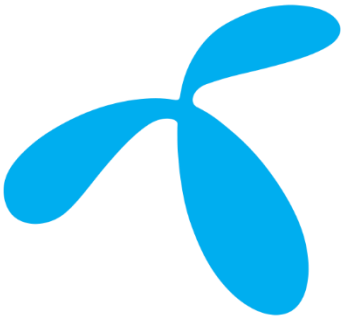
Security

GROUP POLICY



telenor group

Contents

GROUP POLICY

Security

Policy owner: *EVP & Chief Technology Officer*

Approver: *President & Group CEO*

Date of Approval: *2023-07-13*

1. Purpose & Scope

This policy sets out the principles and overall requirements for security. Its purpose is to safeguard Telenor's operations, assets, services, customers and information from security risks and threats.

The policy's scope is Business Security, which includes information security, physical security and external fraud management, and Crisis Management.

For the scope of the areas in this policy, best practices and supporting templates can be found in Group Security guidelines, the Telenor Defendable Architecture framework, and other external references.

2. Security Principles

Security in everything we do: ensure security awareness on all levels, regularly train employees and sub-contractors, and develop security as an integrated part of our daily work.

High security standards: safeguard assets and operations by implementation of relevant security measures according to recognised standards, frameworks and best practices in a sustainable, relevant and risk-based manner. Deviations shall be based on informed decisions.

Protect our customers: ensure customers are protected in their digital life and the Telenor company is recognised as a trusted partner.

Security by Design: integrate security in all aspects of its business and apply the principles of Security by design and Defence in depth.

Emergency Preparedness: ensure effective and trained crisis management processes to respond to critical situations.

3. Requirements

3.1. Security Management and Governance

The Telenor Company shall govern and manage security in a structured way, following a Security Management System in accordance with ISO/IEC 27001, and by adoption of other relevant standards and best practices.

Security governance shall be executed and aligned with the operational environment and with the overall business strategy of the organisation.

3.2. Organisation of Security

The Telenor Company shall organise business security in a way that ensures a holistic and efficient management of security from a central expert function and enable distributed responsibilities and accountabilities. Each Telenor Company shall appoint a Business Security Officer (BSO) with responsibility for Business Security and Crisis Management.

3.3. Human Resource Security

The Telenor Company shall ensure general awareness and understanding of the security threats throughout the organisation and the liabilities that lies upon all. The Telenor Company shall ensure a continuous security competence program, addressing general awareness, education and training, and with special catering to high-risk or special interest groups.

The Telenor Company shall embed security into each stage of an employment life cycle. Personnel with access to sensitive information or objects as per applicable law, shall be security cleared.

3.4. Asset Management

The Telenor Company shall have full control over all assets and their importance and ensure that related detective and protective measures are applied accordingly. An inventory of assets must be established, maintained, owner assigned to each asset and following classification scheme.

3.5. Access Control

The Telenor Company shall ensure control of all accesses to all its information, premises, systems, and services and ensure prevention, detection and response to unauthorised access and usage.

The Telenor Company shall establish and maintain a secure and effective identity and access management process to manage identities, ensure a formal authorisation and approval process and manage user-, privileged- and service accounts.

3.6. Cryptography

The Telenor Company shall ensure relevant and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of its assets and our customers. This shall be done by development and maintenance of an adequate cryptography framework including timely removal, updates, changes or retiring of cryptographic keys, requiring where, what, and how to use cryptography as a protective measure for safeguarding of information, when being processed, in transit and at rest.

3.7. Physical Security

The Telenor Company shall ensure sufficient protection of its premises to avoid loss, damage and interruption of the organisation's operations, infrastructure, information, information processing facilities and other premises.

Protective and detective security measures shall be layered and follow the principles of security in depth, technical and human measures shall, where applicable, support and complement each other.

3.8. Operations Security

The Telenor Company shall ensure correct and secure operations with sufficient and well-structured preventive, detective and corrective controls are implemented.

The Telenor Company shall have the capability to oversee and monitor security operations and fraudulent activities, technical and human covering both the cyber- and physical domain.

3.9. Communications Security

The Telenor Company shall develop, maintain, implement, and operate a robust and resilient network architecture and adherent security controls for its networks and services.

The Telenor Company shall implement, document, and maintain a security architecture and design in accordance with defendable architecture principles.

The Telenor Company shall implement measures and controls to ensure visibility of traffic to detect and prevent misuse and tampering of network and network services.

3.10. Acquisition, Development & Maintenance

The Telenor Company shall ensure that security is an integral part of any acquisition, development, and maintenance processes for the entire life cycle.

The Telenor Company must implement robust and resilient design through all phases of acquisition, development, and maintenance, by applying defendable architecture principles and security in depth principles.

3.11. Supplier and Vendor Management

The Telenor Company shall ensure that security is an integrated part in all relations and agreements with external and internal vendors and partners. For all key strategic

suppliers, vendors, and partners, the Telenor Company shall establish and manage security governance and, where applicable, ensure suppliers and vendors compliance to our security requirements.

3.12. Security Incident Management

The Telenor Company shall implement a consistent, secure and effective management of security incidents.

The Telenor Company shall ensure availability of sufficient capabilities – including tools, processes and people – to perform real-time monitoring, detection, analysis and response to security events and incidents around the clock, for all relevant assets within the security domains and covering basic to advanced threat.

3.13. Security Aspects of Business Continuity

The Telenor Company shall develop and maintain processes and controls to ensure continued security resilience and compliance with security requirements also in adverse situations, e.g., during an incident or crisis.

3.14. Compliance

The Telenor Company shall establish an overview of and ensure compliance to all applicable security-related requirements, including legal and regulatory requirements, as well as customer demands and internal policies.

3.15. Service Security

The Telenor Company shall ensure implementation of relevant and up-to-date technologies, processes, and operational controls to provide a robust infrastructure, with high customer confidentiality, integrity and availability, for provision of critical communication services.

The Telenor Company shall safeguard our customers and protect our infrastructure by all feasible means, by complying to standards and industry best practices.

The Telenor Company shall adopt other recommendations and best practices from relevant standardisation bodies and other recognised organisations such as, but not limited to, GSMA, 3GPP, ETSI, ENISA, ITU, IETF, Internet society, W3C, OWASP and IEEE, as applicable.

3.16. Fraud management

The Telenor Company shall develop and maintain a formal, documented and systematic approach, including relevant processes, risk assessments, controls and technologies for fraud management and prevention. The controls and processes must cover technical as well as administrative fraud.

3.17. Crisis management

The Telenor Company shall be prepared to respond to any crisis in a proactive manner and ensure a quick recovery. The Telenor Company shall prioritise People aspects first in a crisis.

The Telenor Company shall establish a Crisis Management Organisation and develop plans capable to respond to relevant and up to date crisis scenarios.