ON-PREMISE INFRASTRUCTURE SECURITY STANDARD

Introduction

Purpose

The purpose of this document is to guide projects and operational teams, as well as service (applications and systems) designers to adequately secure those services deployed in Monash University hosted on-premises environments. It outlines the Cybersecurity requirements and recommendations in order to ensure cybersecurity risks are mitigated or reduced to the University's acceptable level.

This standard is developed in line with the existing University's cybersecurity standards and does not supersede them. 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

This standard applies to all Monash University staff, students, associates and visitors accessing and using the University's Information Technology (IT) on-premises environments.

For the purpose of this standard, references to 'the University' include the activities of Monash University Australia, Monash University Malaysia, Monash University Indonesia, Monash College, Monash Suzhou, Monash University Prato Centre and the World Mosquito Program Ltd (and its subsidiaries), unless otherwise indicated. In the scope of this document, the following will be addressed:

- On-premises infrastructure in the University:
    - Network infrastructure:
        - LAN
        - WLAN
    - Storage infrastructure
    - Compute infrastructure including hypervisor based and bare metal

Out of Scope

Out of the scope of this document:

- Public cloud hosted environments
- 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	R/A	R/A

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 on-premises environments and their integrated systems.

Security Standard For On-Premises Network Infrastructure

This section covers the minimum security controls for on-premises infrastructure.

Table 1. Minimum Security Requirements		
NIST CSF Function	**Controls**	**Requirements**
Govern	Policy	• Reference risk management policy and procedures are in place and being complied with. Upon a related change, consult this standard and its related baselines with the Cybersecurity Architecture Team. Should the use cases not be covered, commence a risk assessment process as per the University's risk management system. • Applicable legal and regulatory requirements are formally identified based on the information classification. • Environment ownership and shared responsibilities between external vendors, application, cloud infrastructure and cyber security teams are formally identified, including a RACI matrix. • Should an internal or external audit be required, system owners are required to maintain the audit artefacts, including but not limited to configuration snapshots, logs and process documents.
	Asset Management	• Maintain an inventory of approved assets, including but not limited to, software, hardware, documentation, and removable media, and perform a regular review as detailed in the relevant baseline document. • Deploy an automated asset discovery solution to automatically update the asset register where possible. • Where applicable, assets are labelled with protective markings reflecting their sensitivity or classification as per the University's Information Classification and Handling Standard.

Protect	Identity and Access Management: Solution Administration and Privileged Access	• Only when centralised access is disabled, Local authentication (break glass) for solution administration shall be enabled as per TS-network Standard Operating Procedures (SOP). • Enable Out of Band (OOB) management access supported by the University's approved VPN solution. • Change default passwords when infrastructure solutions are onboarded, and implement strong authentication as dictated by the relevant policy. • Perform a regular review of account access and privileges, including but not limited to user and service accounts. • Implement privileged access using a dedicated account for elevated activities, and are only used for administrative purposes, unique and identifiable to a user/process. • Only allow administrative access from dedicated, security hardened workstations that reside on a secure network segment. • Enforce Just-In-Time (JIT) access for administrative purposes.
	Identity and Access Management: Authentication	• Enforce multi-Factor Authentication (MFA) for all users, before access is granted. Where this is not supported (such as local administrator, root, or special service accounts), use passwords that are unique to that system. • The University's standard Single-Sign-On (SSO), authentication and authorisation methods, and procedures, are used for administrative access to the environment. • Shared accounts are avoided and formally approved for a temporary use when justified by a valid business need. • Implement and enforce authentication for infrastructure system integration (Machine-to-Machine).
	Identity and Access Management: Authorisation	• The principle of least-privilege and need-to-know are maintained when accessing the environment. • The access control implementation shall be based on the Roles(RBAC). • Unique identities, credentials and access permissions are centrally managed as the source of truth for authorised devices, processes and users to access systems, data and information.

		• For each system/solution, a formal authorisation process is required. This includes, but not limited to access grant, change, revocation and access review. • Separate accounts used to access non-production and production environments, including user accounts and service accounts.
	Information Asset Protection: Mobile Devices	• Use the University's approved Mobile Device Management (MDM) solution to control access (including administrative access) to infrastructure from mobile devices and to track data on mobile devices. • Should Monash data be transferred to the mobile device, all data is encrypted in-transit and at rest in accordance with the University's policy. • Should Monash data be stored on a mobile device, all content is protected with the Digital Right Management solution in accordance with the University's data governance policy.
	Information Asset Protection: Physical Access	• For on-premises systems, servers, storage and network devices are secured in server or communications rooms, with access restricted to only approved personnel. • Keys or equivalent access mechanisms to server rooms, communications rooms and security containers are appropriately controlled.
	Information Asset Protection: Remote Access	• Remote access to the University's network infrastructure is implemented using the University's approved remote access methods, as per the University's Remote Access Security Standard. • Perform scans on remotely connected devices prior to accessing the network for compliance with the University's relevant policies where possible. • Remote access to the network is encrypted and strongly authenticated with Multi-Factor Authentication (MFA). • Use public key-based authentication where possible.

	Information Asset Protection: Network Isolation	• Where applicable, networks are divided into multiple functional network zones according to the sensitivity or criticality of information or services. • Administrator workstations are placed into a separate network zone to other workstations. • Only authorised protocols and services are allowed to cross the network boundaries. • No privileged access related traffic shall be visible over the non-privileged access zones of the network.
	Information Asset Protection: Network Access Control	• Network access/admission controls are implemented on networks to prevent the connection of unauthorised network devices. • Network access controls are implemented to limit traffic within and between network segments to only those that are required for business purposes. • Unused network ports, protocols, and services listening on a system are disabled and continuously monitored.
	Information Asset Protection: Wireless Network and Devices	• Corporate and guest wireless networks are separated end-to-end and the corporate WLAN, with no convergence points with the backend infrastructure without proper protection. • Wireless LAN, Bluetooth, and NFC capabilities are disabled by default on infrastructure components. • Peer-to-peer (ad hoc) wireless network capabilities are disabled or blocked for infrastructure components.
	Information Asset Protection: Firewalls	• Deploy network firewalls with Next generation Firewall Capabilities to apply layered difference from Network layer to Identity Layer segmentation. • Implement micro-segmentation where possible, It is strongly recommended to do so if the segments are hosting/handling Multiple Classification of data.

	Information Asset Protection: Malware Prevention	• Enable centralised malware protection software on all connected network devices using the University's approved solution. • Anti-malware software and signatures are updated regularly.
	Configuration Management: Secure Configuration	• Secure configurations for all assets in the environment are established, maintained and reviewed regularly. • Secure images or templates for all authorised systems in the environment are maintained and reviewed regularly. These templates are kept up-to-date with the latest stable version and with any security-related patching done. • The master images and templates are continuously validated with integrity monitoring tools and securely stored in a safe location. • Third-party provided images, configurations or server templates are reviewed and hardened prior to being used. • Use automated configuration management tools used to enforce and redeploy configuration settings to systems at regular intervals.
	Data Protection: Encryption	• When data is in transit within or between workloads, data encryption in-transit should be implemented. • Encryption algorithms, protocols, and certificates usage must comply with the University's Cryptography Baseline. • It is preferred to store the encrypted keys of the data handling platform, preferably in Hardware Security Module. • When data is at rest shall be encrypted if they are sensitive or very sensitive in classification irrespective of the location.
	Data Protection: Secrets Management	• Use a centralised key and/or secrets management solution to manage keys, secrets and certificates. • Do not store or hard-code credentials and other secrets in an accessible configuration or code.

Detect	Security Monitoring: Incident Response Planning	• Security events, especially access to sensitive services and privileged access or activities are collected and monitored as per the University's Security Logging Baseline. • Security logs and events are monitored and alerted against by the enterprise Security Information and Event Management (SIEM) solution.
	Security Monitoring: Network	• All traffic leaving the environment is monitored. • Network Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) are installed between network zones. • Enable DNS filtering services to block malicious domains.
	Vulnerability Management: Vulnerability Scanning	• Workloads are continuously scanned for vulnerabilities. • Removable media and devices are scanned for vulnerabilities before connecting them to the on-premises networks and systems.
	Vulnerability Management: Patching	• Security vulnerabilities of Operating System and applications are patched as per the University's Vulnerability Management Standard. • Use a centralised and managed approach to patch or update applications, operating systems and drivers. • Where possible, automated mechanisms are implemented to validate and ensure the integrity of applied patches or updates.
	Vulnerability Management: Penetration Testing	• Perform penetration testing at the initial release and against major changes.
Respond	Cyber Incident Response	• Implement relevant controls to support the incident response and digital forensics process as per the Cyber Incident Response Runbooks. • Cyber Incident Response Runbooks are updated with specific scenarios and these runbooks are tested regularly. • Where possible, automated mechanisms are 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 as part of the University's Big Red Button (BRB) initiative. • High Availability (HA) is implemented according to the enterprise's BCP/DRP requirements.

Security Standard For On-Premises Storage Infrastructure

This section covers the minimum security controls for on-premises storage infrastructure.

Table 2. Minimum Security Requirements		
NIST CSF Function	**Controls**	**Requirements**
Govern	Refer to table 1	Refer to table 1
Identify	Refer to table 1	Refer to table 1
Protect	Identity and Access Management: Solution Administration and Privileged Access	Refer to table 1
	Identity and Access Management: Authentication	Refer to table 1
	Identity and Access Management: Authorisation	Refer to table 1
	Information Asset Protection:	Refer to table 1

	Physical Access	
	Information Asset Protection: Remote Access	• Remote access to the University's storage infrastructure is implemented using the University's approved remote access methods as per the University's Remote Access Security Standard. • Remotely connected devices are scanned prior to accessing the storage for compliance with the University's relevant policies. • When remote access to environments handling sensitive data is required, Bastion Host is used to prevent data leakage, i.e., no data can be downloaded to the end point devices. • Use public key-based authentication where possible.
	Information Asset Protection: Network Access Control	• Network access controls are implemented to restrict storage services communications to strictly defined network resources such as web servers, application servers and storage area networks. • Unused network ports, protocols, and services listening on a system are disabled by default and continuously monitored.
	Information Asset Protection: Network Isolation	• Production and non-production environments are segregated and access to development environment(s) in particular is whitelisted for specific subnets. • Administrator workstations are placed into a separate network zone to other workstations. • Only authorised protocols and service are allowed to cross the network boundaries.
	Information Asset Protection: Removable Media	• Prevent unauthorised media from connecting to systems and/or networks via the use of device access control software, disabling connection ports, or by physical means. • When it is approved by a business need, removable media containing information is encrypted in accordance with the University's University's Cryptography Baseline. • Disable any automatic execution features for removable media.

		• Removable media is stored in a secure manner when not in use. • Labels and markings indicating the classification, owner, system, network, or any other marking that can associate media with its original use, are removed prior to disposal, as per the University's Information Classification and Handling Standard.
	Information Asset Protection: Firewalls	Refer to table 1
	Information Asset Protection: Malware Prevention	• Enable a centralised malware protection software on workstations and servers using the University approved solution. • Anti-malware software and signatures are updated regularly. • Malware scans are automated when removable media is connected.
	Configuration Management: Secure Configuration	Refer to table 1
	Information Asset Protection: Data Lifecycle Management	• Perform regular backup test and restore procedures. • Backups are encrypted and stored in a secure manner. • Encryption keys used to perform the backup encryption process are stored in a secure manner. • Data/information processed in the cloud workloads is classified as per the University's Information Classification and Handling Standard so that relevant security controls like Data Loss Prevention (DLP) can be applied to protect the confidentiality of sensitive information. • Implement DLP capabilities considering data classification as per the University's Information Classification and Handling Standard.

	Data Protection: Encryption	• When data is stored in the environment, encryption at-rest is implemented. • Encrypt storage workloads, servers and devices. • Encryption algorithms, crypto-ciphers, protocols, and certificates usage must comply with the University's Cryptography Baseline.
	Data Protection: Secrets Management	• Use a centralised key and/or secrets management solution to manage keys, secrets and certificates. • Do not store credentials and other secrets anywhere in the storage infrastructure.
Detect	Refer to table 1	Refer to table 1
Respond	Refer to table 1	Refer to table 1
Recover	Refer to table 1	Refer to table 1

Security Standard For On-Premises Compute Infrastructure

This section covers the minimum security controls for on-premises compute infrastructure.

Table 3. Minimum Security Requirements		
NIST CSF Function	**Controls**	**Requirements**
Govern	Refer to table 1	Refer to table 1
Identify	Refer to table 1	Refer to table 1
Protect	Identity and Access Management: Solution Administration and Privileged Access	Refer to table 1
	Identity and Access Management: Authentication	Refer to table 1
	Identity and Access Management: Authorisation	Refer to table 1
	Information Asset Protection:	Refer to table 1

	Physical Access	
	Information Asset Protection: Remote Access	• Remote access to the University's compute infrastructure is implemented using the University's approved remote access methods, as per the University's Remote Access Security Standard. • Remotely connected devices are scanned prior to accessing workstations and servers for compliance with the University's relevant policies where possible. • When remote access to environments handling sensitive data is required, Bastion Host is used to prevent data leakage, i.e., no data can be downloaded to the end point devices. • Use public key-based authentication where possible.
	Information Asset Protection: Endpoint Protection	• Use an enterprise-approved, security-hardened, Standard Operating Environments (SOE) for all workstations and servers. • Harden all administrative infrastructure including, but not limited to, administrator workstations and jump servers. • Implement application whitelisting, including runtime control and local admin access control, on workstations and servers. • Plans for local admin rights and Just-In-Time (JIT) access are considered where appropriate. • Remove unapproved software and applications from all workstations and servers. • Deploy host-based firewalls and/or port-filtering tools to all workstations and servers. • Deploy the university approved anti-virus solutions to all workstations and servers.
	Information Asset Protection: Email and Web Applications	• A list of allowed content types are implemented to control the data that can be sent to the infrastructure. • All encrypted content, traffic and data are decrypted and inspected to allow content filtering before it is delivered to the infrastructure domain.

		• The integrity of content is verified where applicable and blocked if verification fails. For example, firmware updates. • For remote access using jump boxes, only authorised browser or email client plugins or add-ons are installed. This includes blocking the execution of scripts on browsers and email clients. • Should email service be required by an infrastructure component, use Monash approved email relays/service. • Implement controls to prevent the configuration of non Monash email service. • Install and enable URL filtration controls that leverage URL-categorisation services in a whitelisting approach.
	Information Asset Protection: Network Isolation	• Divide networks into multiple functional network zones according to the sensitivity or criticality of information or services. • Production and non-production environments are segregated and access to development environment(s) in particular should be whitelisted for specific subnets. • Administrator workstations are placed into a separate network zone to other workstations. • Only authorised protocols and service are allowed to cross the network boundaries.
	Information Asset Protection: Network Access Control	Refer to table 2
	Information Asset Protection: Removable Media	Refer to table 2
	Information Asset	• Implement micro-segmentation where possible.

	Protection: Firewalls	• Where there are internet-facing web applications hosted in the environment, the University's standard Web Application Firewall (WAF) solution is deployed to prevent application attacks.
	Information Asset Protection: DDoS Protection	• Implement DDoS protection controls for an environment accessible from the internet.
	Information Asset Protection: Malware Prevention	• Enable a centralised malware protection software on workstations and servers using the University's approved solution. • Anti-malware software and signatures are updated regularly. • Malware scans are automated when removable media is connected. • Malware scans are deployed and automated for inbound emails.
	Configuration Management: Secure Configuration	Refer to table 1
	Information Asset Protection: Data Lifecycle Management	Refer to table 2
	Data Protection: Encryption	• When data is stored in the environment, encryption at-rest is implemented. • When data is in transit within or between workloads, encryption in-transit is implemented. • Encrypt compute workloads and servers.

		• Encryption algorithms, crypto-ciphers, protocols, and certificates usage must comply with the University's Cryptography Baseline.
	Data Protection: Secrets Management	Refer to table 1
Detect	Refer to table 1	Refer to table 1
Respond	Refer to table 1	Refer to table 1
Recover	Refer to table 1	Refer to table 1

Version and Update History

Version	Date	Author	Summary of Change
0.1 Draft	9 Nov 2021	Stanley Wijoyo	Initial Draft
0.9 Draft	9 Nov 2021	Simsam Hijjawi	Peer Review
1.0	12 Nov 2021	Dan Maslin	Initial Release
1.1 Draft	02 Dec 2024	Thushara Jaywardhena/Gautm Pal	2024 Annual Review/Peer Review
1.1	04 Dec 2024		V 1.1 Release Approved by Ashok Khatiwada