OUR ENTERPRISE SECURITY
Today's business environment is driven by change. Three fundamental ICT forces – broadband, mobility and cloud – are rapidly reshaping value chains, digitalizing business models and creating possibilities that were previously unimaginable. A revolution is taking place around us – and remarkably, it’s only just getting started. Ericsson’s vision is a Networked Society where every person and every industry is empowered to reach their full potential.

The Networked Society creates benefits for people, business and society. The technological evolution that enables this positive change also brings new privacy and security risks as connected devices, networks and services become potential targets for fraud, information and identity theft, denial-of-service attacks and malware.

Technology also brings new potential ways of using and transferring data in ways that may be restricted or conditioned by law or which create privacy risks in other ways.

### Ericsson as A Trusted partner

More than 40 percent of the world’s mobile traffic passes through networks delivered by Ericsson, and we manage networks that together serve over 1 billion subscribers. This unique global position gives us the responsibility and opportunity to be a thought leader in Security and Privacy. We see leadership as essential for building trust in the technologies that are enabling the Networked Society. This document gives a brief overview of Ericsson’s approach to the privacy and security challenges of the transforming industry.

### Privacy

#### What is privacy?

Privacy is recognized as a fundamental human right by the United Nations (UN) in Article 12 of the Universal Declaration of Human Rights, as well as in other UN conventions. Ericsson is therefore fully committed to ensuring the right to privacy of people, business and society, as we lead ICT transformation across industries and enable the Networked Society.

Definitions of privacy can vary between stakeholders and countries. However, broadly speaking, privacy is the right to be left alone or to enjoy freedom from interference or intrusion, including the right to have some control over how personal information is collected, used, retained and disposed of.

The content of privacy laws varies between countries but such laws often include restrictions or conditions on the usage of information relating to individuals and the cross-border transfer of such information. In addition, adequate organizational and technical security measures are common prerequisites for allowing personal information to be processed.

In summary it means that fulfillment of privacy commitments entails fulfilling legal, ethical and security requirements.

---

**What is Ericsson doing?**

We align our business with legal requirements for privacy, such as for example the European General Data Protection Regulation. We pursue a comprehensive Global Privacy Program which includes top management commitment, dedicated privacy resources, global steering documents on privacy and security, training, audits, privacy breach handling processes, record keeping when required, privacy by design and privacy impact assessments. The Program further includes principles of contractual arrangements with customers and suppliers on data protection.

Respect for the right to privacy, and the importance of protecting information, personal and non-personal, is included in our Code of Business Ethics being further described below. Along with professionalism and perseverance, the concept of respect is one of Ericsson’s three core values and therefore forms part of the foundation of our company culture.

We recognize that securing privacy in a connected world requires a sustained cross-industry effort. New technologies bring new privacy implications, and continuous dialog between industry, governments, regulators and civil society is essential. Ericsson is committed to driving and participating in these multi-stakeholder discussions. Just as Ericsson is committed to the protection of personal information, helping our customers to develop trust relationships with consumers and businesses.
Our Code of Business Ethics
The Ericsson Code of Business Ethics is our tool to be a trusted partner, to conduct business responsibly and to remind us that every action counts. Our aim is to act with responsibility, accountability and transparency as we help to build the Networked Society.

As a Swedish company in existence for over 140 years, with a global presence, we understand the importance of doing business sustainably and creating long-term value and trust that are critical to ongoing business success.

Good governance is fundamental to conducting business responsibly across our operations. Our Ericsson Code of Business Ethics sets the tone for how we conduct business globally. The Ericsson Code of Business Ethics is an overview of our fundamental Group policies and directives, guiding Ericsson’s relationships among employees and with external stakeholders.

The Ericsson Code of Business Ethics contains rules for all individuals performing work for Ericsson, under the staff management of Ericsson or in Ericsson premises, whether as an employee of Ericsson or a subcontractor, or as a private contractor. The Ericsson Code of Business Ethics is periodically reviewed and acknowledged by all employees and is translated into more than 30 languages to ensure that it is accessible to all employees.

Information security
Business success in the Networked Society demands the protection of ever increasing volumes of information. Our approach for securing information relating to individuals and business-critical information is designed to provide a competitive advantage, protect our technology and services leadership.

Information Security at Ericsson ensures that all types of information including information relating to individuals (“Information Assets”) are protected according to the sensitivity of the information; available when needed; and protected from unauthorized access or modification.

Our approach
Ericsson’s approach to Information Security is based on being able to predict, detect and counter threats to the confidentiality, integrity and availability of Information Assets within Ericsson, while ensuring the correct access to the right information when needed.

We do this by building on the following strategic cornerstones:

- Knowing our threats
- Risk based protection
- Building a security conscious culture
- Responding efficiently

We work systematically to evaluate protection needs of information and identify and counter potential threats through Ericsson-specific threat analysis. We have a robust security baseline combined with differentiated security measures that are implemented as determined by information criticality.

By continuously demonstrating leadership in the global information security arena, we aim to achieve and maintain market and customer trust in this area. A security-conscious culture is achieved throughout the strategic, tactical and operational layers of Ericsson globally.

The information security organization, with its clear responsibility for requirement setting, advisory support and follow-up, leverages a holistic overview to gain critical insights to effectively govern this area.

ISO/IEC 27001 Information Security Management System and Certification
Ericsson’s Information Security Management System (ISMS) is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. The ISMS defines how we should manage information security in line with the international information security management standard ISO/IEC 27001.

There is centralized governance of the ISMS component of the Ericsson Group Management System (EGMS).
Ericsson’s ISMS has been certified against the 27001 standard. Our approach is to certify business operations and several Ericsson sites. We continue to increase the number of Ericsson sites included in our existing multi-site certificate.

**Ericsson Group Management System**
The ISMS is part of the Ericsson Group Management System (EGMS). ISO 9001 provides requirements that constitute the platform and enables us to aim for one global ISO 9001 certificate. The most obvious benefits of the certification are in terms of sales and marketing, since most of our customers have ISO 9001 certificate as a prerequisite.

**Security Management Maturity Model**
Security leaders proactively and professionally identify and address top concerns of key stakeholders to maximize the return on security investment. As a trusted business partner, security management is relied upon to provide input to support strategic and tactical business decisions and prioritizations. Ericsson uses its Security Management Maturity Model to measure and continually improve the security organization’s ability to:

- Effectively govern and manage all aspects of security, including compliance with customers, legal and regulatory security, privacy or continuity requirements
- Optimize the protection of the company’s critical business assets – people, information, operations and brand – through a unified, coordinated and competent security organization
- Measure performance
- Standardize global security frameworks and processes critical for quality, consistency and efficiency

**Product and Services Security**
Ericsson approach to today’s ICT security challenges rests on three pillars:

1. **Security as collaboration**
The global nature of ICT security requires vendors, operators, developers, governments and users (including consumers and enterprises) to work together. Through standardization, collaboration, openness and transparency, we can ensure that the optimal level of security is achieved.

Standards and best practices are fundamental to handle threats efficiently while building economies of scale, avoiding fragmentation and ensuring interoperability. Industry stakeholders, policymakers and regulators should set common and open standards that specify what needs to be secure and protected.

Ericsson has a long track record of taking an active and leading role in security standardization organizations to contribute to the development of secure networks and operational methodologies.

2. **Security as an integrated, holistic methodology**
Today’s networks are large and complex. Ericsson believes security technologies and controls should be an integrated part of all products, solutions, deployments, integrations and managed operations. Point security products alone are not sufficient to deliver the required system-wide integrity, robustness and resilience, although they can complement an integrated approach.
Networks can only be operated in a truly secure manner through secure development practices, secure products and secure processes. Ericsson works holistically to provide security – from product development and network architecture to designing operational processes and managing operations. In addition, we offer an expanding portfolio of industry-leading solutions to address specific use-cases and associated security scenarios.

3. Security as a continuous process
We see security as an ongoing activity that keeps pace with technology, applications and usage patterns. Our 24/7 frontline experience as a global ICT leader makes us exceptionally well-equipped to deliver security based on real-world needs and threats.

Ericsson Product Security Incident Response Team (PSIRT) assists customers and Ericsson global support organization in handling the technical and organizational aspects of security incidents. PSIRT address all types of computer and telecom security incidents which occur, or threaten to occur, at Ericsson’s customers that involve Ericsson’s products, solutions and 3rd party products included in those.

We also lead the industry in anticipating the security requirements of 5G, which is the next step in the evolution of mobile communication technologies. 5G security will be defined by qualitative considerations such as new business and trust models, new ways of delivering services in an evolved threat landscape and increased concern about privacy. Tackling these challenges will require tools such as network slicing, trusted computing and alternative ways of handling user identities.

We have a security portfolio of products, solutions and services and our entire portfolio uses Security as an integrated, holistic component.

Guiding principles
In addition to the three pillars of our approach, we have identified some general principles that can effectively guide the ICT industry in addressing security related concerns:

* Services should always be available: networks must be resilient and built in a way that allows fast recovery from attacks
* Security should require minimum effort from users: security solutions must be usable, scalable, manageable and non-intrusive
* Communications should be protected: security needs to be defined, implemented, managed and maintained not only as technical solutions but in compliance checks, secure operational processes and procedures, and with regular auditing and improvement
* All access to information and data should be authorized: there must be proper security mechanisms for authentication, authorization and access control
* Manipulation of data in networks should be possible to detect: the owner or the intended receiver of any data or communication should be able to access the information in its original form or detect if it has been manipulated
* Right to privacy should be protected: users must be able to feel their privacy is respected when using networked services, including secure storage and secure transmission of data. Clarity, transparency and permissibility toward users and compliance with laws and regulations for handling personal information, must therefore be the top priorities when handling private information

Knowing our threats
Threat Intelligence at Ericsson works toward establishing structures and methods for identifying and assessing threats related to the company and its operations, as outlined in the Ericsson Information Security Strategy.

Ericsson conducts its business in an increasingly complex environment. Therefore, it is essential to access relevant and timely information about the Ericsson-specific threat landscape and existing emerging threats. The focus is on actors with the intention and capability to harm or attack Ericsson. These actors can be state-affiliated such as state intelligence agencies conducting corporate espionage or security-motivated intelligence collection, or non-state affiliated such as criminal networks, terrorist organizations or internet activists with financial or political motivations. Threat assessments can have a global, regional or local scope; focus on specific business areas; or be related to other Ericsson-relevant issues.
The purpose of threat intelligence is to inform and support decision-making at different levels of the company and strengthen our capacity to manage risks and prioritize protection measures.

**Business Continuity Management**

Business Continuity Management (BCM) is a management process that identifies potential risks to our organization and provides a framework for building organizational resilience. This includes the capacity for an effective response which safeguards the interests of our customers, key stakeholders, reputation, brand and value-creating activities.

Ericsson has implemented a corporate BCM Framework, which is an integrated part of our EGMS. It is aligned toward ISO 22301 and ISO 27001 to ensure that it meets industry best practice.

Our critical business processes are identified through business impact analysis and risk assessment. Strategies for process recovery are defined and business continuity action plans are prepared to ensure that we can fulfill our commitments to our customers and partners. The plans are continuously reviewed and tested in order to ensure that they stay relevant and up-to-date. BCM and compliance frameworks are continually reviewed by Ericsson’s internal audit and security functions, as well as by impartial third-party.

The BCM framework is interconnected with our crisis management framework in order to support the business in cases where an interruption would escalate significantly in severity.

**Crisis Management**

Crisis is one or several incidents that could have severe impact on Ericsson’s business or staff and cannot be handled with ordinary operational procedures. At Ericsson we handle such events through our crisis management organization. Crisis management includes activities to prepare, respond and recover from a crisis, while maintaining the following priorities:

- Removing threats to life or safety
- Protecting the commercial interest of Ericsson and our customers and partners
- Protecting Ericsson and our customer’s brand
- Ensuring that Ericsson is acting as a responsible corporate citizen

Group Security provides instructions, methods and tools needed to implement and maintain a correct level of crisis management. Group Security also facilitates crisis management exercises and workshops. Our goal is to provide our personnel and our business with the best support possible in a crisis situation, thereby creating value for both our customers and the company as well as filling our role as a responsible corporate citizen.

Ericsson has carried out many successful tasks, including relocation of staff from places of unrest and rescue operations from earthquake-hit areas. Through our systematic work with after action reporting and experience sharing, each event has built on our capability to handle crises.

**Personnel security**

Personnel Security aims to protect people, Ericsson’s brand, and our customers interest. Personnel security includes travel security, security in high risk countries, executive protection and event security. The main purpose of personnel security is to identify and continually address life threatening risks to Ericsson’s staff and partners. The security measures we take enable us to operate safely and create customer value in high risk settings.

We offer information and training to our employees to stay safe when they are at work, regardless of whether they are in their home office, on assignments or on business trips. Group Security provides instructions, methods and tools needed to implement and maintain a correct level of personnel security. We also provide trainings on travel security and security in high risk countries.
We are committed to ensure a safe working environment and healthy workplaces around the world. We have a comprehensive organization and supporting tools to assist personnel in our business activities should an emergency occur. All personnel have access to a dedicated 24/7 emergency number and the latest travel advisories for all countries where we operate.

Looking Ahead
Risk Based Decision Making
“Security as a business enabler” is not a new concept; however, it is often difficult to see how this can be achieved. Ericsson believes that by making information available to end users and decision makers, along with the implementation of transparent security process, decisions that are based on risk will be able to be taken quickly, accurately and effectively.

Ericsson’s approach to security, involving collaboration across products, services and infrastructure, is designed to support the Networked Society vision.
Points of contact

> Ericsson Corporate Security Office
  corporate.security.office@ericsson.com

> Ericsson Product Security Incident Response Team (PSIRT)
  psirt@ericsson.com

> Ericsson Group Privacy
  ericsson.group.privacy@ericsson.com

> Media Relations
  media.relations@ericsson.com