MAHI MIHINARE
ANGLICAN ACTION

SECURITY INCIDENT MANAGEMENT POLICY

Category:	Practice
Last Review Date:	July 2023
Next Review Date:	July 2026
Endorsed by:	The Anglican Action Missioner
Approved by:	The Anglican Action Mission Trust Board

Purpose

The purpose of this Security lncident Management policy is to make sure Mahi Mihinare Anglican Action has the correct management plans and responses in place, in case of an Information System Security lncident.

Statement

This policy defines the requirement for reporting and responding to incidents related to Mahi Mihinare Anglican Action's information systems and operations. lncident response provides the Agency with the capability to identify when a security incident occurs. lf monitoring were not in place, the magnitude of harm associated with the incident would be significantly greater than if the incident were noted and corrected.

Scope

1) The scope of this policy includes all Mahi Mihinare Anglican Action staff and clients. This policy applies to all information systems and information system components of the Agency. Specifically, it includes:
   a. Servers and other devices that provide centralized local and cloud-based computing capabilities
   b. Devices that provide centralized local and cloud-based storage capabilities
   c. Desktops, laptops, and other devices that provide distributed computing capabilities
   d. Routers, switches, and other devices that provide network capabilities
   e. Firewalls, and other devices that provide dedicated security capabilities

2) In the event of a breach of staff or client's information occurs, Anglican Action is required by New Zealand law to notify the Privacy Commissioner and any affected persons as soon as practicable as described in the Privacy Act 2020.

Definitions

Employer	Employer means 'The Anglican Action Mission Trust Board', referred to as 'Mahi Mihinare Anglican Action' or 'The Mission' in this policy.
Agency	Agency means the Employer or Staff member as applicable.
Tangata Whaiora	Tangata Whaiora means any individual whom the agency provides or agrees to provide a service or to whom the agency is legally obligated to provide a service.
Security Incident	Refers to an adverse event in an information system, and/or network, or the threat of the occurrence of such an event. Incidents can include, but are not limited to, unauthorized access, malicious code, network probes, and denial of service attacks.
Staff member	Staff member means all employees (permanent, fixed-term, or casual), consultants, contractors, service providers, students, and volunteers engaged by the Mission.

Policy

1. Business Continuity Plan

a) Mahi Mihinare Anglican Action must prepare, periodically update, and regularly test business continuity plans that provide for the continued operation of critical computer and communication systems in the event of an interruption or degradation of service. For example, server connectivity is interrupted or an isolated malware discovery.
b) The Business Continuity Plan must include roles, responsibilities, and communication strategies in the event of a compromise, including notification of relevant eternal partners. Specific areas covered in the plan include:
    a. Specific incident response procedures
    b. Business recovery and continuity procedures
    c. Data backup processes
    d. Analysis of legal requirements for reporting compromises
    e. Identification and coverage for all critical system component-
    f. Reference or inclusion of incident response procedures from relevant external partners, e.g., IT contractors.
c) At least once every year, the Agency must utilize simulated incidents to mobilize and test the adequacy of response. Where appropnate, tests will be integrated with testing of related plans (other Business Continuity Plans, Disaster Recovery Plans, etc.) where such plans exist. The results of these tests will be documented and shared with key stakeholders.

2. Business Continuity Plan Development

a) The Business Continuity Plan must be updated to reflect the lessons learned from actual incidents as well as reflect developments in the industry.

3) Inability to Access Computer and Communication Systems

a) Access to the Mission's Computer and Communication Systems is important to providing the level of service the mission is committed to. If staff are unable to access the required computer and communication systems, contact should be made in the first instance with their team leader who, if the issue cannot be resolved, will escalate it to the appropriate manager.

4) Intrusion Response

a) The Agency must document and periodically revise the Business Continuity Plan with a test intrusion response procedure. These procedures must include the sequence of actions that staff must take in response to a suspected information system intrusion, who has the authority to perform what responses, and what resources are available to assist with responses.
b) All staff expected to follow these procedures must be periodically trained in and otherwise acquainted with these procedures.

4. Malicious Code Remediation

a) Steps followed will vary based on scope and severity of a malicious code incident as determined by the Agency. They may include but are not limited to: malware removal with one or more tools, data quarantine, permanent data deletion, hard drive wiping, or hard drive/media destruction.

5. Data Breach Management

a) Mahi Mihinare Anglican Action management should prepare, test, and annually update the Business Continuity Plan that addresses policies and procedures for responding in the event of a breach of sensitive customer data.

6. Reporting to Third Parties

a) Unless required by law or regulation to report information security violations to external authorities, senior management, in conjunction with legal representatives must weigh the pros and cons of external disclosure before reporting these violations.
    a. If a verifiable information systems security problem, or a suspected but likely information security problem, has caused third party private or confidential information to be exposed to unauthorized persons, these third parties must be immediately informed about the situation.

b. If sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorired parties, Mahi Mihinare Anglican Action management must be notified immediately.

7. Display of Incident Reporting Contact Information

a) Mahi Mihinare Anglican Action contact information and procedures for reporting information security incidents must be prominently displayed in public communication mediums such as bulletin boards, break rooms, newsletters, and online portals.

8. Notification of Security Incident

a) It isn't always necessary to notify people of a breach. If there's no risk of harm, notifying may do more harm than good. Mahi Mihinare Anglican Action management need to consider each incident on a case-by- case basis. Factors to consider are:
    a. the risk of harm to people affected
    b. whether there's a risk of identity theft or fraud
    c. whether there's there a risk of physical harm
    d. whether there's a risk of humiliation, loss of dignity, or damage to the person's reputation or relationships. For example; the lost information includes mental health, medical, or disciplinary records
    e. what affected people can do to avoid or minimise possible harm, e.g. change a password
    f. whether the Agency has any legal or contractual obligations.

b) If a decision is made to notify, the Agency must do it as soon as reasonably possible. However, if law enforcement is involved, the Agency must first check with them first in case a notification compromises their investigation.

c) If it has been decided that a notification will be made, the notification will be conducted and overseen by the Missioner and senior management. The notification should contain, at a minimum, the following elements:
    a. information about the incident, including when it happened
    b. a description of the compromised personal information
    c. what the Mission is doing to control or reduce harm
    d. what the Mission is doing to help people the breach affects
    e. what steps people can take to protect themselves
    f. contact information for enquiries and complaints
    g. offers of support when necessary, e.g. advice on changing passwords
    h. whether the Mission has notified the Office of the Privacy Commissioner
    i. contact information for the Privacy Commissioner

d) The Agency should notify the people affected directly, such as
    a. by phone
    b. by letter
    c. by email
    d. in person

e) The Agency should only notify people indirectly (e.g. through website information, posted notices, or the media) if:

a. notifying them directly could cause further harm
b. it's too expensive to notify them directly
c. we don't know how to contact them

Key Accountabilities & Responsibilities

Person / Party	Responsibilities
Governance	Review policy every two years or as required
Management	Ensure that staff members are aware of this policy and processes
Leadership	Ensure that staff members are aware of this policy and processes
Staff	Have access to this policy and understand their obligations under it

Related Policies, Legislation, Regulations and Documents

- Privacy Act 2020
- Human Rights Act 1993
- Anglican Action Code of Conduct
- Storage of Information Policy