Owner		Security
Group COO		Public
Approval Date	**Version**	**Approved by**
2023-03-08	5	Board of Directors
No.		**Related**
T 20845-09 Uen		50078926

GROUP POLICY - SECURITY

1 PURPOSE

The purpose of the Telia Company Group Security Policy is to support our purpose of reinventing better connected living by protecting Telia customers, employees, shareholders and the wider societies we operate in from both cyber and physical threats.

With critical business strategies increasingly dependent on digital solutions, Security Risk must now be considered a strategic business risk. As such, business leaders must track identified Security Risks within their business and allocate the appropriate resources for risk reduction activities.

2 SECURITY PRINCIPLES

This section identifies the Security Principles that enable the protection of Products, Processes, Platforms, People and Partners of Telia Company AB, Subsidiaries[1] and Joint Operations[2] from breaches in confidentiality, availability, and integrity. In order to avoid imposing a financial and administrative burden on entities, application of security requirements, based on these Security Principles must comply with regulatory, legislative, customer and national security requirements.

Implementation of security requirements linked to Security Principles must be risk-based and periodically verified.

- **Principle 1:** A Group security organization must be established and continuously improved to **govern** the organization's approach to security and privacy. In particular,
    - *Clear separation in the management, supervision, and independent assurance / audit of Security Risks must be implemented*
    - *The Security Risk Management framework must be integrated with widely recognized security and privacy standards and aligned to the Enterprise Risk Management (ERM) framework*
    - *The amount of Security Risk we are willing to assume in the pursuit of strategic objectives (Risk Appetite) must be defined and communicated*
    - *A security assurance / evidence -based security governance program and security control framework must be implemented*
    - *Business-relevant security outcomes and the overall Security Risk profile must be consistently reported to the Board of Directors and Group Executive Management (GEM) team*
    - *A measurable security training and awareness program must be implemented*
- **Principle 2:** Security requirements and processes that enable the **identification** of security risks to assets must be implemented (NIST CSF – Identify). This includes, but is not limited to,

[1] All entities over which Telia Company AB has majority control.
[2] The joint operations over which Telia Company AB has joint control and management responsibility.

- *Asset*[3] *inventory data and information that enable efficient security requirement implementation must be properly documented and managed in accordance with industry best practices*
- *Mission Critical (MC), Business Critical (BC), and Non-Critical assets must be identified, classified, logically labelled and secured*
- *Projects and initiatives must be managed to support the identification, assessment and management of Security Risks*
- *Security Principles must be mapped to applicable targets during mergers & acquisitions to determine gaps in data and information protection capabilities and security controls*
- *Security must be embedded within the supply chain*
- *Secure coding practices must be implemented*

- **Principle 3:** Security requirements and processes that enable the **protection** from security threats must be implemented (NIST CSF – Protect). In particular,
  - *Identity and access management controls must be in place*
  - *Physical security and monitoring controls must be implemented to, at minimum, prevent and detect intrusion and adverse effects on assets*
  - *Network security measures must be implemented*
  - *Information and data must be protected and preserved based on classification*
  - *Security configuration and hardening must be implemented and based on a Security Baseline*
  - *Security requirements must be embedded in human resource processes*
  - *Operational security processes must be implemented*
- **Principle 4:** Security monitoring requirements and processes must be implemented to **detect** security events (NIST CSF – Detect).
- **Principle 5:** Security requirements and processes that enable proper **response** and **recovery** from security incidents must be implemented (NIST CSF – Respond & Recover). In particular,
  - *Security incident response and recovery processes must be implemented and periodically tested*
  - *Security must be integrated with Business Continuity and Disaster Recovery requirements*

These Security Principles apply to the extent that they do not place Telia Company in violation of domestic laws and regulations. There are Group Instructions and Group Guidelines, containing subsequent detailed requirements, connected to the Security Principles within this Group Policy.

[3] Products, Processes, Platforms, People and Partners (5P) of Telia Company AB, Subsidiaries and Joint Operations

This document presents requirements in accordance with **RFC 2119**; specifically, the use of words **Must**, **Should**, **May**, and **Optional** and their negative counterparts **Must Not**, **Should Not**.

3 ROLES AND RESPONSIBILITIES

This Group Policy applies to Telia Company AB and its Subsidiaries[4] and Joint Operations[5] as their own binding policy to all directors, members of the boards, officers and employees. In addition, Telia Company works towards promoting and adopting this Policy's principles and objectives in other associated companies where Telia Company does not have control but has significant influence.

Each Group Executive reporting to the CEO of Telia Company is responsible for ensuring that this Group Policy is duly communicated and implemented, and that the employees within their area of responsibility are familiar with and follow this Group Policy.

Each country CEO is responsible for ensuring that all relevant entities within the CEO's geographic location has adopted and implemented this Group Policy.

4 BREACHES AGAINST THE POLICY

Any Telia Company employee who suspects violations of the Code of Conduct or this Group Policy must speak up and raise the issue primarily to their line manager, managers manager, People Partner, Ethics & Compliance Officer, or through the Speak-Up Line. The Speak-Up Line is available on Telia Company's internal and external webpages.

Telia Company expressly forbids any form of retaliation for people who speak up. For specific requirements, please see our Group Instruction - Speak Up and Non-Retaliation.

Violations against this Group Policy can lead to disciplinary action, up to and including termination.

5 TARGET GROUP

This Group Policy applies to Telia Company AB, its Subsidiaries and Joint Operations as their own binding policy. In addition, Telia Company works towards adopting Policy Security Principles in all other operations in which Telia Company has ownership interests. The Group Policy also applies to any third-party provider working under contract to any of the above-mentioned entities.

[4] All entities over which Telia Company AB has majority control.
[5] The joint operations over which Telia Company AB has joint control and management responsibility.

6 EXEMPTIONS

If a deviation or exemption from the Group Policy is deemed necessary, the Country CEO or Head of Group function shall escalate the matter to the Group General Counsel and the Document owner jointly. The exemption shall be documented, and a prior written approval must be given.

A Subsidiary-specific corresponding policy shall be compliant with the applicable Group Policy while adapting to the concerned business activities, local laws, local circumstances and language.

7 GROUP GOVERNANCE FRAMEWORK

This Group Policy is part of the Group Governance Framework, which includes without limitation:

a) Code of Conduct, Purpose and Values, Strategy, Group Policies, and Instructions for the CEO as approved by the Board of Directors;

b) Decisions made by the CEO, the Delegation of Obligations and Authority as approved by the CEO, Group Instructions as approved by the CEO or by the responsible Head of Group Function; and

c) Guidelines, best practices, process descriptions, templates or working routines developed within the area of responsibility of Head of Group Function.

8 REFERENCES

References for the development of this Policy included, but are not limited to, National Security Principles, widely recognized security frameworks (NIST CSF, ISO, ISF, etc.), and internal requirements.

9 VERSION HISTORY

Version	Date	Revised By	Items Changed Since Previous Version
V5	**31.01.2023**	**GRC Security**	• Alignment of Group Security with Telia Company purpose • Declaration of Security Risk as a strategic business risk • Emphasis on risk-based security • Re-statement of more clear and concise Security Principles • References and Terms and abbreviations added
V5	**23.02.2023**	**GRC Security**	• Minor editorial changes

10 TERMS AND ABBREVIATIONS

Terms and abbreviations	Definition
Business Critical (BC) asset	Products, Processes, Platforms, People and Partners in which interruptions have the potential to significantly impact the achievement of Telia Company business objectives and commercial ambitions
Mission Critical (MC) service / asset	**Mission Critical Service**: any service defined by national regulatory bodies

Terms and abbreviations	Definition
	as being critical for national security, defined by Telia as national critical infrastructure based on guidance from national regulatory bodies, or provided to Special Customers **Mission Critical Asset:** Products, Processes, Platforms, People and Partners (5Ps) that deliver **mission critical services** to meet national security obligations
Non-critical asset	Products, Processes, Platforms, People and Partners not considered Mission Critical or Business Critical
Security Baseline	Minimum level of security required for the business to operate securely
Security Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Security Principle	Security tenet to support business objectives and prepare instructions
Security Risk	Risks resulting from threats to employee and physical security, national security and cyber security
Security Risk Management	The process of identifying, evaluating, and treating risks