Melbourne Archdiocese
Catholic Schools

Identity & Access Management Standard

IT Security

Introduction

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

Purpose

This standard provides the foundation for identity and access 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 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.

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 Access Provisioning

- Account creation for systems containing “confidential” data must follow a documented process which includes procedures for approving users’ access by MACS' management.
- Access to MACS' electronic data must be authorised, follow the principles of least privilege, and be granted based on segregation of duties.
- Account creation and the process of account authorisation must be documented and auditable.
- Third parties are required to endorse MACS' contractual clauses pertaining to adherence to MACS' Information Security Policy prior to being issued a unique user ID or granted access to MACS' information systems or electronic data.
- User accounts for contractors must always have an expiration date aligned with the contract period. Access must be revoked, and accounts terminated on the account expiration date, unless an extension is requested and approved.

1.2 Access Review

- A periodic review of user access privileges is to be performed on at least an annual basis (quarterly for privileged level access) to ensure that there is no segregation of duties violations.
- Access should be reviewed for in-scope applications and Active Directory groups.
- Access must be validated by a Line Manager or Business Owner (or Principal for Schools). This should include confirmation that users have the minimum level of access required to perform their role; identify any accounts where the user has moved to a new role; identify any accounts where the user has left MACS; identify any accounts to be disabled where the user has taken a long-term leave of absence.
- Access reviews should be logged to ensure they are fully documented and verifiable.
- A periodic review of privileged user access, including Full Domain Administration access, must be performed at least on a quarterly basis.

1.3 Access De-provisioning

- All access should be revoked within 24 hours upon termination. In the event of a staff member, who has privileged access on information systems, has resigned or is terminated, the account must be disabled immediately.
- Access de-provisioning details should be logged to ensure they are fully documented and verifiable.
- When a contractor is off-boarded, the hiring manager is responsible for ensuring all access is revoked.

1.4 Privileged User Access Management

- Privileged access (i.e., administrator accounts, domain user accounts, etc.) should only be allocated to users on a need-to-use basis, based on the minimum requirement for their functional roles.
- Privileged access rights must be controlled via multi-factor authentication (i.e. smart card, soft token, or PIN).
- Every administrative or privileged account must be associated with a named ID and have a one-to-one relationship with a user.
- Privileged provisioning requests and approvals should be logged to ensure they are fully documented and verifiable.

- Privileged access should be assigned to a user ID different from those used for regular activities.
- The use of privileged accounts must be limited to MACS staff and accounts (as required) for authorised business purposes only.

1.5 Service Accounts

- Service accounts should be subject to periodic reviews (*related to 1.1.2*), where the account role and requirement is reviewed and validated/de-provisioned.
- Service accounts should only be used for systems authenticating themselves to each other.
- Service accounts should be non-interactive unless required for a valid business justification. This should be handled through an exception through the *IT Security Risk Management Process* and compensating controls should be implemented.
- Service accounts should be subject to the password requirements per the *Password Management* section.
- Any third-party service accounts should only be provisioned after permission is sought from MACS IT Security.
- Third-party service accounts should not be left in 'always-enabled' state.

1.6 Multi-factor Authentication

- Multi-factor authentication should be performed through secure protocols.
- Multi-factor authentication should be used to authenticate all privileged access.
- Multi-factor authentication should be used to authenticate all users of remote access solutions.
- Multi-factor authentication should be used to authenticate all MACS employees (outside of the MACS office and / or on a non-managed device).

1.7 Third Party Access

- A periodic review of third-party user accounts is to be performed on at least an annual basis, or if privileged – to be performed on at least a quarterly basis (*related to 1.1.2*).
- Access should be reviewed and approved by the third-party manager and business owner, prior to user account onboarding and renewal.

1.8 Account Monitoring/Hygiene

- Accounts should be monitored and reviewed for the following:
  - Accounts not used for 60 days or more, without a valid exemption should be (disabled, reviewed, deleted).
  - Access permissions should be reviewed and modified when moving from one role to another.
  - Unsuccessful logins for privileged user activity.

1.9 Password Management

- Passwords must be mandatory for all user accounts on all network and standalone information systems including operating systems, applications, databases, end user desktops and mobile devices (laptops, tablets, etc.) User passwords must meet the rules below.

Characteristic	Policy
Minimum length	Fourteen (14) characters

Complexity	Alpha and numeric characters and one special character (e.g. %, #). Where possible, tools to verify password quality should be implemented.
Minimum password age	One (1) day
Maximum password age	90 days
Password history	Five (5) passwords
First password expiry for new accounts	Users must change their default password upon first login
Inactive Desktop Lockout	Fifteen (15) minutes
Account lockout threshold	Three (3) minutes
Account lockout duration	Fifteen (15) minutes

In addition to the password policies, the following guidelines apply:

- Passphrases are strongly recommended as the preferred password practice.
- Passwords must not be displayed or stored in clear text on input and fixed screens, hard copy reports or electronic files.
- Temporary passwords are distributed securely to the user (e.g. via email, text message, phone, etc.) and never distributed in the same communication as the user ID.
- Default passwords shipped with information systems must be immediately changed upon installation of the software.
- Passwords should not contain variations of the account ID, username (or any part thereof), personal user information (employee number), and any one common dictionary word in any language, common names, or other easily guessable words.
- If a password reset is requested, the user's identity should be adequately verified before the password reset process commences.
- Where possible and feasible, password managers should be used after consultation with the MACS ITS and IT Security teams.

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="4">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="4">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="4">Additional documentation such as security checklists and runbooks.</td></tr>
</table>