VULNERABILITY MANAGEMENT STANDARD

Introduction

Purpose

The purpose of this document is to guide project and operation teams on the expectations of the Cyber Risk and Resilience team regarding vulnerability management. It outlines the Cybersecurity team's requirements and recommendations in order to ensure cybersecurity risks are mitigated to the university's acceptable level.

This standard is developed as part of the Monash University (MU) cybersecurity standards. This standard will point to baselines to explain specifically where required. Please refer to the cybersecurity standards for specific security requirements (e.g., approved encryption algorithms), as well as the vulnerability management procedure document.

Please engage the Cybersecurity Architecture team for any clarification and if certain service categories or design considerations are not covered by this standard.

In Scope

In the scope of this document the following will be addressed:

- Security patch management
- Vulnerability scanning
- Penetration testing
- Continuous assurance
- These standards apply to all Monash University Group Controlled Entities

Out of Scope

Out of the scope of this document:

- Relevant management and operation models
- Security training and awareness requirements
- Step by step implementation guides
- Vendor product upgrades (e.g. new version of Windows)

RACI Matrix

Actions	Cyber Security	Application Owners	Infrastructure Teams
Develop and maintain security standards	R/A	C/I	C/I
Develop applications in line with security standards	C/I	R/A	C
Implement and maintain infrastructure security in line with security standards	C/I	C	R/A

*KEY: Accountable **(A)**, Responsible **(R)**, Consulted **(C)**, Informed **(I)***

Attributes

Attributes Supported: Protected, Secure, Trusted, Auditable, Isolated, Identified, Resilient, Zoned

Security Architecture Principles

Cyber Security Architecture Principles should be considered in order to protect Monash University's environment and while designing and implementing digital transformations.

Security Standard for Vulnerability Management

Security Patch Management

This section covers the minimum security controls for a patch management plan.

Table 1. Minimum Security Requirements

NIST CSF Function	Controls	Requirements
Identify	Asset Management	● Reference asset management policy and procedures are in place and being complied with. ● An inventory of systems and software used should be recorded and maintained. ● The following details are required, at a minimum: ○ IP ○ Hostname ○ Location ○ Software installed ○ Purpose/Description of asset ○ Integrations ○ Team responsible for Asset Management ○ Internet accessible (Y/N) ○ Highest information classification handled (Public, Restricted, Sensitive, Very Sensitive) ● All these items are listed in the Asset Management Standard. ● Automated asset discovery tools shall be used to detect new systems and assets.
Protect	Vulnerability Management: Security Patch Management	● Reference vulnerability management procedure is in place and being complied with. ● Methods should be established for receiving notifications from vendors stating new patches are available. This is generally achieved by monitoring and subscribing to the vendor's notification service.

	Vulnerability Management: Security Patch Management (Evaluation)	• Reference vulnerability management policy and procedure is in place and being complied with. • A risk rating should be applied to new patches, in accordance with the MU risk management system and/or the True Risk score as per the vulnerability management procedure.

	Vulnerability Management: Security Patch Management (Deployment)	• Reference vulnerability management policy and procedure is in place and being complied with.
		• Patches should be tested before wide-scale rollout, preferably within a non-production environment.
		• Only tested patches should be rolled out, with exception of those deployed within test environments for the purposes of testing.
		• Patches should be deployed using a formal change management procedure.
		• Patches should only be obtained from official vendor sources with verified signatures.
		• Where possible, patching should be undertaken using an automated process.
		• Where possible, the patching process should have little to no impact to end users and business operations.
		• Patches shall be deployed based on the exploitability and severity of the vulnerability as per True Risk score, vendor assessment or CVSS rating. Deployment times shall be at maximum:
		  ○ Critical including CISA Known Exploited Vulnerabilities (KEV) catalog: 48 hours
		  ○ High: 7 days
		  ○ Medium: 30 days
		  ○ Low: 90 days

	Vulnerability Management: Security Patch Management (Interim solutions)	• If a patch is not yet available for a known vulnerability, or in the event where a patch is unable to be applied,:
		  ○ Disable the vulnerable function.
		  ○ Restrict or block access to this function using firewalls or access controls.
		  ○ The use of intrusion prevention systems can detect suspicious traffic related to unpatched systems.
		  ○ Apply appropriate compensating controls.

		○ Follow the MU risk management system for formal risk acceptance for a period of time
Recover	Vulnerability Management: Security Patch Management (Rollback)	● Reference vulnerability management policy and procedure is in place and being complied with. ● A contingency plan should be in place in the event a patch corrupts an existing environment. ● This plan should include failover and fallback procedures, and should list key staff and contacts.

Vulnerability Scanning

This section covers the minimum security controls for a vulnerability scanning plan.

Table 2. Minimum Security Requirements

NIST CSF Function	Controls	Requirements
Identify	Asset Management	● Reference asset management policy and procedures are in place and being complied with. ● An inventory of systems and software used should be recorded and maintained. ● The following details are required, at a minimum: ○ IP. ○ Hostname. ○ Location. ○ Software installed. ○ Purpose/Description of asset ○ Integrations ○ Team responsible for Asset Management ○ Internet accessible (Y/N) ○ Highest information classification handled (Public, Restricted, Sensitive, Very Sensitive). ● All these items are listed in the Asset Management Standard. ● Automated asset discovery tools shall be used to detect new systems and assets.
	Vulnerability Management Scanning	● The environment infrastructure and/or applications should be regularly scanned in order to detect any vulnerabilities that may be present, and to identify any systems that may have been missed within the asset register. ○ Regularly is defined as continuous scanning being preferred and at minimum once per week. ● Vulnerability scanning agents should be installed to monitor Operating System (OS) infrastructure. ● If vulnerability scanning agents cannot be installed for a valid business or technical reason, the Cyber team

		should be consulted to establish compensating controls. ● Cloud monitoring tools should be deployed to monitor cloud environments such as AWS, Azure and GCP.
Detect	Continuous Monitoring	● As part of our continuous monitoring, external facing systems willbe subject to Vulnerability Disclosure Program and Vulnerability Bug Bounty Program. Findings from these programs will be facilitated by the cyber team, with the system owners.

Penetration Testing

This section covers the minimum security controls for a penetration testing plan.

Table 3. Minimum Security Requirements		
NIST CSF Function	**Controls**	**Requirements**
Identify	Asset Management	● Reference asset management policy and procedures are in place and being complied with, as outlined in tables 1 and 2. ● The penetration testing decision matrix should be followed to determine the applicability of penetration testing for a system or application. ● Assets that require penetration testing should be identified with reference to the asset register, and the penetration testing process should be undertaken. Some examples that may be particularly relevant for testing: ○ Systems holding Personally Identifiable Information (PII). ○ Payment processing systems. ○ Systems holding other sensitive information such as credit card details. ○ Systems used for research purposes. ○ Systems holding intellectual property.
	Vulnerability Management: Pre-test	● Reference vulnerability management policy and procedure is in place and being complied with. ● Scoping of the penetration test should be undertaken, including but not limited to: ○ Objectives ○ Internal/External infrastructure and/or applications to be tested ○ Network access controls ○ Services exposed ○ Environment type (prod, test, etc) ○ Remote access/on-premises test ○ Authenticated or unauthenticated test ● Monash Cyber team are informed ahead of time

Detect	Vulnerability Management: Testing	• The penetration testing time window should be agreed upon prior to the test. • Failover and fallback plans should be in place should an issue occur during the test. • In case of external testing, access granted for testers should be maintained as per the Identity best practices. • Penetration testing shall be considered for any significant architectural change and annually for systems in scope for PCI-DSS and holding very sensitive classified information that is Internet accessible
Respond	Vulnerability Management: Post-test	• The outcomes of penetration testing findings should be triaged, prioritised, and risk rated, with a committed timeline for addressing the findings. • Monash University's security analysts practise responsible disclosure and report the vulnerabilities they discover through the Forum of Incident Response and Security.

Continuous Assurance

This section covers the minimum security controls for a continuous assurance plan.

Table 4. Minimum Security Requirements

NIST CSF Function	Controls	Requirements
Identify	Governance, Risk and Compliance	● Consultation should be undertaken with the Cyber Security Operations team, to determine what systems/platforms/applications could potentially be onboarded into the continuous assurance programs in place. ● As part of our continuous monitoring, external facing systems will be subject to Vulnerability Disclosure Program and Vulnerability Bug Bounty Program. Findings from these programs will be facilitated by the cyber team, with the system owners. ● The following continuous assurance mechanisms are also in place: ○ Checkmarx1 Static Application Security Testing (SAST) and Software Composition Analysis (SCA) for Github and Gitlab integrated code repositories ○ ORCA Cloud Security Posture Management (CSPM) for AWS, Azure and GCP ○ Crowdstrike Falcon SaaS Security Posture Management (SSPM)

Metrics

The following metrics shall be used to monitor the effectiveness of implementing the requirements of this vulnerability management standard:

Metric	**KPI goal**
Mean Time to Remediate (MTTR) per severity level: ○ Critical: 48 hours ○ High: 7 days ○ Medium: 30 days ○ Low: 90 days	Percentage across all systems in Monash group: ○ Critical: 95% ○ High: 90% ○ Medium: 80% ○ Low: 80%
Vulnerability scan coverage percentage across the asset inventory	90%
Percentage of compute with vulnerability scan agents successfully installed (where agent installation is possible e.g. excluding appliances, IOT, serverless)	90%
100% of agent-deployed compute detects new vulnerabilities Unauthenticated network sweeps	Within 24 hours Detect within 7 days
Percentage of total known vulnerabilities that are currently operating under an approved, active risk exception/acceptance rather than being remediated.	< 5% of total vulnerability count

Reference

- Monash University Cyber Security Architecture Principles
- Monash University Cybersecurity Standards
- Monash University Asset Management Standard

Definitions

Table 5: Definitions	
Term	**Definition**
Backup	A copy of a system or application's data that can be used for restoration, in the event of data being lost or compromised.
Security Patch	Additional code, usually provided by a vendor, that aims to address known security vulnerabilities within a software.
Penetration Testing	A penetration test is an authorised simulated cyberattack on a computer system, performed to evaluate the security of the system. This can be done by an internal or external party.
Personally Identifiable Information	Information that can be used to identify a person, whether alone or in conjunction with other information.
Risk	Any circumstance or event in which, deliberately or accidentally, harm may be done to a system.
Vulnerability	An issue with the design or configuration of a software or hardware that has the potential to be exploited.

Version and Update History

Next review date: April 2027

Version	Date	Author	Summary of Change
0.1 Draft	18/11/21	Ashley Niklaus	Initial Draft
0.9 Draft			Peer Review with CyberOps
1.0			Initial Release
2.0	9/05/2025	Mathew Radford	Reviewed and updated in 2025. Changes include addition FIRST, VDP, VBP and scope updated to ‘Group of Monash’ and wording changes
3.0	27/05/2026	Rakkhi Joy	Annual review updates. Approved by Ashok.