Seventh loop Tech

ISMS SCOPE DOCUMENT

Code:	006
Version:	0.1
Date of version:	2025/08/21
Created by:	Hammad Zahid Ali
Approved by:	Taimor Ijlal
Confidentiality level:	Internal

Change history

Date	Version	Created by	Description of change
2025-08-23	0.1	Hammad	Scope documentation update in sections

Table of contents

1. Purpose, scope and users

The purpose of this document is to clearly define the boundaries of the Information Security Management System (ISMS) in Seventh Loop Tech.

This document is applied to all documentation and activities within the ISMS.

Users of this document are members of Seventh Loop Tech management, members of the project team implementing the ISMS, and all employees, contractors and relevant third parties who are involved in or affected by, information security activities within the defined scope.

2. Reference documents

- ISO/IEC 27001 standard, clause 4.3
- Project Plan document for ISO 27001 implementation
- List of legal, regulatory, contractual and other requirements

3. Definition of ISMS scope

The organization needs to define the boundaries of its ISMS in order to decide which information it wants to protect. Such information will need to be protected no matter whether it is additionally stored, processed or transferred in or out of the ISMS scope. The fact that some information is available outside of the scope doesn't mean the security measures won't apply to it – this only means that the responsibility for applying the security measures will be transferred to a third party who manages that information.

Taking into account the legal, regulatory, contractual and other requirements, the ISMS scope is defined as specified in the following items:

3.1. Processes and services

The Information Security Management System (ISMS) of Seventh Loop Tech covers the following business processes and services:

- Software Development Services – Design, development, testing, and deployment of enterprise applications and mobile games.

- Cloud Infrastructure Management – Operation and administration of cloud-hosted environments on AWS and GCP.

- Corporate IT Services – Management of internal IT systems, networks, and communication platforms.

- Information Security Governance – Risk assessments, security compliance monitoring, and incident management.

- Customer Support Services – Handling customer queries, support tickets, and related data securely.

- Third-Party Vendor Management – Oversight of suppliers and contractors involved in providing IT or business services.

3.2. Organizational units

The ISMS scope includes the following organizational units of Seventh Loop Tech:

- Information Security & Compliance Department – Responsible for governance, risk, compliance, and oversight of information security initiatives.

- Cloud & Infrastructure Team – Manages cloud hosting environments (AWS, GCP) and ensures secure infrastructure operations.

- Application Development & Maintenance (Cybersecurity Products) – Involved in the design, development, and maintenance of cybersecurity-related applications and solutions.

- IT Operations & Support – Provides internal IT services, endpoint management, and secure system administration.

Below organizational units are separated from the following non-included units, which are outside the scope of the ISMS:

- Human Resources (Payroll & Recruitment) – Limited to HR administrative functions, no involvement in sensitive information systems.

- Finance & Accounting (General Ledger & Bookkeeping) – Handles financial transactions but does not directly impact information security processes.

- Sales & Marketing – Engaged in promotional and business development activities not related to confidential client or security-critical data.

- Facilities & General Administration – Non-IT services including building management, cafeteria, and welfare activities.

3.3. Locations

The ISMS scope for Seventh Loop Tech includes the following locations:

- Head Office – New Yok, USA: This location houses the corporate IT infrastructure, development teams, and primary management functions.

- Cloud Infrastructure (AWS and Microsoft Azure): These environments host the company’s production systems, customer applications, and data storage.

- Backup Data Center – Toronto, Canada: Used for disaster recovery and business continuity purposes.

Exclusions:

- Remote Employees' Home Offices: While remote staff follow security policies (e.g., VPN usage, MFA, endpoint protection), their physical home networks are not directly managed by the ISMS.

Justification: These are privately owned residences outside the direct control of Seventh Loop Tech. Although excluded as physical locations, information security risks are addressed through enforced policies such as secure VPN connections, multi-factor authentication, device encryption, and endpoint protection.

- Third-party Vendor Offices: Vendors providing HR and payroll processing operate under their own ISMS and contractual agreements, hence excluded from Seventh Loop Tech's direct ISMS scope.

Justification: These locations are operated and managed by third-party service providers. Seventh Loop Tech ensures security of related processes and data through legally binding contracts, service-level agreements (SLAs), and vendor risk management practices. The ISMS scope covers vendor management controls but not the vendors' physical premises.

- Branch Sales Offices (Non-IT Dependent)

Justification: These offices are used solely for customer meetings and administrative activities, with no processing, storage, or transmission of sensitive information assets. All sales-related data is processed and stored on cloud infrastructure, which is already included in the ISMS scope.

Separation:

Excluded locations are controlled via access restrictions, vendor contracts, and security policies to ensure they do not compromise the ISMS in scope.

3.4. Networks and IT infrastructure

Networks and IT Infrastructure Included in Scope

The ISMS covers the following networks and IT infrastructure:

1. Corporate LAN & Wi-Fi (Head Office – New York)

    - Used by employees for daily operations.

    - Segmented into Employee VLAN and Guest VLAN to prevent unauthorized access to corporate resources.

2. Cloud Infrastructure (AWS & Microsoft Azure)

    - Includes virtual servers, storage, databases, and security services hosting production and development environments.

    - Access restricted via VPN and role-based access controls (RBAC).

3. VPN & Remote Access Infrastructure

- Secure VPN gateways and firewalls enabling remote employees to access corporate resources.

- Enforced with Multi-Factor Authentication (MFA) and device compliance policies.

4. Endpoint Devices (Laptops, Desktops, Mobile Devices)

- Company-owned devices with full-disk encryption, endpoint protection, and Mobile Device Management (MDM).

3.5. Exclusions from the scope

Networks and IT Infrastructure Not Included in Scope

1. Remote Employees' Home Networks

- Excluded, as they are outside direct operational control of Seventh Loop Tech.

- Logical separation maintained: employees can only connect via secured VPN tunnels; no direct connection from home networks to corporate LAN.

2. Third-Party Vendor Networks (HR & Payroll Systems)

- Managed and secured by the service provider.

- Data exchange occurs via encrypted channels (HTTPS, SFTP) only; no network interconnection with corporate LAN.

3. Branch Sales Offices (Internet & Local Wi-Fi)

- Excluded, as no sensitive information is stored or processed locally.

- Staff connect directly to approved cloud applications over secure HTTPS without accessing corporate LAN.

Separation Mechanisms

- Network Segmentation: Corporate LAN is segmented into production, development, and guest networks with firewall enforcement.

- VPN Enforcement: Only authenticated devices with MDM compliance can connect to internal networks.

- Firewall Rules: Prevent traffic from excluded networks (home ISPs, vendor networks, branch Wi-Fi) to corporate infrastructure.

- Cloud IAM Controls: Separate access policies for production and development environments to avoid cross-environment risks.

4. Validity and document management

This document is valid as of 2025/12/30.

The owner of this document is CISO, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- number of incidents arising from unclear definition of the ISMS scope
- number of corrective actions taken due to an inadequately defined ISMS scope
- time put in by employees implementing the ISMS to resolve dilemmas concerning the unclear scope

CISO
Taimor Ijlal

____

[signature]