Telia Company

Supplier Security Directive

Version 8.0

Table of Contents

1 Description

This document "**Supplier Security Directive**", henceforth referred to as the "**SSD**", describes the security requirements ensuring an appropriate level of security on the Supplier side. The SSD is applicable to suppliers and other identified business partners to Telia Company. Additional security requirements may apply if agreed by involved parties.

The security requirements set forth in the SSD constitute at a minimum level the technical and organizational measures the Buyer requires of Supplier under the Agreement.

2 Definitions

1. "**Affiliate**" shall mean a legal entity directly or indirectly owning or controlling a Party, under the same direct or indirect ownership or control as a Party or directly or indirectly owned or controlled by a Party for so long as such ownership or control lasts. Ownership or control shall exist through direct or indirect ownership of more than fifty (50) per cent of the nominal value of the issued equity share capital or of more than fifty (50) per cent of the shares entitling the holders to vote for the election of directors or persons performing similar functions.
2. "**Agreement**" shall mean the agreement between Buyer and Supplier under which the Supplier Security Directive apply, and to which the Supplier Security Directive is part thereof.
3. "**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) ("**GDPR**") 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.
4. "**Artificial Intelligence (AI) or Autonomous Technology (ATT)**" shall mean a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. This includes General purpose AI models (e.g., Large Language Models) in which an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market.
5. "**Business Continuity Plans (BCP)**" shall mean the documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.
6. "**Buyer**" shall mean Telia Company AB or the relevant Telia Company Affiliate.
7. "**Buyer's Data**" shall mean Personal Data and any other data that the Buyer, Buyer's Customer, Customer's user, or anyone acting on behalf of Buyer, makes available to Supplier and/or data that is created or generated through usage of the Deliverable, including the result of Supplier's processing of such data. Buyer's Data may be protected by applicable legislation, such as trade secrets, copyright or other intellectual property laws and treaties.
8. "**Customer**" shall mean Buyer's Customer.
9. "**Deliverable**" shall mean all separate deliverables specified in the Agreement.

10. "**Deliverable processing Buyer's Data**" shall mean any Deliverable that will access, host, retain, process, or transmit Buyer's Data. This also includes the Supplier developing, supporting, providing, or managing technology, application(s), service(s), or solution(s) used for Buyer business purposes residing within the Supplier's environment or externally hosted.
11. "**Disaster Recovery Plans (DRP)**" shall mean the documentation of a management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities.
12. "**Industry Best Practice**" shall mean a practice, method, process or criteria, such as well as known security best practices supporting high standards of resilience, following acknowledged frameworks such as NIST CSF, ISO 27001/2, ISO 277001, ISO 3100, ISF that is generally accepted and followed by industry members.
13. "**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.
14. "**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.
15. "**Personal Data Breach**" shall mean Supplier's breach of its confidentiality, security and/or Personal Data protection obligations in relation to Buyer's or Customer's Personal Data processed under the Agreement leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by Supplier under the Agreement.
16. "**Processor**" and "**processing**" shall have meanings assigned to them in the GDPR and the Applicable Data Protection Laws.
17. "**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.
18. "**Security Control**" shall mean any technical countermeasure, organizational setup or process, that helps to maintain IT systems security-quality properties.
19. "**Security Event Log**" shall mean a system that Logs e.g. access or attempted access to systems, resources and data (including personal data); changes to system configuration and policies; use of privileges or utility programs and applications; files accessed or deleted; alarms raised by the access control system; activation and deactivation of security systems; account management events; system errors and warnings; restart or shutdown of an application or system itself; or any other significant action that could impact security.
20. "**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.
21. "**Security Risk**" shall mean any uncertainty that may affect Telia Company's objectives and the achievement of desired results. Typically expressed in the form of an undesired future event.
22. "**Security Threats**" shall mean any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the National Security through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
23. "**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.

24. "**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 or to other identified business partner to the Telia Company group
25. "**Supplier Personnel**" shall mean any person working on behalf of the Supplier such as employees, consultants, contractors and sub-suppliers.

3 Scope

This SSD applies when at least one of the following applies:

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; and/or
5. The Buyer has deemed the Supplier as a provider of Sensitive Products and/or Sensitive Services and identified Supplier as such under the Agreement.

4 Supplier's Overall Responsibility

1. The Supplier is fully responsible for the Supplier Personnel's compliance with the SSD.
2. The Supplier shall implement the measures required to ensure compliance to the SSD 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 SSD and what measures the Supplier has taken to comply with the SSD.
4. The Supplier shall inform the Buyer at cert@teliacompany.com about any Security Incident which may have a material impact on the Deliverable as soon as possible but no later than 24 hours when the Security Incident having possible impact on the Deliverable has been identified.
5. The Supplier shall inform the Buyer at cert@teliacompany.com about any zero-day vulnerabilities and other vulnerabilities which may have a material impact on the Deliverable as soon as possible but no later than 24 hours when vulnerability having possible impact on the Deliverable has been identified.
6. The Supplier shall inform the Buyer at controlcenterem-security@teliacompany.com without delay after becoming aware of any actual or reasonably suspected Personal Data Breach affecting Buyer or Customer but no later than 24 hours after the suspected Personal Data Breach affecting Buyer or Customer has been identified.
7. The Supplier shall assure that any processing of Buyer's Data will be compliant with the SSD.
8. 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.
9. The use of Artificial Intelligence or Autonomous Technology in Deliverables or use of Artificial Intelligence or Autonomous Technology to process Buyer's Data must be agreed upon with the Buyer prior to implementation.

5 Security Requirements

5.1 General

1. The Supplier shall present to the Buyer an ISAE3000/SSAE18 SOC2 Type I/II report if the Supplier has such a report.
2. The Supplier shall present to the Buyer an ISAE3000/SSAE18 SOC3 Type I/II report if the Supplier has such a report.
3. The Supplier shall present to the Buyer an ISO certification report if the Supplier has such a report.
4. The Supplier shall implement all requirements based on Industry Best Practices and ensure that the delivery of the Deliverables is fulfilling Industry Best Practices.
5. For clarity, the requirements of this section **Error! Reference source not found.** are not rated in a hierarchical way. Every security category and subsequent requirements are equally important.

5.2 Security Governance

1. The Supplier shall have a security policy and subsequent security processes in place.
2. The Supplier shall have defined and documented roles and responsibilities that establish and continuously improve the Supplier's approach to security and privacy.
3. The Supplier shall assign a single point of contact responsible for ensuring Buyer security requirements (i.e., security configuration recommendations, scheduled downtime, incident management and general security updates, etc.).
4. The Supplier shall follow a risk-based approach enabling the management of Security Risks and Personal Data related risks.
5. The Supplier shall have Business Continuity Plans (BCP) which are implemented and periodically tested.
6. The Supplier shall periodically identify, analyze, and evaluate business continuity risks and take necessary actions to control and mitigate such risks.
7. The Supplier shall contribute to a mutual Business Continuity Plan (BCP) upon request by the Buyer.
8. The Supplier shall have Disaster Recovery Plans (DRP), which are implemented and periodically tested.
9. The Supplier shall contribute to a mutual Disaster Recovery Plan (DRP) at the request of the Buyer.
10. If the Deliverable processes Buyer's Data, the Supplier shall establish processes that help the Supplier's business and production continuity for the Deliverable, including any Deliverable delivery dependencies, recover from adverse situations with minimal impact to operations.
11. The Supplier shall have processes in place to assess the effectiveness of the Supplier's security measures.
12. The Supplier shall have security awareness trainings for the Supplier Personnel including training of legal requirements for the processing of traffic data and sanctions related to the breach of the confidentiality of communications.
13. The Supplier shall ensure Supplier individuals supporting the Deliverable complete cybersecurity and data privacy training.

5.3 Identification of Security Risks

1. The Supplier shall have a standardized and centrally managed asset management solution in place.
2. The Supplier shall ensure the Deliverable processing Buyer's Data and hosted by the Supplier is properly managed in an asset inventory system and configuration management system throughout its lifecycle, from procurement through disposal, ensuring only authorized access to the Deliverable and protecting any Deliverable related data that is stored, processed or transmitted.

3. The Supplier shall have risk management processes in place to identify, analyze, evaluate, and treat Security Risks.
4. The Supplier shall have risk management processes in place to identify, analyze, evaluate, and treat supply chain and third-party Security Risks. On Buyer's request, the Suppler shall provide a list of subcontractors Supplier has engaged or intends to engage for Supplier's provision of the Deliverable(s).
5. The Supplier shall continuously develop and improve the Supplier's cybersecurity and data protection controls to ensure ongoing risk management for the provision of the Deliverable processing Buyer's Data.
6. The Supplier shall be able to provide supporting Deliverable documentation (e.g., data flow diagram, architecture diagram) concerning the Deliverable in scope and how it relates to the Supplier and the Buyer.

5.4 Protection from Security Threats

5.4.1 Access Management

1. The Supplier shall have the following access controls in place:
    a. A defined and documented access control policy for facilities involved in the delivery to the Buyer, sites, network, system, application, and information/data access (including physical, logical, and remote access controls);
    b. Processes to securely manage identities and credentials;
    c. An authorization process for user access and privileges;
    d. Procedures for access rights (joiners, movers, leavers);
    e. Processes for managing changes in access rights (new, changes and deletions)
    f. Processes for the secure use of access privileges for the Supplier Personnel requiring access to the Deliverable;
    g. Assigning, reviewing, and revoking access privileges on a regular basis, based on the principle of need-to-know and principle of least privilege; and
    h. If the Deliverable processes Buyer's Data, all applications included in the Deliverables must have authentication and authorization mechanism including traceability of users implemented.
2. If the Deliverable processes Buyer's Data and is hosted by the Supplier, the Supplier shall also have the following access controls in place:
    a. The Supplier must review all access rights to the Deliverable at least every six (6) months to confirm access or credentials are still needed.
    b. Supplier access to the Deliverable must be based "least privilege" and need-to-know.
    c. The Supplier shall enforce multifactor authentication (MFA) in order to access the data included in the Deliverable.

5.4.2 End-point Device Management

1. If the Deliverable processes Buyer's Data, the Supplier shall adhere to the following requirements regarding Supplier end point devices:
    a. The Supplier shall protect Supplier end point devices with access to the Deliverable from security threats; and
    b. The Supplier shall govern any related risks associated with Supplier endpoint devices accessing the Deliverable or any related Deliverable dependencies.

5.4.3 Artificial Intelligence (AI) or Autonomous Technology (AAT)

2. If the Deliverable contains Artificial intelligence (AI) or Autonomous Technology (AAT), the Supplier shall adhere to the following:
    a. The Supplier shall provide relevant information about the security measures taken in the AI System.
    b. The Supplier shall identify, document, and implement security and data privacy compliancy requirements for AI and AAT included in the Deliverable. Supplier shall fulfil the Buyer's security and data privacy requirements as minimum.

5.4.4 Data Classification and Handling

1. The Supplier shall adhere to the following regarding data security:
    a. Based on the Buyer's classification of the data and information involved (as Secret, Confidential, Internal, or Public), as defined in the sub-section 3 of this Section 5.4.4., the Supplier shall align its security measures with the applicable classification requirements.
    b. The Supplier can only handle Buyer's Data to the extent agreed in the Agreement. This requires, for example, that the Supplier is not allowed to move the Buyer's Data from on-prem to cloud without the Buyers authorization. All rights to Buyer's Data, including any derivatives or adaptations thereof, are solely owned by the Buyer.
    c. The Supplier shall ensure that Buyer's data handling requirements are fulfilled when Buyer's Data is being processed by the Supplier.
    d. The Supplier shall implement measures to protect the Buyer's Data related to the Deliverable hosted by the Supplier from unauthorized access, disclosure or modification in accordance with the Buyer's data classification, regardless of whether it is being transmitted, used, or stored.
    e. The Supplier must consider Buyer demand and capacity requirements for Deliverables.
    f. The Supplier shall prevent avoidable business interruptions for their own business environment required for providing the Deliverables by proactively planning for growth and forecasting, as well as informing the Buyer of important current and future performance concerns the delivery of Deliverables. Proactive planning must include capacity and performance plans to adequately cover the whole life cycle of the Deliverables.
    g. The Supplier shall implement data and information protection measures throughout the life cycle of the Agreement and the Deliverable(s) as per the Agreement to limit and prevent accidental, unauthorized, or unlawful loss, destruction, alteration, or damage to the Buyer's Data, following the relevant legislative and regulatory requirements.
    h. The Supplier shall ensure an adequate protection of data-in-transit, data-in-use, and data-at-rest, especially when processing Personal Data.
    i. The Supplier shall secure the Buyer's Personal Data involved with the Deliverable by design and by default.
    j. The Supplier shall have applicable operational security processes in place for the Deliverable (e.g., patch management, hardening processes, configuration management). The Supplier must periodically perform integrity and completeness checks to validate backup data and information on the Deliverable(s) stored by the Supplier to prevent tampering.
    k. The Supplier shall develop, proactively manage, and review embedded technologies involved with securing the Deliverable in accordance with the shared responsibility matrix agreed between the Buyer and the Supplier, including hardening of the "stack" from the hardware, firmware and / or software to transmission and service protocols.
    l. If the Deliverable processes Buyer's Data and the Buyer purchases security configuration management services, security configuration management controls and security features to prevent malicious activity

as well as their implementation must be approved by the Buyer prior to these controls and security features being provided to the Buyer and implemented.

m. On the termination of the Agreement, the Supplier shall return or destroy (as determined and instructed by the Buyer) all the Buyer's Data and copies thereof while providing the Buyer with a certification of destruction.

n. Data destruction from removable storage devices:

Item for disposal	Method
Paper	Securely destroyed, shredded, or incinerated
Mobile Computing Devices (cell phones, tablets)	Delete all non-public Buyer's Data
Electronic Storage Media (hard drives, USB / memory sticks, RAM, tapes, etc.)	Physically destroy or sanitize media in accordance with Industry Best Practices and verify removal of data
Optical Disks (CDs, DVDs, etc.)	Use optical disk shredder or disintegrator. Disks can also be incinerated, or grinders can be used.

o. After returning the Buyer's Data, the Supplier is obliged to destroy any subsequent copies of the data. For Personal Data specific retention times are set out in the DPA. The Supplier shall confirm in writing to the Buyer that the Supplier has met this requirement upon the request of the Buyer. The Supplier may retain the Buyer Data only to the extent agreed in the Agreement.

p. The Supplier must establish and regularly test its back-up processes and procedures.

q. For the Deliverables hosted by the Supplier, the Supplier shall address risks for any Internet-accessible components associated with the Deliverable (e.g., APIs) by hardening the Deliverable, monitoring Deliverable file integrity, enabling auditing, and monitoring for malicious activities, unless otherwise agreed.

r. The Supplier shall protect the confidentiality and integrity of the Deliverable and/or Deliverable related data in transit and at rest when applicable through the implementation of cryptographic technologies.

s. The Supplier shall ensure Supplier architecture, development and engineering of the Deliverable are in alignment with Industry Best Practices.

t. The adequacy of cybersecurity and data privacy controls implemented by the Supplier for the delivery of the Deliverable in Supplier's development, testing and production environments must be periodically tested in line with Industry Best Practices.

u. The Supplier shall support the Buyer building ensuring the proper service assurance to keep the Deliverable running securely including proper change management.

v. The Supplier shall implement proactive change management for the Deliverable hosted by the Supplier, including the assessment, authorization, and monitoring of technical Deliverable changes so as to not impact production uptime and allow easier troubleshooting of issues.

2. The Supplier shall have data and information protection processes and procedures in place that ensure a consistent and continuously improved approach to security and configuration management.

3. Buyer's data 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

4. Handling requirements related to the confidentiality levels of the data:

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

5.4.5 Network Security

1. The Supplier shall have network security protection measures in place. If the Deliverable processes Buyer's Data, security and data privacy controls must be implemented in the Supplier's network infrastructure supporting the Deliverable to protect its confidentiality, integrity, availability, and safety.
2. The Supplier shall adhere to the following regarding maintenance:
    a. The Supplier shall notify the Buyer without undue delay of critical repairs, maintenance activities and any other activities but not later than 48h before starting such repairs or activities that will have a material impact on the confidentiality or integrity of Buyer's Data or the availability of the Deliverable or subsequent dependencies and functions supporting Deliverables with a timeline for completion of the activities; and
    b. Where there is a need for remote access to the Buyer's environment, the Supplier must use a remote access tool agreed between the Parties to carry out the repair and/or maintenance.
    c. If the Buyer purchases maintenance and/or support services, the Supplier shall properly maintain Deliverable performance (e.g., security patches, firmware patches, etc.) to ensure continued effectiveness on a level agreed in the SLA(s).
    d. If the Buyer purchases maintenance and/or support services, the Supplier shall proactively manage Deliverable related risks associated with technical vulnerabilities which includes, but is not limited to, Industry Best Practice patch and change management practices agreed with the Buyer.

5.5 Detecting Security Threats

1. The Supplier shall monitor for potential Security Threats, Security Incidents, and unauthorized activity.
2. If the Deliverable hosted by the Supplier processes Buyer's Data, the Supplier shall identify and manage Deliverable-related threats to the cybersecurity and data privacy of the Deliverable, its data and related processes.
3. The Supplier shall enable the centralized collection and review of Security Event Logs for the Deliverable hosted by the Supplier.
4. The Supplier shall have a process for identifying, analyzing, and determining whether a Security Incident or unauthorized activity is occurring.
5. The Supplier shall have processes to detect and respond to potential malicious activity affecting to the delivery of the Deliverable through a formalized intake of security-related tickets; including e.g. log monitoring; and analyzing threat intelligence feeds.
6. The Supplier shall identify, prioritize, and mitigate identified vulnerabilities.
7. The Supplier shall continuously improve detection processes for Security Threats.

5.6 Responding to Security Incidents

1. The Supplier shall establish plans, processes, and procedures for the management of Security Incidents which must be followed in the event of a Security Incident.
2. The Supplier shall continuously develop, test, and improve its plans, processes, and procedures for the management of the Security Incidents.

3. The Supplier shall assist the Buyer in the Buyer's efforts to respond to a Security Incident originating from or affecting the Supplier's Deliverable at no cost or at a cost that is determined before a Security Incident occurs.
4. All reporting related to Security Incidents shall be treated as confidential information and be encrypted by the Supplier, using Industry Best Practice encryption methods such as PGP or equal.
5. If the Deliverable processes Buyer's Data, the Supplier shall establish and maintain a viable and tested capability to respond to cybersecurity or data privacy-related incidents that may affect the Buyer or the Buyer's customers without undue delay.

5.7 Recovering from Security Incidents

1. The Supplier shall establish plans, processes, and procedures for recovering from a Security Incident which must be followed in the event of a Security Incident.
2. The Supplier shall continuously develop, test, and improve its plans, processes, and procedures for recovering from a Security Incident.
3. The Supplier shall aid the Buyer in the Buyer's efforts to recover from a Security Incident originating from the Deliverable.

5.8 Physical and Environmental Security

1. The Supplier shall adhere to the Buyer's physical security requirements to protect Buyer information and data 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.
2. If the Supplier has access to Buyer's physical premises, the Supplier shall abide by the following requirements:
    a. An ID Card must be used for identification purposes, according to contractual and business requirements. The ID card must be worn visibly at all times.
    b. Users are responsible for actions performed with their access keys and/or access cards. User ID, User ID cards, keys, and PIN-codes/passwords assigned to single users must not be shared.
    c. Lost or suspected compromise of access credentials, keys or cards must be immediately reported.
    d. Users must not assist any unauthorized person to access Buyer's premises or assets.
3. For any Deliverable that is externally hosted on the Supplier premises, the Supplier shall ensure the compliance of the following requirements:
    a. The Supplier must protect its own facilities against external and environmental threats and hazards, including power/cabling failures and other disruptions caused by failures that may negatively affect the Deliverable.
    b. The Supplier must implement physical perimeter and access protection related to the deliverable.
    c. The Supplier must have a process in place to securely dispose physical media related to the Deliverable.
    d. The Supplier must maintain a current list of personnel with authorized access to Supplier facilities related to the Deliverable.
    e. The Supplier must have physical access control mechanisms in place to identify, detect and respond to physical security incidents.
    f. The Supplier must have risk management processes in place to identify, manage and mitigate physical security risks related to facilities in which the Deliverable is hosted.
    g. The Supplier must inform the Buyer of any physical security incident related to the Deliverable in accordance with the notification requirements stated in the section 4 of this SSD.

5.9 Personnel Security

1. The Supplier must have screening and vetting process in place for employees, consultants, contractors, and subcontracts prior to being granted access to Buyer data and Deliverables.
2. The Supplier must inform the Buyer of any Deliverable related personnel that fails to comply with established security policies and standards.
3. Supplier must ensure that Supplier's personnel who are given access to non-public Buyer information, have committed to confidentiality or non-disclosure towards the Supplier prior to being given access.
4. The Supplier must notify the Buyer of Supplier personnel changes related to the Deliverable (e.g., Supplier personnel reassignments, transfer, assignment change, termination) when access is not fully managed by the Buyer.
5. The Supplier must ensure its personnel is compliant with the Supplier Security Directive.
6. The Supplier must ensure that any Supplier Personnel performing assignments under the Agreement is trustworthy and meets any established security criteria for the assignment.
7. Supplier personnel identified as needing National security clearance must adhere to Buyer national security clearance processes.

5.10 Supplier's Relationship with the Supplier's Sub-contractors

1. The Supplier shall reflect the content of this SSD in the Supplier's agreements with its sub-contractors who 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 this SSD.
3. The Supplier shall regularly monitor, review, and audit its sub-contractors' compliance with the content of this SSD.
4. The Buyer has the right to audit how the Supplier and its sub-contractors fulfil the requirements of this SSD.
5. The Supplier shall identify, manage, and mitigate cybersecurity and data privacy risks associated with Supplier sub-contractors to ensure sustained operations should a Supplier sub-contractor become compromised, untrustworthy, or defunct.

5.11 Compliance

1. The Supplier shall comply with all the Regulatory Requirements and the contractual requirements of the Agreement, including but not limited to the Applicable Data Protection Laws and contractual requirements related to the Personal Data and security, and the Supplier must be able to document how it meets these requirements.
2. The Supplier shall, at the request of the Buyer, provide the Buyer with a compliance status report with regards to the security requirements without any unjustified delay.

6 Version History

Version	Date	Author	Status
Version 7	2023	N/A	Approved
Draft 8	25.04.2024	Security Governance	Alignment with ISO 27001/27002: 2022 and internal steering documentation
Draft 8	28.06.2024	Security Governance	Approved by Security Legal
Draft 8	02.07.2024	Security Governance	Approved by CSO
Version 8: Approved	02.07.2024	Security Governance	Approved by CPO