Information Security Requirements for Suppliers

ISRS

Security Requirements

Introduction

The Ericsson Information Security Requirements for Suppliers (the "Requirements") represent the minimum level of information security requirements that the Supplier must adhere to for all supplier relations where the Supplier:

1. Processes, stores and/or has access to Ericsson Information.
2. Has access to Ericsson network/infrastructure.
3. Develops or customizes software for Ericsson.
4. Provides IT hardware or software products along with support and maintenance services.

The Requirements are not intended to be an exhaustive list of information security requirements. In addition to the Requirements, each Service offering may necessitate specific requirements that must be addressed with the appropriate information security controls to be further defined in the relevant Agreement.

This document undergoes reviews regularly and will be updated from time to time.

Contents

1 Information Security Requirements

Supplier must evidence a systematic approach to information security management through adherence to the latest version of the international standard ISO/IEC 27001 or, subject to written agreement, an equivalent standard.

1.1 Information Security Management

a. Top management at Supplier must set the direction for and show commitment to information security. At a minimum, there must be a high-level information security policy and supporting program that applies enterprise-wide.

b. The information security policy under subsection a. above, must be approved by the Supplier's management, published within Supplier´s organization and communicated to relevant Supplier personnel.

c. Suppliers' information security policy must be reviewed by Supplier at planned intervals, but no less than once per every twenty-four (24) months, or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

d. One or more qualified persons must be designated with responsibility to maintain the information security program.

e. Supplier conducts periodic information security awareness campaigns to educate employees on their responsibilities for creating and maintaining a secure workplace.

f. Supplier must maintain appropriate segregation of duties where relevant.

1.2 Risk Management

Supplier must have a risk management framework/process in place which identify and address information security risks.

1.3 Human resource security

a. Supplier must perform pre-employment Background Verification Checks for all Supplier personnel in accordance with applicable laws. Evidence of such background checks must be maintained and provided to Ericsson (upon Ericsson's request).

b. Before gaining access to Ericsson Information, Supplier personnel must be bound by confidentiality restrictions under a written agreement with the with the Supplier (such as an employment agreement or NDA). Such agreement shall prohibit Supplier personnel from disclosing Ericsson Information to third parties, and must not be less restrictive than Supplier's confidentiality undertakings towards Ericsson under the Agreement.

c. Supplier personnel with access to Ericsson network infrastructure and/or Ericsson Information must sign Ericsson's Non-Disclosure and Access Instruction document (NDI).

d. Supplier must have a disciplinary process in place to address information security violations.

1.4 Asset management

a. Supplier must handle Ericsson Information as Confidential Information and safeguard it by adhering to the Requirements outlined in this document.

b. Supplier must register and maintain an inventory of information technology assets that are part of the Service.

c. Ericsson Information must not be stored, printed, copied, disclosed or processed by Supplier for other purposes than fulfilling its obligations under the Agreement.

d. Supplier must establish processes for the return of Ericsson assets in case of Supplier personnel's termination or change of employment.

e. Supplier must establish and maintain procedures for the secure removal of Ericsson Information in accordance with Industry Best Practices (including from electronic media before it is available for re-use).

f. Upon conclusion or termination of the Agreement, Supplier must return or securely destroy in accordance with Industry Best Practice all copies of Ericsson Information in Suppliers possession, including all backup and archival copies, in any electronic or non-electronic form. Upon request, Supplier must provide written confirmation or, where applicable, certification of destruction to Ericsson.

1.5 Access control

a. Access to Ericsson's assets from a network outside Ericsson's control by individuals or bodies who are not part of Ericsson is only allowed through an approved Ericsson remote access solution.

b. Access to Ericsson Information must be restricted to unique individuals and on a need-to-know basis.

c. Shared accounts are strictly prohibited. Each individual accessing Ericsson Information must have their own unique account.

d. Multi-factor authentication (MFA) must be implemented for all access to systems and networks containing Ericsson Information in accordance with Industry Best Practice.

e. Supplier must implement password selection and management controls according to Industry Best Practice when accessing Ericsson Information such as but not limited to password complexity, maximum allowed incorrect logon attempts and password expiry duration for all passwords.

f. Supplier must have a process that requires approval to add, change, or delete users to its networks and systems that processes, transmits, or stores Ericsson Information.

g. Supplier must have a process for the revoking/update of access in case of termination or change of employment.

h. Supplier must review access privileges to systems and networks handling Ericsson Information, including administrative access privileges. Periodic reviews should be performed at least every twelve (12) months and for privileged users at least every three (3) months.

i. Supplier must have a process to administer and manage privileged accounts.

j. Records must be kept in an auditable manner showing which Ericsson Information has been accessed, modified, disclosed, or disposed.

1.6 Cryptography

a. Cryptographic controls must be implemented in compliance with all relevant agreements, legislation, and regulations.

b. Supplier must have ability to communicate securely with Ericsson through encrypted email, using Industry Best Practice encryption techniques.

c. Ericsson Information must be protected using encryption techniques in transit and at rest in in accordance with Industry Best Practice.

d. Cryptographic keys must be centrally managed with processes in place for key generation, renewal, access, distribution, storage, archival, revocation and destruction in accordance with Industry Best Practice.

e. Root certificates must not be used in an operational environment.

1.7 Physical and environmental security

a. Supplier must restrict physical access to facilities and data centers where Ericsson Information is processed or stored to unique individuals and on a need-to-know basis.

b. Information Processing Facilities where Ericsson Information is processed must be monitored and access-controlled at all times (24x7).

c. Supplier must protect Information Processing Facilities where Ericsson Information is processed against external and environmental threats and hazards.

d. A clear desk and clear screen policy must be enforced to protect Ericsson Information and assets.

e. Physical access to locations where Services are performed for Ericsson must be restricted, using individual swipe/proximity cards or other equivalent system.

f. Physical access to locations where Services are performed for Ericsson must continuously log physical access related events such as date, time, swipe/proximity card-id, door-id, access denied, or access granted.

1.8 Operations security

a. Supplier's systems must be provisioned with sufficient capacity to ensure continued availability in the event of a security incident or increased demand.

b. Supplier must ensure that malicious software protection is deployed in its systems and kept up to date, in accordance with Industry Best Practice.

c. All privileged user actions must be logged. Any changes to these logs by a system, privileged or end user must be detectable. Log records must also be independently reviewed periodically.

d. Information about important security related events must be recorded in logs including event types such as failed log-on, system crash, changes of access rights and event attributes such as date, time, User ID, file name, type of user activity and IP address.

e. Log records must be stored encrypted for at least six (6) months and be made available to Ericsson upon request.

f. Back-ups must be performed and maintained to ensure continuity and delivery expectations under the Agreement.

g. A vulnerability management process must be in place to prioritize and remediate vulnerabilities based on nature/severity of the vulnerability.

h. A patch management process must be in place to ensure that patches are applied in a timely manner.

i. Supplier must perform penetration testing of systems and infrastructure that are used to support Ericsson engagement at least annually, using Industry Best Practice.

j. Supplier must synchronize the clocks of all relevant information processing systems to a Single Reference Time Source.

k. Hardening following current Industry Best Practice must be applied to all systems to reduce the attack surface.

l. Supplier shall implement policies designed to prevent the storage of Ericsson Information on portable devices without prior written authorization from Ericsson.

m. Supplier must ensure that Ericsson Information and application/systems is segregated from suppliers own or other customer systems and data by appropriate physical, technical and/or logical means.

n. Development, testing, and production environments containing Ericsson Information must be logically and physically separated from each other.

o. Supplier must not use Ericsson Information in any artificial intelligence unless specifically agreed under the Agreement.

1.9 Communications security

a. Systems containing Ericsson Information must be hardened in accordance with Industry Best Practice, including but not limited to removing or disabling software and functionalities that are not being used.

b. Supplier must implement a layered security approach, utilizing security hardened firewalls, intrusion detection/prevention systems, network segmentation, and other relevant measures in accordance with Industry Best Practice to protect Ericsson Information.

c. Supplier must implement email security solution in accordance with Industry Best Practice to protect against malicious attacks such as malware, email spoofing, phishing attacks, and spam.

1.10 Subcontractor relationships

a. Disclosing Ericsson Information to a subcontractor, must only be allowed with prior written consent from Ericsson and only for the purposes of fulfilling the Supplier's obligations under the Agreement.

b. Subcontractor must be restricted to only the necessary access, use, retention, and disclosure of Ericsson Information needed to fulfill contractual obligations.

c. Supplier is responsible for passing the same obligations found herein by way of written agreement to its subcontractors.

d. Supplier must assess the risk associated with new subcontractors prior to onboarding and must have a third-party risk management process in place.

e. Supplier must regularly monitor, review and audit subcontractor´s compliance with the Requirements.

1.11 Incident management

a. Supplier must have a documented security incident management process to detect and handle incidents.

b. Supplier must notify Ericsson immediately after becoming aware of an incident impacting Ericsson Information. Such notification must be made in no event later than within twenty-four (24) hours or as otherwise agreed upon from gaining knowledge of any occurred or suspected incident to:

   i. the Ericsson contact set out in the Agreement; and

   ii. gs.sim.dispatch@ericsson.com

c. All reporting of security related incidents shall be treated as Confidential Information and be encrypted, using Industry Best Practice encryption methods.

d. Supplier must cooperate fully with Ericsson in dealing with these reports. Cooperation may include providing access to computer-based evidence data for forensic evaluation.

e. Supplier shall cooperate with Ericsson to ensure that mutually agreeable, appropriate security measures and procedures are implemented as part of remediation actions against a security incident or weakness affecting the Services or involving Ericsson Information.

1.12 Business Continuity Management

a. Supplier must implement business continuity and disaster recovery plans that are documented and tested at least annually and, upon Ericsson's request, provide copies.

b. Supplier must ensure that information security and ICT readiness requirements are embedded into the business continuity and disaster recovery plans.

c. Upon Ericsson's request, Supplier must contribute in mutual business continuity and disaster recovery activities as designated by Ericsson.

1.13 System acquisition, development, and maintenance

The following information security requirements are applicable for Suppliers providing development or customization services for software or hardware including processing of Ericsson Information

a. Supplier must have a documented software development life cycle (SDLC) methodology.

b. System source/object code must be protected from unauthorized access. Access privileges to the source code repository must be reviewed periodically and limited to authorized employees.

c. Ericsson Information from a production system must not be used in test and development systems.

d. Supplier must ensure that the software and/or other products processing Ericsson Information are free from all known security vulnerabilities or other security defects.

e. Upon Ericsson's request, Supplier must disclose any third-party software/plug-in (proprietary or open source) used in development of the software that support processing of Ericsson Information.

f. Supplier must follow documented change management procedures for requesting, testing, and approving application and infrastructure related changes.

1.14 Software Supply chain security

Supplier must specify and document third party software components used and their respective version numbers, both open source and proprietary components, and provide Ericsson with a software bill of materials (SBOM) that conforms to the SPDX Specification V2.2.1/ISO 5962:2021 and to the SBOM specification for suppliers (see *Conditions and Guidelines - Suppliers & Partners - Ericsson)* for all software (provided either standalone or embedded in hardware) delivered to or made available to Ericsson.

2 Compliance

a. Supplier internal audits and/or assessments concerning information security must be performed regularly by trained Supplier personnel, or a third party designated by Supplier, and any findings must be corrected promptly.

b. Upon Ericsson's request, Supplier must within ten (10) days be able to demonstrate compliance with the Requirements and any other information security requirements agreed

with Ericsson. Any identified non-compliance must be corrected immediately without additional cost to Ericsson.

c. Supplier shall, at the request of Ericsson, provide Ericsson with evidence regarding subcontractor's compliance with these Requirements.

d. Upon Ericsson's request, Supplier must provide to Ericsson any and all results from penetration and/or vulnerability testing or allow Ericsson to perform penetration and/or vulnerability testing on systems or environments managed or hosted by Supplier where Ericsson Information is processed or stored.

e. Supplier must retain and protect all necessary records to demonstrate compliance with the Requirements.

3 Definitions

For the purposes of this document, the following words and expressions must have the meaning assigned to them below unless the context would obviously require otherwise.

Agreement	The agreement between Supplier and Ericsson, pursuant to which Ericsson will purchase, in-license, or lease products (including software and other products protected by IPRs), services or other deliverables from Supplier, to which these Requirements apply.
Background Verification Checks	Background verification checks will have the same meaning as set out in ISO/IEC 27001/27002.
Ericsson Information	Information proprietary to Ericsson, Ericsson's customers, other third parties which have business relations with Ericsson and other information being part of the Service. Ericsson Information includes Personal Information.
Industry Best Practice	Means that degree of skill, care and foresight and operating practice that would reasonably and ordinarily be expected of a skilled and competent supplier of services engaged in the same type of undertaking as that of the recipient or any contractors (as applicable) under the same or similar circumstances.
Information Processing Facilities	Any physical location housing systems that process or store Ericsson Information.
Personal Information	Personal Information must mean any information that can be related to an identified or identifiable natural person ('data subject'), or as otherwise defined by law, regulation, or contractual agreement. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity.
Service	Any services, products or other deliverable provided by Supplier to Ericsson under the Agreement.

Single Reference Time Source	Time server source that it is directly linked to a reliable source of UTC (Coordinated Universal Time) which is the primary time standard globally used to regulate clocks and time, i.e. Stratum1.
Supplier	The company who has entered into the Agreement with Ericsson and will provide Services. Where the term "Supplier" imposes an obligation or requirement on Supplier as per this document, the term also includes Supplier´s affiliates, subcontractors and Personnel.