Minimum Cybersecurity Standard (MCS)

Introduction

Purpose

Considering security at the design phase is more effective and cost-saving than at a later phase of the change management process. The purpose of this document is to guide projects and operations teams as well as service designers to bake cybersecurity into their design. It points to the minimum required cybersecurity controls that should be considered early in the concept design phase. If any of the requirements listed in this document are not achievable, compensating controls should be discussed and endorsed with the cyber architecture team (cyberteam-architecture-l@monash.edu).

Please refer to Monash University's (MU) Cybersecurity Standards for specific security requirements (e.g., password policy and approved encryption algorithms).

In Scope

In the scope of this document:

- Minimum security practices and controls that a system or application design should consider
- Complete technology stack where possible (Infrastructure and applications)

Out of Scope

Out of the scope of this document:

- 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

Security Principles

Cyber Security Architecture Principles are considered to guide the security by design process.

Minimum Security Requirements

Cybersecurity Governance, Risk and Compliance (GRC)

NIST CSF Function	Table 1: GRC Minimum Security Requirements
Identify	• Both a project and an operational RACI matrix should be formalised. • Third party assurance actions should be taken when new services/solutions/components are considered and onboarded

Asset Management

Asset management describes the approach taken to governance, and the implementation of asset management practices as part of the design phase.

NIST CSF Function	Table 2: Asset Management Minimum Security Requirements

Identify	• Information asset details and their status that are involved in the change should be formally documented and approved in the format of an asset register. This includes, but is not limited to, hardware, software, and data flows.
	• Where applicable, ensure an enterprise-approved tool is used to continuously discover and update the solution's asset register.
	• End of Sale (EoL) and End of Support (EoS) components should be retired and/or upgraded/replaced with supported components, this includes but is not limited to, hardware, software, and firmware components.
	• The replacement, retirement, or upgrade of these components must be planned as soon as it is identified and must be done in the nearest change cycle where possible.
	• Should the need for the EoL/EoS component be justified by a strong business case, these components can remain in the environment or on boarded for the first time, given:
	  ○ It isn't connected to the external, untrusted environments, for example, the Internet, STS VPN with uncontrolled MU entities
	  ○ It is fully segregated with OSI Layer-3 and above protection
	  ○ It is continuously monitored against a security baseline where anomalies can be identified
	  ○ These components access internal resources on an on-demand, whitelisted, and need-to-know basis

Vulnerability Management

Embedding vulnerability management practices in the operational model of the system/application is important to streamline the operational aspects of the system/application.

NIST CSF Function	Table 3: Vulnerability Management Minimum Security Requirements
Detect	• If workloads are not built based on MU Standard Operating Environment (SOE) images, ensure Operating Systems', middleware/runtimes, and applications' security patching is formalised. • If not part of the MU network range and if hosted in a cloud service provider environment, ensure the IP address ranges hosting the new system are reported to the Cyber Risk and Resilience team to be covered by the vulnerability scanning solution, where applicable. • Penetration testing should be discussed at the earliest possible stage of the change to facilitate its planning and execution. • The adoption/development of an ongoing assurance program covering the above three vulnerability management aspects should be discussed with the Cyber Risk and Resilience team.

Identity and Access Management

Properly designed and implemented Identity and Access Management (IAM) practices are key to a secure design. They are used to verify that an individual or a service are who they claim to be. This determines what they are allowed to access, and that their activities are tracked in a controlled manner.

Authentication

NIST CSF Function	Table 4: Authentication Minimum Security Requirements
Protect	• Users should be authenticated before access to an application or data is granted. • Machine to Machine (M2M) should also be authenticated before communications between systems are established, e.g. API calls. • MU Okta is the preferred authentication solution. • If MU Okta is not feasible or the approved MU Identity's authentication frameworks are not supported, other authentication methods could be used,

	e.g., user account and password. However, this should be reviewed on a case to case basis. ● Multi-Factor Authentication (MFA) should be used to access all Monash University's applications and services that use Monash identities as usernames, any exceptions should be addressed on a case by case basis. ● Secrets involved in the authentication process should be securely managed using an enterprise approved solution such as MVault or AWS Secret Manager. ● Compliance with User Access Control Standard is required.

Authorisation

NIST CSF Function	Table 5: Access Control Minimum Security Requirements
Protect	● Define roles and permissions based on business requirements. ● Verify whether a person or service has permissions to access particular resources. ● Access control or user authorisation should be managed at the application or platform level instead of SSO or authentication level. ● A user access review procedure should be in place in line with User Access Control Standard.

Session Management

A web session is a sequence of HTTP request and response transactions associated with the specific user or process/machine/system. An application uses sessions to manage user access once a user has authenticated and authorised. Session Management can apply to Machine-to-Machine integrations depending on the implementation.

NIST CSF Function	Table 6: Session Management Minimum Security Requirements
Protect	● Define session timeout based on the criticality of an application or system. Critical applications normally use shorter session lifetime than less critical applications.

	• Securely handle session identifiers, including when storing and transferring these identifiers. • Verify session identifiers before granting access to required resources i.e. as an authorisation factor. • Delete session identifiers once a session has expired.

Configuration Management

The way in which an application's or system's configuration is to be securely managed, once the change has been implemented, is an important factor to consider at the design phase.

NIST CSF Function	Table 7: Configuration Management Minimum Security Requirements
Protect	• The configuration involved in the change should be identified and protected using an enterprise-approved tool/solution, e.g. Puppet or Ansible.
Detect	• Where possible, configuration integrity checks should be implemented.

Security Monitoring

The generation, collection and analysis of system and application events and logs are key to facilitating the implementation of the Cyber Incident Response Plan (IRP), and any potential digital forensics activities.

NIST CSF Function	Table 8: Security Logging Minimum Requirements
Detect	• Local logging is enabled on appropriate sources. System logs should contain detailed information such as event source, data, user, timestamp, etc., and should be stored locally without impacting the system's performance. • Locally stored logs should have a retention period to ensure the logs have already been exported to the enterprise SIEM solution i.e. Splunk where possible.

	• At the design stage, ensure to liaise with the Splunk team to agree on the accepted log and event formats and how the logs are going to be ingested and parsed for operational and/or security use cases. • Logs generated by the locally implemented security controls, e.g. Access Control Lists (ACL), Host-Based Firewalls (HBF), and Web Application Firewalls (WAF), should be collected and shipped to Splunk where feasible. • Monitoring and alerting dashboards should be built, preferably within Splunk where possible. • All change logs related to the other categories in this document should be considered.

Information Asset Protection

Information asset protection describes an organisation's internal body of knowledge. It is considered to be of vital importance, and compliance within this section is vital to a successful implementation of the security by design principle.

NIST CSF Function	Table 9: Information Asset Protection Minimum Security Requirements
Protect	• Ensure the data classification of the data and/or information involved in the change are known as per MU Data Classification Standard.

Endpoint Protection

An endpoint is any physical or virtual device that is connected to MU's network, for example, laptops, servers, and mobile phones. Security API endpoints are planned to be covered in the subsequent releases.

NIST CSF Function	Table 10: Endpoint Protection Minimum Security Requirements
Protect	• By liaising with the relevant team, e.g. Technical Services (TS), ensure the latest versions of any security-related updates/patches are applied.

	• In the event of EoL/EoS being used, TS should be consulted and an operational plan should be formalised. • Ensure the enterprise-approved malware protection software installed on endpoints. If not feasible, a different malware protection solution can be used subject to a standalone review. • Application whitelisting should be employed on servers and workstations as appropriate, and where possible. • Locally deployed security controls such as Host-Based Firewalls (HPF) should be configured with non-permissive rules following a whitelisting approach i.e. default deny rule that drops all traffic, except for that which is explicitly allowed.
Identify	• By liaising with the right team, e.g. TS, ensure that malware protection scans are automated and centrally managed where possible.

Data Lifecycle Management Protection

Describes the flow of business data and the importance of securing this data.

NIST CSF Function	**Table 11: Data Lifecycle Minimum Security Requirements**
Protect	• Ensure the data and/or information involved in the change is encrypted whilst in transit and at rest, utilising the MU approved encryption algorithms. • Data and/or information should remain in approved environments i.e. on-premises and/or cloud service providers.
Recover	• System data, as well as systems's configuration, should be backed up on a regular basis in an automatic manner where possible. Backup restore process must be formal and tested, and an offline backup should be maintained where applicable.

Mobile and Mobile Storage Protection

Describes the controls around the use of mobile/removable storage devices, and how these can be restricted or protected.

NIST CSF Function	Table 12: Mobile and Mobile Storage Minimum Security Requirements
Protect	• Where applicable, formally approved tools should be used to control data on mobile devices. • Where applicable, removable storage devices should utilise encryption at rest principles.

Email and Web Application Protection

Details the security concerning websites, web applications, email services, and web services such as APIs.

NIST CSF Function	Table 13: Email and Web Application Minimum Security Requirements
Protect	• Web Application Firewalls (WAF) should be implemented to protect web applications. • Approved email relays should only be used • Only authorised browsers and/or email client plugins should be installed. • Script execution must be controlled within all browsers and clients.

Network and Internet Protection

Describes the security around network and internet connections.

NIST CSF Function	Table 14: Network and Internet Minimum Security Requirements
Protect	• System and application designers should consider the segmentation of the underlying network where applicable. • Where the above is not applicable e.g. teams managing their own workloads in a given AWS account, network segmentation is required to segregate the public and private workloads. • Monash Private Cloud (MPC) is the default hosting platform. Exceptions should be addressed on a case by case basis.

	• If MPC hosting is not applicable, Internet protection controls such as NG Firewalls and WAFs should be considered. • Uncontrolled, direct Internet connection to MU environment e.g. any application tier or system components, should not be implemented. Genuine business cases can be considered for such implementation in a case by case approach.

Open Source Security

Open source software is widespread and inherently customisable, and often utilised within the university sector. This section describes the security around the use of open source software.

NIST CSF Function	Table 15: Open Source Software Minimum Security Requirements
Protect	• When open source components are utilised, continuous vulnerability scanning is required, where possible. • Formal plan to fail over to a supported solution should be considered in the event of the technical and security support of a given open source software being discontinued.

Secure Software Development Lifecycle (SDLC)

SLDC describes a framework for the entire software lifecycle, from inception to decommission. This section details the security around the entire software lifecycle.

NIST CSF Function	Table 16: Software Development Lifecycle Minimum Security Requirements
Protect	• Ensure MU SDLC guidelines are followed. • Ensure Application Design Checklist is checked.

Business Continuity and Disaster Recovery Plans

Both these plans serve to describe a set of policies, tools and procedures, in order to enable the continuity of business as usual, and/or the recovery from a disastrous security event.

NIST CSF Function	Table 17: Disaster Recovery Minimum Security Requirements
Recover	• Where applicable and in accordance with MU Disaster Recovery and Business Continuity Plans (BCP/DRP), the availability requirements of the new application and/or service should be documented. • Where relevant, BCP/DRP procedures are tested for the new application/system to confirm the system's resiliency as per the above document.

Version	Date	Author	Summary of Change
0.1 Draft		Simsam Hijjawi	Initial Draft
0.1 Draft		Ash Niklaus Liou Liu Dom Catacutan	Peer Reviewed
1.0		Ed Messina Dan Maslin	Initial Release
2.0	21-Nov-2022	Simsam Hijjawi	Asset management and vulnerability management new controls
2.0	22-Nov-2022	Ed Messina	Release review