CLOUD SECURITY STANDARD

Introduction

Purpose

The purpose of this document is to guide project and operation teams within Monash Group to align with the requirements of the Cyber Risk and Resilience team regarding Cloud Security. It outlines the Cybersecurity team's recommendations in order to ensure cybersecurity risks are minimised 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, and associates who use the University's Information Technology (IT) Cloud environments, and 3rd parties who provide cloud services to Monash University and they have access to Monash data.

For this standard, references to 'the University' include the activities of Monash University Australia and all entities connected with this University, unless otherwise indicated. In the scope of this document, the following will be addressed:

- Minimum security practices and controls in a cloud-hosted system, including but not limited to:
    - Infrastructure-as-a-Service (IaaS)
    - Platform-as-a-service (PaaS)
    - Software-as-a-service (SaaS)
- Private cloud environments:
    - Monash Private Cloud and Secure Data Enclave
    - MeRC where applicable

Out of Scope

Out of the scope of this document:

- Relevant management and operation models
- Detailed security requirements
- Step-by-step implementation guides

RACI Matrix

Document key audience: CyberSecurity team, Application Owners, Infrastructure teams

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

Security Architecture Principles

Cyber Security Architecture Principles should be considered in order to protect Monash University's cloud environments and their integrated systems.

Security Standard For Cloud Environments

This section covers the minimum-security controls for vendor agnostic cloud environments.

Table 1. Minimum Security Requirements		
NIST CSF Function	**Controls**	**Requirements**
Identify	Governance, Risk and Compliance	• Reference risk management policy and procedures are in place and being complied with. Upon a related change and review, 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. • Environment ownership and shared responsibilities between external vendors, application teams, cloud infrastructure teams 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	• Compliance of all assets residing in the cloud environment are maintained as per the University's Asset Management Standard. • Maintain an inventory of approved software and cloud resources/services, including Software-as-a-Service (SaaS) solutions and perform a regular review as detailed in the relevant baseline document. • Where applicable, deploy an automated asset discovery solution in the public cloud environment. • Maintain an up-to-date list of used assets and service consumers for private cloud service offerings in the University. • Tag or label assets with protective markings reflecting their sensitivity or classification as per the University's Information Classification and Handling Standard.

	Security Awareness and Training	• DevOps and relevant support teams are security-aware and trained where relevant.
Protect	Identity and Access Management: Authentication	• Enforce Multi-Factor Authentication (MFA) for all users before access is granted, via the University's approved user Identity Management service. • Privileged access is implemented using a dedicated account for elevated activities, is only used for administrative purposes, and is unique and identifiable to a user/process. • Local accounts are used only when centralised access is disabled as a (break-glass) account. • Shared accounts are avoided and formally approved for a temporary use when justified by a valid business need. • Third party access is managed in line with the requirements in this section and the University's Remote Access Security Standard. • Infrastructure system integration (Machine-to-Machine) is authenticated, using one of the university's approved authentication methods as per the relevant security baseline.
	Identity and Access Management: Authorisation	• Maintain the principle of least-privilege and need-to-know when accessing cloud resources and/or services. • By default, disable public access to cloud resources unless a validated business need is requiring this access. • 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 plan is required. This includes, but not limited to access grant, change, revocation, and access review(s).
	Information Asset Protection: Endpoint Protection	• Implement application allowlisting mechanisms on all relevant cloud resources. • An enterprise-approved, security-hardened, Standard Operating Environment (SOE) is used for all applicable cloud resources. • All administrative infrastructure including, but not limited to, administrator workstations and jump servers, are hardened. • Remove unapproved resources and applications from the cloud environment with reference to the relevant baseline document.
	Information Asset Protection: Data Lifecycle Management	• Data stored in the system, as well as configuration items and secrets, are backed up on a regular basis and in an automatic manner where possible. • Backups are encrypted and immutable. • Perform backup test and restore procedures on a regular basis. • 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.
	Information Asset Protection: Network Isolation	• Maintain network segmentation for network infrastructure within cloud environments, inter-cloud networking and hybrid cloud setups. • Production and non-production environments are segregated and access to development environment(s) is allowlisted for specific subnets.
	Information Asset	• Deploy Monash Cybersecurity approved and managed network firewalls to inspect both inbound and outbound network traffic, and prevent network layer security attacks.

	Protection: Firewalls	• Deploy the University's standard Web Application Firewall (WAF) solution for Sensitive workloads to prevent application attacks. If this is not feasible, the cloud provider's WAF could be used as an alternative solution in consultation with Monash Cybersecurity.
	Information Asset Protection: DDoS Protection	• Implement DDoS protection controls for an environment accessible from the internet.
	Information Asset Protection: API Connection	• Use an API based integration where possible. • Use the University's standard integration platform, MiX, to manage API calls between the University's workloads on-premises and in the cloud. • If integration with an external vendor is required, a third-party "risk assessment" and "controls assessment" is conducted.
	Information Asset Protection: Malware Prevention	• Malware protection software is centrally managed and enabled on computing instances using the university-approved solution. • Maintain and update the scanning engine and signature database regularly. • If a university-approved malware protection is not present on a computing instance, the Cyber Security team must be contacted to facilitate its installation immediately.
	Configuration Management: Secure Configuration	• Establish and maintain secure configurations for all assets in the cloud. • Align cloud workload configuration with the University's secure configuration baselines where possible. • Third party provided images or server templates or any other configuration item, are reviewed and securely hardened prior to being used.
	Data Protection:	• When data is stored in the cloud environment, encryption at-rest should be implemented.

	Encryption	• When data is in transit within or between cloud workloads, encryption in-transit is implemented. • Encryption algorithms, crypto-ciphers, protocols, and certificates usage must comply with the University's Cryptography Baseline.
	Data Protection: Key and Secrets Management	• Use a centralised key and secret management solution to manage keys and secrets. • Do not store or hard-code credentials and other secrets in an accessible configuration or code.
Detect	Security Monitoring: Logging and Alerting / Incident Response Planning	• Generate logs and events as required by the University's Security Logging Baseline for systems, applications and other workloads in the cloud. • Collected and correlated security logs and events are used to perform threat hunting, cyber incident response and digital forensics activities. • Security logs and events are monitored and alerts are managed by the enterprise Security Information and Event Management (SIEM) solution. • Teams must engage the SIEM Data Operations team to coordinate log ingestion and define detection rules in SIEM, based on business and security requirements.
	Vulnerability Management: Vulnerability Scanning	• Cloud workloads and services are continuously scanned for vulnerabilities using the University's approved solutions. • Security vulnerabilities are detected, triaged and patched as per the University's Vulnerability Management Standard.
	Vulnerability Management: Patching	• A centralised and managed approach following the University's patch management and cloud providers' best practices are used to patch or update relevant cloud resources. • 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 should be done with reference to the University's Vulnerability Management Standard
Respond	Cyber Incident Response	• Relevant controls to support the incident response and digital forensics process are implemented as per the Cyber Incident Response Runbooks. • Cyber Incident Response Runbooks are updated with cloud specific scenarios where possible, and these runbooks are tested regularly. • Where possible, implement automated mechanisms 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. • High Availability (HA) is implemented according to the enterprise's BCP/DRP requirements.