Information Security Management Policy

1. Purpose

Shred-X and Med-X are committed to protecting the confidentiality, integrity, and availability of information assets, ensuring the security of customer, employee, supplier, and company information.

This policy establishes the framework for maintaining an effective Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2022 and supports the organisation's strategic objectives, legal obligations, and customer requirements.

2. Scope

This policy applies to all employees, contractors, consultants, temporary staff, third-party service providers, and any person with access to Shred-X and Med-X information, systems, applications, facilities, or services.

3. Policy Statement

Shred-X and Med-X will:

- Maintain and continually improve an Information Security Management System (ISMS) aligned with ISO/IEC 27001:2022.
- Identify, assess, and treat information security risks using a structured risk management process.
- Protect information assets against unauthorised access, disclosure, alteration, loss, or destruction.
- Comply with applicable legal, regulatory, contractual, and customer security requirements.
- Implement and maintain appropriate information security controls as defined in the Statement of Applicability.
- Ensure information security responsibilities are assigned and understood throughout the organisation.
- Provide ongoing information security awareness, education, and training to personnel.
- Monitor, review, and measure the effectiveness of security controls and ISMS objectives.
- Promptly identify, report, manage, and learn from information security incidents.
- Support business continuity and resilience through effective security and recovery planning.
- Promote a culture of security awareness and continual improvement across the organisation.

4. Roles and Responsibilities

Leadership is responsible for providing direction, resources, and oversight of the ISMS.

Managers are responsible for implementing security requirements within their areas of responsibility and ensuring compliance with this policy.

All personnel are responsible for:

- Protecting information assets under their control.
- Following approved security policies and procedures.
- Reporting security incidents, vulnerabilities, and suspected breaches immediately.
- Completing required security awareness training.

5. Risk Management

Information security risks shall be identified, assessed, treated, monitored, and reviewed through the organisation's risk management framework. Security controls will be selected and maintained to reduce risks to acceptable levels and support business objectives.

6. Compliance

Shred-X and Med-X will maintain compliance with applicable legislation, privacy obligations, contractual commitments, and ISO/IEC 27001:2022 requirements. Compliance will be verified through monitoring, internal audits, management reviews, and external certification audits.

7. Continual Improvement

The ISMS will be reviewed regularly to ensure its ongoing suitability, adequacy, and effectiveness. Opportunities for improvement identified through audits, incidents, risk assessments, customer feedback, and management reviews will be implemented where appropriate.

8. Approval

This policy is approved by Senior Management and is communicated to all personnel and relevant interested parties. It will be reviewed at least annually or whenever significant business, regulatory, technological, or security changes occur.

General Manager:
June 2026

Document Control

This Policy remains a controlled document for the nominated facility, Head Office Ormeau.

Changes are prompted by the Document Owner; updates are issued for approval.

All unauthorised copies either electronic or printed are considered uncontrolled documents.

Document Name:	SXMXISMSPOL001 Information Security Management System Policy v3.2 06/2026
Document Owner:	National IMS Manager
Approved By:	Infrastructure Manager - FIS AU
Approval Date:	03/06/2026

Version #	Date	Summary of Change	Updated By
1.0	07/2020	New Document	National IMS Manager
2.0	06/2022	Reviewed & updated	National IMS Manager
3.0	06/2024	Reviewed & updated	National IMS Manager
3.1	06/2025	Reviewed & updated	National IMS Manager
3.2	06/2026	Reviewed & reformatted onto New Document Control Format, previously SXMXNATPO001	National IMS Manager

Support Documentation / References

- ISO/IEC 27001 standard, clauses 5.2 and 5.3
- Statement of Applicability
- List of Legal, Regulatory and Contractual Obligations
- Business Continuity Plan
- Incident Security Management Procedure
- Information Security Management System Manual