Melbourne Archdiocese
Catholic Schools

Business Continuity and Disaster Recovery Standard

IT Security

Introduction

This standard provides the foundation for security requirements for Business Continuity and Disaster Recovery at Melbourne Archdiocese Catholic Schools (MACS). It aims to minimise the disruption to business operations in the event of a disaster and facilitate a timely recovery.

Purpose

This standard provides the foundation for the business continuity and disaster recovery, 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

Please note that the following Standard statements must be read in accordance with the MACS Business Continuity and Disaster Recovery Policies and Procedures. The following Statement statements expand on the Policies and Procedures, by detailing the security requirements of Business Continuity and Disaster Recovery for MACS.

1.1 Business Continuity Planning (BCP) and Maintenance

- MACS must establish the context and process for developing and managing BCPs. This includes definition of objectives and scope, of the BCP activities, timelines, assumptions, resource allocation and milestones.
- A comprehensive understanding of the external and internal business drivers and constraints must be developed through conducting risk and vulnerability analysis.
- Business Impact Analysis (BIA) must be conducted to identify and analyse critical business processes and activities and evaluate impact and probabilities of failure.
- BCP response strategies must be developed based on the results of the BIA for continuity planning.
- Based on the results of the BIA and the response strategies developed, resource requirements will be determined and documented. A detailed continuity plan must be developed accordingly, taking into account information from the BIA and response strategies.
- Appropriate communication strategies and plans must be developed to ensure internal and external stakeholders are informed in the event of an incident and subsequent disruption and recovery.
- Staff shall be trained, ensuring MACS' staff are familiar with their individual roles and responsibilities. Appropriate testing is conducted to validate the usability of contingency and recovery plans to help identify changes that need to be made to keep these plans current.
- BCPS must be updated on a regular basis to ensure that the contingency and recovery measures remain current and accurate. The maintenance schedule documented within the BCP should drive this process.
- If a third party has responsibilities, in relation to business continuity, it must be involved with the above standard requirements for MACS Office.
- If a third party has responsibilities, in relation to the business continuity impacting MACS, they must provide their own annual testing and results to MACS as part of the third party management program.

1.2 BCP Testing

MACS' BCPs are to be tested regularly to confirm their currency and appropriateness. At a minimum:

- A test schedule will be documented and maintained within all MACS BCPs;
- The test schedule will indicate how and when each element of the plan will be tested;
- The testing schedule may take a phased approach, however all components of the BCP must be tested at least annually;
- Testing approaches adopted may include:
  - Desktop reviews: normally conducted as a physical examination of the document to ensure completeness and readability.
  - Desktop scenario exercise: an approach that involves an examination of how the BCP will be used to guide actions and decisions following activation. This approach uses

hypothetical disruption scenarios to examine assumptions made during the development of the plan

- Recovery scenario exercise: this approach involves the activation of BCPs based on a hypothetical scenario. The exercise can be conducted as a limited activation, involving only a few BCPs, the activation of only parts of individual BCPs or can involve full scale activation across MACS schools and the office.

At a minimum, the following testing timetable is to be adopted:

Testing Approach	Testing Frequency
Desktop review and desktop scenario exercise	Annual
Recovery scenario exercise	Bi-annual

- If a third party has responsibilities, in relation to business continuity, it must be involved with the above standard requirements for MACS Office.

1.3 Security Requirements for Disaster Recovery

- MACS must align its IT Disaster Recovery (IT DR) plans to its organisation-wide Business Impact Analysis (BIAs) and Business Continuity Plans (BCPs).
- Technical reviews of the IT DR plans must be performed to ensure that the IT DR plan's technical recovery capabilities align with the critical systems' Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- Any discrepancies identified in the review must be addressed by adjusting the DR plan.
- MACS must ensure the DR plans support the BCP's broader continuity strategies by verifying that recovery procedures, resources and communication protocols are consistent and cohesive across both plans.
- Recovery procedures and resources must be used to build resilience in the event of an IT disaster. This should include the use of redundant servers, alternate network paths, and storage solutions across multiple locations to ensure that if one component fails, others can seamlessly take over.
- Failover mechanisms such as load balancers and clustering, must be configured to automatically redirect traffic and workloads to operational systems in the event of a failure.
- If a third party has responsibilities, in relation to disaster recovery, it must be involved with the above standard requirements for MACS Office.

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>