INFORMATION SECURITY

Autism Spectrum Australia (Aspect) recognises the importance of information security in achieving its mission and ensuring the confidentiality, integrity, and availability of information. This policy outlines Aspect's commitment to aligning information security measures in accordance with ISO 27001:2022 standards.

Commitment

Aspect is committed to:

- Protecting confidential and sensitive information from unauthorized access, disclosure, alteration, or destruction.
- Complying with all relevant information security laws, regulations, and contractual obligations. We will regularly assess our compliance status and make necessary adjustments.
- Ensuring that information security responsibilities are defined and communicated to all employees, contractors, and third parties.
- Continuously assessing and managing information security risks.
- Providing appropriate training and awareness programs to ensure all personnel understand their information security responsibilities.
- Regularly monitoring, reviewing, and improving our information security practices.

Scope

This policy applies to all employees, contractors, consultants, and third-party partners who have access to Aspect's information assets. It encompasses all forms of information, whether electronic, paper-based, or verbal.

Information Security Objectives

Aspect is committed to achieving the following information security objectives:

- Ensuring the confidentiality (through information classification), integrity, and availability (in line with appropriate access management) of information.
- Identifying and assessing information security risks and implement appropriate controls.
- Complying with applicable laws, regulations, and contractual obligations related to information security.
- Continuously improving information security measures through regular reviews and audits.
- Promoting awareness and providing training to all personnel on information security best practices.

Responsibilities

Board

The Board's primary responsibility is to establish corporate governance and approve and oversee the organisation's overall strategy and risk management, including Information Security.

The Board is responsible for the organisation's risk overall; identifying and monitoring oversight of corporate risks; and setting the risk appetite within which it expects Management to operate.

The Board delegates oversight of the Risk Management Framework to the Finance, Audit & Risk Committee and it is managed by the Executive and Management teams.

The Board is responsible for ensuring the necessary resources are made available to management to manage the organisation's risks.

Information Security Officer (ISO)

Aspect has a designated ISO who is responsible for overseeing the information security program, including:

- identifying and mitigating potential cyber threats and vulnerabilities;
- responding to cyber incidents;
- developing, and implementing security policies and procedures; and
- providing security awareness training to all employees (as part of an overall cyber security awareness training managed by Head of People, Culture and Safety).

Executive

The Executive team is responsible for:

- Setting the strategic direction for information security.
- Providing leadership and commitment to information security.
- Managing the necessary resources for information security initiatives.
- Monitoring and reviewing the effectiveness of information security controls.

Leadership Network

The Leadership Network is responsible for:

- Supporting and enforcing information security policies and controls.
- Monitoring the necessary resources for information security initiatives.
- Reporting security incidents and breaches to the ISO.

Employees and Contractors

All employees and contractors are responsible for:

- Being aware of the risks associated with their actions.
- Complying with information security policies and procedures.
- Reporting any suspected security incidents or vulnerabilities to the appropriate channels.
- Protecting Aspect's information assets from unauthorised access, disclosure, or misuse.
- Following the requirements of the information classification and access management systems.
- Participating in information security training and awareness programs.

Risk Management

Aspect maintains a risk management process, aligned to ISO 27001:2022, to:

- Identify and assess information security risks.
- Implement and maintain controls to mitigate identified risks.
- Regularly review and update the risk assessment and treatment plan.

Information Security Controls

Aspect maintains a comprehensive set of information security controls to protect data, systems, and networks. These controls are based on ISO 27001:2022 requirements and are regularly reviewed and updated.

Incident Response

Aspect addresses security incidents promptly through maintaining an incident response process to:

- Detect and report information security incidents.
- Assess the impact of incidents.
- Implement appropriate measures to contain and recover from incidents.
- Investigate incidents to determine root causes and prevent recurrence.
- To identify and document lessons learned.

Training and Awareness

Aspect provides information security training and awareness programs to ensure that all personnel understand their responsibilities and best practices for information security.

Monitoring and Review

The Information Security Policy is regularly reviewed and updated to reflect changes in technology, threats, and the organisation's structure and operations.

Document Control

This policy will be maintained, documented, and made available to all personnel who have access to Aspect's information assets.

External Framework

ISO/IEC 27001:2022 - Information Security Management Systems
Australian Signals Directorate Essential Eight

Relevant Procedures and Guidelines

Acceptable use of Technology by Students
Bring your Own Smartphone (Staff)
Business Continuity Planning
Computer Hardware and Software Acquisition and Lifecycle Management
Continuity of Supports
Incident Investigation
Incident Management Framework
Incident Response and Reporting
Information Technology Incident Management
Mobile Device Provision and Use
Program Steering Committees Terms of Reference
Project Control Groups Terms of Reference

Legislation References

Commonwealth
Copyright Act 1968 (Cth)
Electronic Transactions Act 1999 (Cth)
My Health Records Act 2012 (Cth)
Privacy Act 1988 (Cth)
Spam Act 2003 (Cth)

New South Wales
Privacy and Personal Information Protection Act 1998 (NSW)

Victoria
Privacy and Data Protection Act 2014 (Vic)

Australian Capital Territory
Privacy Act 2014 (ACT)

South Australia
South Australian Cyber Security Framework

Queensland
Information Privacy Act 2009 (Qld)

Northern Territory
Information Act (NT)

Tasmania
Personal Information Protection Act 2004 (Tas)