Melbourne Archdiocese
Catholic Schools

Infrastructure Security Standard

IT Security

Introduction

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

Purpose

This standard provides the foundation for infrastructure 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 Cryptography

- Cryptographic solutions must be used to:
  - Protect MACS information when at rest (e.g., on portable devices, handheld devices, removable media, backup media etc.) using strong encryption algorithms based on industry standards, such as AES-256 or 3DES.
  - Protect MACS information when data is in transit out of MACS in both hardcopy and electronically transmitted formats using secure protocols based on industry standards, such as AES-256 or 3DES.
  - Protect MACS information when it is managed by third-parties or cloud computing service providers, etc.
- Where cryptographic solutions are restricted or cannot be used, mitigating controls must be identified and implemented in consultation with IT Security.
- Cryptographic requirements must be adhered to when selecting algorithms (e.g., recognised as secure and recommended by industry standards).
- Data owners must issue and enforce confidentiality agreements, including non-disclosure agreements, on Third Parties accessing sensitive information.
- Unless explicitly requested and approved, access and use of de-identified data must be allowed.

1.2 Key Management

- Secure and approved methods must be used for generating cryptographic keys. Key length must be of sufficient length to ensure security based on current best practices and standards.
- Keys must be stored in secure, encrypted environments (e.g., hardware security modules, etc.).
- If keys need to be distributed, it must be done using secure channels to only authorised users or systems receiving them, and must for a specific usage with appropriate justification and approval
- Keys must be regularly rotated
- Old and/or compromised keys must be securely retired, revoked or deactivated immediately
- The use of public key infrastructure (PKI) must include:
  - Establishment of a certificate authority (CA)
  - Creation of a registration authority (RA)
  - Procedures to operate the PKI
  - Comprehensive documentation must be maintained for cryptographic systems, including algorithms used, key management procedures, and protocol configurations
- Application communication over public or internal networks must use TLS 1.2 or higher to encrypt data in transit. This should be used for all mail servers and web servers.
- Any incidents or events related to cryptographic systems must be reported to IT Security immediately

1.3 Infrastructure Management

- Digital communications, such as email and digital information transfers, sent or received by MACS must be:
  - Monitored for accidental and deliberate information loss;
  - Be scanned for malware;
  - Be logged, in conjunction with the Logging and Monitoring Standard

- In conjunction with the requirements identified for data security in *Data Security Standard*, office systems (such as printers, photocopiers, scanners, etc.) must be:
  - Protected from misuse by being located within a physically secure environment (e.g., a user with access to confidential and sensitive data should not be processing and/or printing such information outside of the MACS office);
  - Restricted for use by only authorised users; and
  - Protected by processing information, in conjunction with the Cryptography Standard and purged/disposed/decommissioned (if applicable) upon completion or after the required retention period, in conjunction with the Asset Management Standard
- Removable media must not be used, unless there is a valid justification and has been approved by IT Security.
- Cyber health of endpoints must be checked before allowing them to access and use production resources.
- MACS must avoid single point of failure in systems and infrastructure.
- Technical solutions should be implemented to prevent the unauthorised use of removable media.
- Any third-party developed applications must include contractual requirements to notify MACS regarding any security incidents they have suffer that impact any MACS entity (office, schools).

1.4 Endpoint Management

- MACS must have an EDR solution deployed on their servers and staff devices.

1.5 Backup Management

- Data backups must be enforced and considerations to malicious attacks such as ransomware and must assess whether the backup process provides adequate business continuity.
- Backups must be scheduled according to the availability and integrity requirements of the information that is being backed up. A backup schedule must be documented and maintained for MACS' critical information systems.
- Recovery process for backups must be tested on a regular basis to validate the backups by attempting to restore the information held on the backup solution to an appropriate MACS system or IT infrastructure.
- The validation and recovery process must be provided for individuals involved in the backup and restore processes. A documented record must be maintained for such training or awareness.
- Backup media must be treated as being part of an equivalent classification level as the source information system. Sensitive data, when stored on the, must be appropriately encrypted.
- Access to backup solution must be restricted to authorised personnel, in accordance with the Identity and Access Management Standard.
- Backed up data must be retained for at least one year or in line with legislative requirements for backup information stored on the backup solution. Backups and backup media must be disposed of in accordance with appropriate disposal requirements in accordance with the *Data Security Standard* or legislative or regulatory requirements.
- Production backup media must be replicated or transported offsite regularly with appropriate physical protection, for example, on encrypted media, in a secure container, within a secure vehicle, and following an auditable and verifiable process.
- Non-production data off-siting should be based on business requirements and operational needs.
- The frequency of sending backup media off-site must be documented in the backup schedule related to the system and driven by the classification of information stored in the system.

1.6 Configuration Management

- There must be documented processes for the hardening and configuration of new MACS IT systems, including the process of establishing, testing, deploying and maintaining hardened baselines.
- A best practice / industry standard should be used to ensure that the documented processes define minimum information security control requirements that are fit-for-purpose (e.g., Centre for Internet Security (CIS) benchmarks, ACSC Essential Eight Maturity Model (Levels One, Two or Three) for Restrict Microsoft Office Macros and User Application Hardening, etc.).
- Hardening and configuration documentation must be reviewed and approved by IT Security on a periodic basis (at least annually, or when a material change has occurred).
- Hardening and configuration of MACS IT systems must include:
  - Hardening to remove unnecessary services, smart installation functionalities, utilities, accounts;
  - Changing default passwords and settings;
  - Removal of applications not required for the IT system;
  - Controlling access to removable media; and
  - Deployment of malware protection (in accordance with IT Security requirements).
- When implementing/installing an IT system, it must follow the following processes:
  - Recording the asset, in conjunction with the *Asset Management Standard*;
  - Restricting access, in conjunction with the *Identity & Access Management Standard*;
  - Scanning for vulnerabilities, in conjunction with the *Vulnerability Management Standard*
  - Patching, in conjunction with the *Vulnerability Management Standard*.
- There must be a documented process to monitor any deviations from the approved baselines. All security baseline deviations for software configuration must be monitored regularly.
- Any third-party developed applications must include contractual requirements to notify MACS regarding any security incidents they have suffer that impact any MACS entity (office, schools).

1.7 Mobile Device Management

- Only mobile devices supplied or approved by MACS are permitted to store and process MACS information and access MACS IT systems.
- MACS-issued mobile devices and personal mobile devices that access MACS information must be configured to a defined standard, using a Mobile Device Management (MDM) solution. The solution should be able to remotely disable the mobile device (if necessary), securely delete any MACS information stored on the mobile device (if necessary) and should only allow MACS-approved applications.
- MACS-issued mobile devices and personal mobile devices that access MACS information must have appropriate protections implemented around, but not limited to:
  - Access controls, in conjunction with the *Identity & Access Management Standard*;
  - Malware protection, firewall, in conjunction with the *Network Security Standard*;
  - Logging and monitoring, in conjunction with the *Detection and Incident Response Management Standard*; and
  - Patch management, in conjunction with the *Patch Management Standard*.

1.8 Internet Access

- Internet access via internet browsers must be configured, in conjunction with the Hardening Standard. Specifically, it should follow a best practice / industry standard (e.g., ACSC Essential Eight Maturity Model (Levels One, Two or Three) for User Application Hardening).
- External websites that are assessed as inappropriate or a risk must be blocked.

- Approved internet browsers must be configured to:
  - Prevent users from disabling or modifying the security settings
  - Block any installation of extensions or plug-ins, unless approved by the IT Security team after a risk assessment;
  - Automatically receive security patches in accordance with the *Vulnerability Management Standard*
  - Prevent accessing any known malicious content
  - Prevent access to external website categories that are deemed inappropriate or a risk to MACS

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 *A board-approved overarching governance structure to enable compliance by MACS and its subsidiaries for Information Governance and Cyber Security.*	**Governance Framework**			
Policy *High level direction regarding Information Governance and cyber security.*	**Cyber Security Policy**	Information and Records Management Policy – MACS office	Risk Management Policy	ICT Acceptable Use Policy
Supporting security Procedures and Guidelines *The Recommendations and guidance to support the implementation of the Cyber Security policy.*	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 *Documentation to support implementation of information security controls.*	Additional documentation such as security checklists and runbooks.			