Melbourne Archdiocese
Catholic Schools

Cyber Security Policy

Managing cyber security threats at MACS

Introduction

This policy provides the foundation for management of cyber security at Melbourne Archdiocese Catholic Schools (MACS). It sets the baseline for management and protection of MACS information, communication and technology (ICT) assets in a cyber security context.

Purpose

This policy provides the foundation for cyber security management at MACS and its schools and supports commitment to meet its business needs and statutory, legal, audit and moral obligations. This policy forms part of a suite of documents that explain MACS' approach to information governance and cyber security, referred to as the 'Cyber Security Policy' (CSP). Refer Appendix A for additional details and context.

Scope

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

Principles

It is the responsibility of all MACS Staff 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.

Policy statements

1. **Security Governance Risk and Compliance**
    - Information security threats and risks to MACS assets must be identified, assessed, appropriately responded to, and monitored through formalised and organisation wide security risk management procedures.
    - Exemptions requests must be documented, reviewed by appropriate management, and accepted by the accountable organisation manager.
    - Compliance with the Information Governance and Cyber Security policy Suite must be measured and monitored to ensure effective implementation and maintenance. MACS is responsible for conducting audits and reviews at planned intervals to assess and inform data, information, and system security.
    - MACS must comply with all applicable state, federal, and/or territory regulatory requirements. Applicable regulatory and compliance requirements related to cyber security and data protection must be identified, and processes established to ensure requirements are understood and met.
2. **Information Classification, Handling and Protection**
    - MACS IT assets and systems (for example, hardware, software and electronic data and information) must be recorded in an inventory or asset register with asset owners and data ownership clearly assigned. Inventory or asset registers must be maintained and updated as required on an ongoing basis.

- All MACS information assets must be classified, labelled (where applicable), and handled in accordance with MACS policies for information and records management and with consideration to asset sensitivity and criticality.
- A robust data backup and recovery process must be in place for all critical systems to support the integrity and availability of critical information assets.
- All MACS data at rest and in transit must be encrypted using approved cryptographic methods in accordance with the MACS Information Classification, Handling and Protection Guideline.
- All systems collecting, accessing, processing, storing, transmitting, and/or otherwise interfacing with personally identifiable information must have a data retention policy in place to ensure that data is retained only for the required period.
- Processes must be in place to securely dispose of data that is no longer required. All information must be retained in accordance with local regulatory or legislative requirements.

3. Identity and Access Management

- Access to MACS information systems and assets must be securely established and managed.
- User access requests (for example system access requests, requests to update access privileges, or requests to revoke user access rights) must be assessed and approved in accordance with defined user access management procedures.
- User access must be authenticated, authorised, terminated, and reviewed periodically. User identities (physical and digital), passwords, tokens, tags, and account privileges must be managed to ensure sound authentication, registration, segregation of duties, privileges allocation, and termination of user access where appropriate.
- Privileged access rights must be authorised according to the principle of 'least privileged' and authenticated via multi-factor authentication (i.e. smart card, soft token, or PIN). Privileged access is to be reviewed at least biannually, with immediate remediation (for example immediate access revocation) as required.

4. End User Security

- All MACS Staff that have access to MACS IT systems, assets and services including but not limited to computer, email, internet, corporate devices, must adhere to specific rules regarding the use of MACS IT systems, assets and / or services. All MACS personnel must be aware of and adhere to the control requirements defined in the "ICT Acceptable Use Policy".
- All MACS Staff must undergo security awareness training upon induction and at regular intervals.
- All MACS Staff must report any observed or suspected security incidents as per MACS Cyber Security Incident Response Plan.

5. Vendor and Third-Party Security

- Security risks associated with contracted third parties (i.e. suppliers, vendors, cloud service providers, etc.) who maintain direct or indirect access to MACS systems and data, must be operationally and contractually controlled.
- All third party services, including Cloud services must be consumed following a formalised risk assessment to identify the necessary security controls that must be implemented by the third party / Cloud Service Provider, and formally documented to manage security risks to an acceptable level. Third parties must be reviewed periodically to assess compliance to contractual cyber terms.

6. Patch and Vulnerability Management

- MACS IT systems are subject to defined security patch management processes to identify, prioritise, and remediate security weaknesses. Remediation must be prioritised based on system criticality, risk analysis, the potential business impact, and available mitigation options.
- MACS vulnerability management processes must be documented and implemented to identify, prioritise, and remediate security weaknesses. The remediation must be prioritised based on the potential business impact and available mitigation options. Where appropriate,

technical solutions and tools must be leveraged and adopted on an ongoing basis to ensure that MACS is conducting effective vulnerability scanning and decommissioning out-of-band legacy systems across its critical IT infrastructure.

7. **Network Security**
    - MACS networks must have appropriate controls in place to protect the network, information, and assets in accordance with the MACS Network Security Procedure.
    - The ability to connect unauthorised devices to the network (wired or wireless) must be controlled, and remote access must be managed, and access secured via use of multi-factor authentication.
8. **Application Security**
    - End user desktop computers, mobile computers (for example laptops, tablets), must be protected with adequate security mechanisms to prevent the unauthorised disclosure and / or modification of data.
    - Cryptography must be used for protecting sensitive data during its transmission and storage. Data masking must be used to obscure (mask) sensitive information in non-production environments.
9. **Infrastructure Security**
    - All MACS devices must be securely protected in accordance with approved standards to adequately protect IT systems that support MACS processes and services. End user desktop computers, mobile phones, mobile computers (for example laptops, tablets), as well as portable computing devices (for example portable hard drives, USB memory sticks, etc.), must be protected with adequate security mechanisms to prevent the unauthorised disclosure and/or modification of MACS data. Baseline configurations must be maintained and reviewed on an annual basis.
    - All MACS building facilities, including office spaces, conference rooms, visitor lounge, and schools must appropriate security measures in place, (for example CCTV monitoring systems, controlled entry and exit points) to support the safety and security of employees, contractors, visitors, students, other users and assets.
    - The IT facilities (for example data centres, computer rooms, etc.) that store and process critical information must be constructed, maintained, and monitored in a way that data is adequately protected from physical and environmental threats.
    - Data must be backed up on a regular basis, protected from unauthorised access or modification during storage, and available to be recovered in a timely manner in the event of incident or disaster.
10. **Detection and Incident Response Management**
    - Key security related events, such as user privilege changes, must be recorded in logs and protected against unauthorised changes. Logs must be analysed on a regular basis to identify anomalous or potential unauthorised activity and facilitate appropriate follow-up action.
    - Potential security incidents must be handled appropriately through formalised Cyber Incident Response Plans as applicable at school level or enterprise level. Security incidents must be reported to regulating authorities and necessary bodies as specified in local regulations and legislations for security breach incidents. Security incidents must be prioritised based on their impact, reported accurately, and handled appropriately in accordance with MACS security incident management processes, and used as future references for resilience against similar security incidents.

Procedures and Guidelines

Procedures used to put this policy 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
Person accountable for IT in each MACS school	Inform MACS of breach of policy	
General Manager, IT Security, Risk and Audit	Review breach of policy	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.

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 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 and/or MACSEYE (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) and the board of Melbourne Archdiocese Catholic Schools Early Years Education Ltd (MACSEYE) 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, MACSS and MACSEYE.

Procedure

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

Process

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

MACS Staff

The term Staff or staff member refers to all people who carry out work in any capacity for MACS or its subsidiaries, and includes MACS board directors, board committee members, executives, employees, volunteers, consultants, contractors and School Advisory Council members, as the context requires.

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 policy into action are stored within the MACS Cyber Security Procedure repository

Related MACS policies and documents

ICT Acceptable Use Policy
Information and Recordkeeping Policy – MACS Office
Privacy Policy
Privacy Collection Notice – Parents and Students
Risk Management Policy
Emergency and Critical Incident Management Policy
Child Safety and Wellbeing Recordkeeping Procedures

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)

Policy information

Responsible director	Director, Finance, Infrastructure and Digital
Policy owner	Chief Technology Transformation Officer
Approving authority	MACS Board
Assigned board committee	Child safety and risk management
Approval date	11 August 2024
Risk Rating	Extreme
Review by	August 2024
Publication	Gabriel, CEVN

POLICY DATABASE INFORMATION	
Assigned framework	Governance
Supporting documents	See list of supporting documents and related policies above
Superseded documents	CEM IT Security Policy
New policy	New

Appendix A - MACS Information Governance and Cyber Security Policy Suite

<table>
<tr><td>Framework
A board-approved overarching governance structure to enable compliance by MACS and its subsidiaries for Information Governance and Cyber Security.</td><td colspan="3">Governance Framework</td></tr>
<tr><td>Policy
High level direction regarding Information Governance and cyber security.</td><td>Cyber Security Policy</td><td>Information and Records Management Policy – MACS office</td><td>Risk Management Policy</td><td>ICT Acceptable Use Policy</td></tr>
<tr><td>Supporting security Procedures and Guidelines
The Recommendations and guidance to support the implementation of the Cyber Security policy.</td><td colspan="3">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.</td></tr>
<tr><td>Additional Documentation
Documentation to support implementation of information security controls.</td><td colspan="3">Additional documentation such as security checklists and runbooks.</td></tr>
</table>