Silknet JSC

Supplier Security Rules

2024

This document (the "Security Rules") describes the security requirements applicable to suppliers of Silknet JSC (hereinafter referred to as "Silknet"). Additional security requirements may apply in particular cases if agreed between the parties.

These Rules are an integral part of the contract(s) concluded between Silknet and the supplier.

1. Definitions

1.1. "Information Asset/Information" shall mean any information and knowledge (particularly, technical means for storing, processing and transmitting information, employees and their knowledge on the processing of information), which has value for the organization and is classified as such.

1.2. "Silknet's Data" shall mean information assets that Silknet, or a person acting on behalf of Silknet, makes available to the Supplier, including but not limited to personal data, as well as any data generated as a result of Supplier's processing of such data.

1.3. "Information Processing Facilities" shall mean any information processing system, services or infrastructure, or the physical locations housing them.

1.4. "Log" shall mean to record details of information or events in an organized record-keeping system, usually sequenced in the order in which the information or events occurred.

1.5. "Personal Data" for the purposes of these Rules shall be interpreted according to the Law of Georgia on Personal Data Protection of June 14, 2023 (including any amendments thereto). According to the Law, personal data means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, including by his/her name, surname, identification number, location data and electronic communication identifiers, or by physical, physiological, mental, psychological, genetic, economic, cultural or social characteristics.

1.6. For the purposes of interpreting "Personal Data" Suppliers that are not established Georgia, may rely on General Data Protection Regulation (Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 94/46/RC) (the "GDPR").

1.7. "Supplier" shall mean the legal person/organization/union having a contractual relationship with Silknet.

1.8. "Supplier Personnel"/ "Personnel" shall mean any person working on behalf of the Supplier such as employees, consultants, contractors and sub-suppliers.

1.9. "Security Control" / "Control" shall mean a combination of organizational and/or technical measures, that modifies the level of risk by minimizing the impact, eliminating the vulnerability or preventing the materialization of threats.

1.10. "Information Security Incident"/ "Incident" shall mean a single or a series of unwanted or unexpected security events that have a significant probability of compromising business operations and threatening security. Information security incident includes, *inter alia,* any Personal Data breach/incident.

1.11. "Sensitive Information Assets" shall mean information assets classified by Silknet.

1.12. "Sensitive Product" shall mean any product provided by or to Silknet, which contains Silknet's sensitive information assets or may in any way impact Silknet's business continuity.

1.13. "Sensitive Service" shall mean any service provided by or to Silknet, which contains Silknet's sensitive information assets or may in any way impact Silknet's business continuity.

1.14. "Pseudonymisation" shall mean the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. For the purposes of interpreting "Pseudonimisation" Suppliers that are not established Georgia, may rely on GDPR.

1.15. "Depersonalisation"/ "Anonymisation" shall mean the processing of data in such a manner that the data cannot be attributed to the data subject or attributing them to the data subject involves disproportionate effort, expense and/or time. For the purposes of interpreting "Depersonalisation"/"Anonymisation" Suppliers that are not established

Georgia, may rely on GDPR.

1.16. "Personal Data Breach/Incident" shall mean breach of security of data leading to the unlawful or accidental damage or loss of data, or the unauthorised disclosure, destruction, alteration of or access to data, or the collection/obtaining of data, or other unauthorised processing. For the purposes of interpreting "Presonal Data Breach/Incident" Suppliers that are not established Georgia, may rely on GDPR.

2. Scope of Application

2.1. The Security Rules apply when:

2.1.1. The Supplier will/may access or process Silknet's Data.

2.1.2. The Supplier will/may access Silknet's information processing facilities, the locations of their supply or their perimeter.

2.1.3. The Supplier will/may access Silknet's network, information or IT systems including remote access.

2.1.4. The Supplier will/may handle Silknet's information processing, storage equipment or the equipment used for destroying such information.

2.1.5. The Silknet has deemed the Supplier as a provider of Sensitive Products and/or Sensitive Services; and/or Supplier has/may have access to Silknet's sensitive information; Supplier has/may have impact on Silknet's business continuity; and/or is identified as such.

2.2. The Security Rules apply to Supplier's personnel, and it's sub-contractors if such persons may within the scope of their activities meet or may meet any of the preconditions set out in Clause 2.1.

3. The Supplier´s overall responsibility

3.1. The Supplier is fully responsible for the Supplier Personnel's compliance with the Security Rules.

3.2. The Supplier is obligated to implement measures that ensure compliance with these Rules, as well as to adopt controls predetermined by Silknet before commencing any tasks assigned by Silknet.

3.3. Upon request from Silknet, the Supplier is obligated to inform Silknet about how it complies with the requirements of these Rules and what measures have been taken to fulfill these Rules.

3.4. Silknet is authorized, based on prior agreement, to independently assess the existing information security controls.

3.5. Upon Silknet's request, the Supplier is obligated to complete an information security questionnaire and provide the corresponding evidence.

3.6. Upon Silknet's request, the Supplier is obligated to provide documents, certificates, reports, and audit findings of vulnerability and penetration testing related to information security.

3.7. Upon Silknet's request, the Supplier must, prior to the contract coming into force or before commencing the performance of obligations defined by the contract, implement the recommendations established by Silknet, apply controls, and provide evidence of their implementation.

3.8. Upon Silknet's request, the Supplier must fulfill the information security requirements outlined in the contract, apply controls, and provide evidence of their implementation.

3.9. Silknet is authorized to regularly monitor the implemented recommendations and controls.

3.10. The Supplier must immediately notify Silknet of any information security incidents (including, but not limited to, those related to the processing of personal data).

3.11. The Supplier ensures that any processing of Silknet's data complies with these rules.

3.12. The Supplier must return or destroy (as determined by Silknet) any data, copies, and informational assets belonging to Silknet upon the termination of the contract or upon Silknet's request, and provide written confirmation of compliance with this requirement.

3.13. The Supplier shall not permit access to Silknet's data to any third party (this may also pertain to new, expanded, updated, extended, or otherwise modified real-time network or information system access) without prior written consent from Silknet.

3.14. The Supplier shall implement the measures required to ensure compliance to the Security Rules prior to commencing any assignment for the Silknet.

4. Security Requirements

4.1. Risk management

4.1.1. The Supplier shall identify and evaluate security risks related to confidentiality, integrity and availability of information and based on such evaluation implement appropriate technical and organizational measures to ensure a level of security which is appropriate to the risk and the acceptable rating.
4.1.2. The Supplier is obligated to have documented, approved, actionable, and continuous risk assessment and management processes and practices, endorsed by its leadership, to manage risks within its operations.
4.1.3. The Supplier shall periodically assess the risks related to information systems and processing, storing and transmitting of information.
4.1.4. The Supplier is obligated to establish a process for monitoring risk management activities and evaluating their effectiveness.
4.1.5. The Supplier shall identify and evaluate security risks related to information confidentiality, integrity and availability and based on such evaluation implement appropriate technical and organizational measures to ensure a level of security which is appropriate to the risk of the specific personal data types and purposes being processed by the Supplier, including inter alia as appropriate:
4.1.5.1. The pseudonymisation and encryption of personal data, as well as anonymization of personal data where possible;
4.1.5.2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
4.1.5.3. The ability to restore the availability, integrity and confidentiality of Silknet's data in a timely manner in the event of a physical or technical incident;
4.1.5.4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;
4.1.6. The Supplier shall have documented processes and routines for managing risks when processing personal data on behalf of Silknet.
4.1.7. The Supplier shall periodically assess the risks related to information systems and processing, storing and transmitting personal data.
4.1.8. The Supplier shall periodically assess risks associated business continuity risks;
4.1.9. The Supplier is obligated to implement controls in accordance with the threats and vulnerabilities arising during the period of cooperation with Silknet, to ensure the appropriate level of security.

4.2. Information security policies

4.2.1. The Supplier shall have a defined and documented information security management system (ISMS), scope, including information security policies and procedures in place, which shall be approved by the Supplier's management. They shall be published within Supplier´s organization and shared to relevant Supplier personnel.
4.2.2. The Supplier is obligated to periodically review and update security policies and procedures as needed to align with updated information security requirements, including those established by legislative and regulatory bodies.
4.2.3. Silknet is authorized to review the agreed-upon information security requirements once a year and, if necessary, modify the information security requirements to address changes in legislative or regulatory requirements or altered risk ratings.

4.3. Organization of information security

4.3.1. The Supplier shall have management approved, defined and documented security roles and responsibilities within its organization.
4.3.2. The Supplier shall appoint at least one person who has appropriate security competence and who has an overall responsibility for implementing the security measures under the Security Rules and who will be the contact person for Silknet's Information Security Unit.

4.4. Human resource security

4.4.1. The Supplier is obligated to have a management-approved, defined, and documented human resource security policy and system to ensure proper determination of employee responsibilities, background checks, and the provision of appropriate training for skill development and awareness enhancement.

4.4.2. The Supplier must ensure that its personnel handle information in accordance with the confidentiality level stipulated in the contract.

4.4.3. The Supplier is obligated to ensure that its relevant personnel have been introduced to, understand, and have confirmed adherence to the management-approved acceptable use policy within the organization. They must also be aware of the information, facilities, and business technology security rules and requirements agreed upon with Silknet under the contract (including any usage restrictions). Silknet is authorized to request a signed document from each of the Supplier's employees, stating that they understand, will comply with these rules, and will ensure the agreed-upon use of information, business technologies, and facilities.

4.4.4. The Supplier is obligated to ensure that any specialist performing contractually assigned tasks is trustworthy, meets the established security criteria throughout the task duration, and has undergone appropriate background checks.

4.4.5. Supplier shall not, without informing and getting the Silknet's prior written approval, assign any Supplier Personnel to Silknet's work that:

4.4.5.1. have any conflict of interest in relation to Silknet or the relevant assignment, or

4.4.5.2. has been convicted to imprisonment for any criminal offense during the three (3) year period prior to the engagement or the assignment:

4.4.5.2.1. If (a) that Supplier Personnel will in any manner process Personal Data relating to Silknet customers or staff, or to Silknet's customers'; or

4.4.5.2.2. that Supplier Personnel will assist with tasks classified as sensitive by Silknet.

4.4.6. The Silknet shall provide information about what tasks are classified as sensitive at the time of entering into the Agreement or the latest two weeks prior to a Supplier's Personnel engagement or assignment commences.

4.4.7. The Supplier shall ensure that Supplier Personnel with security responsibilities are adequately trained to carry out security related duties. The Supplier shall provide or ensure periodical security awareness training to relevant Supplier Personnel. Such Supplier training shall include, without limitation:

4.4.7.1. How to maintain customers security of information (i.e. the protection of the confidentiality, integrity and availability of information);

4.4.7.2. Why information security is needed to protect customers information and systems;

4.4.7.3. The common types of security threats (such as personal data theft, malware, hacking, data leak and insider threat);

4.4.7.4. The importance of complying with information security policies and applying associated standards/procedures;

4.4.7.5. Personal responsibility for information security (such as protecting customer's privacy-related information and reporting actual and suspected Security Incidents).

4.4.8. The Supplier is obligated to regularly inform its relevant personnel about any changes to information security policies and procedures.

4.5. Asset management

4.5.1. The Supplier is required to maintain a defined and documented policy and system for asset management approved by its management. The Supplier must also conduct regular inventory of information assets, ensuring up-to-date records of all relevant assets and their respective owners. Information assets include (but are not limited to) IT systems, backup and/or portable information carriers containing sensitive information, access permissions, software, and configurations

4.5.2. The Supplier is required to regularly assess risks associated with information assets, label, process, and protect information in accordance with predefined information classification policies and systems, as well as in compliance with applicable security standards and Georgian personal data protection legislation. This also includes, but is not limited to, the storage, disposal, physical transfer, and destruction of media processing, storing, or transmitting such information.

4.5.3. The Supplier is required to implement measures to safeguard data transmitted, stored, or processed on behalf of Silknet to the agreement from accidental, unauthorized, or unlawful loss, destruction, alteration, or damage.
4.5.4. The Supplier is required to implement measures defining restrictions and conditions related to remote work.
4.5.5. The Supplier is required to establish and enforce security measures to protect information based on its classification during remote work.
4.5.6. The Supplier is required to adopt and implement a policy regarding the use of privately owned devices, (BYOD) defining the relevant restrictions and conditions for use.
4.5.7. The Supplier is required to establish and implement security measures to protect information based on its classification when processed by privately owned devices.
4.5.8. The Supplier is required to assign appropriate classification to Silknet's data based on the classification assigned to it by Silknet and the nature of the data and ensure proper protection and handling of classified data.
4.5.9. The Supplier is required to have the following defined and documented:
4.5.9.1. Characteristics (such as personal data) and classification of Silknet data based on Silknet's confidentiality classification scheme.
4.5.9.2. Supporting information assets used in the processing, transmission, and storage of Silknet's data.
4.5.9.3. Assigned owners and responsible personnel.
4.5.9.4. Defined access permission.
4.5.9.5. Rules for secure processing, transmission, sharing, storage, and destruction of Silknet's data.
4.5.9.6. A report on the risk assessment and treatment of information assets related to Silknet's data, including defined risk owners and responsibilities.
4.5.9.7. A report on business continuity risks related to information assets associated with Silknet's data, including defined risk owners and other relevant responsibilities.
4.5.9.8. A report on the risk assessment of personal data related to Silknet, including defined risk owners and corresponding responsibilities.
4.5.10. Silknet reserves the right to request the information outlined in section 4.5.9 (in the form of an audit report) from the Supplier.

4.6. Access control

4.6.1. The Supplier shall have management-approved defined and documented access control rules and procedures for Information Processing Facilities and perimeter,, sites, network, business technologies and information systems, applications and information/data access (including physical, logical and remote access controls), an authorization process for user access and privileges, procedures for revoking access permissionand an acceptable use of access privileges for the Supplier Personnel in place.
4.6.2. The supplier shall have a formal and documented user registration and de-registration process implemented to enable assignment of access permissions.
4.6.3. The Supplier shall assign all access privileges based on the principle of need-to-know and principle of least privilege.
4.6.4. The Supplier shall use strong authentication (multi-factor) for remote access users and users connecting from untrusted network.
4.6.5. The Supplier shall ensure that the Supplier Personnel has a personal and unique identifier (user ID), and use an appropriate authentication technique, which confirms and ensures the identity of users.
4.6.6. The Supplier is required to regularly ensure the review of access permissions, privileged access permissions, and related procedures.

4.7. Cryptography

4.7.1. The Supplier is required to implement and ensure the use of modern, secure, appropriate, and effective cryptographic techniques for properly classified information, in accordance with Silknet's confidentiality classification scheme and the specific requirements of the data, such as personal data.
4.7.2. The Supplier shall protect cryptographic keys.

4.8. Physical and environmental security

4.8.1. The Supplier is required to maintain a physical security policy approved by management to ensure the appropriate security of any system, infrastructure, or physical location involved in the processing of information.
4.8.2. The Supplier shall protect information processing facilities against external and environmental threats and hazards, including power/cabling failures and other disruptions caused by failures in supporting utilities (such as electricity, data transmission cables, etc.). This includes physical and access perimeters security.
4.8.3. The Supplier shall protect goods received or sent on behalf of the Silknet from theft, manipulation and destruction.

4.8.4. Admission to Silknet's premises and Silknet's leased premises

4.8.4.1. The Supplier's admission to Silknet's premises and property (such as data processing facility buildings, office buildings, technical sites) is subject to the following:
4.8.4.1.1. The Supplier shall follow internal regulations (such as regulations for "restricted areas") for Silknet's premises when performing the assignments under the Agreement.
4.8.4.1.2. Supplier Personnel shall carry ID card or a visitor's badge visible at all time when working within the Silknet's premises.
4.8.4.1.3. After completing the assignment, or when Supplier Personnel are transferred to other tasks, the Supplier shall without delay inform the Silknet of the change and return any keys, key cards, certificates, visitor's badges and similar items.
4.8.4.1.4. Keys or key cards shall be personally signed for by Supplier Personnel and shall be handled according to the written rules given upon receipt. Loss of the Silknet's key or key card shall be reported without delay to the Silknet.
4.8.4.1.5. Photographing or audio/video recording in or at the Silknet's premises without permission is prohibited.
4.8.4.1.6. Goods shall not be removed from Silknet's premises without permission.
4.8.4.1.7. Supplier Personnel shall not allow unauthorized persons access to the premises.

4.9. Operations security

4.9.1. The Supplier shall have an established change management system in place for making changes to business processes, Information Processing Facilities and systems. The change management system shall include tests and reviews before changes are implemented, such as procedures to handle urgent changes, roll back procedures to recover from failed changes, logs that show, what has been changed, when and by whom.
4.9.2. The Supplier shall implement malware protection to ensure that any software used for the processing, transmission and storage of Silknet's data by Supplier, as well as delivery of any products or services by the Supplier is protected from malware.
4.9.3. The Supplier shall make backup copies of critical information and test back-up copies to ensure that the information integrity and availability can be restored as agreed with the Silknet.
4.9.4. The Supplier shall Log and monitor activities, such as creating, reading, copying, amendment and deletion of processed data, as well as exceptions, faults and information security events and regularly review these. Furthermore, the Supplier shall protect and store (for at least 12 months) Log information, and on request, deliver monitoring data to the Silknet. Anomalies / incidents / indicators of compromise shall be reported according to the incident management requirements 4.13.
4.9.5. The Supplier shall manage vulnerabilities of all relevant technologies such as operating systems, databases, applications proactively and in a timely manner and ensure timely implementation and management of above system updates.
4.9.6. The Supplier shall establish security baseline configurations (hardening) for all relevant technologies such as operating systems, databases, applications. In case of supply of Silknet products, based on Silnet's request the Supplier must create, agree and implement baseline security configurations.
4.9.7. The Supplier shall ensure development is segregated from test and production environment.
4.9.8. The Supplier must conduct penetration and vulnerability testing with regard to information assets related to Silknet data, products or services regularly.

4.10. Communications security

4.10.1. The Supplier shall to ensure network security monitoring and control, which includes maintaining an appropriate level of network security and implementing necessary measures. This encompasses protecting the network using a firewall, defining firewall rules and assigning responsible personnel, periodically reviewing these rules, and implementing segregation procedures to safeguard information systems and mitigate security risks.

4.10.2. The Supplier shall ensure that audio and video communication classified as confidential/ secret (as further detailed below) is secure which means that un-encrypted communication may not be used.

4.11. System acquisition, development and maintenance (when software development or system development is provided to the Silknet by Supplier)

4.11.1. The Supplier shall implement and enforce rules for development lifecycle of software and systems including change and review procedures.

4.11.2. The Supplier shall test security functionality during development in a controlled environment.

4.12. Supplier relationship with sub-suppliers

4.12.1. The Supplier shall reflect the content of this Security Rules in its agreements with sub-suppliers that perform tasks assigned under the agreement between Silknet and the Supplier.

4.12.2. The Supplier shall regularly monitor, review and audit sub-supplier's compliance with the Security Rules.

4.12.3. The Supplier shall, at the request of the Silknet, provide the Silknet with evidence regarding sub-supplier's compliance with the Security Rules or an additional security measures.

4.13. Information Security Incident management

4.13.1. The Supplier shall have established management-approved procedures for incident management.

4.13.2. All reporting of security related incidents shall be treated as confidential information and be encrypted, using industry standard encryption methods, i.e. PGP.

4.13.3. The security incident report shall contain at least the following information:

4.13.3.1. Notwithstanding the requirement for immediate notification, the Supplier shall, comprise a written preliminary report to the Silknet of any security incident that could possibly affect the Silknet, Silknet's business continuity or Silknet's assets in any imaginable way

4.13.3.2. Sequence of events, including actions taken during the incident handling

4.13.3.3. Affected infrastructure, systems and information

4.13.3.4. Estimated (or, upon a high level of uncertainty, worst-case) consequences/impact

4.13.3.5. Consequence/impact reducing measures already implemented

4.13.3.6. Risk mitigation measures already implemented

4.13.3.7. Consequence/impact reducing measures to be implemented, including implementation plan (date; responsible; dependencies)

4.13.3.8. Risk mitigation measures to be implemented, including implementation plan (date; responsible; dependencies)

4.13.3.9. Lessons learned summary.

4.13.4. The Supplier shall provide the Silknet with support in case of administrative proceedings, forensic investigation or court proceedings.

4.14. Business continuity management

4.14.1. The Supplier shall identify business continuity risks and take necessary actions to manage and mitigate such risks.

4.14.2. The Supplier shall have management-approved business continuity policy, documented processes and practices for handling business continuity.

4.14.3. The Supplier shall ensure that information security is embedded into the business continuity plans.

4.14.4. The Supplier shall periodically assess the efficiency of its business continuity management, and

compliance with availability requirements (if any).

4.15. Compliance

4.15.1. The Supplier shall comply with all relevant legislation and contractual requirements including but not limited to Personal Data protection.

4.15.2. The Supplier shall, on request, provide the Silknet with a compliance status report with regards to these Security Rules without any unjustified delay.

4.15.3. The Silknet has the right to audit how the Supplier and its sub-suppliers fulfil the Security Rules or corresponding requirements.

***