LMS-IT500
Laxton Information Security

Document Number: 1.2

Date: June 2026

Change History

Date Updated	Changes Applied	Updated By
April 2024	Initial document drafting	Charles Grove
June 2025	Minor wording and formatting changes	Hennie Meeding
August 2025	Added infosec training statement	Charles Grove
June 2026	Added references to LMS-IT523 (PKI), LMS-IT524 (IPSEC VPN), and LMS-IT525 (Zabbix Monitoring)	Charles Grove

Contents

1 Purpose 4

2 Scope 4

3 Referenced Documents and Policies 4

4 Information Security Policy Statement 4

5 Roles and Responsibilities 5

6 Threat Intelligence 5

7 ISMS Governance 6

7.1 Overview 6

7.2 Top Management Commitment 6

7.3 Incident Preparedness and Planning 6

7.4 Compliance with Information Security Policies 7

8 Security Objectives 7

9 Risk Management 7

10 Information Security Controls 7

11 Training and Awareness 8

12 Compliance and Monitoring 8

13 Review and Approval 8

1 Purpose

This policy establishes Laxton's commitment to protecting its information assets through the implementation of an Information Security Management System (ISMS) aligned with ISO/IEC 27001. It defines objectives, governance, and scope of information security across all business units, systems, and staff.

2 Scope

This policy applies to all employees, contractors, third-party vendors, and systems handling or processing Laxton's data, including cloud-hosted environments (Microsoft 365, Azure, DevOps), on-prem infrastructure, and BYOD / endpoints.

3 Referenced Documents and Policies

This policy refers to the following documents and policies:

- LMS-IT504 – Risk Management
- LMS-IT501 – Acceptable Use and Data Protection
- LMS-IT511 – Endpoint Security and Device Management
- LMS-IT512 – Digital Access

4 Information Security Policy Statement

Laxton is committed to ensuring the confidentiality, integrity, and availability of its information assets through the implementation, maintenance, and continual improvement of an Information Security Management System (ISMS) aligned with ISO/IEC 27001.

This policy provides direction and support for information security in accordance with business requirements, relevant laws, and regulatory obligations.

The objectives of this policy are to:

- Protect Laxton's information assets against all internal, external, deliberate, or accidental threats.
- Ensure that information is protected from unauthorized access and that the confidentiality of information is assured.
- Maintain the integrity of information and ensure its accuracy and completeness.
- Ensure the availability of information and associated services when required by the business.

- Establish risk-based controls and a continuous improvement approach to adapt to evolving threats.

This policy applies to all employees, contractors, third parties, and systems involved in processing Laxton's information. Senior management shall ensure the implementation of this policy and its integration into all business functions.

5 Roles and Responsibilities

To support the effective implementation and operation of the Information Security Management System (ISMS), Laxton defines clear roles and responsibilities for information security throughout the organization.

- **Executive Management** is responsible for endorsing this policy and providing the necessary resources and direction to implement and maintain the ISMS.
- **Information Security Officer (ISO) (as part of the Technical Director's role)** is responsible for managing the ISMS, monitoring risks, advising management on security issues, and coordinating incident response and compliance efforts.
- **IT Department** is responsible for the implementation and maintenance of technical controls, system hardening, user access, monitoring, and endpoint security.
- **Department Heads and Managers** must ensure that staff under their supervision follow security procedures and complete relevant training.

All Employees, Contractors, and Third Parties must comply with the information security policies and procedures and report any observed or suspected security weaknesses or incidents. Roles and responsibilities are documented, communicated, and reviewed regularly to ensure continued alignment with Laxton's business and regulatory requirements.

6 Threat Intelligence

Laxton maintains a proactive approach to identifying and responding to emerging threats by leveraging internal monitoring capabilities and external threat intelligence sources.

The Information Security Officer (ISO) or a designated security function is responsible for:

- Collecting, analyzing, and disseminating threat intelligence relevant to Laxton's industry, technology stack, and regulatory environment.
- Subscribing to credible threat intelligence feeds, government advisories, and cybersecurity forums (e.g., ISACs, CERTs, vendor bulletins).
- Integrating threat intelligence into risk assessments, incident response, and change management processes.
- Ensuring that relevant teams are informed of actionable threats and mitigation strategies in a timely manner.

Threat intelligence supports Laxton's ability to detect, prevent, and respond to evolving cyber risks and to continually enhance the organization's security posture.

7 ISMS Governance

7.1 Overview

- The ISMS is led by the Chief Technology Officer (CTO) (as part of Technical Director's role).
- The Information Security Officer (ISO) is responsible for day-to-day ISMS implementation.
- Security roles and responsibilities are defined across departments and documented in operational procedures.
- Security is embedded in all business and IT processes through collaboration between IT, HR, Legal, and Operations.

7.2 Top Management Commitment

Laxton's executive leadership is accountable for ensuring the success of the ISMS through visible support and active involvement.

Management is responsible for:

- Aligning the ISMS with business goals and regulatory obligations
- Approving security objectives and strategic direction
- Providing resources for implementation and ongoing improvement
- Reviewing ISMS performance through scheduled management reviews
- Promoting a culture of security across the organization

7.3 Incident Preparedness and Planning

Cross-reference with LMS-IT503:

- Laxton maintains an Incident Response Plan (IRP) to respond to and recover from security incidents.
- This plan includes defined roles, communication procedures, escalation paths, and integration with business continuity.
- Periodic tabletop exercises and post-incident reviews are used to validate readiness.
- See LMS-IT503 – Incident Response Policy for operational procedures.

7.4 Compliance with Information Security Policies

- All Laxton employees, contractors, and third parties must comply with the organization's information security policies and procedures.
- Non-compliance is subject to disciplinary action, including revocation of access and potential legal consequences.
- Regular awareness training and internal audits support policy adherence.
- Departments must ensure local processes are aligned with ISMS expectations.

8 Security Objectives

- Protect the confidentiality, integrity, and availability of Laxton's data.
- Comply with applicable legal, contractual, and regulatory requirements (e.g., GDPR, POPIA).
- Prevent and respond to information security incidents.
- Promote security awareness and accountability across the organization.
- Ensure business continuity through proactive risk and disaster planning.

9 Risk Management

Security risks will be identified, assessed, and treated according to Laxton's risk management methodology. The risk register will be reviewed quarterly, and treatment plans implemented based on priority and impact.

10 Information Security Controls

Laxton will implement ISO/IEC 27001 Annex A control categories to address identified risks, including:

- Access Control
- Cryptographic Controls
- Physical and Environmental protection
- Secure development and operations
- Incident response and recovery
- Supplier and service provider management

11 Training and Awareness

All staff must complete annual security awareness training. Department-specific training will be provided where applicable (e.g., for developers, finance, or IT admins).

We make use of Infosec for Security Awareness and Phishing Training.

12 Compliance and Monitoring

Compliance with this policy will be monitored via internal audits, reviews, and automated tools where applicable. Non-compliance or security violations may result in disciplinary actions and remediation procedures.

13 Review and Approval

This policy will be reviewed and updated during its annual review cycle, or as significant changes are made to device policy configurations.

Charles Grove

Reviewed by:
Charles Grove
IT Manager

7/27/2026

Hendrik Meeding

Approved by:
Hennie Meeding
Chief Operating Officer

7/27/2026