Melbourne Archdiocese
Catholic Schools

Security Detection & Incident Response Management Standard

IT Security

Introduction

This standard provides the foundation for management of security incident detection and incident at Melbourne Archdiocese Catholic Schools (MACS). It sets the standard for secure and effective management of incidents and events.

Purpose

This standard provides the foundation for security incident 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 Security Incident Management Responsibilities

- The GM, IT Security, Audit, and Risk is the primary responsibility over the IT Security incident response capability and has the final say in incident handling and response activities.
- All suspected security incidents must be reported to the MACS IT Security team upon discovery. For schools, they must do this by following the *Incident Response Plan*.
- Responsibilities with respect to IT Security incidents should be clearly communicated to the involved parties and stakeholders (including internal and external stakeholders, senior leadership, legislative bodies, etc.) and it should be ensured that those responsible for IT Security incident management understand the priorities for handling IT Security incidents.
- If a third-party is involved in security incident management, they must have documented responsibilities in collaboration with the MACS IT Security team, where applicable

1.2 Security Incident Management Detection

- Log records should be configured to generate from operating systems, applications, services (including cloud-based services).
- Log generators should be configured securely, to share their logs with the logging infrastructure systems and services.
- A security incident and event management (SIEM) tool or other tools should be used to continuously detect and monitor log events for known malicious and suspicious activity.
- There must be detection and monitoring mechanisms over email, web, file sharing, collaboration services, and other common attack vectors to detect malware, phishing, data leaks and exfiltration, and other adverse events. Continuous network monitoring should be deployed to detect and respond to threats in real-time to protect the MACS network. Any tools, systems, etc. used for continuous network monitoring must:
    - be protected against attack or unauthorised changes, e.g., only authorised users have access to make approved changes;
    - analyse system behaviour that deviates from established patterns, or consist of suspicious intrusion characteristics
    - be configured to alert the relevant stakeholders, such as IT Security, when unauthorised and/or suspicious activity is detected. Such activities can include malware, vulnerability exploitation, traffic exchange with malicious sources, etc. This should be performed in accordance with the IT Security Incident Response Plan.
    - be reviewed and updated periodically.
- Where there is insufficient monitoring / detection of log events, regular manual reviews of such log events should be conducted.
- Logs should have the following requirements:
    - Must contain a unique user identifier associated with an activity;
    - Must contain the source IP address of the user activity or external event that occurred.
    - Must contain the activity undertaken, for example: logon, log off, create, modify, delete or copy.
    - Retained / Archived regularly / on a periodic basis;
    - Retained for at least 12 months, unless approved for an alternate retention period by IT Security);
    - Protected against unauthorised disclosure, modification and destruction;

  - Contain date and time of the activity being logged;
  - Must not contain unencrypted passwords, Confidential and Sensitive data;
  - Be synchronised to a consistent time source; and
  - Be monitored by the IT Security team, where response follows the MACS IT Security Incident Response Plan, in conjunction with the *Emergency and Critical Incident Management Policy*

- As part of the Architecture Review Team reviews, it should be determined if any systems being introduced or enhanced adhere to the Security *Incident Management Detection* requirements for MACS office.

1.3 Security Incident Management Response

Security incident response should be performed in accordance with the MACS IT Security Incident Response Plan.

The MACS IT Security Incident Response Plan should be developed and maintained, and include:

- Roles and responsibilities, contact and communication information, processes for handling incident / event scenarios, criteria for prioritisation and escalation as appropriate;
- Involvement from internal and external stakeholders, as appropriate;
- Communication processes to those responsible for carrying the plan out and to involved parties and stakeholders (including internal and external stakeholders, senior leadership, legislative bodies, etc.);
- Documented and defined criteria, in order for adverse events to be declared when the criteria are met;
- Processes pertaining to incident containment and eradication. This can in the form of incident playbooks, or sub-processes that are aligned and have linkage to the Security Incident Response Plan; and
- Security incident categorisation and prioritisation; this should take into account the scope, likely impact and time-critical nature of incidents / events;

The security incident response plan should be reviewed annually or when a significant change is needed. Reviews should be based on findings from any assessments performed (tabletop exercises, simulations, tests, internal and external reviews / audits), including from BCP, DRP, past incidents.

If a third-party is involved in incident management, they must have documented responsibilities for incident response in collaboration with the MACS IT Security team, where applicable

1.4 Post-incident Review

Post-incident reviews must be performed for any critical and high-rated incidents. The reviews must include:

- Investigation and response details;
- Incident details (e.g., severity, impact, regulatory/breach implications, root cause, etc.);
- Lessons learnt, if any; and
- Recommendations, if any, including treatment / action owners and the target due date of implementation.

If a third-party is involved in incident management, they must conduct post-incident reviews in collaboration with the MACS IT Security team, where applicable

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.			