SECRET MANAGEMENT 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 Secret Management and its hosting environment. 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 in line with the existing MU 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

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

- Minimum security practices and controls for management of secrets in a cloud-hosted system.
- Minimum security practices and controls for management of secrets for systems hosted on-premises in MU.
- Security requirements for managing secrets for users accessing sensitive and very sensitive information and/or operating in the critical applications space.
- The hosting environment of the secret management solution or system.
- All secret types, including but not limited to passwords, keys, tokens and certificates.
- At the discretion of Monash University, from time to time identified teams or individuals will be required to use an approved password management tool as directed by eSolutions. The use of this tool will depend on the user's access to organisational data and systems.

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

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 environments and their integrated systems.

Security Standard For Secret Management

This section covers the minimum security controls for secret management in both cloud and on-premises 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 changeor review, system owners should consult this standard and its related baselines. Should the use cases not be covered, they should commence a risk assessment as per the MU risk management manual. • Applicable legal and regulatory requirements are formally identified based on the information classification. • Secrets and secret management solutions ownership and responsibilities should be identified, including a RACI matrix. • Should an internal or external audit be required, system owners should maintain the required audit artefacts, including but not limited to configuration snapshots, logs and process documents. • A complete risk assessment should be performed where a third-party secret management solution is used instead of the MU approved solution(s).
	Asset Management	• Reference asset management policy and procedures are in place and being complied with as per the MU Asset Management Standard. • The secret management solution(s) should maintain a status of inventory of secrets, owners, applications and systems that use the secrets. • The status of the secrets should be reviewed regularly.

		• All aspects of a secret's life cycle i.e. creation, rotation, expiration, etc. should be managed within the secret management solution(s). • Where applicable, an automated asset discovery solution should be deployed in the hosting environment of the secret management solution.
Protect	Identity and Access Management: Authentication	• Users should be authenticated before access is granted. • Strong authentication (MU Managed MFA solution) should be enforced for all users and/or systems accessing the secret management solution and its hosting environment. • 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. • Third-party access should be managed in line with the requirements in this section and MU Remote Access Security Standard. • An emergency access should be set up for the secrets management solution and its hosting environment, limited to emergency or "break-glass" scenarios where normal administrative accounts can't be used.
	Identity and Access Management: Authorisation	• The principle of least-privilege and need-to-know should be maintained when accessing the secret management solution and its hosting environment. • Public access to secrets should be disabled by default. • Accounts, including user accounts and service accounts used to access non-production and production environments, should be separated. • Unique identities, credentials and access permissions should be centrally managed as the source of truth for authorised devices, processes and users to access systems, data and information. • A formal authorisation plan should be in place. This includes, but not limited to access grant, change, revocation, and access review.

	Information Asset Protection: Endpoint Protection	• An enterprise-approved, security-hardened, Standard Operating Environment (SOE) should be used for all applicable resources hosting and/or accessing the secret management solution. • Unapproved resources and applications should be removed from the hosting environment with reference to the relevant baseline document. • A hardened jump server should be used to perform any privileged tasks.
	Information Asset Protection: Data Lifecycle Management	• Secrets should be backed up by MU administrators/privileged users, on a regular basis and in an automatic manner where possible. • Backups should be encrypted and stored in a secure manner. • Backup test and restore procedures should be done on a regular basis. • Secrets should be classified as sensitive information as per the MU Information Classification Standard so that relevant security controls like Data Loss Prevention (DLP) can be applied to protect their confidentiality. • DLP capabilities should be implemented where possible.
	Information Asset Protection: Network Isolation	• The network infrastructure within the hosting environment should maintain sufficient network segmentation. • Production and non-production environments should be segregated and access to development environment(s) in particular should be whitelisted for specific subnets. • Secret management solution(s) should be built on a different network subnet than the application itself. • Secrets should be stored in a private network where both inbound and outbound internet access are disabled. • Where secrets exchange is required between on-premises systems and MU managed public cloud, MU private links should be used.
	Information Asset Protection:	• Malware protection software should be centrally managed and enabled in the hosting environment of the secret management solution using the university-approved solution.

	Malware Prevention	• The malware scanning engine and signature database should be reviewed and updated regularly.
	Configuration Management: Secure Configuration	• Establish and maintain secure configurations for all assets in the hosting environment of the secret management solution. • The workload configuration should align with MU Standard Operating Environment Security Standard where possible. • Secrets should not be stored or hard-coded in an accessible configuration or code where possible. • Secrets used in the non-production environments should not be used in the production environments. • Secrets used in the production environments should not be used for non-production purposes. • Secrets should be purged from memory after processing is done.
	Data Protection: Encryption	• Secrets stored in the environment should have an encryption at-rest mechanism implemented. • When data is in transit within or between workloads, encryption in-transit should be implemented. • Encryption algorithms, crypto-ciphers, protocols, and certificates usage must comply with the MU Cryptography Baseline.
	Data Protection: Secrets Management	• A MU approved, centralised secret management solution should be used to manage secrets securely. • Application/system data and secrets should be stored in separate locations. • Secrets should be dynamically generated and complex where possible, to prevent brute-force attacks. • Secrets should not be written down on a piece of paper, notes and other form physical items. • Secrets should not be stored in unapproved devices, including but not limited to personal workstations, mobile phones, tablets and removable media. • Secrets should have expiration time set. • All secrets should be rotated regularly following the relevant secrets rotation policy.

Detect	Security Monitoring: Logging and Alerting / Incident Response Planning	• The secret management solution and the hosting environment should generate security logs and events as required by MU Security Logging and Alerting Baseline. • Collected and correlated security logs and events should be used to perform threat hunting, cyber incident response and digital forensics activities. • Logs should not contain secrets and/or other sensitive information. Where possible, an automated mechanism to scan for logs which contain such information should be implemented.
	Vulnerability Management: Vulnerability Scanning	• The environment supporting the secret management solution should be continuously scanned for vulnerabilities using MU approved solutions. • Where a Continuous Integration or Continuous Deployment (CI/CD) pipeline is used, an automated scan to detect secrets or other sensitive information in accessible configuration or code should be performed. • Security vulnerabilities should be detected, triaged and patched as per the MU Vulnerability Management Standard.
	Vulnerability Management: Patching	• A centralised and managed approach following MU patch management practices should be used to patch or update the relevant resources supporting the secret management solution. • Where possible, automated mechanisms should be implemented to validate and ensure the integrity of applied patches or updates.
	Vulnerability Management: Penetration Testing	• Penetration testing should be done at the initial release and against major changes of the secret management solution and its integrations, with reference to the MU Vulnerability Management Standard.
Respond	Cyber Incident Response	• Relevant controls to support the incident response and digital forensics process should be implemented as per the Cyber Incident Response Runbooks.

		• Cyber Incident Response Runbooks should be updated with specific scenarios where possible and these runbooks should be 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) of the secret management solution(s) should be implemented according to the enterprise's BCP/DRP requirements.

Definitions

Table 5: Definitions	
Term	**Definition**
Break-glass Account	A break glass account is used to bypass normal access control procedures in the case of a critical emergency, in which a user or admin may require a higher level of access than normal, in order to address an issue.
Continuous Deployment	A software release process that uses automated testing to validate if changes to a codebase are correct and stable for immediate autonomous deployment to a production environment.
Continuous Integration	The practice of automating the integration of code changes from multiple contributors into a single software project.
Jump Server	A jump server is a system on a network used to access and manage devices in a separate security zone.
RACI Matrix	“Responsible, Accountable, Consulted, and Informed.” A RACI matrix illustrates the given task’s goals, roles, and responsibilities.
Removable Media	Any type of storage device that can be removed from a computer while the system is running. Examples: USB flash drives, external hard drives, licence dongles, CDs and DVDs.
Secrets	Digital authentication credentials, including but not limited to passwords, keys, APIs, tokens and certificates for use in systems, services, and accounts.

Version and Update History

Version	Date	Author/ Reviewer	Summary of Change
0.1 Draft	24/03/2022	Stanley Wijoyo	Initial Draft
0.9 Draft	25/03/2022	Simsam Hijjawi	Peer Review
Draft			Review
1.0			Initial Release
1.1	26/06/2025	Parminder Bhatti	Language simplification and linked URL updates
1.2	30/06/2025	Ashok Khatiwada	Approved for Release