Owner	Security
CPO	Public
Approval Date	**Owner**
2021-06-16	Head of Sourcing Sustainability
No.	**Version**
T 4511-16	7.0

Supplier Security Directive

Table of contents

1 Description

This document “Supplier Security Directive” describes the security requirements applicable to suppliers and other identified business partners to Telia Company. Additional security requirements may apply if agreed by involved parties.

2 Definitions

1. “**Agreement**” shall mean the agreement between Telia Company and Supplier or other identified business partner to the Telia Company group under which the Supplier Security Directive apply, and to which the Supplier Security Directive is part thereof.
2. “**Buyer**” shall mean Telia Company AB or the relevant Telia Company Affiliate.
3. “**Buyer’s Data**” shall mean data or other information that the Buyer, or a person acting on behalf of the Buyer, makes available to the Supplier, including but not limited to Personal Data and the result of Supplier’s processing of such data.
4. “**Information Processing Facilities**” shall mean any information processing system, services or infrastructure, or the physical locations housing them.
5. “**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.
6. “**Personal Data**” shall mean any information relating to an identified or identifiable 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 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.
7. “**Applicable Data Protection Laws**” shall mean all information subject to applicable data protection laws, including without limitation to the “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 directives, laws, regulations and rulings valid at the given time.
8. **"Regulatory Requirements”** shall mean all applicable laws, rules, regulations and treaties, in force from time to time, of any international political and economic organization (e.g. the European Union), country, state, administrative agency or governmental body (e.g. the relevant Financial Services Authority, Data Protection Authority, Consumer Protection Agency or Chemicals Agency), as well as any applicable case law, orders, decisions, licences, recommendations, policies, standards and guidelines issued by the said bodies, courts and/or by self-regulatory or advisory organisations and industry sector groups.
9. “**Services**” shall mean the services to be provided by the Supplier to the Buyer, or a person acting on behalf of the Supplier as further defined in the Agreement between the parties.
10. “**Supplier**” shall refer to the counter-party who supplies any kind of deliverables to Buyer identified as “Supplier”, “Vendor, “Partner” or the equivalent in the relevant Agreement.
11. “**Supplier Personnel**” shall mean any person working on behalf of the Supplier such as employees, consultants, contractors and sub-suppliers.
12. “**Security Control**” shall mean any technical countermeasure, organizational setup or process, that helps to maintain IT systems security-quality properties.
13. “**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.
14. “**Sensitive Products**” and “**Sensitive Services**” shall mean any product or Services defined as sensitive by the Buyer. Sensitive Products or Sensitive Services shall be clearly documented in the applicable Agreement.

15. "**Industry Best Practice**" shall mean a practice, method, process or criteria, such as well as known security best practices supporting high standards of resilience, and use of unbroken protocols etc, that is generally accepted and followed by industry members.
16. "**Information Security Management System**" or "**ISMS**" shall mean the relevant part of the overall management system, based on a business risk approach, intended to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.
17. "**Cloud computing**" or "**Cloud**" shall mean a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
18. **"Software as a Service**" or "**SaaS**" Shall mean a service which its capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.
19. **"Platform as a Service**" or "**PaaS**" Shall mean a service which its capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
20. **"Infrastructure as a Service**" or "**IaaS**" shall mean a service which its capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
21. "**Private cloud**". Shall mean a type of cloud computing deployment model on which the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
22. "**Community cloud**". Shall mean a type of cloud computing deployment model on which the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
23. "**Public cloud**". Shall mean a type of cloud computing deployment model on which the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
24. "**Hybrid cloud**". Shall mean a type of cloud computing deployment model on which the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).
25. "**Pseudonymization**" 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

3 Scope

The Supplier Security Directive applies when:

1. The Supplier will process Buyer's Data, excluding the contact information required to establish or maintain a business relationship.
2. The Supplier will have unescorted access to Buyer's premises, excluding external areas.
3. The Supplier will access Buyer's network or IT systems, including remote access.
4. The Supplier will handle Buyer's information processing equipment.
5. The Buyer has deemed the Supplier as a provider of Sensitive Products and/or Sensitive Services and identified Supplier as such under the relevant Agreement.

4 The Supplier´s overall responsibility

1. The Supplier is fully responsible for the Supplier Personnel's compliance with the Supplier Security Directive.
2. The Supplier shall implement the measures required to ensure compliance to the Supplier Security Directive prior to commencing any assignment for the Buyer.
3. The Supplier shall, at the request of the Buyer, inform the Buyer how the Supplier complies with the Supplier Security Directive and what measures the Supplier has taken to comply with the Supplier Security Directive.
4. The Supplier shall inform the Buyer at cert@teliacompany.com 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 24 hours after the Security Incident has been identified. See Section "Security incident management" below.
5. The Supplier shall assure that any processing of Buyer's Data will be compliant with the Supplier Security Directive.
6. The Supplier shall not allow any access to Buyer'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 Buyer.

5 Security requirements

5.1 Risk Management

5.1.1 Security risk management

1. The Supplier shall periodically identify, analyze, evaluate and treat security risks.
2. The Supplier shall be able to provide evidence of risk assessments upon request related to the services/products that the Buyer has purchased.

5.2 Information security policies

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, published within Supplier´s organization and communicated to relevant Supplier Personnel.

5.3 Organization of information security

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

5.4 Human resources security

1. The Supplier shall ensure that any Supplier Personnel performing assignments under the Agreement is trustworthy and meets any established security criteria for the assignment.

5.5 Asset management

5.5.1 Physical Assets

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. Assets include, but are not limited to, information, IT systems, backup and/or removable media containing information, access rights, software and configuration.

5.5.2 Data

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

2. The Supplier shall return or destroy (as determined by the Buyer) any of the Buyer's Data and copies thereof. The Supplier shall confirm in writing to the Buyer that the Supplier has met this requirement on termination of the Agreement.

5.6 Access control

1. Have defined and documented access control policy for facilities, sites, network, system, application and information/data access (including physical, logical and remote access controls).
2. Have 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.
3. Assign all access privileges based on the principle of need-to-know and principle of least privilege.

5.7 Encryption

1. When encryption is required according to section 6 "Information security confidentiality classification description and handling requirements" or according to the agreement concluded between the parties, the Supplier shall ensure proper and effective use of encryption according to Industry Best Practices.
2. The Supplier shall use encryption methods which are considered secure according to Industry Best Practices.

5.8 Physical and environmental security

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.

5.9 Operations security

1. Implement malware protection to ensure that any software used for Supplier's provision of the deliverables to the Buyer is protected from malware.
2. Implement operational and technical security controls such as log management, firewalls, antivirus and encryption according to the established security standard.
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 Buyer.

5.10 Communications security

1. The Supplier shall ensure that at least all communication of information classified as internal, confidential or secret is secured according to the Buyer's information classification description in section 6 (Information security confidentiality classification description and handling requirements).

5.11 Supplier relationship with sub-contractors

1. The Supplier shall reflect the content of the Supplier Security Directive in its agreements with sub-contractors that perform tasks assigned under the Agreement.
2. The Supplier shall, at the request of the Buyer, provide the Buyer with evidence regarding sub-contractor's compliance with the Supplier Security Directive.

5.12 Security incident management

1. The Supplier shall have established procedures for Security Incident Management.
2. The Supplier shall inform the Buyer at cert@teliacompany.com about any Security Incident without undue delay after the Security Incident has been identified.
3. All reporting of security related incidents shall be treated as confidential information and be encrypted, using Industry Standard encryption methods such as PGP or equal Industry Standard encryption.

5.13 Business continuity management

1. Have documented processes and routines for handling business continuity including disaster recovery.
2. Ensure that information security is embedded into the business continuity plans
3. Periodically identify, analyze and evaluate business continuity risks and take necessary actions to control and mitigate such risks.
4. Contribute in mutual Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) upon request by the Buyer.

5.14 Compliance

1. The Supplier shall comply with all Regulatory Requirements and contractual requirements including but not limited to Personal Data protection.
2. The Supplier shall, on request, provide the Buyer with a compliance status report with regards to the security requirements without any unjustified delay.
3. If an ISAE3000/SSAE18 SOC2 Type I/II and/or SOC3 report is available, it shall be provided to the Buyer.
4. The Supplier shall, at the request of the Buyer, inform the Buyer how the Supplier complies with the security requirements and what measures the Supplier has taken to comply with the security requirements.
5. The Supplier shall regularly monitor, review and audit sub-contractor´s compliance with the security requirements.
6. The Supplier shall, at the request of the Buyer, provide the Buyer with evidence regarding sub-contractor's compliance with the security requirements
7. The Buyer has the right to audit how the Supplier and its sub-contractors fulfil the security requirements or corresponding requirements.
8. If an incident falls under legal requirements to be reported to the authorities, the Buyer shall be entitled to perform incident audit within three (3) hours' notice.
9. If an incident does not fall under legal requirements to be reported to the authorities, the Buyer shall be entitled to perform incident audit with five (5) days' notice.

6 Information security confidentiality classification description and handling requirements

6.1 Information security confidentiality classification description

Class	Description	Examples of information types
Secret	Unauthorized access or **disclosure of information could seriously damage Telia Company**, its organization, critical functions, workforce, business partners and/or customers.	-Annual report or financial results before public release. -Certain information based on legal requirements, specific customer agreements or non-disclosure agreements
Confidential	Unauthorized access or **disclosure of information could damage Telia Company**, its organization, critical functions, workforce, business partners and/or customers.	-Certain information based on legal requirements (i.e., personal data of customers or employees) -Sensitive business plans, strategies, and decisions (i.e., marketing plans)
Internal	Unauthorized access or **disclosure of information could cause minor damage Telia Company**, its organization, critical functions, workforce, business partners and/or customers.	-Information that is meant for TC's internal use -Communication materials targeted to all TC employees (i.e., related to TC organization, strategy, products, employee services)
Public	Unauthorized access or **disclosure of information causes no damage Telia Company**, its organization, critical functions, workforce, business partners and/or customers	-Annual report and result after they have been released -Marketing materials and published press releases. -Information that needs to be published based on legal requirements

6.2 Information security confidentiality classification handling requirements

Class	Who may access	How to store	How to transfer	How *to* use	How to assess need for protection (risk-based approach)

Secret	Appointed persons only	Logically and physically secure storage i.e., encrypted, or locked	Through secure communication channels or in a secure portable storage (locked)	To be used within secure areas that are protected from insight and eavesdropping	It shall be very hard to break the protection. Only highly motivated and/or resourceful attackers could dismantle the protection.
Confidential	A limited *and controlled* group of persons only	Logically and physically controlled and trusted storage with strict access control	Through secure communication channels, within a controlled and trusted network, or in a secure portable storage	To be used by authorized persons for business purposes only within a controlled workspace or place protected from insight and eavesdropping	It shall be hard for unauthorized persons to get access to the information. Only well motivated attackers could dismantle the protection.
Internal	Those who perform work for Telia Company	Under logical and physical access control	Through protected communication channels or within a trusted network	To be used by authorized persons for business purposes only within a controlled workspace or place protected from insight and eavesdropping	It shall be unlikely for unauthorized persons to get access to the information. Only motivated attackers could dismantle the protection.
Public	No restrictions	No restrictions	No restrictions	No restrictions	No restrictions