სილქნეტი
SILKNET

INFORMATION SECURITY POLICY

Verion 2.0
Silknet JSC
2025

Table of Contents

1. Glossary

Information security – Ensuring confidentiality, integrity, and availability of information;

Information Security Policy – A set of norms and principles developed based on the Law of Georgia on Information Security and other normative acts, international standards and other treaties, that serve to ensure information security for JSC Silknet (hereinafter "Silknet", "Company" or "Organisation");

Information – A set of data that has a purpose and an intended use. Information may exist in various forms: printed or handwritten on paper, stored in an electronic form, transferred directly or as a copy/electronic copy, by email or electronic media, digital devices, verbally or through other means;

Information System – *A*ny combination of information technology and actions carried out by using such technology that facilitates the management and/or decision-making;

Information Asset (hereinafter "Asset") – All information and knowledge (particularly, technological means for the storage, processing, and transfer of information, personnel and their knowledge of information processing) that is valuable to Silknet;

Information Asset Owner – An individual or a structural unit that has the mandated and regulated rights and responsibilities to develop, manage, control, develop, support and protect an asset;

Information Security Risk Owner – An individual or a structural unit responsible and authorized to identify, evaluate and manage the risks associated with information assets;

Confidentiality – A characteristic of an asset that implies its availability exclusively to authorized individuals or processes, based on a prior request;

Integrity – A characteristic of the accuracy and completeness of an asset, an undisputed knowledge that data and information is correct, unchanged by authorized individuals and reflect facts accurately;

Availability – Based on the request of an authorized individual, a characteristic of accessibility and usability, i. e. an undisputed knowledge that the information will be available to the authorized individuals in the required form whenever needed;

Control – A combination of organisational and/or technical measures that change the risk level by preventing realisation of threat, eliminating vulnerability or minimising the impact;

Threat – a potential reason for an undesired event;

Information Security Risk (hereinafter – "Risk") *– A likelihood that an information security threat will exploit the vulnerability of an information security asset or assets and cause negative impact to the Organisation;* ssss

Vulnerability – A weakness of an asset or a control that may be exploited by one or more threats;

Impact – Damage (e. g., financial or reputational) that may be inflicted to the Organisation in the event of risk realization;

Information Security Incident - An undesired or unexpected information security event or series of events that can compromise business operations and create an information security threat.

2. Policy Purpose and Scope

Digital information and hardcopy documents, as well as the processes, people, software and hardware, corporate network, **information systems** and media devices that are involved in processing such information, are the valuable **information assets** for Silknet. Therefore, it is a strategic goal of the Company and its management to protect **confidentiality**, **integrity** and **availability of such information assets.**

The purpose of this Policy is to develop a comprehensive and consistent approach to **information security** management. In addition, the Policy is aimed at ensuring the development of the processes and **controls** that will contribute to timely identification of **information security risks**, as well as improving the planning, implementation and **monitoring** of **information assets processing practices.**

This Policy applies to all Silknet personnel, temporary workers, contractors and all the individuals who have access to the Company's information assets. Next to this, the information security principles laid out in this Policy should be adhered whenever a new initiative / process is planned throughout the Company.

Violation of the Policy may be considered serious breaches of trust, which can result in disciplinary action up to and including termination of employment and/or compensation of damages by the violating party.

This Policy is aligned to the Law of Georgia on Information Security and ISO/IEC 27001:2013 Security Standard.

The organization, due to its specifics, processes a large amount of personal data. That is why the organization is obliged to properly protect the legality of personal data processing, in accordance with the Law of Georgia on Personal Data Protection.

3. Information Security Objectives and Principles

Information Security Objectives

Application of **information security** in Silknet aims to achieve the following objectives:

- Protect **confidentiality, integrity** and **availability of information assets;**
- Identify and mitigate **information security risks** to acceptable level by implementing **risk** treatment plans;
- Safeguard the information of employees, subscribers, suppliers and business partners;
- Comply with applicable security laws, regulations, and contractual requirements;
- Continuously improve the **information security** policies, processes and documentation;
- Develop positive **information security** culture and awareness among employees.

Information Security Principles

This Policy is based on the following **information security** principles:

- **Supporting the mission and strategy of Silknet**: mitigating the risks caused by **information security** threats by integrating **information security** into the Company's business processes;
- **Fostering a positive security culture:** providing effective **information security controls** that support the needs of Silknet; building effective interaction between the Information Security Unit and other business units in insuring the proper information security;
- **Delivering quality and added value**: the costs incurred for implementation of **information security controls** are in proportion to the risks arising from **information security threats** and their potential **impact**;
- **Clearly defining role and responsibilities**: **information security** is the responsibility of every Silknet employee. Besides, Silknet ensures that key roles and responsibilities are formally defined and assigned to individuals with appropriate authorities;
- **Utilizing a risk-based approach**: timely identification of **information security risks** through a consistent and repetitive process and their minimization to an acceptable level by means of optimal risk treatment plans. Integration of risk assessment outcome into the decision-making process;
- **Promoting continuous improvement**: Silknet operates in a dynamic business and technological environments. **Information security risk** landscape is continuously evolving. **Information security management** is therefore periodically re-evaluated, reviewed and improved to ensure that appropriate organizational and technical controls are in place.

4. Information Security Management

For effective and efficient realization of **information security** principles and objectives, Silknet has implemented the **Information Security Management System (ISMS).** The system is based on the iterative model of continuous improvement (i.e., Deming Cycle) and aims the regular evaluation of the constantly changing business environment, organisational context and threat landscape, as well as their integration into the **ISMS**. Further details about **ISMS** planning, operation, monitoring and continuous improvement are provided in the Information Security Management System Policy.

The detailed information on the scope of the **ISMS** is provided in the **Information Security Context, Requirements and Scope** document, which takes into account the Company's internal and external factors, the needs and expectations of key stakeholders (e. g., shareholders, directors, employees, regulators, subscribers, etc.), as well as applicable legal, regulatory and contractual requirements.

Information Security Risk Management

The effectiveness of **information security** is primarily dependent on the ability of Silknet to timely identify and assess the risks related to its **information assets** and implement necessary **controls** to mitigate them to the acceptable level.

Information security risks are identified and managed as part of a regular **risk** assessment process, as well as **ISMS** internal and external audit, management of **information security incidents** and other operational activities, as described in the Information Security Risk Assessment & Treatment Policy.

Information Security Risk Owner is responsible for development, approval and implementation of the information security **risk** treatment plan. **Risk** assessment reports together with the agreed risk treatment plans are submitted by the Information Security Manager to the **Information Security Council** for further review and monitoring.

Information Security Incidents Management

Growing complexity of Silknet technologies, close interaction with the third parties and continuous evolution of new threats significantly increases the likelihood of **information security** incidents. To this end, Silknet has developed the **Information Security Incident Management Procedure**, which is aligned to the Law of Georgia **on Information Security** and the Computer Security Incident Handling Guide published by the National Institute of Standards and Technology (NIST). The procedure establishes a comprehensive and consistent company-wide approach to responding to **information security incidents**.

5. Responsibilities

Supervisory Board

Responsible for development of the overall **information security** strategy and policy.

Information Security Council

Information Security Council includes members of the top management and is chaired by the General Director of Silknet. The purpose of the Information Security Council is to support and supervise continuous improvement of **information security**. Besides, the composition of Information Security Council allows board discussions of information security issues and consensus-based, informed decision-making.

Information Security Manager

Information Security Manager coordinates information security management across the Company; is responsible for development, periodic review and improvement of information security related policies, procedures, guidelines and rules; ensures an appropriate level of information security awareness among the Silknet personnel.

Information Asset Owner

Information Asset Owner is responsible for applying information security requirements in practice; in particular, for defining controls and monitoring their implementation to safeguard the information asset.

Each Director and Head of Business Unit

Each director and head of business unit is responsible for making sure that the principles and requirements of this Policy are properly integrated into the operations of their own business unit.

All Silknet personnel, temporary workers, contractors and third parties who have access to **Silknet's information assets**, are individually responsible for reading, understanding and following this Policy. Their responsibilities also include immediately informing the Information Security Management about any violation of this Policy.

6. Document Revision

The owner of this Policy is the Information Security Manager who is responsible for reviewing the document at least annually or in case of major changes to the organisational context, updating it as needed and submitting to the **Information Security Council** for further review. The Policy reviewed by and agreed with the Information Security Council is ultimately approved by the General Director of Silknet.

7. Requirements and Restrictions

Information Ownership Right

Any information that is created, stored and processed as part of Silknet's business processes is the property of Silknet. This information is processed in accordance with the policies and procedures established throughout the Company, except when such processing is against the requirements of the applicable law.

Access control

Access to information and information processing facilities are limited to only authorized individuals based on the "**least privileges"** and "**need-to-know"** principles and is protected by effective authentication and authorisation mechanisms.

In addition, to ensure that access is legitimate and accurate, **Information Asset Owners** periodically carry out user access review and, if necessary, adjust access to information assets under their ownership accordingly.

Prohibited Software

Only software pre-approved by Silknet is allowed to be used for business purposes. As an additional control, Silknet has defined a list of non-standard and prohibited software and through appropriate monitoring tools ensures that any use of such software is promptly identified and restricted.

Data Storage and Transfer

To minimise the risks of unauthorized disclosure of information when exchanging data with subscribers, business partners and public, only pre-authorised secure storage, transfer and communication technologies are used throughout the Company.

It is strictly prohibited to use technologies other than those officially provided or authorised by Silknet. Based on Silknet's needs, in exceptional cases, a specific solution can be used only with the prior approval of the employee's line manager and the Information Security Council.

Employee Rights

Silknet allows its employees to use corporate business technologies (e.g. digital platforms of the company) for personal matters on the condition that they do so responsibly and in compliance with effective laws, regulations and requirements of Silknet's Acceptable Use Policy. As an additional control, use of business technologies for personal purposes is subject to strict monitoring from Silknet.

Password Security

Access to Silknet’s corporate resources and information is protected by effective authentication mechanisms. The security characteristics of the password used as part of authentication, are regulated by the Password Management Policy and are in line with the industry best practices. For mission-critical systems, Silknet additionally uses a two-factor authentication (2FA) mechanism, which, along with standard password requires end-users to provide an additional authentication element, such as, a randomly generated one-time password (OTP).

Use of Corporate Email

For business purposes only Silknet’s corporate email is used. Use of personal emails is restricted and strictly monitored.

Besides, as part of regular awareness trainings, employees are informed about common threats associated with the use of email, as well as the recommendations and tips on effective ways of dealing with them.

Internet Use

Internet is a major resource of running Silknet’s business activities effectively and efficiently and should be used in line with Silknet’s business interests. Use of internet by personnel is strictly monitored using various security tools to minimise the likelihood of unauthorized disclosure of information.

Antivirus and Security Updates

The devices of Silknet personnel (e. g., personal computers, laptops, mobile devices), as well as the server infrastructure are protected by effective antivirus software. End-users do not have the system privileges to delete or deactivate the antivirus on their devices or block its regular updates. Any suspicious event or file identified by the antivirus is thoroughly analysed by Information Security Unit for further prompt response.

Technical Vulnerability Management

Silknet ensures periodic vulnerability scans of the corporate network, information systems and resources. Quick response to the identified vulnerabilities, including coordination of security updates installation is the responsibility of the Information Security Unit.

8. Exceptions

All exceptions from this Policy should be approved by the Information Security Council of Silknet.