Melbourne Archdiocese
Catholic Schools

Third-Party Security Management Standard

IT Security

Introduction

This standard provides the foundation for management of contracted third-parties (i.e. suppliers, vendors, cloud service providers, etc.) at Melbourne Archdiocese Catholic Schools (MACS). It sets the standard for secure and effective management of contracted third-parties who maintain direct or indirect access to MACS systems and data.

Purpose

This standard provides the foundation for third-party security 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 Third Party Security Management Program

- A third party security management program should be established to govern the 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 to ensure the risks are operationally and contractually controlled.
- The third party security management program should include details around the strategy, objectives, plan, roles and responsibilities of the program. This should be communicated to the appropriate organisational stakeholders.
- The third party security management program should be developed and maintained with appropriate documentation such as governing procurement policy and underlying processes that guide implementation and maintenance of program processes.
- Third parties must participate in the Third Party Security Management Program, prior to providing services to MACS.

1.2 Third Party Selection and Evaluation Process

- Where there is a business need to provide external parties with physical access to MACS' information facilities, access to information systems or for them to store or process MACS data (including student data), a risk assessment must be carried out to identify requirements for specific information security measures.
- The risk analysis must consider the type of access required, the value of the information, the information security measures employed by the external party, and the implications of the access for the security of MACS' information and information systems.
- Access to MACS' facilities or data by external parties must not be provided until the appropriate measures have been implemented and agreement has been signed defining the terms and conditions for the connection.
- The MACS Security Team or equivalent and / or an authorised partner, is responsible for performing the risk assessments and evaluating the third party's security control environment.
- Information security credentials should be sourced from third parties using one or more of the following ways –
    - Certification - if the external party can produce a current certificate showing compliance to the relevant standard, e.g. ISO 27001, if supported with a relevant and documented scope (e.g. Statement of Applicability), then they may be considered to have complied with this requirement.
    - External Audit - if the external party has had their information security policies and practices audited by a trusted and independent organisation, and they are able to deliver a satisfactory report of that audit and demonstrate the relevance to the provided services to MACS, then they may be considered to have complied with this requirement.
    - MACS assessment - if the external party has had their information security policies and practices audited by MACS including the presentation of artefacts attesting to the operational effectiveness of any given control, they may be considered to have complied with this requirement.
- Third parties must participate in the Third Party Security Management Program, specifically through the participation of the risk assessment for the Third Party Selection and Evaluation Process.

1.3 Contracting with Third Parties

- Third parties must contractually and operationally commit to meeting MACS commercial, security, and regulatory compliance obligations. The following requirements must be included in third party agreements:
  - External parties are covered by a confidentiality agreement that explicitly states that persons with access to MACS facilities or proprietary information are not to disseminate any information about MACS, its capabilities, or activities without written authorisation from IT Security, Legal and the Business Owner.
  - The obligation of the third party to notify MACS in cases of security incidents which may affect MACS (e.g. third party virus outbreak, successful third party network compromise, etc.).
  - The obligation of the third party to maintain confidentiality, integrity, and availability of MACS information.
  - The possibility of renegotiating or terminating the contract if the terms and conditions are not satisfied, for example an undisclosed security incident or third party failing to meet agreed service levels.
  - Subcontracting issues in case the third parties (e.g. Cloud Service Providers) make use of other suppliers for the delivery of the services and these suppliers maintain direct or indirect access to MACS' data. The third party must ensure that any suppliers they utilise to fulfil contract requirements meet MACS security and regulatory compliance obligations.
  - All outsourcing contracts must include an agreement on minimum required security control obligations of the third party.
  - Controls must be in place to ensure the security of remote connections between the parties. The third party must utilise existing MACS security infrastructure and take responsibility for the maintenance of the respective security controls that have been established by MACS.
  - Ownership of licensing and intellectual property must be clearly defined.
  - All contracts must include a "right to audit" clause ensuring that management and / or an authorised representative may physically and or logically evaluate a third party's control environment. The contract must also include the right for MACS to perform independent security assessments, vulnerability assessments, and penetration testing to evaluate and assess the security environment of the third party.
  - The type, volume, and frequency of any files and/or reports that will be exchanged between the two parties; and
  - The business continuity and disaster recovery arrangements for the resumption of the third-party services in case of service interruption or data loss/destruction.

1.4 Integration with Cybersecurity and Enterprise Risk Management

- The vendor management program should be integrated into the IT Security and Enterprise risk management processes, to ensure alignment and transparency of any identified and / or ongoing monitoring of risks.
- The vendor management program should have documented processes for reporting of vendor non-compliance and / or breaches.

1.5 Ongoing Third Party Risk Management

- All third-parties handling information classified as Confidential or Sensitive or systems deemed material to MACS must be subject to annual security review by MACS' security team., equivalent or an authorised representative.
- This security review must be conducted against the security requirements and respective controls identified in MACS' cybersecurity framework and those outlined in contractual agreement. The

results of these annual reviews must be communicated to the third party and the third party must commit to specific timelines for remediating any identified security issues.

- If the third party does not agree on remediating security issues, then the business owner or contract owner must manage the risk through following relevant risk acceptance and/or management process.

1.6 Incident Management with Third Parties

- Relevant third parties must be included in the incident planning, response and recovery activities as determined in the *MACS Incident Response Plan*.
- Relevant third parties must be identified (including their roles and responsibilities for incident response) and participate in incident response exercises and simulation.

1.7 Conclusion of Third Party Relationship

- The third party security management program must include provisions, processes and plans for activities that occur after the conclusion of a partnership or service agreement with a vendor.
- Processes for terminating vendor relationships should be established around activities related to component support and obsolescence, access, assets / data (e.g., leakage, return/disposal, etc.) and risks due to the termination of the relationship.

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

<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>