CYBER SECURITY POLICY

Policy number	16	**Version**	3.0
Update by	Deirdre Looney	**Approved by Board on**	18/08/2023
Responsible person	AMS Board	**Scheduled review date**	02/09/2024

Introduction

Australian Marist Solidarity (AMS) is the international development arm of the Marist Brothers Star of the Sea Province and the Marist Association of St Marcellin Champagnat. It has a particular focus on empowering young people to transform their lives and community. Promoting the dignity of the human person, as safeguarded by internationally recognised human rights conventions, is a core value of AMS.

AMS is committed to proactively protecting our systems and databases and ensuring our employees and those who operate under the auspices of AMS understand their role in protecting the technology and information of the organisation.

Purpose

The purpose of this document is to identify and define key cyber security risks and commit the organisation to maintaining satisfactory procedures to mitigate and manage these risks.

Scope

This policy applies to all Board members, committee members, staff, contractors, partners, agents and volunteers who operate under the auspices of Australian Marist Solidarity.

Definitions

Cyber security is the protection of electronic information from unauthorised access.

Personal or sensitive information should be prioritised in considering cyber security measures.

Personal information is information or an opinion about an identified person (or a person that can reasonably be identified), regardless of whether that information or opinion is true or recorded in a material form.

Sensitive information is a subset of personal information and may include, for example, a person's religious or philosophical beliefs, sexual orientation or health information.

(ACNC, 2021)

Policy

AMS is committed to protecting its information assets and the information it holds about its employees, contractors, partners, donors, agents and volunteers. AMS will put in place procedures to protect its information assets against unauthorised access and use, theft, modification, destruction and unauthorised disclosure.

Implementation

The implementation of this policy will be guided by the AMS Operations Manual and will address the following common cyber security risks:

- Unauthorised access to a device, network or system;
- Viruses or other malicious software that can collect, change or delete information and spread throughout a network; and
- Fake emails or websites set up to trick someone into revealing personal or sensitive information.

Related procedures will include the following:

1. The management of passwords, including the requirement to create strong passphrases; how passphrases should be stored and the importance of having unique passphrases for different logins.
2. Email security measures including only opening email attachments from trusted contacts and businesses; blocking junk, spam and scam emails and identifying, deleting and reporting suspicious looking emails.
3. The management of sensitive data including ways to store physical files and sensitive data, such as in a locked room or drawer; to understand what constitutes sensitive data and how sensitive data is to be destroyed when no longer required. Please refer to the AMS Privacy Policy on our website https://www.australianmaristsolidarity.net.au/about-us/policies/ for further details on how sensitive information is handled.
4. Rules for the handling and management of technology, including how devices such as laptops can be accessed away from the workplace; how to store devices not in use; how to report a loss or theft of a workplace device; how system updates and spam filter updates will be rolled out to employee devices; when to physically shut down computer devices and mobile devices when not in use; the need to lock screens when computers are left unattended and how to manage data stored on removable devices to prevent viruses being loaded to business systems.
5. Plan and prepare for an incident by identifying the assets that are important to AMS such as financial, information or technological assets; consider risks to these and steps that can be taken to reduce the impact of an incident; ensure clarity of how potential incidents are reported and managed.
6. Appropriate insurance to mitigate the cost of managing the consequences of a cybersecurity incident.
7. Responding to a Cyber-Security Breach

AMS IT services are managed externally. This includes management of: servers, users, routers / firewalls, wi-fi access points, switches, Azure Tenant and Office 365 Tenant. Firewalls are used to prevent unauthorised access from external networks and computer systems to internal networks and the provider constantly monitors the firewalls for attacks or breaches.

Multi-factor authentication, higher level of password complexity, geo-blocking, as well as limited and separate administration accounts ensure access to systems is controlled. Password policy requires complex passwords that are changed regularly. Website security and maintenance is managed externally, with regular backup and software updates performed.

Monitoring and Review of Policy

AMS will undertake a review of this policy in accordance with the AMS Policy Review Process, or sooner if required. This review will be undertaken by the Chief Executive Office with oversight of the AMS Finance, Audit and Risk Committee and authorised by the AMS Board of Directors.

Related Resources

- AMS Fundraising and Donations Policy
- AMS Complaints Policy
- AMS Safeguarding Policy
- AMS Whistleblower Policy

- AMS Privacy Policy
- AMS Risk Management Policy
- AMS Risk Management Matrix and Register
- Communications Policy
- Social Media Policy
- AMS Code of Conduct
- https://www.acnc.gov.au/for-charities/manage-your-charity/governance-hub/governance-toolkit/governance-toolkit-cybersecurity
- https://acfid.asn.au/good-practice-toolkit/quality-principle-6-communication

Authorisation

MSinclair

Michael Sinclair

Signature of Company Secretary

Name of Company Secretary

August 2023

Date of approval by the Board