Baseline Information Security and Privacy Requirements for Suppliers

Requirements Specification

ENT Group Baseline Information Security and Privacy Requirements for Suppliers (BISPRS) are applicable for all supplier relations where the supplier shall process ENT Group information within their IT-environment and is a way to ensure that the information stays protected, both in transit between ENT Group and the Supplier and in the custody of the supplier, at the level required by ENT Group.

The requirements represent the minimum level that the Supplier, its affiliates, subcontractors and their Personnel performing any Services on behalf of ENT Group, shall comply with in order to maintain ENT Group's level of commitment to the protection of ENT Group Information where services may include the processing of ENT Group Information.

Supplier shall protect ENT Group Information by implementing applicable requirements as set forth in this Document and evidence a structured approach to information security and data protection by being aligned with the latest version of the international standard ISO/IEC 27001 or other established standard, unless otherwise agreed in writing.

Communications to ENT Group 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: etk.company@ericsson.com, appointed point of contact or as otherwise specified in contractual agreements.
This document undergoes reviews on a regular basis and will be updated from time to time. ENT Group 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.

1. Information Security

Supplier shall evidence a structured approach to information security through working in alignment with the latest version of the international standard ISO/IEC 27001 or equivalent standard.

1.1 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. Suppler shall announce and notify ENT Group of any planned changes to its security policies. No changes to Supplier policies that weaken the security protections or contradict this document shall be allowed.

1.2 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 ENT Group Information without authorization or detection.

1.3 Human resource security

a. Personnel at the supplier, with access to ENT Group Information, shall have has signed an internal Non-Disclosure Agreement (NDA) with the Employer.
b. Personnel at the supplier with access to ENT Group Network Infrastructure and information shall sign a Statement about the obligation of professional secrecy.
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 ENT Group Information shall be required to take appropriate security and privacy training on a regular basis.
f. Non-compliance by Personnel in relation to this Document shall be addressed through appropriate disciplinary actions imposed by Supplier.

1.4 Asset management

a. The supplier shall handle ENT Group Information as Confidential information.
b. ENT Group Information shall not be excessively stored, printed, copied, disclosed or processed by other means outside the purpose for use.
c. ENT Group Information shall be processed and stored logically separated from the Suppliers own information and from that of other customers.
d. Upon conclusion or termination of Supplier's work for ENT Group, the Supplier shall sanitize and securely destroy (or at ENT Group's request, return to ENT Group) all copies of all ENT Group Information, including all backup and archival copies, in any electronic or non-electronic form.

1.5 Access control

a. Access to ENT Group's information systems or networks from a network outside ENT Group's control by individuals or bodies who are not part of ENT Group is only allowed through an approved Third-Party Connection (TPC) provided by ENT Group.
b. Access to ENT Group Information shall be restricted to Personnel individually and on a role-defined and need to know basis.
c. Access to systems and networks that contain ENT Group Information shall enforce two factor authentication methods.
d. There shall be a password selection and management controls in place for accessing ENT Group Information, the password management system shall support either of the following two systems.

System 1

i. Passwords shall be at least 8, and up to 64, characters in length, without further requirements for complexity (e.g., upper/lower case, numeric and special characters, etc.), though all characters shall be allowed
ii. Passwords shall not expire, unless there is reason to believe the password may have been compromised
iii. During the selection process, passwords shall be checked for sequential or repetitive characters (e.g., 12345678, aaaaaaaa, etc.), context, commonly used passwords , previous breaches, and dictionary words. These shall be disallowed.

System 2

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 types of characters: - 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 15 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 ten (10) attempts with a fourty-five (45) minutes 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 are Identity and Access management (IAM) controls in place for access to ENT Group Information:
    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 ENT Group Information has been accessed, modified, disclosed or disposed.

1.6 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 ENT Group through encrypted email, using industry standard encryption techniques.
c. ENT Group 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.

1.7 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 ENT Group Information and Assets.
c. Physical access to where Services are performed for ENT Group shall be restricted, by the use of individual swipe/proximity cards or other equivalent system and strengthened with PIN code.
d. d. Physical access to where Services are performed for ENT Group shall log physical access related events such as date, time, swipe/proximity card-id, door-id, access denied, or access granted.

1.8 Operations security

The following Operations security requirements are applicable for Suppliers providing Services that support the processing of ENT Group 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 ENT Group 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.

1.9 Communications security

a. Systems containing ENT Group 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 ENT Group Information or 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 ENT Group 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.

1.10 System acquisition, development and maintenance

a. Operational environments containing ENT Group Information shall be separated from development and testing environments.
b. The use of ENT Group Information from a production system shall not be permitted in test and development systems.

1.11 Sub-contractor relationships

a. Disclosing ENT Group Information to a third party, such as a Sub-Processor, shall only be allowed with prior written consent from ENT Group and only for the purposes identified in contractual agreements with ENT Group.
b. Sub-Processors shall be restricted to only the necessary access, use, retention and disclosure of ENT Group Information needed to fulfill contractual obligations.
c. Sub-Processors shall be given clear instructions on security measures for protecting ENT Group Information.

1.12 Incident Management

a. Supplier shall have a documented security incident management process to detect and handle incidents. Supplier shall report confirmed security incidents or weaknesses involving ENT Group Information or Services for ENT Group as soon as practicable or as otherwise agreed upon. Security related incidents should be reported to: etk.company@ericsson.com, appointed point of contact or as otherwise specified in contractual agreements.
b. Supplier shall cooperate fully with ENT Group in dealing with these reports. Cooperation may include providing access to computer-based evidence for forensic evaluation.

1.13 Business Continuity Management

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

a. Supplier shall implement a Business Continuity Plan that is tested annually.
b. Supplier shall conduct a Business Impact Analysis and Risk Assessment to identify and mitigate potential threats and hazards to ENT Group Information.
c. Business continuity incidents that have an impact on the execution of the Service to ENT Group shall be logged, analyzed, and reviewed by the Supplier and reported to ENT Group in a timely manner or as otherwise agreed upon.

2. Data Privacy

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

a. Supplier's top management shall set direction for and show commitment to privacy. There shall be privacy policies and processes in place that apply enterprise-wide and assignment of overall responsibility for privacy to a top-level executive or equivalent. Roles and responsibilities related to the Processing of Personal Information should be clearly defined and allocated. Suppler shall announce and notify ENT Group of any planned changes to its privacy policies. No changes to Supplier policies that weaken the privacy protections or contradict this document shall be allowed.
b. Supplier shall ensure protection and privacy of Personal Information related to Services in accordance with any applicable data protection legislation and regulations and ENT Group instructions.
c. Personal Information or Anonymous data shall not be used for any other purpose than the purposes defined in the agreement with ENT Group.
d. Supplier shall not transfer Personal Information from workstations to external storage devices (e.g. USB, DVD, external hard drives).
e. Where appropriate, Supplier shall pseudonymize Personal Information.
f. Personal Information shall not be accessed without prior authorization.
g. Authorized Personnel shall only have access to the least amount of Personal Information to carry out their job duty. The use of common user accounts should be avoided. In cases where this is necessary, it should be ensured that all users of the common account have the same roles and responsibilities.
h. Personnel with access to Personal Information shall be required to take appropriate data privacy training at least once a year or more frequently if reasonably required by the ENT Group (e.g. in case of incidents, implementing privacy/security changes and updates and alike).

i. Supplier shall have in place processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures to ensure the security of the Processing. Processes shall be tested, and the tests shall be documented at least once a year.
j. Personal Information shall be retained for only as long as necessary to fulfill the stated purposes in contractual agreements with ENT Group, or as required by law or regulations, and shall thereafter be appropriately returned or securely and completely disposed at the choice of ENT Group.
k. The disposal of Personal Information shall be recorded to certify to ENT Group that such disposal has taken place.
l. Where the return or disposal of some, or all of the Personal Information is prevented by law or regulation, the Personal Information shall be kept confidential or anonymized and shall no longer be actively processed. ENT Group shall be informed if such obligations exist immediately when supplier becomes aware of them.
m. Personal Information shall not be excessively stored, printed, copied, disclosed or other means of Processing outside the purpose for use.
n. Supplier shall follow ENT Group's instructions and assist ENT Group to comply with the requests to exercise Data Subject rights under applicable laws and regulations.
o. In the event that Supplier receives a request from a Data Subject, such request shall be transferred to ENT Group without undue delay. Supplier shall not respond to Data Subject requests unless instructed and authorized to do so by ENT Group.
p. Inaccurate Personal Information shall be corrected in accordance with ENT Group's instructions.
q. Disclosing Personal Information to a third party, such as a Sub-Processor, shall only be allowed with prior written consent from ENT Group, for the purposes identified in an agreement with ENT Group or in ENT Group instructions and in a manner that is aligned with applicable data protection regulations. If Sub-Processor fails to fulfil its data protection obligations, Supplier shall remain fully liable to the ENT Group for the performance of Sub-Processor's obligations.
r. Prior to Supplier transferring Personal Information to a Sub-Processor, Supplier shall ensure responsibilities of Supplier and of the Sub-Processor are clearly described and agreed in a commercial contract that sets out the same data protection obligations as the agreement between Supplier and ENT Group. ENT Group shall have the right to evaluate the terms of such contract. The terms and conditions set out below shall be added to the contract:
    i. The clear agreement that ENT Group is either the Data Controller or Data Processor and Supplier and Sub-Processor are processors or sub-processors.
    ii. The clear agreement that Supplier and ENT Group have the right to audit the Sub-Processor with respect to data privacy.
    iii. The clear definition of what constitutes Personal Information.
    iv. The clear definition of applicable law(s) for Processing Personal Information and for transferring such information cross international border.
    v. Clear instructions on when and where the 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 Information to the same or higher level of protection as provided by ENT Group.
s. Third Party Sub-Processors shall be restricted to only the necessary access, use, retention and disclosure of Personal Information needed to fulfill contractual obligations.
t. Records shall be kept in an auditable manner showing which Personal Information has been transferred to which countries. Supplier should have a register of the IT resources used for the Processing of Personal Information on ENT Group's behalf (hardware, software, and network).

u. u. Supplier shall have a process in place to report and handle Privacy Breaches as well as address inquiries, complaints and disputes.
v. v. Supplier shall report Privacy Breaches Supplier becomes aware of to ENT Group immediately, without undue delay or as otherwise agreed in writing. Supplier shall co-operate fully with ENT Group in dealing with these reports.
w. w. Where legally required, Supplier shall agree to cooperate with data privacy related government body or agency, however notice must be given to ENT Group prior to such cooperation.

3. 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 ENT Group, Supplier shall be able to demonstrate compliance with this BISPRS and any other security and privacy requirements or measures that have been agreed with ENT Group. Identified non-compliance shall be dealt with as agreed by the parties.

4. 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 Information elements have been irreversibly 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 Information.
Data Processor	Natural or legal person, public authority, agency or any other body which processes Personal Information on behalf of the Data Controller.
Data Subject	An identified or identifiable person to whom specific Personal Information 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).

ENT Group Asset	Information assets and Physical assets that have been entrusted to the Supplier or are part of the service.
ENT Group Information	Information proprietary to ENT Group, ENT Group's customers, other third parties which have business relations with ENT Group and other information being part of the Service. ENT Group Information includes Personal Information.
Personal Information	Personal Information 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 “Personal Information”, “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 ENT Group on behalf of the Supplier.
Privacy Breach	The breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing	Processing of Personal Information means any operation or set of operations which is performed upon Personal Information, 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 ENT Group.
Subcontractor	Business partners, vendors and providers of outsourced business.
Sub-Processor	A sub-processor is a supplier who processes ENT Group Information on behalf of Supplier.