ERICSSON

Physical Security Supplier Requirements in High Risk Areas

Security Requirements

Abstract

This document outlines Physical Security requirements on suppliers working on behalf of Ericsson in countries or areas defined as high or extreme security risk.

Contents

1 Introduction

The security of Ericsson's personnel, products, services, solutions and IT environments is critical to Ericsson's business. Ericsson's most crucial asset is Ericsson's people, including suppliers' resources performing work on behalf of Ericsson for Ericsson's customers. Ericsson expects all its suppliers to uphold Ericsson standards concerning safeguarding personnel, which is essential in High Risk Areas.

This document describing Ericsson's Physical Security Supplier Requirements (PSSR) presents physical security measures applicable for all supplier relations where the supplier is performing services for Ericsson in High Risk Areas. The supplier will be informed if the project is located in an area defined as a High Risk Area by Ericsson.

Section 2 of this document includes the standard physical security measures always applicable in High Risk Areas. Section 3 includes supplemental physical security measures that, in whole or in part, can be applicable, e.g., as a result of a Security Risk Assessment that Ericsson chooses to perform for the relevant project. The supplier must at all times comply with the standard physical security measures as well as any supplemental physical security measures specified by Ericsson when providing services in High Risk Areas.

Supplier must ensure that its subcontractors performing services in High Risk Areas, complies with the requirements herein applicable to the Supplier. Supplier acknowledges that it is responsible and liable for the acts or omissions of a subcontractor to the same extent as if the Supplier would have performed or committed the acts or omissions itself.

2 Standard Physical Security requirements

The following standard physical security measures always apply for suppliers delivering services to Ericsson in High Risk Areas.

2.1 Physical Security risk and incident disclosure

Physical security-related incidents that have or may have an impact on Ericsson's operations and/or personnel must be reported to Ericsson.

2.2 Physical Security risk management

Supplier must;

a) have and adhere to a documented physical security risk management process including at least a physical risk security assessment and physical security plan for its operations and personnel (this process may be supplier specific),

b) inform Ericsson if, in the area Supplier is delivering services for Ericsson, Supplier discover new physical security risks,

c) educate and update its staff on the physical security measures stated in this document,

d) provide Supplier's point of contact at Ericsson with the contact information to the Supplier's responsible person for physical security,

e) notify Supplier's point of contact at Ericsson about the number of personnel working for Ericsson and the frequency of deployment,

f) share site coordinates for its personnel in advance for security assessment purposes as well as to ensure that journey management plans are followed,

g) inform its personnel about the applicable policies when Ericsson's customer's site security and physical security policies applies, and

h) ensure that all travels to and within high risk areas by supplier personnel are at such personnel's own free will.

2.3 Security service provider

When delivering services to Ericsson's customers in High Risk Areas, Ericsson may engage third party security service providers to ensure the physical security of Ericsson and non-Ericsson personnel. Ericsson and the Ericsson appointed security service provider shall have the authority to instruct the Supplier personnel during Ericsson business related activities when it comes to travel and movements.

2.4 Physical Security deployment onboarding

Personnel involved in projects within a High Risk Area must go through a physical security onboarding session by Ericsson or by the Ericsson appointed security service provider before personnel are deployed at such High Risk Area.

3 Supplemental Physical Security requirements

Depending on the assessed situation in the High Risk Area where personnel are to be deployed, some or all of the supplemental requirements listed below can be applicable.

The risk situation in High Risk Areas can change with short notice. Thus, the continuous risk monitoring by Ericsson and its partners may result in a need to amend the supplemental physical security supplier requirements in this Section 3. The Supplier agrees to accept amendments to this document for specific projects as reasonably required by Ericsson to ensure Ericsson's compliance with applicable laws.

3.1 List of supplemental physical security supplier requirements in High Risk Areas

3.1.1 Travel security risk management

1. Movement of Supplier personnel must be tracked and monitored for the duration of trips related to Ericsson business activities, as far as legally permissible under the relevant data protection laws.

2. Supplier must provide drivers and vehicles to its personnel for Ericsson business travel purposes, using vehicles fit for purpose depending on the type of terrain/road.

3. Vehicles provided by Supplier must be equipped with tracking, geofencing and first aid kit.

4. Supplier must confirm that personnel engaged in the relevant project for Ericsson has gone through basic driving training and awareness.

5. Services of unarmed or armed security escorts, where assessed by the Ericsson appointed security service provider as necessary, are to be engaged by the Supplier to cover local movement of Supplier personnel.

6. Routes to be used must be plotted and assessed by Supplier as well as presented to Ericsson Security for review and sign-off. No deviation from the signed-off route shall be allowed by Supplier personnel unless instructed by Ericsson Security or the Ericsson appointed security service provider.

3.1.2 Deployment risk management

7. Supplier personnel undertaking project activities requiring visiting Ericsson's customer offices / customer sites must be local and residing in the specific city/area. Ethnic tensions must be considered.

8. Before deployment of Supplier personnel, security clearance must be formally provided and approved by the Ericsson appointed security service provider.

9. Supplier personnel must have software installed on their mobile work phones that ensures they can be tracked 24/7, to the extent permitted by privacy laws and regulations.

10. In the case Ericsson sets up a Command Operating Center ("COC"), all Supplier personnel are required to strictly follow all security recommendations from the COC.

11. No movement allowed by Supplier personnel outside the designated area/s after working hours without Ericsson or Ericsson appointed security service provider approval.

12. Night activities are only approved for certain matters and only within designated area/s (e.g., in customer data center manned 24/7 by security guards).

13. Supplier personnel are, when working for Ericsson, not allowed to visit areas classified as no-go by Ericsson Security.

3.1.3 Emergency/security incident management

14. Supplier must ensure emergency support is available to its personnel and emergency contact numbers provided when required.

15. Supplier must confirm that local personnel, if deployed for Ericsson projects, has relevant medical insurance.

16. Supplier personnel must follow Ericsson advice on alternative communication in case of unavailability of mobile service.

17. Supplier personnel which are part of Ericsson project team, must map out medical facilities in respective locations, indicating their capacities to handle medical emergencies.

18. Supplier personnel must in case of a serious widespread physical security situation (natural disaster, terrorist attack, etc.), comply with all instructions and directives issued by local authorities.

4 Compliance

Supplier internal audits and/or assessments concerning physical security requirements in High Risk Areas must be performed regularly by trained personnel. Findings must be evaluated for possible corrective actions.

Ericsson has the right to perform an audit of the Supplier's compliance to the standards/measures/requirements set out in this document no more than once per calendar year, or when there is a suspected or verified security issue or event.

Supplier agrees to maintain appropriate records of how they comply with the requirements in this document. If requested by Ericsson, Supplier shall without undue delay provide any certificate and/or any other documentation necessary to demonstrate compliance with this document and any other security requirements or measures that have been agreed with Ericsson. Identified non-compliance must be corrected promptly without additional costs to Ericsson. If identified non-compliances are not corrected in due time, Ericsson has the right to withdraw the assignment with immediate effect.

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.

COC	Command Operations Center. A function established for daily monitoring and assessment of the security situation, as well as for approving deployments for all projects in a high-risk country or area.
Ericsson	Telefonaktiebolaget LM Ericsson ("**LME**") and direct and indirect subsidiaries controlled by LME.
High risk area	A country or specific area/s of a country where the security environment presents persistent and serious challenges and risks for business. Factors that impact the security risk include but are not limited to military conflict, insurgency, terrorist attacks, strikes and riots, vandalism, kidnapping, and violent and acquisitive crime.
Project	A defined scope of services and/or products to be delivered to a customer within a certain timeframe at an agreed price and quality.
Security risk assessment	An assessment performed by Ericsson of the physical security risks related to a project in a High Risk Area.
Security Incident	A Security Incident is an event that occurs due to a weakness, failure, gap or violation of Ericsson's security measures which directly or indirectly harm assets, resources and/or operations for which Ericsson is responsible.
Physical Security Incident	A Physical Security Incident is an incident that directly or indirectly harm the physical security of people or physical assets. This include (but is not limited to) threats, violence, attacks, crime, vandalism, and kidnappings.
Supplier	In this context; Entity providing services to Ericsson