Baseline Information Security and Privacy Requirements for Suppliers

INSTRUCTION

1/00021-2849 Uen Rev H

Preface

The Ericsson Baseline Information Security and Privacy Requirements for Suppliers (BISPRS) represent the minimum requirements that the Supplier, its affiliates, subcontractors and their Personnel performing any Services on behalf of Ericsson, where Services may include the Processing of Ericsson Information, shall comply with in order to maintain Ericsson's level of commitment to the protection of Ericsson Information.

Ericsson Information includes information proprietary to Ericsson, Ericsson's customers, other third parties which have business relations with Ericsson and other information being part of the Service(s) for Ericsson.

The Supplier shall ensure that any additional requirements regarding security and privacy required as part of contractual agreements and applicable laws and regulations are also complied with.

This document undergoes reviews on a regular basis and will be updated from time to time. Ericsson together with the Supplier will review such changes and agree in good faith as to how (in what way and/or by which means or measures) and when the Supplier will comply with the updates.

Contents

1 Baseline Information Security and Privacy Requirements for Suppliers

Supplier shall protect Ericsson Information by implementing applicable controls as set forth in this Document in alignment with the latest version of the international standard ISO/IEC 27002, unless otherwise agreed in writing.

For the purpose of the obligation of the Supplier, “alignment” means that the Supplier regularly must consider all controls included in the said standard and take conscious decisions as to if a specific control should be implemented fully, partly, or not at all, or, if alternative protection measures must be or are implemented. However, the Supplier must always ensure that Ericsson Information is not at risk.

Communications to Ericsson regarding security incidents, exceptions to requirements in this BISPRS, or other security related issues or inquiries must be protected from improper access or interception using encryption.

Security related incidents should be reported to: corporate.security.office@ericsson.com, appointed point of contact or as otherwise specified in contractual agreements.

Support on how to use encrypted e-mail: How do I communicate securely by email with Ericsson users.

2 Information Security

2.1 Information Security Policy

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

b. The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness.

2.2 Organization of Information security

a. One or more qualified Personnel shall be designated with responsibility to maintain the information security program.

b. Supplier shall maintain Separation/Segregation of Duties to prevent error and fraud by ensuring that at least two individuals are responsible for separate parts of any task, so that no single role or account, can access, modify or use Ericsson Information without authorization or detection.

2.3 Human resource security

a. Supplier shall have a process to ensure that all Personnel with access to Ericsson Information sign the Non-Disclosure Agreement (NDA) of the Supplier.

b. Personnel with access to Ericsson Network Infrastructure and information shall sign an acknowledgement that they have read and understood Ericsson's Non-Disclosure and Access Instruction document.

c. Supplier shall have a Personnel onboarding process that includes verifying the identity of Personnel and the background and skill they state.

d. Supplier shall have a Personnel termination process that includes revoking access rights, seizing IT equipment, invalidating company access card as well as notification of continuous confidentiality obligations.

e. Personnel with access to Ericsson Information shall be required to take appropriate security training on a regular basis.

f. Non-compliance by Personnel in relation to this BISPRS shall be addressed through appropriate disciplinary actions imposed by Supplier.

2.4 Asset management

a. The supplier shall handle Ericsson Information as Confidential information.

b. The Supplier shall use encryption for transfer of Ericsson information, including Ericsson Information transferred in email.

c. Ericsson Information shall not be excessively stored, printed, copied, disclosed or Processed by other means outside the purpose for use.

a. Ericsson Information shall be processed and stored logically separated from the Suppliers own information and from that of other customers.

b. Upon conclusion or termination of Supplier's work for Ericsson, the Supplier shall sanitize and securely destroy (or at Ericsson's election return to Ericsson) all copies of all Ericsson Information, including all backup and archival copies, in any electronic or non-electronic form.

2.5 Access control

a. Access to Ericsson's information systems or networks from a network outside Ericsson's control by individuals or bodies who are not part of Ericsson is only allowed through an approved Third Party Connection (TPC) provided by Ericsson.

b. Access to Ericsson Information shall be restricted to Personnel individually and on a need to know basis.

c. Access to systems and networks that contain Ericsson Information shall enforce two factor authentication methods.

d. There shall be a password selection and management controls in place for accessing Ericsson Information that include the following:

    i. Verification of user identity before any password resets.

    ii. Passwords are at least 8 characters and have at least 3 of the following four character types: - Upper case letters - Lower case letters - Westernized Arabic numerals (1, 2, ….9) - Non-alphanumeric (special) characters (e.g.? |, %, $, #, etc.) or equivalent international language representations.

    iii. Passwords cannot be identical to the last 5 previously used passwords over a 12-month period.

    iv. Passwords have a maximum validity of 90 days

    v. Default, temporary or pre-set passwords are set to unique values and changed immediately after first use.

    vi. Limit repeated access attempts by locking out the user ID after not more than six (6) attempts with a thirty (30) minute minimum lockout duration.

    vii. If a session has been idle for more than fifteen (15) minutes, require the user to re-enter the password to reactivate the terminal.

    viii. Passwords must never be transmitted, displayed or printed in clear text.

e. There shall be Identity and Access management (IAM) controls in place for access to Ericsson Information that provide methods for:

    i. using unique User IDs

    ii. authorizing and administering access rights and access privileges

    iii. ensuring that access rights and access privileges remain appropriate

    iv. checking that obsolete access rights have been deleted on a regular basis, at least every 6 months and for privileged access at least every 3 months.

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

2.6 Cryptography

a. Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

b. The Supplier shall have ability to communicate securely with Ericsson through encrypted email, using industry standard encryption techniques.

c. Ericsson Information shall be protected by the use of encryption techniques or equivalent protection measures in transit and in rest.

d. Cryptographic keys shall be centrally managed in order to ensure processes are in place for generation, distribution, storage, archival, retrieval and destruction.

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

2.7 Physical and environmental security

a. Physical access to Supplier buildings shall be restricted to Personnel individually and on a need to have basis.

b. A clear desk policy shall be enforced to protect Ericsson Information and Assets.

c. Physical access to where Services are performed for Ericsson shall be restricted, by the use of individual swipe/proximity cards or other equivalent system and strengthened with PIN code.

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

2.8 Operations security

The following Operations security requirements are applicable for Suppliers providing Services that support the processing of Ericsson Information in a production environment.

a. Supplier shall register and maintain an inventory of information technology components that are part of the Service.

b. Systems shall be provisioned with sufficient capacity to ensure continued availability in the event of a security incident.

c. Systems shall ensure malicious software protection is deployed and kept up to date.

d. All privileged user actions shall 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.

e. Information about important security-related events shall 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 and IP address, where technically feasible.

f. Log records shall be stored for at least 6 months and made available to Ericsson when requested.

g. Back-ups shall be performed and maintained to ensure continuity and delivery expectations.

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

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

2.9 Communications security

a. Systems containing Ericsson Information shall be protected by firewall(s) and properly hardened, i.e. removing or disabling software and functionalities that are not being used.

b. Supplier networks used to access Ericsson Information or Ericsson networks shall have security controls that can protect against unauthorized traffic interception or interference by making use of firewalls, intrusion detection/prevention, etc.

c. Wireless network connections transferring Ericsson Information shall be encrypted according to best practice.

d. Supplier shall deploy technology to scan Supplier’s corporate email for viruses and malicious code and links and keep such technology up to date.

2.10 System acquisition, development and maintenance

a. Operational environments containing Ericsson Information shall be separated from development and testing environments.

b. The use of Ericsson Information from a production system shall not be permitted in test and development systems.

2.11 Sub-contractor relationships

a. Disclosing Ericsson Information to a third party, such as a Third Party Sub-Processor, shall only be allowed with prior written consent from Ericsson and only for the purposes identified in contractual agreements with Ericsson.

b. Third Party Sub-Processors shall be restricted to only the necessary access, use, retention and disclosure of Ericsson Information needed to fulfill contractual obligations.

c. Third Party Sub-Processors shall be given clear instructions on security measures for protecting Ericsson Information.

2.12 Incident management

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

b. Supplier shall report confirmed security incidents or weaknesses involving Ericsson Information or Services for Ericsson as soon as practicable or as otherwise agreed upon.

c. Supplier shall cooperate fully with Ericsson in dealing with these reports. Cooperation may include providing access to computer-based evidence data[1] for forensic evaluation.

2.13 Business Continuity Management

The following Business Continuity Management requirements are applicable for Suppliers providing Services that support Ericsson infrastructure or the processing of Ericsson Information in a production environment.

a. Supplier shall implement a Business Continuity Plan (BCP) that is tested annually.

b. Supplier shall conduct a Business Impact Analysis and Risk Assessment (BIA/RA) to identify and mitigate potential threats and hazards to Ericsson Information.

c. Business continuity incidents that have an impact on the execution of the Service to Ericsson shall be logged, analyzed, and reviewed by the Supplier and reported to Ericsson in a timely manner or as otherwise agreed upon.

[1] Evidence data may reside on devices such as office desktops/work-stations, laptops, network file servers, removable memory devices, backup tapes, etc.)

3 Data Privacy

The following data privacy requirements are applicable for when Supplier is Processing Personal Data on behalf of Ericsson. These requirements are in addition to the requirements already placed on Ericsson Information. Data Privacy at a local level must always be undertaken within the context of applicable legal and contractual requirements.

a. Top management shall set direction for and show commitment to privacy. At a minimum there shall be a high-level privacy policy that applies enterprise-wide and assignment of overall responsibility for privacy to a top-level executive or equivalent.

b. Supplier shall ensure protection and privacy of Personal Data related to Services in accordance with relevant data protection legislation and regulations.

c. Personal Data, including redacted or Anonymized Personal Data, shall not be used for any other purpose than meeting contractual agreements with Ericsson.

d. Personal Data collected for different purposes shall be processed separately.

e. Personal Data shall not be accessed without prior authorization.

f. Authorized Personnel shall only have access to the least amount of Personal Data to carry out their job duty.

g. Personnel with access to Personal Data shall be required to take appropriate data privacy training on a regular basis.

h. Personal Data shall be retained for only as long as necessary to fulfill the stated purposes in contractual agreements with Ericsson, or as required by law or regulations, and shall thereafter be appropriately returned or disposed at the choice of Ericsson.

i. The disposal of Personal Data shall be recorded to certify to Ericsson that such disposal has taken place.

j. Where the return or disposal of some or all of the Personal Data is prevented by law or regulation, the Personal Data shall be kept confidential or anonymized and shall no longer be processed. Ericsson shall be informed if such obligations exist immediately when supplier becomes aware of them.

k. Personal Data shall not be excessively stored, printed, copied, disclosed or other means of Processing outside the purpose for use.

l. The Data Subject shall be provided with access to his or her Personal Data for review.

m. In the event the Data Subject does not have direct access to his or her Personal Data, the Personal Data shall be transferred to Ericsson in order to support any Data Subject request, without answering the request unless authorized to do so.

n. Inaccurate Personal Data shall be corrected when the Data Subject or Ericsson on the Data Subject's behalf, has made a request for correction.

o. As long as the correctness of data is disputed the data shall be blocked for processing.

p. Disclosing Personal Data to a third party, such as a Third Party Sub-Processor, shall only be allowed with prior written consent from Ericsson and only for the purposes identified in contractual agreements with Ericsson. Ericsson shall have the right to evaluate the contractual terms and conditions described in section 3.q.

q. Prior to Supplier transferring Personal Data to a Third Party Sub-Processor, the Supplier shall ensure responsibilities of Supplier and of the Third Party Sub-Processor are clearly described and implemented as part of the commercial contract. The terms and conditions set out below shall be analyzed on a case by case basis:

    i. The clear agreement that Ericsson is either the Data Controller or Data Processor and the Supplier and Third Party Sub-Processor are the data Sub-Processors

    ii. The clear agreement that Supplier has the right to audit the Third Party Sub-Processor with respect to data privacy.

    iii. The clear definition of what constitutes Personal Data.

    iv. The clear definition of applicable law(s) for processing Personal Data and for transferring such information cross border.

    v. Clear instructions on when and where the Third Party Sub-Processor is expected to report a Privacy Breach.

    vi. Clear instructions on security measures for protecting privacy including the appropriate technical and organizational measures to safeguard the Personal Data to the same or higher level of protection as provided by Ericsson.

r. Third Party Sub-Processors shall be restricted to only the necessary access, use, retention and disclosure of Personal Data needed to fulfill contractual obligations.

s. Personal Data shall not be transferred to or accessed from a country other than the country of the Data Subject's citizenship without prior written consent from Ericsson.

t. Records shall be kept in an auditable manner showing which Personal Data has been transferred to which countries.

u. Reasonable steps shall be taken to ensure Personal Data is correct and accurate.

v. Supplier shall have a process in place to report and handle Privacy Incidents and/or Breaches as well as address inquiries, complaints and disputes.

w. Supplier shall report confirmed Privacy Breaches to Ericsson as soon as possible or as otherwise agreed in writing. Supplier shall co-operate fully with Ericsson in dealing with these reports.

x. Where legally required, Supplier shall agree to cooperate with data privacy related government body or agency, however notice must be given to Ericsson prior to such cooperation.

4 Compliance

a. Supplier internal audits and/or assessments concerning security and privacy shall be performed regularly by trained Personnel and findings shall be evaluated for possible corrective actions.

b. Upon 30 days' request from Ericsson, Supplier shall be able to demonstrate compliance with this BISPRS and any other security and privacy requirements or measures that have been agreed with Ericsson. Identified non-compliance shall be dealt with as agreed by the parties.

5 Definitions

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

Anonymous	Personal Data elements have been removed so that the remaining information cannot identify an individual or the identification would require a disproportional amount of time, expense and effort. Also referred to as “de-identified” and “anonymized”.
Data Controller	Natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
Data Processor	Natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the Data Controller.
Data Subject	An identified or identifiable person to whom specific Personal Data relates. It is someone who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more specific factors (physical, physiological, mental, economic, cultural, social).
Ericsson Asset	Information assets and Physical assets that have been entrusted to the Supplier or are part of the service.
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 Data.

Personal Data	Personal Data shall mean any information that can be related to an identified or identifiable living 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 identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. The terms “personally identifiable information (PII)”, “Personal Data”, “private information”, “sensitive Personal Data”, “special categories of data” and “legally protected information” are often used interchangeably to refer to information relating to individuals. The terms “customer data” and “subscriber information” are commonly used to refer to information relating to subscribers or other end-users.
Personnel	Each individual performing work for Ericsson on behalf of the Supplier.
Privacy Breach	The unauthorized access, use or disclosure of Personal Data in a manner not permitted by law, regulation or contract, which compromises the security and privacy of Personal Data and which creates a substantial risk of identity theft, fraud or harm against an individual.
Privacy Incident	The unauthorized access, use or disclosure of Personal Data, or any similar term referring to situations where persons other than authorized users, and for other than authorized purpose, have access or potential access to Personal Data. Not all Privacy Incidents are considered to be Privacy Breaches.
Processing	Processing of Personal Data means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means (for example: collection, recording, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, deleting or destruction, etc.).

Service	A delivery of goods or services by Suppliers to Ericsson.
Subcontractor	Business partners, vendors and providers of outsourced business.
Supplier	The company which has received a purchase order from Ericsson and will provide Services.
Third Part Connection (TPC)	Access to Ericsson's information systems or networks from a network outside Ericsson's control by individuals or bodies who are not part of Ericsson. A TPC Solution applies whenever an Ericsson business wants to establish a IS/IT environment between the external company and ECN at Ericsson according to the Business Agreement between Ericsson and other external parties. **Note:** A valid Business Agreement must be in place for a Third Party Connection to be implemented.
Third Party Sub-Processor	A Third Party Sub-Processor is a supplier who processes Ericsson Information on behalf of the Supplier.