Silknet JSC

Security Policy

2019

This document (the "**Security Policy**") describes the security requirements applicable to Suppliers (as defined below) to Silknet JSC (hereinafter referred to as "**Silknet**"). Additional security requirements may apply in particular cases if agreed by involved parties.

This Policy applies to all suppliers of goods and/or services to Silknet, also to any natural or legal persons which is supplied by Silknet with goods/services and/or to any natural or legal persons that Supplier uses for the provision of the services/delivery of the goods to Silknet, including Supplier's or their contractors' employees and consultants, contractors and subcontractors regardless if they are permanently employed, temporarily contracted, directly employed or supervised.

For the purposes of this Policy, Supplier shall mean any Silknet's contracting party, based on the context of the relevant agreement.

This Policy is an integral part of the contracts concluded between Silknet and any natural or legal person.

1 Definitions

Silknet1.1 "**Silknet's Data**" shall mean data or other information that the Silknet, or a person acting on behalf of the Silknet, makes available to the Supplier, including but not limited to Personal Data, and the result of Supplier's processing of such data.
1.2 "**Information Processing Facilities**" shall mean any information processing system, services or infrastructure, or the physical locations housing them.
1.3 "**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.
1.4 "**Personal Data**" shall mean all information that, subject to applicable data protection laws, including without limitation EU Data Protection Directive (EU Directive 95/46/EC of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), Directive on privacy in electronic communications (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector) and 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) and any amendments, replacements or renewals thereof (collectively the "EU Legislation"), all binding national laws implementing the EU Legislation and other binding data protection or data security Policy, laws, regulations and rulings valid at the given time, identifies a natural person. An identifiable natural person is one who can be directly or indirectly identified by reference to an identifier such as a name, address, social security or identification number, subscription number, IP address, location data, an online identifier, traffic data or message content or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
1.5 "**Services**" shall mean the services to be provided by the Supplier to the Silknet, or a person acting on behalf of the Supplier as further defined in the Agreement between the parties.
1.6 "**Supplier Personnel**" shall mean any person working on behalf of the Supplier such as employees, consultants, contractors and sub-suppliers.
1.7 "**Security Control**" shall mean a technical countermeasure, an organizational setup or a process that helps to maintain IT systems security-quality properties.
1.8 "**Security 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.
1.9 "**Sensitive Products**" and "**Sensitive Services**" shall mean any product or services defined as sensitive by the Silknet. Sensitive Products or Sensitive Services shall be clearly documented in the applicable Agreement.

1.10 "**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.

2 Scope

2.1 The Security Policy applies when:

2.1.1 The Supplier will process Silknet's Data.
2.1.2 The Supplier will access Silknet's premises.
2.1.3 The Supplier will access Silknet's network or IT systems including remote access.
2.1.4 The Supplier will handle Silknet's information processing equipment.
2.1.5 The Silknet has deemed the Supplier as a provider of Sensitive Products and/or Sensitive Services and identified Supplier as such under the relevant Agreement.

3 The Supplier´s overall responsibility

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

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

3.3 The Supplier shall, at the request of the Silknet, inform the Silknet how the Supplier complies with the Security Policy and what measures the Supplier has taken to comply with the Security Policy.

3.4 The Supplier shall inform the Silknet about any Security Incident (including but not limited to incidents in relation to the processing of Personal Data) as soon as possible but no later than within 24 hours after the Security Incident has been identified. See "Security Incident Management" bellow.

3.5 The Supplier shall guarantee that any processing of Silknet's Data will be compliant with the Security Policy.

3.6 After termination of the Agreement, the Supplier shall return or destroy (as determined by the Silknet) any of Silknet's Data and copies thereof in Supplier's possession. The Supplier shall confirm in writing to the Silknet that the Supplier has met this requirement on termination of the Agreement or at the request of the Silknet.

3.7 The Supplier shall not allow any access to Silknet's Data (it may also concern new, extended, updated, prolonged or in any other way changed real-time network access) in breach of the Agreement to any party without prior written approval by the Silknet.

4 Security Requirements

4.1 Risk management

4.1.1 Security risk management

4.1.1 The Supplier shall identify and evaluate security risks related to 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.

4.1.2 The Supplier shall have documented processes and routines for handling risks within its operations.

4.1.3 The Supplier shall periodically assess the risks related to information systems and processing, storing and transmitting information.

4.2 Security risk management for Personal Data

4.2.1 The Supplier shall identify and evaluate security risks related to 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:

4.2.1.1 The pseudonymisation and encryption of personal data;

4.2.1.2 The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

4.2.1.3 The ability to restore the availability and access to Silknet's Data in a timely manner in the event of a physical or technical incident

4.2.1.4 A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

4.2.2 The Supplier shall have documented processes and routines for handling risks when processing Personal Data on behalf of Silknet.

4.2.3 The Supplier shall periodically assess the risks related to information systems and processing, storing and transmitting Personal Data.

4.3 Information security policies

4.3.1 The Supplier shall have a defined and documented information security management system (ISMS) including an information security policy and procedures in place, which shall be approved by the Supplier's management. They shall be published within Supplier´s organization and communicated to relevant Supplier Personnel.

4.3.2 The Supplier shall periodically review the Supplier's security policies and procedures and update them if required to ensure their compliance with the Security Policy.

4.4 Organization of information security

4.4.1 The Supplier shall have defined and documented security roles and responsibilities within its organization.

4.4.2 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 Policy and who will be the contact person for Silknet's security staff.

4.5 Human resource security

4.5.1 The Supplier shall ensure that the Supplier Personnel handles information in accordance with the level of confidentiality required under the Agreement.

4.5.2 The Supplier shall ensure that relevant Supplier Personnel is aware of the approved use (including use restrictions as the case may be) of information, facilities and systems under the Agreement. Silknet has the right to request a signed receipt from each and every Supplier Personnel stating that he or she has understood and will comply with the Security Policy and the approved use of information, systems and facilities.

4.5.3 The Supplier shall ensure that any Supplier Personnel performing assignments under the Agreement is trustworthy, meets established security criteria and has been, and during the term of the assignment will continue to be, subject to appropriate screening and background verification.

4.5.4 Supplier shall not, without informing and getting the Silknet's prior written approval, assign any Supplier Personnel to Silknet's work that (i) have any conflict of interest in relation to Silknet or the relevant assignment, or (ii) has been convicted to imprisonment for any criminal offense during the three (3) year period prior to the engagement or the assignment, if (a) that Supplier Personnel will in any manner process Personal Data relating to Silknet customers or staff, or to Silknet's customers' or (b) that Supplier Personnel will assist with tasks classified as sensitive by Silknet. 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.

4.5.5 The Supplier shall ensure that Supplier Personnel with security responsibilities are adequately trained to carry out security related duties.

4.5.6 The Supplier shall provide or ensure periodical security awareness training to relevant Supplier Personnel. Such Supplier training shall include, without limitation:

4.5.6.1 How to handle customer information security (i.e. the protection of the confidentiality, integrity and availability of information);

4.5.6.2 Why information security is needed to protect customers information and systems;

4.5.6.3 The common types of security threats (such as identity theft, malware, hacking, information leakage and insider threat);

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

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

4.6 Asset management

4.6.1 The Supplier shall have a defined and documented asset management system in place, and maintain up-to-date records of all relevant assets and their owners. Information assets include but are not limited to IT systems, backup and/or removable media containing sensitive information, access rights, software and configuration.

4.6.2 The Supplier shall label, treat and protect information according to a pre-defined information classification system in accordance with valid security standards at that time (including removable media storage, disposal and physical transfer).

4.6.3 The Supplier shall implement measures to ensure protection against accidental, unauthorized or unlawful loss, destruction, alteration or damage to Silknet data transmitted, stored or otherwise processed

4.6.4 The Supplier shall keep an updated list of Silknet's data processed. The list shall contain the following information:

4.6.4.1 The processed data;

4.6.4.2 Storage details, such as asset name, location etc.

4.7 Access control

4.7.1 The Supplier shall have a defined and documented access control policy for facilities, sites, network, system, application and information/data access (including physical, logical and remote access controls), an authorization process for user access and privileges, procedures for revoking access rights and an acceptable use of access privileges for the Supplier Personnel in place.

4.7.2 The supplier shall have a formal and documented user registration and de-registration process implemented to enable assignment of access rights.

4.7.3 The Supplier shall assign all access privileges based on the principle of need-to-know and principle of least privilege.

4.7.4 The Supplier shall use strong authentication (multi-factor) for remote access users and users connecting from untrusted network.

4.7.5 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.

4.8 Cryptography

4.8.1 The Supplier shall ensure proper and effective use of cryptography on information classified as confidential and secret (such as Personal Data) in accordance with the Silknet's confidentiality classification scheme as further detailed below.

4.8.2 The Supplier shall protect cryptographic keys.

4.9 Physical and environmental security

4.9.1 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. This includes physical perimeter and access protection.

4.9.2 The Supplier shall protect goods received or sent on behalf of the Silknet from theft, manipulation and destruction.

4.9.3 **Admission to Silknet's premises and Silknet's leased premises**

4.9.3.1 The Supplier's admission to Silknet's premises and property (such as datacentre buildings, office buildings, technical sites) is subject to the following:

4.9.3.1.1 The Supplier shall follow local regulations (such as regulations for "restricted areas") for Silknet's premises when performing the assignments under the Agreement.

4.9.3.1.2 Supplier Personnel shall carry ID card or a visitor's badge visible at all time when working within the Silknet's premises.

4.9.3.1.3 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.

4.9.3.1.4 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.

4.9.3.1.5 Photographing in or at the Silknet's premises without permission is prohibited.

4.9.3.1.6 Silknet's goods shall not be removed from Silknet's premises without permission.

4.9.3.1.7 Supplier Personnel shall not allow unauthorized persons access to the premises.

4.10 Operations security

4.10.1 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.

4.10.2 The Supplier shall implement malware protection to ensure that any software used for Supplier's provision of the deliverables to the Silknet is protected from malware.

4.10.3 The Supplier shall make backup copies of critical information and test back-up copies to ensure that the information can be restored as agreed with the Silknet.

4.10.4 The Supplier shall Log and monitor activities, such as create, 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 6 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 4.14.

4.10.5 The Supplier shall manage vulnerabilities of all relevant technologies such as operating systems, databases, applications proactively and in a timely manner.

4.10.6 The Supplier shall establish security baselines (hardening) for all relevant technologies such as operating systems, databases, applications.

4.10.7 The Supplier shall ensure development is segregated from test and production **environment.**

4.11 Communications security

4.11.1 The Supplier shall implement network Security Controls such as service level, firewalling and segregation to protect information systems.

4.11.2 The Supplier shall ensure that voice communication classified as confidential and secret (as further detailed below) is secure this means that un-encrypted communication may not be used.

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

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

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

4.13 Supplier relationship with sub-suppliers

4.13.1 The Supplier shall reflect the content of this Security Policy in its agreements with sub-suppliers that perform tasks assigned under the Agreement.

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

4.13.3 The Supplier shall, at the request of the Silknet, provide the Silknet with evidence regarding sub-supplier's compliance with the Security Policy.

4.14 Security Incident management

4.14.1 The Supplier shall have established procedures for Security Incident management.

4.14.2 The Supplier shall inform the Silknet about any Security Incident (including but not limited to incidents in relation to the processing of Personal Data) as soon as possible but no later than within 24 hours after the Security Incident has been identified.

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

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

4.14.4.1 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 or the Silknet's assets in any imaginable way

4.14.4.2 Sequence of events, including actions taken during the incident handling

4.14.4.3 Affected portions of the infrastructure, systems and information

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

4.14.4.5 Consequence reducing measures already implemented

4.14.4.6 Risk-reducing measures already implemented

4.14.4.7 Consequence reducing measures to be implemented, including implementation plan (date; responsible; dependencies)

4.14.4.8 Risk reducing measures to be implemented, including implementation plan (date; responsible; dependencies)

4.14.4.9 Experiences summary

4.14.5 The Supplier shall provide the Silknet with support in case of forensic investigation.

4.15 Business continuity management

4.15.1 The Supplier shall identify business continuity risks and take necessary actions to control and mitigate such risks.

4.15.2 The Supplier shall have documented processes and routines for handling business continuity.

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

4.15.4 The Supplier shall periodically assess the efficiency of its business continuity management, and compliance with availability requirements (if any).

4.16 Compliance

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

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

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