



Vulnerability Management Standard

IT Security

Introduction

This standard provides the foundation for vulnerability management at Melbourne Archdiocese Catholic Schools (MACS). It sets the standard for secure and effective management of identified vulnerabilities through the implementation of appropriate authentication components and controls.

Purpose

This standard provides the foundation for vulnerability management, as it relates to cyber security management, at MACS and its schools and supports commitment to meet its business needs and statutory, legal, audit and moral obligations. This standard forms part of a suite of documents that explain MACS' approach to information governance and cyber security.

Scope

This standard applies to all ICT within MACS, including that used by MACS employees, contractors, consultants, volunteers, and other users ("MACS personnel").

Principles

It is the responsibility of all MACS personnel to work together to protect and secure the information held by MACS, which includes the personal information from our staff and the community, and internal corporate information.

- Our staff are educated on the responsible use of technology, the importance of digital wellbeing, how to engage with technology respectfully and protect ourselves and each other.
- We will be a system where we are supported by digital solutions that are safe, uphold confidentiality, and where sensitive information is protected against unauthorised access; we aim to uphold confidentiality, integrity, and availability.

MACS Schools

For MACS schools, please refer to the Target State Design Principles and Target State Design – Blueprint which was developed for the MACS School Environment as the minimum compliance requirement.

Once the Target State has been achieved for the School, the Security Standard Statements should be considered for implementation as they provide a comprehensive overview of what MACS expects at a foundational level of security for this area. There will be other Standards for other areas. Each school should estimate the level of effort, impact, the importance of change, and associated risks with adhering and/or not adhering to the Standard, as it relates to the School's risk profile and tolerance.

Standard statements

1.1 Vulnerability Management

- The MACS IT Systems must be regularly scanned for vulnerabilities. A vulnerability scanner with an up-to-date vulnerability database should be used.
- Vulnerabilities should be identified through additional activities including, but not limited to, penetration testing, security assessments, threat intelligence, vendor intelligence, performance of threat hunting activities and other sources (as appropriate).
- A best practice / industry standard should be used to ensure that scans are performed regularly and patches, updates or other mitigations for any identified vulnerabilities are applied in a timely manner, e.g. *ACSC Essential Eight Maturity Model (Levels One, Two or Three)*.
- All vulnerabilities must be assigned a priority rating and recorded in a centralised system for Vulnerability Management.
- Technical vulnerability assessments must be performed at least on an annual basis. The procedures for these assessments should follow a defined methodology, with identified roles and responsibilities.
- Any findings from technical vulnerability assessments must be recorded, analysed and managed through to remediation or risk acceptance, in accordance with the *Cybersecurity Risk Management Process*.

1.2 Patch Management

- Patch deployment must be in accordance with the required timelines according to risk levels to address identified vulnerabilities and reduce security risks. This should be performed to ensure all operating systems and applications are in vendor support.
- Patches should follow a defined, documented patch management process. This must:
 - include details of how patch levels are monitored for MACS IT systems;
 - include details of how patches are identified and obtained from authorised and trusted sources;
 - include a process of testing patches before implementation. This should be against defined criteria;
 - include methods for managing a situation where a patch has failed. This should include roll-back processes.
- An exception process, if a patch must be delayed, or cannot be implemented. This should follow a process that documents the justification and be performed in conjunction with the IT Security Risk Management Process.
- As part of the Architecture Review Team reviews, it should be determined if any systems being introduced or enhanced adhere to the Vulnerability Management requirements for MACS office.

1.3 Threat Intelligence

- Threat intelligence should be created and/or used to cover the need to collect threat-related information from different internal and external sources, analyse threat-related information to produce threat intelligence and for sharing such information with internal and external stakeholders and parties in a consistent and timely manner.
- Threat intelligence should include details about the source, type of threat, attributes associated with the threat and the methods and techniques being used.

Procedures and Guidelines

Procedures used to put this standard into action are stored within the MACS Cyber Security Procedure repository. These procedures are currently being developed and will be published once approved.

Roles and reporting responsibilities

Role	Responsibility	Reporting requirement (if applicable)
Person accountable for IT in each MACS school	Inform MACS of breach of standard	
General Manager, IT Security, Risk and Audit	Review breach of standard	Report to regulatory body if required

Definitions

Crown Jewels

IT assets that have high confidentiality, integrity and availability requirements due to being critical for core business processes or for child safety assurance.

Data

A subset of information in an electronic format that allows it to be retrieved or transmitted.

Framework

A board-approved overarching governance structure to enable compliance by MACS and its subsidiaries and MACS schools services with a range of regulatory requirements, and to ensure good governance in the operations of MACS and its subsidiaries and MACS schools services.

Guidelines

Recommendations and guidance to support the implementation of a policy or procedure. Guidelines are not mandatory and may be developed and approved by a MACS executive, or the principal / service director in a MACS school.

Melbourne Catholic Archdiocese Schools Ltd (MACS)

MACS is a reference to Melbourne Archdiocese Catholic Schools Ltd, and / or its subsidiaries, MACSS (as the context requires).

MACS board or board

The board of Melbourne Archdiocese Catholic Schools Ltd (MACS), being also the board of Melbourne Archdiocese Catholic Specialist Schools Ltd (MACSS) in an ex officio capacity (as the context requires).

MACS executive

A member of the executive leadership team (ELT) of MACS or the ELT as a group.

MACS office

Staff employed in MACS offices at James Goold House, Catholic Leadership Centre and MACS regional offices.

MACS school or school

A school which operates with the consent of the Catholic Archbishop of Melbourne and is owned, operated and governed by MACS, directly or through MACSS (as the context requires). References to schools or MACS schools also includes boarding premises of schools operated by MACS and specialist schools operated by MACSS.

Personally identifiable information

Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not. Personal information includes but is not limited to name, address, phone number, email, and date of birth.

Policy

A high-level, principles-based directive that must be complied with across MACS and MACSS.

Procedure

A step-by-step or detailed instruction for the implementation of MACS policy that is mandatory across MACS and MACSS.

Process

A process is a method of implementation of a MACS framework, policy or procedure.

Personnel

All users of information and communication technology (ICT) within MACS, including MACS employees, students, contractors, consultants, volunteers, and other users.

Risk

Risk is defined as the effect of uncertainty on objectives. An effect is a deviation from the expected – positive and/or negative. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances or knowledge) and the associated likelihood of occurrence.

Risk management

The coordinated activities to direct and control an organisation regarding risk.

Sensitive information

Sensitive information is personal information that includes information or an opinion about an individual's race or ethnic origin, religious beliefs, sexual orientation, political affiliations, criminal record, health or genetic information and some aspects of biometric information.

User

The individual operating a MACS ICT system or resource, such as a computer, mobile device, email service, or student management service.

Related policies and documents

Supporting documents

Procedures used to put this standard into action are stored within the MACS Cyber Security Procedure repository.

Related MACS policies and documents

Cyber Security Policy
ICT Acceptable Use Policy
Information and Recordkeeping Policy – MACS Office
Privacy Policy
Risk Management Policy
Emergency and Critical Incident Management Policy
Child Safety and Wellbeing Recordkeeping Policy

Legislation and standards

Criminal Code Act 1995 (Cth)
Copyright Act 1968 (Cth)

Privacy Act 1988 (Cth)
Spam Act 2003 (Cth)
Telecommunications (Interception and Access) Act 2017 (Cth)
Telecommunications Act 1997 (Cth)

Standard information

Responsible director	Director, Finance and Digital
Standard owner	General Manager, IT Security, Risk and Audit
Approving authority	General Manager, IT Security, Risk and Audit
Approval date	February 2025
Review by	General Manager, IT Security
Major review by	February 2029
Publication	CEVN

Appendix A - MACS Information Governance and Cyber Security Policy Suite

Framework <i>A board-approved overarching governance structure to enable compliance by MACS and its subsidiaries for Information Governance and Cyber Security.</i>	Governance Framework			
Policy <i>High level direction regarding Information Governance and cyber security.</i>	Cyber Security Policy	Information and Records Management Policy – MACS office	Risk Management Policy	ICT Acceptable Use Policy
Supporting security Procedures and Guidelines <i>The Recommendations and guidance to support the implementation of the Cyber Security policy.</i>	1. Security Risk and Compliance Management Procedure 2. Information Classification, Handling and Protection Procedure 3. Identity and Access Management Procedure 4. End User Security Procedure 5. MACS Vendor Management Procedure 6. Patch and Vulnerability Management Procedure 7. MACS Network Security Procedure 8. Application Security Procedure 9. Infrastructure Security Procedure 10. Cyber Security Incident Response Plan These procedures are currently being developed and will be distributed once approved.			
Additional Documentation <i>Documentation to support implementation of information security controls.</i>	Additional documentation such as security checklists and runbooks.			