STANDARD OPERATING ENVIRONMENT SECURITY STANDARD

Introduction

Purpose

The purpose of this document is to guide project and operation teams in the expectations of the Cyber Risk and Resilience team regarding the secure design, development and operation of their Standard Operating Environments (SOE) and the security of the SOE build environments. SOE is defined as a standardised build of an Operating System (OS) and associated software that can be used for servers, containers, workstations, laptops and mobile devices. This standard 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).

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:

- Server/Container SOE: Windows and Linux
- Workstation SOE: Windows, Linux and MacOS

Out of Scope

Out of the scope of this document:

- Non-Monash SOEs
- Mobile devices SOEs (mobiles and tablets). Refer to the Mobile Device Management Baseline
- Relevant management and operation models
- Security training and awareness requirements

- Step by step implementation guides

RACI Matrix

Actions	Cyber Security	Application Owners	Infrastructure Teams
Develop and maintain security standards	R/A	I/C	I/C
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

Attributes

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

Security Architecture Principles

Cyber Security Architecture Principles shall be considered to protect Monash University's environment.

Security Standard for MU SOEs

Server / Container SOEs

This section covers the minimum-security controls for server / container SOEs.

Table 1. Minimum Security Requirements		
NIST CSF Function	**Controls**	**Requirements**
Govern	Governance, Risk and Compliance	• Reference risk management policy and procedures are in place and being complied with, while SOEs are being designed and built. Upon a related change on a baseline SOE, system owners shall align with the MU Change Management System and shall consult with this standard and any related baselines. Should the change use cases not be covered, they shall commence a risk assessment as per MU risk management system. • Applicable legal and regulatory requirements are formally identified and based on the information classification. • SOE ownership and responsibilities shall be identified, including a RACI matrix per SOE type. • Should an internal or external audit be required, system owners shall maintain the required audit artefacts, including but not limited to configuration snapshots, logs and process documents.
Identify	Asset Management	• Reference asset management policy and procedures are in place and being complied with and as per the MU Asset Management Standard. • SOE categories and types shall be defined and formalised and an SOE asset register shall be developed where different SOE types, SOE owners and SOE user group, are listed as per the MU Asset Management Standard.

		• Per SOE type and as part of the relevant asset register, a list of the following shall be maintained and regularly reviewed:
		  ○ approved operating systems and OS builds and.
		  ○ approved enterprise and third-party applications/tools including approved browsers and runtimes.
		• An asset discovery solution shall be deployed to maintain an up-to-date inventory of compute SOE across MU with reference to the approved OS and applications list. This shall include traditional servers and workstations as well as container images (e.g., Docker, Kubernetes nodes) and Infrastructure as Code (IaC) templates
		• An asset disposal process shall be formalised and followed to ensure the secure disposal of SOE and SOE build environments related data/assets, and shall align with the MU Information Classification and Handling Standard and the MU Asset Management Standard

Protect	Identity and Access Management: Authentication	• SOE image users shall be authenticated at all levels, including but not limited to, the boot/BIOS level and the OS level before access is granted; this includes administrative access to the SOE build tools. • SOE images shall have a logon banner that requires users to acknowledge and accept their security responsibilities before access is granted. • Where applicable, user session management parameters such as session inactivity protection and re-authentication requirements shall be considered when the SOE is designed, built and rolled out. • Privileged access to the SOE build environments is implemented using a dedicated account for elevated activities, is only used for administrative purposes, and is unique and identifiable to a user/process. Phishing-resistant Multi-Factor Authentication (MFA)authentication shall be implemented for the privileged access to the SOE build environment/solution as per MU Identity and Enterprise Engineering related standards. Those teams shall be consulted along with the cyber team to

		identify the right privileged access method for a given environment. • Local administration accounts to the SOE build environments shall only be used in emergency situations as break glass accounts. • Third party access to the SOE build environments shall be managed in line with the requirements in this section and MU remote access best practices. • System integration (Machine-to-Machine) shall be authenticated with mutual TLS (mTLS) or OAuth 2.0 with short-lived tokens. • Server / Container SOE's local administration accounts are defined as part of the SOE build process and integrated with a Local Administrator Password Solution (LAPS) to ensure local admin passwords are fundamentally unique per machine and automatically rotated.
	Identity and Access Management: Authorisation	• The principle of least-privilege and need-to-know shall be maintained when accessing the SOE build environment. • Access to the SOE build environments shall be limited to a defined group of administrators and not from internal or external untrusted zones. • Local accounts used for provisioning the SOE shall be explicitly approved by considering segregation of duties. • Local accounts credentials shall be unique for each local user where applicable. • Accounts, including user accounts and service accounts used to access the SOE build environments, or those that are needed for a given SOE functionality, shall be separated. • A formal authorisation plan shall be in place. This includes, but is not limited to, access grant, change, revocation, and access review(s).
	Security Awareness and Training	• SOE supporting teams shall be security-aware and trained.

	Information Asset Protection: Endpoint Protection	• Only MU-approved Privileged Access Workstations (PAW) shall be allowed to access the SOE build environment. • For each SOE type, the applicable MU endpoint protection solutions/mechanisms shall be part of the SOE build process of that SOE. For example, host-based firewalls and anti-malware solutions.
	Information Asset Protection: Data Lifecycle Management	• SOE-related information shall be backed up as per MU backup and restore policy and with reference to any relevant regulatory requirements. • SOE images, builds, secrets, and any related data, shall be backed up on a regular basis and in an automatic manner where possible. • Backups shall be encrypted and stored in a secure manner. • Backup test and restore procedures shall be performed on a regular basis. • Data Leakage Prevention (DLP) capabilities shall be implemented to monitor SOE data transfer.
	Information Asset Protection: Network Isolation	• The network infrastructure supporting the SOE development process (cloud environments, on-prem, or hybrid) shall maintain sufficient network segmentation. • Production and non-production SOE build environments shall be segregated, and access to development environments shall be whitelisted for specific subnets.
	Information Asset Protection: Malware Prevention	• The university approved malware protection software must be included as part of the SOE build. • The scanning engine and signature database of protection software shall be updated prior to releasing the SOE image. • The agent version shall be verified as currently supported prior to releasing the SOE image.
	Configuration Management: Secure Configuration	• Establish and maintain secure configurations for all SOE types. • SOE configuration shall align with MU secure configuration baselines where possible.

		• Third party provided images or server / container templates or any other configuration item, shall be reviewed and hardened prior to being used to build an SOE. • The integrity of the SOE configuration files shall be maintained using relevant tools and shall be supported by a robust monitoring and alerting mechanism. • Where possible, the process of building SOEs shall be automated.
	Data Protection: Encryption	• Encryption at-rest shall be implemented for SOE images, builds and other data. • Full disk encryption shall be enabled as part of the SOE image. • Where possible, the full disk encryption process shall be centrally managed. • Encryption algorithms, crypto-ciphers, protocols, and certificates usage must comply with the MU Cryptography Baseline.
	Data Protection: Keys and Secrets Management	• An MU approved, centralised key and secret management solution shall be used to manage keys and secrets that are involved in the SOE build and release processes. • Where possible, credentials and other secrets shall not be stored or hard coded in an accessible configuration or code. • Where possible, keys and secrets shall have expiration time set.
Detect	Security Monitoring: Logging and Alerting / Incident Response Planning	• SOEs shall be built to support the generation of logs and events as required by MU Security Logging and Alerting Baseline. • The SOE build environments shall generate logs and events as required by MU Security Logging and Alerting Baseline. • The SOE build environments and the deployed SOE images shall be synchronised with a central, MU approved time synchronisation service, for example, Network Time Protocol (NTP) serviceto ensure the generated logs and events are

		useful in an investigation such as troubleshooting, cyber incident response, and digital forensics. • Collected security logs and events shall be used to perform threat hunting, cyber incident response and digital forensics activities. • Collected security logs and events shall be stored in a secure manner.
	Vulnerability Management: Vulnerability Scanning	• The SOE build environments and SOE images, builds and other files, shall be continuously scanned for vulnerabilities using MU approved solutions. The university approved Vulnerability Management software / Agent shall be included as part of the SOE build where possible. • SOE related security vulnerabilities shall be detected, triaged and patched as per the MU Vulnerability Management Policy and Standard.
	Vulnerability Management: Patching	• A centralised and managed approach following MU patch management and the relevant best practices shall be used to patch or update the toolset used in the SOE build process. • SOEs shall have the latest patch(es) installed before being used to build compute. • Where possible, automated mechanisms shall be implemented to validate and ensure the integrity of applied patches or updates.
	Vulnerability Management: Penetration Testing	• Penetration testing shall be performed at the initial release and against major changes of SOEs with reference to the MU Vulnerability Management Standard. • Penetration testing shall be performed on the SOE build environments when an environment is initially set up and upon major changes of that environment with reference to the MU Vulnerability Management Standard.
Respond	Cyber Incident Response	• Relevant controls to support the incident response and digital forensics process shall be implemented as per the Cyber Incident Response playbooks.

		• Cyber Incident Response playbooks shall be updated with SOE and SOE build environments specific scenarios where possible, and these playbooks shall be tested regularly. • Where possible, automated mechanisms shall be implemented to support the cyber security incident response plan.
Recover	Business Continuity and Disaster Recovery: Resiliency	• Business Continuity Plans and Disaster Recovery Plans are developed and tested regularly to ensure SOE management services are sustainable and recoverable.

Workstation/End User SOE

This section covers the minimum-security controls for workstation/end user SOEs.

Table 2. Minimum Security Requirements		
NIST CSF Function	**Controls**	**Requirements**
Identify	Governance, Risk and Compliance	Refer to table 1
	Asset Management	Refer to table 1

	Security Awareness and Training	Refer to table 1
Protect	Identity and Access Management: Authentication	• Users shall be authenticated at the OS level before access is granted; this includes administrative access to the SOE build tools. • Privileged access to the SOE build environment is implemented using a dedicated account for elevated activities, is only used for administrative purposes, and is unique and identifiable to a user/process. • Phishing-resistant Multi-Factor Authentication (MFA)authentication shall be implemented for the privileged access to the SOE build environment/solution as per MU Identity team's related standard. • Local administration accounts to the SOE build environments shall only be used in emergency situations as break glass accounts. • Workstation SOE build process shall consider limited remote support access options/tools for each SOE type. • Third party access to the SOE build environments shall be managed in line with the requirements in this section and MU remote access best practices. • • Workstation SOE's local administration accounts are defined as part of the SOE build process and integrated with a Local Administrator Password Solution (LAPS) to ensure local admin passwords are fundamentally unique per machine and automatically rotated.
	Identity and Access Management: Authorisation	Refer to table 1

	Information Asset Protection: Endpoint Protection	Refer to table 1
	Information Asset Protection: Data Lifecycle Management	Refer to table 1
	Information Asset Protection: Network Isolation	Refer to table 1
	Information Asset Protection: Malware Prevention	Refer to table 1
	Configuration Management: Secure Configuration	Refer to table 1
	Data Protection: Encryption	Refer to table 1
	Data Protection: Key and Secrets Management	Refer to table 1

Detect	Security Monitoring: Logging and Alerting / Incident Response Planning	Refer to table 1
	Vulnerability Management: Vulnerability Scanning	
	Vulnerability Management: Patching	A centralised and managed approach following MU patch management and the relevant best practices shall be used to patch or update the toolset used in the SOE build process. ● SOEs shall have the latest patch(es) installed before being used to build workstations ● Where possible, automated mechanisms shall be implemented to validate and ensure the integrity of applied patches or updates.
	Vulnerability Management: Penetration Testing	Refer to table 1
Respond	Cyber Incident Response	Refer to table 1
Recover	Business Continuity and Disaster Recovery: Resiliency	Refer to table 1

Reference

- Monash University Cyber Security Architecture Principles
- Monash University cybersecurity standards

Definitions

Table 2: Definitions	
Term	**Definition**
MU	Monash University.
SOE	Standard Operating Environment, a standardised image used for deployment of servers, containers or workstations.

Version and Update History

Next review date: April 2027

Version	Date	Author	Summary of Change
0.1 Draft	07/1/22	Simsam Hijjawi	Initial Draft
0.9 Draft	17/1/22	Stanley Wijoyo Ashley Niklaus	Peer Review
1.0			Initial Release
1.1	11/12/2024	Abi Vijay/Thushara Jayawardhena	2024 Annual Review/Peer Review. Release approved by Ashok Khatiwada
1.2	17/06/2025	Abi Vijay/Thushara Jayawardhena	2025 Annual Review/Peer Review. Release approved by Ashok Khatiwada
2.0	27/05/2026	Rakkhi Joy	2026 Annual Review. Approved by Ashok