Saint Mary’s College of California
Information Technology Policy

Patch Management Policy

No: 1.0

Chief Information Officer, James Johnson

April 25, 2024

April 25, 2024

ITS - Information Technology Services

CONTENTS

Saint Mary’s College of California (SMC) recognizes the importance of effective patch management

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

Saint Mary's College 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 de[redacted]nt.
- Ensuring compliance with this policy and relevant regulations.

must:

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

should:

- Promptly provide patches and updates for their software used wit organization, in accordance with service-level agreements (SLAs) ractual agreements.

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

- using automated tools to detect missing patches.
- Promptly receiving and assessing for relevant patches.

- The IT Department systematically prioritizes

	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 Tc ɚ X - Ű r	

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

- If applicable, the IT team will employ patch management software solutions with automated tools for patch deployment.
- Saint Mary’s College follows the change management process for patch deployment. The change management team in IT oversees the planning

- Relevant stakeholders will be promptly notified of any relevant outages.

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

- The IT Department will develop a plan that outlines the steps to be taken in case of issues following patch deployment.
- 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.

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:

- 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.
- Non-compliance by contractors or third-party vendors may lead to contract termination, financial penalties, or legal action as stipulated in contractual agreements.
- Non-compliance that results in security breaches or data loss may lead to legal action against the responsible party or parties.
- 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.

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

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

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

2/25/2024	Publish	James Johnson