down.	
Chromebook Operating System - ChromeOS	Devices running supported	Not yet defined until they get deployed in the production environment	

	ChromeOS versions		
Apple iOS	Devices running supported iOS versions		
ERP/Student Information System - Patches	Software Updates impacting Colleague, Self-Service (GXP 2.0), Web API	Maintenance Window on Sunday mornings 5-10 AM PDT/PST	Ferrilli - Our Managed Service Provider
ERP/Student Information System - Custom Patches	Custom Software Updates impacting Colleague	Weekday mornings 6-7 AM PDT/PST	AIS - Our Managed Service Provider
Data Center – Firewalls	Campus Firewalls		Our Managed Service Provider handles the management and patching of the firewalls. They are in a HA (redundant) configuration so there is no downtime.
Data Center – Core Switches	Switches running IOS	Maintenance Window on Sunday Mornings 5-10 AM PDT/PST	
Data Center – Access Layer Switches	Switches running IOS	Maintenance Window on Sunday Mornings 5-10 AM PDT/PST	
Data Center – Wireless Controllers	Meraki Cloud	Maintenance Window M-F 5-7 AM and Sunday 5-10 AM	
Data Center – Phone System	GoTo Cloud PBX		GoToConnect - Managed Service Provider
Data Center – Storage Arrays	Storage for all virtual servers - SAN	Twice a year	Operations & Desktop Engineer
Data Center – VMWare Hosts	Virtual Desktop Servers	Server Maintenance Window on Sundays	Systems Engineer and Data Architect
Applications	3rd party applications		Adobe, Google Chrome, Firefox, Hyland and other 3rd party apps you use that you need to patch.
Campus - Access Layer Switches	Switches running IOS	M-F Maintenance Window 5-7 AM or Sunday Maintenance Window	

3rd Party Systems on the St. Mary's Network			
Azure Cloud: Domain Controllers, etc.	OS patches	Friday Maintenance window on 3rd Friday of the month 9 pm - 1 am PST	RapidScale - Managed Service Provider
Azure Cloud: Colleague	OS Patches, File Maintenance	Maintenance Window on 4th Sunday of month 5-10 AM PDT/PST	Ferrilli - Managed Service Provider
Azure Firewall	Virtual Palo Alto Firewall	Performed during Sunday Maintenance Window or pre-arranged time with AIS- Must make arrangements with AIS. Updating this firewall will cause an outage for all services in Azure.	Our Managed Service Provider handles the management and patching of the firewalls

- **Automation:** If applicable, the IT team will employ patch management software solutions with automated tools for patch deployment.
- **Change management:** Saint Mary's College follows the change management process for patch deployment. The change management team in IT oversees the planning and execution of patch-related changes to ensure that they are well-coordinated and meet business needs.

f. Patch Documentation

Careful patch documentation will be kept aiding in tracking and auditing patching activities. This will facilitate our regulatory compliance and accountability. The process encompasses:

- **Record keeping:** Our system administrators are responsible for maintaining detailed records of all patches applied. This includes recording the date of application, patch version, and the specific systems affected.
- **Documentation repository:** The IT Department ensures that Colleague patch documentation is stored in a centralized repository for auditing and tracking. This repository is accessible to authorized personnel and promotes transparency.

g. Emergency Patching

To ensure swift response to high-risk vulnerabilities, the following will be followed during emergency patching:

- **Emergency procedures:** The IT Department will define and implement emergency procedures to expedite the patching process, reducing the potential impact of vulnerabilities.

- **Emergency notifications:** Relevant stakeholders will be promptly notified of any relevant outages.

h. Rollback Plan

To prepare for potential complications to maintain system stability, we will build a rollback plan, which includes:

- **Contingency plan:** The IT Department will develop a plan that outlines the steps to be taken in case of issues following patch deployment.
- **Backups:** Ensuring the availability of data and system backups is a responsibility shared between our system administrators. These are vital for data recovery and system restoration in the event of patch-related failures.
- **Colleague Software Updates:** Ellucian Colleague software updates, once installed in Production, cannot be uninstalled. Testing is crucial before deploying. If a patch is installed that causes issues, SMC will have to wait for the vendor to release a fix.

i. User Awareness – Communication

User communication about patching processes will be conducted to create a security-conscious organizational culture. End users will also play a key role in reporting vulnerabilities and maintaining security awareness. We will follow these guidelines in improving user awareness:

- **Communication:** The IT Department conducts effective end user communication to educate employees on the significance of reporting vulnerabilities promptly and fostering their understanding of the patching process.
- **User notifications:** Our IT communication team will inform all users about scheduled patch deployments and any necessary actions they should take.

Compliance and Reporting

Saint Mary's College will perform ongoing assessment of policy adherence to demonstrate compliance with industry standards. We will also encourage the reporting of security incidents for early detection and prompt mitigation. Responsibilities related to compliance and reporting include:

- **Regular auditing:** The IT Team performs regular audits to ensure compliance with the patch management policy.
- **Incident reporting:** Our Incident Response Team will establish a process for reporting security incidents related to patch management to enable prompt identification and resolution.

Patch Management Policy Maintenance

Policy Review and Revision

Saint Mary's College IT Department will follow these processes to make sure the Patch Management Policy remains effective and up to date:

- **Annual review:** We will conduct an annual review of the Patch Management Policy. This review will assess the policy's relevance, alignment with best practices, and success in addressing emerging threats.
- **Feedback mechanism:** We will administer the collection and assessment of feedback to identify areas for improvement.
- **Policy updates:** Any identified deficiencies or areas requiring improvement will result in updates to the Patch Management Policy. Our IT team will document these updates and communicate to all relevant stakeholders.

Policy Enforcement

The IT Department, in collaboration with Human Resources and Legal, will oversee policy enforcement. Non-compliance with the Patch Management Policy may result in disciplinary actions, as outlined in the policy.

Exceptions

Saint Mary's College understands that exceptions to this policy may be necessary under certain circumstances. Exceptions may be granted under the following conditions:

- In cases where immediate patch deployment may disrupt critical business operations, exceptions may be considered. The IT department must give their approval for exceptions.
- In instances where legacy systems or software that are no longer supported by vendors require specific patches and applying them would cause system instability.
- When compliance with this policy conflicts with regulatory requirements or standards. For these cases, users must formally request exceptions, which the IT team must approve after evaluation.
- For third-party software or services when (Company Name) has limited control over patch deployment. Justification and documentation should accompany these exceptions. The IT team is responsible for approving exceptions.

Violations and Penalties

Non-compliance can have serious consequences, as it may expose the organization to security risks and operational disruptions. Violations of this policy may result in the following penalties:

- **Employee violations:** Any employee found to be in violation of this policy may be subject to disciplinary action, which can include verbal or written warnings, suspension, or termination of employment, as deemed appropriate by the Human Resources department and in accordance with the organization's HR policies.
- **Contractors and third-party vendors:** Non-compliance by contractors or third-party vendors may lead to contract termination, financial penalties, or legal action as stipulated in contractual agreements.
- **Legal implications:** Non-compliance that results in security breaches or data loss may lead to legal action against the responsible party or parties.
- **Financial penalties:** Violations that result in financial losses to the organization may lead to financial penalties, restitution, or damages sought through legal means.

Saint Mary’s College reserves the right to take appropriate action in response to policy violations, with penalties commensurate with the severity and impact of the violation.

Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Saint Mary’s College
1928 Saint Marys Rd.
Moraga, CA 94575

Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
2/25/2024	Publish	James Johnson