Information Security Management System (ISMS) Policy

Document Classification:	**L0 – Public Information**
Document Ref:	**Information Security Management System (ISMS) Policy**
Version Date:	**20.07.2026**
Document Author:	**Sophie Wismayer**
Document Owner:	**Sophie Wismayer**

Document Control

Version	Date	Revision Author	Summary of Changes
1.0	15.07.2026	Sophie	Initial draft

Approval

Name	Position	Signature	Date
Nick Camilleri	Managing Director	**Signed by:** Nick Camilleri **EMail:** nick@avantech.com.mt **Signing time:** 20-07-2026 11:14:18 **IP address:** 195.158.111.117	20.07.2026
Steve Casaletto	Director of Technology	**Signed by:** Steve Casaletto **EMail:** steve@avantech.com.mt **Signing time:** 21-07-2026 15:02:50 **IP address:** 195.158.111.117	20.07.2026

1. Purpose

The purpose of this Information Security Management System (ISMS) Policy is to establish the framework for protecting the confidentiality, integrity, and availability of the organisation's information assets. This policy demonstrates the organisation's commitment to implementing, maintaining, and continually improving an Information Security Management System in accordance with ISO/IEC 27001:2022.

2. Scope

This policy applies to:

- All employees, contractors, consultants, temporary staff, and third parties who access the organisation's information or information systems.
- All information assets, regardless of format, including electronic, physical, and verbal information.
- All business processes, information systems, facilities, and technologies within the defined scope of the ISMS.

The formal scope of the ISMS is documented separately in the ISMS Scope Statement.

3. Policy Statement

The organisation is committed to:

- Protecting information assets from unauthorized access, disclosure, modification, destruction, or loss.
- Ensuring information is available to authorized users when required.
- Managing information security risks using a structured risk management process.
- Meeting applicable legal, regulatory, contractual, and business requirements.
- Continually improving the effectiveness of the ISMS.
- Providing sufficient resources to establish, implement, maintain, and improve the ISMS.
- Promoting a culture of information security awareness throughout the organisation.

4. Information Security Objectives

The organisation shall establish measurable information security objectives that:

- Support business objectives.
- Are monitored and reviewed regularly.
- Address identified information security risks.
- Promote continual improvement.
- Are communicated to relevant stakeholders.

Examples include:

- Reducing security incidents.
- Improving vulnerability remediation timelines.
- Achieving employee security awareness training completion targets.
- Maintaining compliance with applicable legal and contractual obligations.

5. Risk Management

The organisation shall:

- Identify information security risks.
- Assess risks using an approved methodology.
- Evaluate risks against established acceptance criteria.
- Treat risks using appropriate controls.
- Monitor residual risks.
- Review risks periodically and when significant changes occur.

Risk treatment decisions shall be documented and approved by management.

6. Roles and Responsibilities

Executive Management

Executive Management shall:

- Demonstrate leadership and commitment to the ISMS.
- Approve information security policies.
- Allocate appropriate resources.
- Support continual improvement.

Information Security Manager (or ISMS Manager)

The Information Security Manager shall:

- Maintain the ISMS.
- Coordinate risk assessments.
- Monitor security performance.
- Report ISMS performance to management.
- Coordinate internal audits and management reviews.

Department Managers

Department Managers shall:

- Ensure compliance with security policies.
- Identify information security risks.
- Support implementation of security controls.
- Ensure employees receive appropriate training.

Employees and Users

All users shall:

- Comply with information security policies and procedures.
- Protect organisational information.
- Report suspected security incidents promptly.
- Complete mandatory security awareness training.

7. Information Security Principles

The organisation shall protect information by implementing controls that support:

- Confidentiality
- Integrity
- Availability
- Authenticity
- Accountability
- Non-repudiation where applicable

Security controls shall be selected based on risk assessments and business requirements.

8. Compliance Obligations

The organisation shall comply with:

- Applicable laws and regulations.
- Customer and contractual requirements.
- Industry standards.
- Internal policies and procedures.
- Privacy and data protection obligations where applicable.

9. Security Awareness

The organisation shall ensure that:

- Personnel receive appropriate security awareness training.
- Employees understand their security responsibilities.
- Specialized training is provided where necessary.
- Security awareness activities are conducted regularly.

10. Incident Management

All personnel shall immediately report actual or suspected information security incidents.

The organisation shall:

- Record security incidents.
- Investigate incidents.
- Implement corrective actions.
- Learn from incidents to improve security.

11. Business Continuity

Information security shall be integrated into business continuity and disaster recovery planning to ensure critical information and services remain available during disruptions.

12. Performance Evaluation

The organisation shall monitor the effectiveness of the ISMS through:

- Internal audits.
- Management reviews.
- Security metrics and KPIs.
- Risk reviews.
- Corrective actions.
- Continuous monitoring where appropriate.

13. Continual Improvement

The organisation is committed to continually improving the suitability, adequacy, and effectiveness of the ISMS by:

- Addressing nonconformities.
- Implementing corrective actions.
- Reviewing risks.
- Updating policies and procedures.

- Monitoring changing business, legal, regulatory, and technological environments.

14. Policy Compliance

Failure to comply with this policy may result in disciplinary action, contractual remedies, or legal action where appropriate.

Any exceptions to this policy must be documented, risk assessed, approved by authorized management, and reviewed periodically.

Approval

By approving this policy, Executive Management confirms its commitment to establishing, implementing, maintaining, and continually improving the organisation's Information Security Management System in accordance with ISO/IEC 27001:2022.