REMOTE ACCESS SECURITY STANDARD

Introduction

Purpose

The purpose of this document is to guide various teams and system/service owners in Monash University (MU) in securing remote access to those services/systems as they are developed, deployed, offered, and/or operated by MU teams. It outlines the Cyber Risk And Resilience team's requirements and recommendations in order to make sure cyber risks that are associated with user remote access are mitigated or reduced 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.

This standard includes:

- Security Principles
- Security Control Standards

In Scope

In the scope of this document:

- Control standards and considerations for remote access
- Remote access solution(s) and their hosting environment(s)

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	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 Remote Access

This section covers the minimum-security controls for remote access solutions and the hosting environment to support them.

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, 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 system. • Applicable legal and regulatory requirements are formally identified based on the information classification. • Remote access policies and procedures should be formalised and maintained. • If a non-standard remote access method is required, a specific risk assessment should be undertaken.
Identify	Asset Management	• Reference asset management policy and procedures are in place and being complied with as per the MU Asset Management Standard.
	Security Awareness and Training	• Remote access supporting teams, students, and staff should be security-aware and trained where relevant.

	Identity and Access Management: Authentication	• Users should be authenticated before access is granted.
		• Systems should display a login banner that requires users to acknowledge and accept their security responsibilities and legal obligations before access is granted.
		• The MU or Federated Single Sign On (SSO) and Multi-Factor Authentication (MFA) solution should be used to authenticate remote access users.
		• Privileged access is implemented with a zero trust context based elevation requiring additional auth methods as the preferred option over a dedicated account.
		• Unidentifiable access and shared accounts should be avoided.
		• For the remote access hosting environment, local accounts are used only when centralised access is disabled as a break-glass account.
		• Where third-party or an external account access is required, they should only be granted for specific purposes and have a short/defined expiry time.
		• Out of Band (OOB) management access is highly recommended for privileged access with a solution following shared-nothing architecture with highest granularity of control in Identity and Access Management controls
		  • VPN-based remote access sessions for users without “Always On” connectivity shall be limited to a maximum duration of 24 hours, after which re-authentication is required, and shall be automatically terminated following 1 hour of inactivity based on user-generated traffic.
		  • Always-On VPN users shall be re-authenticated after a maximum authentication lifetime of 14 days. The VPN client shall not remain disconnected from the gateway for more than 15 minutes before re-authentication is required, and inactive sessions shall be terminated after 24 hours. **However**, VPN session persistence settings shall not

		exceed the lifetime of the corresponding IdP authentication token.
Protect	Identity and Access Management: Authorisation	• The principle of least-privilege and need-to-know should be maintained when accessing the environment, workloads and services. • User accounts used to access non-production and production environments, should be separated. • For each system/solution, a formal authorisation plan should be in place as per the MU Information Classification and Handling Standard. This includes, but not limited to access grant, change, revocation, and access review(s). • SOE-based remote access is restricted to Remote Access VPN connections and shall only be granted following the verified compliance with defined security posture controls as defined by the "STANDARD OPERATING ENVIRONMENT SECURITY STANDARD"
	Information Asset Protection: Endpoint Protection	• MU-approved, security-hardened, Standard Operating Environment (SOE) images should be used for all applicable resources involved in building and operating the remote access solution(s). • A hardened jump server should be used to perform any privileged tasks. • Unapproved resources and applications should be removed from the environment with reference to the relevant baseline document. • Any end device access, not conforming to this standard shall follow a formal exception process.
	Information Asset Protection: Mobile Devices	• When mobile devices such as laptops, tablets, and mobile phones, are used to access MU's environment, Mobile Device Management (MDM) solutions or mechanisms should be used to control this process.

	Information Asset Protection: Remote Access Solution Environment	• Devices remotely connecting to the remote access solution environment(s) should be profiled/scanned prior to accessing the environment(s) for compliance with MU relevant policies where possible. • Remote access to the remote access solution(s) environment(s) should be encrypted and authenticated inline with Application Security Baseline and Cryptographic Baseline . • The remote access solution should be centrally managed and endpoint-hosted solutions should be avoided.
	Information Asset Protection: Data Lifecycle Management	• The remote access solution(s) environment(s) data, configuration and secrets should be backed up 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.
	Information Asset Protection: Network Isolation	• Network infrastructure within the remote access solution(s) environment(s) should maintain sufficient network segmentation. • Remote access to production and non-production environments should be segregated and access to development environment(s) in particular should be allowlisted for specific subnets. • Where a jump server is used for remote access, it should reside in a private subnet where both inbound and outbound internet access are disabled/controlled. • Where applicable, full tunnelling should be enforced and split tunnelling should be disabled to ensure remote access flows are inspected by MU controls.

	Information Asset Protection: Firewalls	• Network firewalls should be deployed to prevent network-level security attacks and facilitate network segmentation. • Relevant Network Firewall policies shall be application-aware and identity-aware. It shall control the access to the level of granularity of the identity and application. • Where applicable, Web Application Firewall (WAF) capabilities should be deployed to prevent application-related attacks. • Domain Name System (DNS) filtering services should be enabled to block malicious domains and mitigate DNS related risks.
	Information Asset Protection: DDoS Protection	• Where applicable, Distributed Denial of Service (DDoS) protection controls should be implemented to secure the remote access solution(s) environment(s).
	Information Asset Protection: Malware Prevention	• The remote access solution(s) environment(s) should be scanned by the MU malware protection solution.
	Configuration Management: Secure Configuration	• Establish and maintain secure configurations for all assets in the remote access solution(s) environment(s). • The remote access solution(s) environment(s) configuration should align with the industry security configuration best practices. • While the remote access solution(s) environment(s) is being built, third party provided images or server templates or any other configuration item, should be reviewed and securely hardened prior to being used.

	Data Protection: Encryption	• When data is stored in the remote access solution(s) environment(s), encryption at-rest should be implemented. • When data is in transit within or between networks, data encryption in-transit should be implemented. • Encryption algorithms, crypto-ciphers, protocols, and certificates usage must comply with the MU Cryptography Standard.
	Data Protection: Key and Secrets Management	• A centralised key and secret management solution should be used to manage keys and secrets involved in the remote access process. • Credentials and other secrets should not be stored or hard-coded in an accessible configuration or code.
Detect	Security Monitoring: Logging and Alerting	• Systems, applications and other workloads in the remote access solution(s) environment(s) should generate 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. • Where possible, security logs and events should be monitored and alerted against by the MU approved SIEM solution.
	Security Monitoring: Network	• All traffic leaving the environment should be monitored. • Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) should be installed between zones and hosts where applicable. • At minimum, all privileged access user sessions shall be screen recorded with all Input and Output actions on intermediary points between user end device and the target system.
	Vulnerability Management:	• Workloads and services should be continuously scanned for vulnerabilities using MU approved solutions.

	Vulnerability Scanning	Security vulnerabilities should be detected, triaged and patched as per the MU Vulnerability Management and Standard.
	Vulnerability Management: Patching	• A centralised and managed approach following MU patch management procedures should be used to patch or update the remote access environment(s) solution(s). • Where possible, automated mechanisms should be implemented to validate and ensure the integrity of applied patches or updates. • Where possible, the connecting parties should have an accepted level of security patching that is aligned to MU patch management procedures.
	Vulnerability Management: Penetration Testing	• Penetration testing should be done at the initial release of new remote access mechanisms, regularly where possible and when major changes are introduced on those mechanisms, 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, automated mechanisms should be implemented to support the cyber security incident response plan.
Recover	Business Continuity and Disaster Recovery: Resiliency	• Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) covering the resilience of the remote access solution(s) are developed and tested regularly. • High Availability (HA) should be implemented according to the enterprise's BCP/DRP requirements.


Cyber Risk and
Resilience

Definitions

Table 2: 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.
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.

Version and Update History

Version	Date	Author/ Reviewer	Summary of Change
0.1 Draft	11/02/2022	Stanley Wijoyo	Initial Draft
0.9 Draft	16/02/2022	Ashley Niklaus/ Simsam Hijjawi	Peer Review
Draft			Review
1.0			Initial Release
1.1 Draft	02/12/2024	Ashok Khatiwada/Thushara Jayawardhena/Gautam Pal	Annual Review
1.1	04/12/2024		V 1.1 Release Approved by Ashok Khatiwada
1.2 Draft	17/04/2026	Thushara Jayawardhena/ Abi Vijayaraghavan	Annual Review/Peer Review
1.2 Draft	30/06/2026	Raj Udayanga	V 1.2 Stakeholder Review
1.2	30/06/2026	Ashok Khatiwada	V 1.2 Release Approved by Ashok Khatiwada