Melbourne Archdiocese
Catholic Schools

Data Security Management Standard

IT Security

Introduction

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

Purpose

This standard provides the foundation for data security, 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 Data Classification

- Classifications assigned to assets must indicate the level of potential consequences to that information asset if altered, disclosed, stolen, lost, or destroyed. This should consider their value, criticality, and sensitivity to loss, damage, or unauthorised disclosure.
- Electronic data and information (at rest and in-transit) require additional security measures against cyber risks and threats.
- Information content must be classified by assigning an impact level in accordance with the worst-case consequence of loss or disclosure of the information.
- The impact assessment must be conducted in accordance with risk evaluation criteria.
- Information assets must be reassessed on a periodic basis, or at least annually, and declassified when there is no need to retain the initial classification level.
- Based on the results of the impact assessment, information content must be labelled with one of the following classifications:
  - Public
  - Business Use
  - Confidential
  - Restricted

Classification	Content Description	Examples
Public	This classification applies to information that has been explicitly approved by MACS management for release to the public. This information is in the public domain or readily available to a wide range of people. The public availability of such information does not have any negative consequences or operational or business impacts to MACS and/or its students and staff.	• Annual reports • Marketing brochures and promotional material • Online website content • Press releases • Job advertisements • Office/schools locations and contact details
Business Use	This classification applies to internal information that is intended for business use only. Its unauthorised disclosure and/or modification could have a moderate to significant impact on MACS, its business partners, and / or its business operations.	• Internal business policies, processes, and procedures • Organisation charts • Day-to-day emails (not containing PII) • Project status reports
Confidential	This classification applies to sensitive information about or belonging to students, staff or the office, which is intended for limited use within MACS only. Its unauthorised disclosure and/or modification could have a significant impact on MACS, its students, staff, partners, and / or operations. Confidential information should be labelled according to the nature of the information (e.g. legal privilege, health data, PII, etc).	• Personally Identifiable Information (PII), for example, name and date of birth. • IT system and network diagrams and configuration data • Communications with regulators or business partners • Legal advice, litigation, and dispute resolution material • Unpublished strategic plans • Encryption keys

		• Network architectures and facilities diagrams • Privileged user account passwords • Financial information (e.g. payment cards details, bank account numbers, etc.) • Personnel remuneration
Restricted	This information is similar to that which is classified as “confidential” however it is intended for limited, authorised, and named staff solely. Restricted requires the highest levels of protection, as its disclosure is likely to result in extensive adverse impact on MACS, such as financial loss, reputational ramifications, impact to child safety, sanctions, penalties, and legislative/regulatory breaches.	• Personally Identifiable Information (PII), for example, name and date of birth. • A collection/database student information including (but not limited to): • Student health records • Disability information

- Third parties providing any information to MACS for use should follow the Data Classification processes.

1.2 Data Lifecycle

- The Data Control Environment (state of operation in which data assets are holistically managed throughout MACS) at MACS must be securely maintained across the lifecycle of data during creation, storage, transmission, retention and disposal/destruction.
- Any information processed, managed on behalf of MACS by third-parties must follow the Data Lifecycle processes that has been implemented.

1.3 Data Loss Prevention

- MACS must block access to personal email, file sharing, file storage services, and other personal communications applications and services from organisational systems and networks.

1.4 Data Inventory Management

- The Data Owner must maintain current details of their key information assets in a Data Asset Inventory. The Data Asset Inventory must include:
  - Information asset name and location;
  - A description of the information asset (including vendor or version number where applicable);
  - The name of the business process or processes that make use of the information asset;
  - Physical location (if applicable);
  - The security zone placement (refer to Network Security Standard);
  - The asset owner and custodian details contact details;
  - The classification of the information asset; and
  - Any applicable retention, regulatory, or legal requirements.
- The Data Asset Inventory must be regularly updated in accordance with any change that may affect an asset.

- The Data Asset Inventory must be stored in a central repository and reconciled annually to maintain consistency of information. Access to the Data Asset Inventory should be limited to authorised employees only.

1.5 Printing and Collection

- Documents must be collected from printers immediately after printing, if locked printing is not in place.
- Staff ordering the prints must be present at the printer when prints are made.
- Once printed, documents must be securely retained and disposed of in-line with safeguards commensurate to the data classification of the documents.

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>