

Information Security Policy

Luxsoft N.V.

CONFIDENTIAL



(SMES) Solutions for Management and Employment Support N.V.

Managing Director

14.11.2025

This Document is intended only for the following users:

<u>User Types</u>
General Users (All Employees)

Version Control:

<u>Document Version</u>	<u>Document Author</u>	<u>Approved By</u>	<u>Document Purpose</u>	<u>Release Date</u>
1.0	Ms. Iryna Kozlova – CCISO	Mr. Anatolii Snehirov – UBO	Initial Release	12/11/2025

Table of Contents

1.	Purpose	3
2.	Scope	3
3.	Policy Statements	3
4.	Responsibilities	4
4.1.	The Certified Chief Information Security Officer (CCISO)	4
4.2.	The Management of the Company	5
4.3.	Employees, Contractors, and Other Third-Party Personnel	5
5.	Acceptable Use	6
5.1.	Purpose	6
5.2.	General Use and Ownership	6
5.3.	Security and Proprietary Information	6
5.4.	Prohibited Activities	7
6.	Email Usage	7
6.1.	Purpose	7
6.2.	Ownership	7
6.3.	Requirements	7
7.	Internet Usage	8
7.1.	Purpose	8
7.2.	Requirements	8
7.3.	Non-Business Browsing	8
8.	Policy Compliance	8
9.	Enforcement	9

1. Purpose

This Information Security Policy outlines Luxsoft N.V.'s commitment to safeguarding the confidentiality, integrity, and availability of its information assets. The policy ensures that appropriate measures are in place to protect the company, its business partners, and stakeholders from risks associated with information security, in compliance with the Curaçao laws, CGA regulations, international information security standards. This policy establishes a framework for managing information security risks, supporting business operations, and ensuring compliance with legal, regulatory, and contractual obligations.

2. Scope

This policy applies to all information assets owned, managed, or processed by Luxsoft N.V., including data held on computer systems, networks, and other media. It covers all employees, contractors, third-party vendors, and systems involved in the company's operations, including those with access to Luxsoft N.V.'s information systems.

3. Policy Statements

Luxsoft N.V. maintains and communicates an Information Security Management System consisting of topic-specific policies, standards, procedures and guidelines that:

1. Serve to protect the Confidentiality, Integrity, and Availability of the Information Resources maintained within the Company using administrative, physical and technical controls.
2. Provide value to the way we conduct business and support institutional objectives.
3. Comply with all regulatory and legal requirements, including:
 - Remote gambling and software technical standards
 - Contractual agreements
 - All other applicable laws or regulations

Current document is developed in order to ensure that:

- Information will be protected against unauthorized access;
- Confidentiality of information will be assured;

Integrity of information will be maintained;

- Regulatory and legislative requirements will be met;
- Continuity plans will be produced, tested and maintained;
- Information security awareness amongst all staff will be created;
- All breaches of information security, actual or suspected, will be reported to, and investigated by the person or persons responsible for security;
- Copyright of intellectual property will be respected; and
- Information will be protected against malicious code.
- The information security policies are reviewed no less than annually or upon significant changes to the information security environment.

4. Responsibilities

4.1. The Certified Chief Information Security Officer (CCISO)

The CCISO is responsible for:

- Maintaining the policies and providing advice on information security and guidance on their implementation.
- Ensure compliance with applicable information security requirements.
- Formulate, review and recommend information security policies.
- Approve supporting procedures, standards, and guidelines related to information security.
- Provide clear direction and visible management support for information security initiatives.
- Assess the adequacy and effectiveness of the information security policies and coordinate the implementation of information security controls.
- Ensure that ongoing security activities are executed in compliance with policy.
- Review and manage the information security policy exception request process.
- Review information security incident information and recommend follow-up actions.
- Promote information security education, training, and awareness throughout the Company, and initiate plans and programs to maintain information security awareness.

4.2. The Management of the Company

The Management of the Company is responsible for:

- Implementing this policy within their business area and to ensure that all employees understand their obligation to protect the Company's assets and comply with security standards and related procedures.
- Ensure that an appropriate risk-based Information Security Program is implemented to protect the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of the Company.
- Ensure that information security processes are integrated with strategic and operational planning processes to secure the organization's mission.
- Ensure adequate information security financial and personnel resources are included in the budgeting and/or financial planning process.
- Ensure that the Security Team is given the necessary authority to secure the Information Resources under their control within the scope of the Company Information Security Management system.
- Designate an Information Security Manager (CCISO) and delegate authority to that individual to ensure compliance with applicable information security requirements.
- Ensure that the Information Security Manager (CCISO), in coordination with the Security Team, reports annually to Executive Management on the effectiveness of the Information Security Management.

4.3. Employees, Contractors, and Other Third-Party Personnel

All Employees, Contractors, and Other Third-Party Personnel are responsible for:

- Understand their responsibilities for complying with all Information Security Policies and procedures.
- Use Company's Information Resources in compliance with all Information Security Policies.
- Seek guidance from the Information Security Team for questions or issues related to information security.
- Conduct themselves in an ethical manner.

- Data/information obtained inappropriately should not be used.
- Finding a system weakness is not a license to take advantage of it.
- Every user has a responsibility to carry out his/her work diligently and will be held accountable for misuse of the Company's computer systems.
- When the confidentiality of information is unclear, its classification should be ascertained.
- Report any known violation or system weakness to the person or persons responsible for the Company's security or to your line manager.
- All intrusions should be reported, investigated and the Incident Response Policy should be adhered to.

5. Acceptable Use

5.1. Purpose

This section outlines the acceptable use of Luxsoft N.V.'s information systems, including computers, networks, software, and data, to support business operations while minimizing security risks.

5.2. General Use and Ownership

- All data created or stored on company systems is the property of Luxsoft N.V.
- Employees may use systems for incidental personal purposes, provided it complies with this policy and does not interfere with business operations.
- The company may monitor systems, networks, and data for security and compliance purposes.
- Sensitive or confidential information must be encrypted or password-protected.

5.3. Security and Proprietary Information

- Employees must secure passwords and accounts, using password-protected screensavers (activated within 5 minutes of inactivity) or logging off when unattended.
- Confidential information (e.g., customer data, business strategies, or trade secrets) must not be left accessible to unauthorized individuals.

- Portable devices containing sensitive data must use secure encryption.
- Employees must not post company-related content to external platforms without approval, and any approved postings must include a disclaimer that opinions are personal unless part of official duties.
- All devices connected to the company network must run approved antivirus software with updated definitions.

5.4. Prohibited Activities

The following are strictly prohibited:

- Violating intellectual property rights, including unauthorized copying or distribution of software, music, or other copyrighted materials.
- Introducing malicious programs (e.g., viruses, worms, or Trojan horses).
- Sharing account credentials or allowing unauthorized access to company systems.
- Transferring sensitive data to personal devices without management approval.
- Engaging in activities that violate local or international laws, including sexual harassment or hostile workplace laws.
- Conducting security breaches, such as accessing unauthorized data or systems.
- Performing network monitoring, port scanning, or other activities that intercept data not intended for the user, unless authorized.
- Distributing fraudulent offers or warranties not part of job duties.

6. Email Usage

6.1. Purpose

Email systems are provided for business purposes to support Luxsoft N.V.'s operations.

6.2. Ownership

All emails created, sent, or received via company systems are the property of Luxsoft N.V. The company reserves the right to access and disclose email contents as needed.

6.3. Requirements

- Emails must be treated as formal business communications.
- Sensitive data in emails or attachments must be encrypted and not sent in clear text over the internet.
- Distribution of copyrighted or proprietary information via email requires management approval.
- Prohibited content includes offensive, harassing, or discriminatory material, chain letters, or unverified virus warnings.
- Employees must not open executable email attachments (e.g., .exe, .vbs) from unknown sources.
- Incidental personal use is permitted but subject to the same rules as business emails.

7. Internet Usage

7.1. Purpose

Internet access is provided to conduct Luxsoft N.V.'s business operations.

7.2. Requirements

- Internet access must use approved software and company gateways.
- Accessing illicit, hacking, or dubious websites is prohibited.
- Downloading software or executable files requires management approval.
- Web browsing leaves a trail, and employees must exercise caution.
- Technicians requiring access to specific sites for security purposes must obtain prior approval and use isolated systems.

7.3. Non-Business Browsing

Limited personal browsing is permitted during breaks, subject to compliance with this policy.

8. Policy Compliance

The Information Security Team will verify compliance through methods such as audits, system reviews, and incident reports. Exceptions to this policy require prior approval from the CISO.

9. Enforcement

Violations of this policy may result in disciplinary action, including termination of employment, and potential civil or criminal penalties. Vendors or contractors violating the policy may face sanctions, including termination of contracts or loss of access rights.

By: **UBO of Luxsoft N.V.**

Name: Anatolii Snehirov

Date: 12.11.2025

Signature

A handwritten signature in blue ink, appearing to be 'AS', written over a light blue horizontal line.