Version 2.0 – 06th November 2023

Information Security Policy

LINK Mobility Group Holding ASA and its subsidiaries

Note: This is a public version of the LINK Mobility Information Security Policy. Some information has been redacted to prevent disclosure of sensitive information, technical details, systems information, or other security measures where disclosure may jeopardize established information security management system.

Version	Date	Approver	Comments
1.0	13.02.2018	N/A	Initial draft
1.2	27.03.2018	N/A	Updated draft
1.3	28.03.2018	N/A	Draft split
1.4	04.04.2018	Compliance Officer	Final
1.5	12.04.2019 20.08.2019	Compliance Officer	Updated draft
1.5	10.10.2019	CTO	Final
1.6	03.09.2020	CTO	Adding cryptography information
1.7	03.06.2021	CTO	Adding sections for Access control, data encryption, and static app testing
1.8	23.09.2021	CTO	Merge of Governance system and Security Policy
2.0	06.11.2023	Board of Directors of LINK Mobility Group Holding ASA	Redesign of the entire policy for alignment with NIS2 and ISO 27001:2022 requirements

Information Security Policy

1. Company information

LINK Mobility Group Holding ASA and all subsidiaries hereinafter jointly referred to as “LINK”, “LINK Mobility” or “company”.

LINK Mobility Group Holding ASA and LINK Mobility Group AS hereinafter jointly referred to as “LINK Mobility Group”.

LINK Mobility Group is incorporated and registered in Norway and is subject to Norwegian law. LINK Mobility Group subsidiaries are registered in different countries and are subject to local laws. For the purpose of this Policy, a subsidiary is any company where LINK Mobility Group holds control through 50% or higher direct or indirect ownership.

1.1. Purpose of Information Security Policy

The purpose of this Information Security Policy, hereinafter referred to as the "Policy", is to obtain an optimal and consistent, with the requirements of international norms and applicable legal acts (i.e., NIS2, GDPR), way how to secure information so that information and systems preserve their confidentiality, integrity, availability, and authenticity.

LINK Mobility Group aims to ensure confidentiality, integrity, availability, and authenticity of information by providing organizational and technical security measures to be used within LINK.

Furthermore, the purpose of this Policy is to assure those who have a relationship with the company that the use of information and systems is subject to a set of industry standards, best practices, and guidelines.

In this Policy, the following will be described:

- definition of information security and information security management systems;
- information security objectives or the framework for setting information security objectives;
- principles to guide all activities relating to information security;
- commitment to satisfy applicable requirements related to information security;
- commitment to continual improvement of the information security management system;
- assignment of responsibilities for information security management to defined roles;
- procedures for handling exemptions and exceptions.

1.2. Scope and Applicability

This Policy and its supportive policies apply to any information belonging to the company – including information not directly related to the company, but for which LINK Mobility may be made responsible – regardless of the means of storage or disclosure.

This Policy applies to all of LINK:

- each LINK subsidiary is encouraged to further implement information security policies that are at least equivalent to this Policy and supporting documents;
- all LINK subsidiary organizations shall determine external and internal factors that are relevant to their purpose and that will affect the organization's ability to achieve the intended result of the information security management system.

This Policy further applies to all employees, without exception, both permanent employees and people who temporarily work for LINK and also as consultants (hereafter collectively referred to as employees) regardless of the company or subsidiary of the actual employment.

1.3. Continuity

This Policy will be revised as a part of the management's review and audit. Whenever revised, the original document, including any templates and forms, must be archived for 3 years.

To ensure the adequacy of the Information Security Policy and Information Security Management System, both are subject to continual improvement. Information Security Management System is described in section 2.1.2. Information Security objectives are described in section 2.1.3.

1.4. Definitions

The definitions from the NIS2 Directive have been marked by adding [NIS2] before the definition. LINK Mobility choses to use wider definition of the word "Incident" then used in NIS2 directive as described below and explained in detail in section 3.5.

In the context of this Information Security Policy, the following definitions apply:

- **Access** – Granted to an employee, user, or non-physical entity, it applies to both physical and logical access to LINK Mobility assets.
- **Access Control** – The process of managing access to LINK Mobility assets, including processes such as granting access, revoking access, changing access, etc.
- **Account** - The collection of resources and permissions within a given system assigned to a specific user of a computer system.
- **Anti-Virus/Anti-Malware Solution** – A tool used for detecting and protecting computer systems against malicious software.
- **Asset** - Anything of value to LINK Mobility, including information, hardware, software, network, personnel, and information processing facilities.

- **Authentication** - The process of confirming an entity's identity.
- **Authorization** – The process of assigning permissions for a specific activity or resource.
- **BYOD** – "Bring Your Own Device".
- **Cloud** – A data processing model based on using services provided by a service provider involves sharing IT resources over the Internet and charging fees based on the extent of their utilization.
- **Data at rest** – Data at rest refers to data that is stored on a physical medium, such as a but not limited to: hard drive, flash drive, or backup tape.
- **Data in transit** - Data in transit refers to information that is currently moving from one location or device to another over a network or communication channel.
- **Encryption** – The process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext.
- **Event** – any observable occurrence in an asset, system or network. Events can be safe or malicious. For instance, a user logging into a system is an event, as is an attempt to access a file.
- **Event log** – A record of events performed on or by a particular system.
- **Information** – Any data, information, or knowledge that is stored, processed, transmitted, or communicated within LINK Mobility or LINK Mobility systems.
- **Information Classification** – The process of assessing the criticality of information processed by LINK.
- **Information Security** – Practices taken to ensure confidentiality, availability, integrity, and authenticity of Information in LINK Mobility.
- **Information Security Incident** – Event or series of events that lead to a breach of information security, a compromise of the confidentiality, integrity, authenticity, or availability of data, or any unauthorized access or attempts to access information systems.
  - [NIS2] **Incident** - Event compromising the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data or of the services offered by, or accessible via, network and information systems
  - [NIS2] **Large-scale cybersecurity incident** - An incident that causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States.
  - [NIS2] **Incident handling** - Any actions and procedures aiming to prevent, detect, analyze, and contain or to respond to and recover from an incident.
  - [NIS2] **Significant Incident** – Within the NIS2 framework, a "significant incident" usually implies a higher threshold of impact or disruption. An incident would be considered "significant" if it meets certain criteria established by the NIS2 Directive, which might involve factors like the number of users affected, the duration of the incident, or its geographic spread.
- **Information Security Management System (ISMS)** – The process of ensuring proper management of information security within LINK Mobility.
- **Key Asset** – Asset of LINK Mobility that has a significant impact on the organization's operations.
- **Malware** – Malicious software that could be used to compromise information security at LINK Mobility.

- **Multi-Factor Authentication** – A method of confirming an individual's identity that requires additional verification through the input of a one-time code or another form of user interaction.
- **Non-Personal Account** – Accounts that are not assigned to a specific employee. These can be shared accounts used by multiple employees or system accounts.
- **Password Manager** – Tools that allow for storing passwords in encrypted form and enable the password to be decrypted only when the decryption password is provided.
- **Penetration Test** – A process of testing LINK Mobility applications and systems to detect vulnerabilities that could lead to information security breaches.
- **Personal Account** – An account that is assigned to a specific employee, and only that employee has access to it.
- **Phishing** – A social engineering method aimed at deceptively coercing the victim into providing information to the attacker.
- **Privileged Access Rights** – Permissions assigned to an account that grants a user the ability to perform actions beyond those of a regular user. These may include special privileges or elevated levels of access within an IT environment.
- **Recovery Point Objective (RPO)** – Maximum tolerable amount of data loss that a system or organization can afford in the event of a disruption or outage. It is measured in terms of time, indicating how much data can be lost between the last backup or data synchronization and the occurrence of an incident.
- **Recovery Time Objective (RTO)** - Targeted duration within which a system or service needs to be recovered and brought back to full functionality after a disruption or outage.
  - [NIS2] **Risk** - Means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident.
- **Session** - Time-delimited two-way link, enabling interactive expression and information exchange between two or more communication devices or ends.
- **Software development kit (SDK)** – Collection of software development tools in one installable package.
- **System** – Comprehensive framework comprising of assets like hardware, software, and protocols designed to facilitate the efficient and secure management of digital information and processes.
  - [NIS2] **Vulnerability** - Means a weakness, susceptibility, or flaw of ICT products or ICT services that can be exploited by a cyber threat.
- **Vulnerability Scan** – Automated method of detecting vulnerabilities for LINK Mobility systems and applications. It is performed using tools specifically designed for this purpose.

Note: In the internal version of LINK Mobility Information Security Policy this includes more definitions related to systems used by LINK Mobility.

2. Information Security Governance

Overall approval of the LINK Information Security Policy lies with LINK Mobility Group Holding ASA Board of Directors. Approval of supportive policies lies with appropriate management.

2.1. Context of the organization

LINK Mobility is one of the leaders in mobile communication systems and CPaaS solutions in Europe. LINK has ~700 employees across ~18 countries. LINK's ~50 000 customers worldwide in 2022 sent 17 billion messages, averaging more than ~3 000 000 messages per customer, resulting in 2022 revenue of NOK ~5.2 billion.

LINK Mobility Group, within the information security area, serves as a guide to its subsidiaries, providing them with requirements and guidelines for organizational and technical security measures.

This Information Security Policy determines high-level external and internal factors relevant to LINK Mobility Group and its subsidiaries' purpose and ability to achieve the intended result of the information security management system.

All subsidiary entities can and should determine further local external and internal factors that are relevant to its purpose and that will affect the organization's ability to achieve the intended result of the information security management system.

Internal and external factors may vary depending on several factors including organizational culture, local legislation, and contracts.

CONTEXT	COMMENT	EXTERNAL / INTERNAL
Contract obligations	LINK is committed to complying with Information Security requirements provided by its customers.	External
Obligations in laws and regulations	Legal obligations such as GDPR and NIS2 require LINK to ensure proper security measures for its information.	External
Insurance companies	Insurance companies are required to collect all relevant documentation related to information security and GDPR. LINK needs to provide documented information and ensure proper management of the information security process to meet insurance companies' requirements.	External

CONTEXT	COMMENT	EXTERNAL / INTERNAL
Compatibility with legal obligations and iso 27001 requirements	LINK Mobility is obligated to be in compliance with the NIS2 Directive. To achieve this, LINK established its information security management system based on ISO 27001:2022 requirements.	External
Defined roles and responsibilities	LINK Mobility has defined roles and responsibilities that were present before establishing information security processes. An information security management system must be implemented in existing processes.	Internal
Employee education	Each employee must undergo training in the information security area. Participation in the training must be confirmed by an appropriate certificate.	Internal
Compliance with policies	LINK Mobility systems and processes must be compliant with policies and procedures.	Internal

2.1.1. Understanding the needs and expectations of interested parties

LINK has determined that below mentioned parties are most relevant to the operation of its Information Security: Management System:

INTERESTED PARTIES	IMPACT	INTEREST	REQUIREMENTS
LINK Mobility Group CEO	High	High	Obtaining compliance for the information security management system.
LINK Group GLT	Medium	High	Obtaining compliance for the information security management system.
LINK Group Managers	Medium	High	Obtaining compliance for the information security management system.
Local Managing Directors	High	Medium	Obtaining compliance for the information security management system.
Enterprise Customers (Banks, Insurance, Health)	Medium	High	Obtaining compliance for the information security management system to ensure the security of the transmitted and stored data
Telecommunications Operators	Medium	Medium	Contractual requirements with operators to ensure safety

INTERESTED PARTIES	IMPACT	INTEREST	REQUIREMENTS
OTT Providers, Agregators	Medium	Medium	Contractual requirements with OTT providers and agregators
LINK Sales Departments	Medium	High	Compliance as a Sales Argument
Contractual Obligations With Customers	Medium	Medium	Providing privacy policy and documented process for the security of processing.
General Data Protection Regulation	High	Medium	Compliance with Article 32 of the GDPR
NIS2 And Local Transpositions	High	High	Obtaining compliance with NIS2 requirements for information security.

2.1.2. Information Security Management System and its Scope

Information in the context of Information Security refers to any data, information, or knowledge that is stored, processed, transmitted, or communicated within LINK Mobility or LINK Mobility systems. Examples of these include digital data, documents, records, intellectual property, personal data, financial data, and more.

Information Security in LINK Mobility refers to practices taken to ensure:

- **Confidentiality** – Information managed by LINK Mobility must be kept confidential and accessible only to authorized individuals or systems.
- **Availability** – Information and systems used for processing this information must be accessible to authorized individuals or systems.
- **Integrity** – Information must be protected against unauthorized modification, deletion, or addition.
- **Authenticity** – Information must come from trusted sources and be protected against impersonation or spoofing.

These practices include organizational and technical security measures to protect information.

The **Information Security Management System** established in this Policy is LINK Mobility's way of ensuring proper management of the Information Security process within LINK Mobility and its subsidiaries.

LINK Mobility Group ISMS scope is:

"ensuring information security within LINK Mobility and its systems by providing clear guidance and controls for multiple Information Security Management Systems".

ISMS aims to achieve the information security goals set in this policy by providing required information security policies, procedures, instructions, and technical measures.

LINK Mobility subsidiaries can and should establish their own Information Security Management System to address their own information security needs and objectives.

LINK Mobility subsidiaries can and should establish their own Information Security Management System to address their own information security needs and objectives, tailored to meet the specific requirements of each subsidiary, taking into account local regulations and business operations.

ISMS established by LINK Mobility subsidiaries must be compliant with this Policy and LINK Mobility ISMS.

2.1.3. Information Security Objectives

LINK Mobility's goal is to maintain an information security level that at the minimum ensures:

- compliance with EU regulations (GDPR, NIS2),
- compliance with international standards and best practices within the information security area,
- meeting enterprise clients' needs and requirements regarding information security.

To achieve LINK Mobility's goals, this Policy establishes ISMS objectives. Objectives shall be measured on a regular basis, at least once a year as a part of ISMS management review. Supportive policies can have separate objectives, related to the specific topic.

Each LINK subsidiary can set up its own ISMS objectives in their respective policies.

ISMS objective must:

- be adequate to the scope of the Information Security Management System,
- be adequate to the organization's business requirements and information security strategy,
- take into account information security attributes that consist of Confidentiality, Integrity, Availability, and Authenticity,
- take into account applicable information security requirements, and results from risk assessment and risk treatment,
- be measurable (if practicable),
- be monitored and updated as appropriate,
- be communicated and available as documented information,
- verified and aligned with LINK business goals.

OBJECTIVE	HOW TO MEASURE	GOAL
All policies related to information security must be approved	Information Security Policy must be approved by the Board. Supportive policies must be approved by a respective accountable person.	100%
All LINK employees must have completed a yearly GDPR training	Verification of completion certificates	90%
All LINK employees must have completed a yearly information security training	Verification of completion certificates	90%
All personal devices must be compliant with the BYOD policy	Verification of use of personal devices and their configuration	100%
All significant incidents must be handled according to documented procedures	Verification of incident reports	100%
All LINK employee workstations must be encrypted and password-protected	Verification of employee workstations encryption	100%
LINK servers & systems accessible from the internet must provide data at rest and data in transit encryption	Verification of servers and systems disk encryption and used protocols	100%
All LINK production systems must have a risk assessment conducted and documented	Verification of conducted yearly risk assessment	90%
All LINK systems must be compliant with information security policies and supportive policies.	Verification of LINK systems compliance with policies	90%
Remediation plans for penetration test findings must be presented within the given timeframe	Verification of presented remediation plans for penetration test findings	90%
Remediation actions for penetration test findings must be implemented	Verification of implemented remediation actions for penetration test findings.	90%

Objectives established in this policy and objectives established by LINK subsidiaries must be measured

in set intervals to ensure that the ISMS is effective in managing and mitigating risks. For each objective, there must be relevant KPIs identified that will provide data points to measure the success or progress toward the objective. Documented measurement intervals may be tailored to the specified objective, but can't be set longer than 1 year. The outcome of the measurements must be presented to top management at least once a year during the management review of the ISMS.

2.2. Legal requirements and relation to other policies

This Policy was created to meet the requirements of:

- **NIS2:** Directive (EU) 2022/2555 of the European Parliament and the Council of 14. December 2022 on measures for a high common level of cybersecurity across the Union;
- **GDPR:** Regulation of the European Parliament and the Council (EU) 2016/679 of 27. April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data
- Other generally applicable provisions of the European Union and national regulations regarding the protection of personal data.

This Policy was created based on the best practices and guidelines described in ISO 27001:2022.

This Policy is part of a family of LINK Mobility policies describing Information Security, Personal Data Protection, Supplier relations, etc., which will be referenced throughout this policy.

All LINK Employees shall familiarise themselves with all policies mentioned in the Policies section on LINKNet.

2.3. Responsibilities

2.3.1. RACI

The terms "responsible" and "accountable" have specific implications, especially when considering frameworks like the RACI model (Responsible, Accountable, Consulted, Informed) that is used in LINK to define roles and responsibilities.

When using the term in this policy, we refer to the following definitions:

- Responsible: Refers to the person(s), teams, or entities that carry out the task or process. This person does the work to achieve the task. The individual or team responsible for a particular information security task will carry out the procedures, documentation, monitoring, or other activities related to that task.
- Accountable: Refers to the person, team, or entity ultimately answerable for the activity, process, or decision and holds the "yes" or "no" authority and veto power. The individual or team accountable for an information security activity ensures that the activity is carried out in accordance with relevant procedures, policies, regulations, laws, or standards. They own the outcome, whether it's success or failure.

2.3.2. Individual and team RACI identification

Top management (BoD and GLT)

Top management includes the Board of Directors in LINK Mobility Group Holding ASA (BOD) and LINK Mobility's Global Leadership Team (GLT).

- Accountability for the establishment of an Information Security Policy and information security objectives – approval of the document.
- Ensuring the integration of the Information Security Management System with business processes.
- Ensuring the availability of resources needed by the Information Security Management System.
- Communication of the Information Security Management System in the organization.
- Ensuring that the Information Security Management System achieves its objective.
- Directing and supporting individuals performing roles related to Information Security Management Systems.
- Promoting continuous improvement of the Information Security Management System.
- Supporting process owners in the implementation of an Information Security Management System.
- Participating in Information Security Management System management review.
- Promoting the continual improvement of Information Security Management Systems.
- Being accountable for appointing Asset Owners, if it cannot be carried out by COOs and/or Managing Directors.

COOs and/or Managing Directors

- Being accountable for the creation of an Information Security Management System on the local level.
- Taking accountability for the implementation of an Information Security Management System on a local level.
- Designating responsibilities for implementation and maintenance of Information Security Management System on a local level.
- Documenting the context of the organization and determining external and internal factors that may affect the Information Security Management System on a local level.
- Participating in Information Security Management System, and management review on a local level.
- Ensuring local Information Security Management System compliance with the Information Security Policy established by LINK Mobility.
- Communication with respective information security or data protection authorities when required.
- Being accountable for appointing Asset Owners.

LINK Mobility Managers (VP/Director)

Responsibilities apply to both LINK Mobility group department managers and local managers;

- Establishment of supportive policies and procedures.
- Ensuring implementation of Information Security Management Systems within their departments.
- Ensuring that personnel have appropriate access.
- Ensuring that personnel has been familiarized with the Information Security Policy, supportive policies, and procedures relevant to their role in the organization.
- Ensuring that processing of information in their department is done following the Information Security Policy, supportive policies, and procedures.

Product Managers

- Being accountable for the implementation of information security for platforms and products.
- Being accountable for conducting information security risk assessments for platforms and products.
- Designating responsibilities for information security for platforms and products.
- Cooperating with LINK Mobility information security team.
- Authorizing or designating responsibility for authorizing access to systems.
- Authorizing the implementation of corrective actions.
- Being accountable for the Information Security Supplier's Due Diligence.
- Accepting residual risks or designating responsibility for accepting residual risks.
- Taking Managing Director responsibilities regarding Information Security Management System if there's no MD in place.

Product Owners

- Being responsible for the implementation of information security for platforms and products.
- Being responsible for conducting a risk assessment for platforms and products.
- Cooperating with LINK Mobility information security team concerning external vulnerability scanning, penetration testing, and internal or external audits.
- Implementing corrective actions as a result of vulnerability scanning or penetration testing.
- Implementation of technical or organizational security measures for platforms and products.
- Being responsible or designating responsibility for Information Security Supplier Due Diligence.
- Maintaining Access Control register to platform or products or designating responsibility for it.
- Creating or designating responsibility for documenting and maintaining internal procedures.
- Designating responsibilities for developing software and administering production systems for platforms and products.

Information Security Team Leader

Responsibilities may apply to Information Security Officers on a local level;

- Conducting internal audits of the information security for LINK Mobility Group in a scope defined by GLT.
- Overseeing external audits of the information security for LINK Mobility subsidiaries in a scope defined by GLT.
- Maintaining and updating the Information Security Policy.
- Providing input to security questionnaires for group systems.
- Verifying implementation of Information Security Policy through the organization.
- Coordinating risk management process for information security.
- Creating and monitoring information security controls.
- Coordinating external penetration testing or conducting internal penetration testing and verifying corrective actions.
- Coordinating or conducting vulnerability scanning of systems and verifying corrective actions.
- Conducting management reviews of the Information Security Management System.
- Ensuring corrective actions related to audit findings.
- Creating improvement plans for the Information Security Management System.
- Cooperating with the Product Manager and Product Owner to ensure proper management of security incidents.

Data Protection Officer (Acting CISO)

- As listed in Article 39.1 of GDPR.
- Overseeing daily work of Group Information Security team.

Asset Owner

- Management of assets through their entire lifecycle based on information security policy.
- Determining asset classification based on information classification and risk attributes.
- Granting access to information and other associated assets based on the organization's adopted access control policies.
- Management of access control rights to owned information or systems.
- Ensuring adequate security measures to preserve information security principles for information and other associated assets.
- Taking an active part in the risk assessment process for managed assets and information.
- Establishing guidelines for handling managed assets based on the information security policy and their classification.

Internal IT

- Managing devices throughout their lifecycle, including configuring and wiping employees' devices at the beginning and end of their lifecycle.
- Providing technical support for the employees.
- Implementing appropriate security measures for employees' devices and systems/services used by employees in LINK.
- Managing and maintaining LINK Azure Active Directory.
- Granting or revoking access rights to LINK systems and services managed by Internal IT based on information received from relevant individuals.
- Verification of installed software on employees' workstations.

HR Specialist

- Following the onboarding, offboarding, and position change procedures.
- Including information security requirements for internal HR processes.
- Ensuring that all employees have completed GDPR and information security training.
- Verification of the completion status of GDPR and Information security training and informing relevant individuals about the results.
- Verification of candidates' competencies during a recruitment process for positions that have an impact on information security within the organization.
- Ensuring that employees sign appropriate confidentiality or non-disclosure agreements that remain in effect during and after their employment.

System administrator

- Management of LINK Mobility systems based on the information security policy and relevant information security procedures.
- Participating in the risk assessment process as a technology expert.
- Designing and implementing technical security measures for LINK Mobility systems.
- Supervising the operation of LINK Mobility systems and implemented security measures.
- Capacity and availability management for LINK Mobility systems.
- Responding to events or incidents related to information security involving LINK Mobility systems.
- Supervising access to managed LINK Mobility systems.
- Providing appropriate remediation actions for detected vulnerabilities.

Employees/consultants

- Familiarizing themselves with the information security policy and its supporting policies.
- Familiarizing themselves with information security procedures and instructions related to their role and function within the organization.
- Adhering to established policies, procedures, and instructions.
- Completing information security and GDPR training during the onboarding or position change process and refreshing the certification at least once a year.
- Responding to and reporting information security events and incidents.
- Reporting any irregularities related to information security to the person responsible for information security.
- Implementation of tasks related to ISMS.
- Participating in the process of continuous improvement of the ISMS by providing feedback and suggestions to managers or information security specialists.

Individuals with allocated information security responsibilities can assign security tasks to others. However, they remain accountable and should determine that any delegated tasks have been correctly performed.

Every LINK Mobility subsidiary must define and document responsibilities within its own Information Security Management System.

In the event of role conflicts that can't be resolved through the segregation of duties or segregation of duties is not possible for any given reason, appropriate monitoring of the activities of individuals involved in the conflict must be ensured.

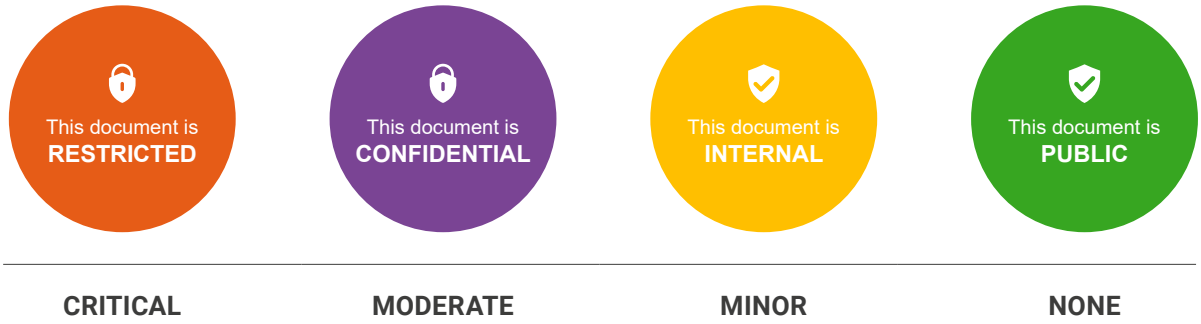
2.4. Classification of information

All information should be subject to the Information Classification process to ensure proper handling of information within LINK Mobility. Information Classification in LINK Mobility is based on the consequences attribute of a Risk Assessment. The Information Classification process is standardized across LINK Mobility and cannot be changed in any way within LINK Mobility or its subsidiaries.

Each piece of information within this Information Security Policy defines a standard set of Information Classification Levels that should be used when creating, sharing, or transmitting information. Each piece of information within LINK Mobility must have a designated owner. Responsibility for the Information Classification of such information lies with the owner of the information.

When assessing Information Classification, the owner of the information must take into account the potential consequences of improper handling of information or data breach.

Information Classification in LINK Mobility:



Note: In the internal version of LINK Mobility Information Security Policy, the above table has additional column with sample information and examples for each label.

In case of doubt, employees should reach out to their direct manager or Information Security team if the former is not available.

2.4.1. Labeling of information

Information should be labeled following its classification to ensure proper handling of information. The labeling of information can vary depending on the type of information.

Information with the classification **PUBLIC** doesn't need to be labeled.

Note: In the internal version of LINK Mobility Information Security Policy, this section describes how to label data for physical and electronic type of information.

2.4.1.1. Changing data label

Due to the possibility of changes in information classification over time and the potential for errors in classification,

LINK Mobility acknowledges the possibility of changing previously assigned data labels.

Note: In the internal version of LINK Mobility Information Security Policy, this section describes how to change the classification for physical and electronic type of information, including the authorization of change.

2.4.2. Acceptable use of information and other associated assets

Acceptable use of information and other associated assets is documented in the **Handling of Information** procedure. Additionally handling may be documented in supportive policies, depending on the type of information and asset.

Note: Handling of Information procedure describes on how to handle information in accordance to its classification.

2.4.3. Information transfer

Information transfer is documented in the **Handling of Information** procedure.

Note: Handling of Information procedure describes on how to transfer information in accordance to its classification.

2.5. Risk assessment

2.5.1. Risk identification

Risk Identification is performed for each risk area in accordance with processes and methodology defined by the accountable and responsible for each area. Risk areas are defined in the LINK Risk Management Framework.

2.5.2. Risk assessment

To perform risk assessment the responsible person must determine and document the Probability and Consequence of the identified risk to define the inherent risk level. Template for assessment available in Excel, with risk assessment matrix. A scale for consequence and probability is used.

The risk assessment must be documented by probability and by consequence related to confidentiality, integrity, availability, and authenticity.

Note: In the internal version of LINK Mobility Information Security Policy this section includes tables with descriptions for risk probability and consequence.

LINK reaction to the calculated risk depends on the risk value:

- At the risk level “high” risk measures are always planned and implemented.
- For risk level “medium” it is recommended to plan and initiate risk measures.
- The risk level “low” is the risk where measures are normally not necessary.

Note: In the internal version of LINK Mobility Information Security Policy this section includes risk level matrix for assessing risk level based on the probability and consequences.

2.5.3. Risk management

In this Policy, the most important information regarding risk management in the context of information security has been outlined. Risk management at LINK Mobility is carried out based on the **LINK Mobility Risk Management Framework**. It is required to follow the **LINK Mobility Risk Management Framework**.

There are four types of risk management according to the **LINK Mobility Risk Management Framework:**

RISK MANAGEMENT TYPES
Accept
Avoid
Mitigate
Transfer

Note: In the internal version of LINK Mobility Information Security Policy the table above have descriptions for each risk management type.

The choice of risk management type depends on the current risk profile. For each risk marked as "mitigate" in the risk management type, it is required to implement a control along with assigning a responsible and accountable person.

The **LINK Mobility Risk Management Framework** defines the following Maturity Levels for Controls:

MATURITY LEVEL
Not implemented
Reactive
Fragmented
Defined
Mature
Optimized

Note: In the internal version of LINK Mobility Information Security Policy the table above have descriptions maturity level.

Controls must be reviewed at least once a year for effectiveness. It is required to conduct regular follow-ups of the assessment, residual risks, and control through assistance from the LINK Legal & Compliance team.

The Board of Directors in LINK Mobility Group Holding ASA is to approve risk profiles annually, based on a proposal from management. In the context of this Policy, the risk that meets the approved risk profile is considered a residual risk.

The outcome of risk assessment and risk management must be documented.

2.6. Information Security Internal Audit

To verify the compliance of LINK Mobility systems and processes with the requirements of this Policy, international standards, and legal requirements related to information security, LINK Mobility conducts internal audits in accordance with the **LINK Mobility Information Security Internal Audit Guidelines**.

Note: LINK Mobility Information Security Internal Audit Guidelines specifies on how LINK Mobility conducts yearly audits, manage non-compliances and audit findings, documents the results and communicates them.

3 Information Security Conduct

3.1 Information security in HR

3.1.1. Screening, recruitment

A screening process must be performed in line with the LINK Recruitment Policy. All new hires must be verified taking into consideration all relevant privacy and employment-based legislation and should, where permitted, include the following:

- Availability of satisfactory references (e.g. business and personal references).
- A verification (for completeness and accuracy) of the applicant's CV.
- Confirmation of claimed academic and professional qualifications.
- Independent identity verification (e.g. ID card, passport, or other acceptable document issued by appropriate authorities).
- Verification of criminal records if applicable

Handling of the personal data of potential employees must be in line with the **LINK Employee Personal Data Policy.**

3.1.2. On- and off-boarding, disciplinary process

On- and off-boarding process in LINK is based on the creation of an Employee account in the HR system and follows these steps:

- All employees must be onboarded into HR system before LINK e-mail can be created.
- All employees must be promptly offboarded from HR system at the date of the termination of the agreement.
- All personal e-mail accounts must have a corresponding row in HR system or a documented exception.
- Each employee must sign a confidentiality agreement (or special statements) as provided in the employment template contract and Personal Data Protection Policy Appendix 1.

- Each employee must be aware of the possibility of a disciplinary process if the employee acts in breach of the Information Security Policy requirements.

Note: In the internal version of LINK Mobility Information Security policy, this section specify HR system and mailbox used in LINK Mobility.

3.1.3. Training

All employees are being informed during the training about the policies and procedures in LINK. LINK offers the following online training (internal link) to its employees:

- Information security for all employees: This security awareness training (this course aims to educate all LINK employees about better information and computer security overall).
- GDPR for all employees: This basic GDPR training aims to educate all LINK employees toward a better understanding of key GDPR concepts.
- GDPR Privacy by design: This training aims to educate all LINK employees who take part in the creation of new software on the Privacy By Design wheel (with an emphasis on data protection by design, and security of processing).
- Compliance for all Employees: This training aims to educate all LINK employees in the basic concepts of ESG (Environmental, Social, and Governance) concepts.

The list of available training courses may change during the life cycle of this policy, but it will always include at least information security, GDPR, and compliance areas.

All new hires should complete the training during the first day of onboarding and an automatic reminder should be sent to employees who didn't complete their training. Each person with a linkmobility.com email address has to complete the above-mentioned training at least once a year and renew the certificate and signature under the Personal Data Protection Policy Appendix 1 statement.

Individuals who take on a specific information security role are competent in the knowledge and skills required by the role.

Note: In the internal version of LINK Mobility Information Security policy, this section includes a link to online training for employees.

3.1.4. Change of position

In the case of an employee changing positions within LINK Mobility, a position change process is initiated.

During the position change process, changes in the roles performed by the employee must be defined. Relevant information should be communicated to the individuals responsible for granting and authorizing access to systems to grant, modify, or revoke existing access.

An employee undergoing a position change process must complete all necessary documentation and undergo training related to the new position and role.

3.2. Access control

The access control process described in this policy pertains to all individuals who currently have or seek access to LINK Mobility systems.

The access control requirements outlined in this section apply to internal access within LINK Mobility. Customer access to platforms and products has not been described in this information security policy. However, it is recommended that the following sections be applied to ensure the security of customer accounts:

- Section 3.2.7.1 Password policy
- Section 3.2.7.3 Lockouts

If methods other than SSU (Self-Sign Up) are used for customer account registration, it is advisable to apply the entire section 3.2.7 Password management.

3.2.1. Access Control Principles

The Access Control process in LINK Mobility is carried out through Role-Based Access Control ("**RBAC**"):

- All roles and systems in LINK Mobility must be identified.
- Roles must have defined baseline access to systems.
- Individuals must have assigned roles that reflect their position and given tasks in the organization.
- Access must be assigned using "need to know" and "zero trust" principles meaning that users should be given minimal access needed to complete their tasks.
- Access to systems not assigned to a specific role may be granted, but this fact must be recorded.
- All users must have assigned personal accounts with a unique identifier.
- In general, the use of non-personal accounts for daily tasks is prohibited, accepted use has been described in this policy.
- All authorizations must be listed in the access control register. There might be multiple access control registers across LINK.

These access control registers must contain information about:

- Unique identifier of the assigned authorization
- Name of assigned authorization
- Employee name
- Employee role
- Privileges assigned to this role
- Purpose of authorization
- Date of provisioning access
- Date of de-provisioning access

Entries in the access control registers may be deleted after 3 years from the deactivation of respective access.

Access control registers must be reviewed by asset owners to confirm that all granted accesses are in line with the actual state and there are no unregistered accesses or mistakes. Reviews must be conducted at least once a quarter.

Access control register must be always reviewed in the situation of:

- Offboarding
- Change of position
- Prolonged employee leave (over 30 days)

3.2.2. Access Provisioning

The access provisioning process includes both creating a new account and modifying an existing account to grant new permissions.

Access provisioning must follow these rules:

- Individuals responsible for access authorization should designate individuals responsible for the provisioning of access.
- Provisioning of access and authorization of access should be carried out by different individuals to ensure segregation of duties. In cases where this is not feasible and the same person authorizes and grants access, additional security measures should be implemented, such as monitoring access granted by that person.
- Granting access to the system can only occur upon authorization from the relevant individual.
- Created accounts must possess a unique identifier (e.g. login) and adhere to the password policy requirements.
- Created accounts must be personal. Sharing personal accounts is prohibited. In cases where sharing is unavoidable, the Non-Personal Account policy should be followed.
- Accounts in systems using e-mail as an identifier must always be created using LINK Mobility domain e-mails.

3.2.3. Authorization

Authorization of system access should be based on an employee's role, with basic access assigned to each role. The person responsible for access authorization must define access roles for the specific system.

Authorization for access not assigned to a role can be granted based on an employee's or their supervisor's request. This request should specify why the access is needed, and the duration if the access is temporary.

3.2.4. Access requests

Access granting should always be preceded by a valid access request directed to the responsible access authorization personnel. Access requests should specify to whom access will be granted, for what purpose, and with what privileges.

This request can be made by:

- An employee seeking specific access.
- The HR department during the onboarding process or position changes (including automatic messages from the HR system).
- The employee's supervisor.

If the request involves granting additional access, the purpose of access acquisition and the timeframe for performing tasks should be specified.

Note: In the internal version of the Information Security Policy, this section specifies HR system used in LINK Mobility.

3.2.5. Access transfer

Access transfer can occur when an employee with specific access leaves the organization and there's a need to transfer their access to another employee must follow these rules:

- LINK Mobility does not allow the transfer of access to a personal account of an employee. Access transfers should be limited to the transfer of rights within a specific area or system
- Transferring access to shared mailboxes, shared workspaces, or other non-personal systems is allowed upon appropriate approval.
- Access transfer must always adhere to local regulations and guidelines.
- Employees before departure should store all company-related files in a shared folder location as agreed with the employee manager.

Note: In the internal version of the Information Security Policy, this section includes an example for the transfer of rights. It has been redacted to not disclose systems used in LINK Mobility.

3.2.6. Deprovisioning

Access revocation can occur in the following situations:

- Employee departure from the organization.
- Change in the employee's position or role.
- Extended employee absence (beyond 30 days).

In the event of any of the above scenarios, the granted accesses must be carefully reviewed and revoked accordingly.

- All accesses must be revoked no later than on the last day of the employee's tenure in a specific role.

- For prolonged employee absence, accesses should be revoked upon receiving information about the absence exceeding 30 days.
- If the absence period was not anticipated, accesses should be revoked no later than the 31st day of the absence.
- All LINK Mobility systems must terminate a user's session upon access revocation.

3.2.7. Password management

Password management in this Policy refers to the activity of creating, using, modifying, deleting, and storing passwords used to authenticate to LINK resources.

All LINK systems must follow this policy to ensure that company resources will be accessible only to authorized personnel.

3.2.7.1. Password policy

All passwords used in LINK Mobility must meet or exceed the following requirements:

- Passwords used in LINK Mobility must be strong and meet LINK Mobility length and complexity requirements
- Password must be unique, meaning that the same password cannot be used in two different places.

Note: In the internal version of LINK Mobility Information Security Policy this section specifies the requirements for password length and complexity.

- Password shall not consists of easy to guess information.

Note: In the internal version of LINK Mobility Information Security Policy this section includes information about what shouldn't be used as a password.

The use of MFA (Multi-Factor Authentication) is required whenever it is available.

It is highly recommended to generate complex passwords and store them in the password manager. Storing passwords in any other way than approved by the LINK Mobility password manager is prohibited.

Change of passwords is not required except for non-personal accounts, described in section 3.2.8 of this policy. Internal IT employees are obligated to verify the identity of the user requesting a password change.

3.2.7.2. Temporary passwords & resets

During the creation of a user account, the system administrator should allocate a temporary password to the user that complies with the password policy requirements. This temporary password must be changed by the user after their initial login. It is recommended that systems automatically prompt the user to change their password upon their first login.

- If possible, a temporary password must also be assigned if a user requests a password reset.
- Multi-factor authentication (MFA) can be temporarily disabled, for instance, if the device used for authentication is lost. In such cases, the appropriate information security team should be informed.

- User passwords must also be reset in the event of loss/theft of equipment or password leakage.
- Before providing a user with a password or temporarily disabling MFA, the administrator must verify the user's identity, for example, through a video call using other communication channels used in LINK Mobility.
- Passwords should be conveyed using password managers. Whenever possible, avoid transmitting passwords in plain text, through messaging apps, or emails. It is acceptable to transmit passwords via SMS.
- All LINK Mobility systems must terminate a user's session upon resetting a password.

Note: In the internal version of LINK Mobility Information Security Policy this section specifies communication channels used in LINK Mobility.

3.2.7.3. Lockouts

- To address the risk of brute-force attacks and unauthorized access it is required to implement "lockouts" if possible.
- A user account should be locked after few unsuccessful authentication attempts.
- Account locks can involve manual solutions where a system administrator must manually unlock the user account or temporary locks that automatically unlock the user account.
- Temporary locks should last for a fixed period of time.
- Each time a lockout is triggered, an appropriate alert should be sent to the relevant individuals. Internal IT is responsible for responding to these alerts and notifying relevant individuals if necessary.

Note: In the internal version of LINK Mobility Information Security Policy this section specifies a number of unsuccessful authentication attempts before initiating lockout, duration of temporary lockouts and temporary lockouts resets.

3.2.7.4. Passphrases

- Passphrases are generally used for public/private key authentication. They are necessary to unlock the private key and gain access to the system.
- It is required for passphrases to follow the same guidelines as passwords in this policy.
- To provide greater security against dictionary attacks it is recommended for passphrases to be longer and consist of multiple words.

3.2.8. Use of Non-Personal Account

The use of a non-personal account (NPA) is allowed only under special circumstances and approval from the product owner.

- If the use of NPA is inevitable following rules must apply:
- Access to the account must be approved by a product owner.
- Password to NPA must be stored in a password manager, and access to it must be controlled.

- Password to NPA must be changed each time an employee that had access to it leaves the organization or loses access following any other circumstances (e.g. change of position).
- The use of NPA must be monitored and an appropriate event log, alerting the product owner or designated personnel.

System accounts are considered non-personal accounts in this Policy.

3.2.9. Remote access

Remote access refers to the capability of connecting to a LINK Mobility network or system remotely. This section covers connections made using protocols:

- Remote access may only be used to access the LINK Mobility system or network; the use of VPN connections for recreational purposes is strictly prohibited.
- Remote access may only be utilized through appropriately secured LINK Mobility devices or devices complying with the Bring Your Own Device Policy.
- The networks used for remote access to LINK Mobility resources must meet the requirements specified in section 3.10 of this Policy.
- Remote access must comply with the access control requirements outlined in section 3.2 of the Information Security Policy
- All remote access systems must require strong user authentication. Unauthenticated access is prohibited.
- The remote access granted to a user must be personal. The use of shared credentials is prohibited.
- It is highly recommended to use Multi-Factor Authentication for remote access.
- It is highly recommended to use a whitelist of devices allowed to use remote connections to prevent remote access by devices not approved by LINK Mobility.
- Remote access systems must allow for user accountability and connection identification.
- Using VPN clients not approved by LINK Mobility is prohibited.
- Sharing authentication details with other employees or external parties is prohibited.
- Secure protocols with industry standard strong cipher suites that ensure encryption of remote access traffic are mandatory.
- Remote access systems must automatically terminate sessions after a prolonged period of inactivity.
- Artificial network traffic caused by services and sending pings must not extend the user's session time.
- The maximum session lifetime must be set to a fixed period of time, and connections must be terminated after this period.

Note: In the internal version of LINK Mobility Information Security Policy this section includes information about protocols used for remote access to LINK systems.

Note: In the internal version of LINK Mobility Information Security Policy this section includes information about authentication methods that may be used for remote access to LINK systems.

Note: In the internal version of LINK Mobility Information Security Policy this section includes requirements for traffic routing configuration.

Note: In the internal version of LINK Mobility Information Security Policy this section includes specific requirements for maximum session lifetime.

3.2.10. Privileged access rights

- Granting privileged access rights must always be approved by the Asset Owner.
- Granting privileged access rights must be limited to the required minimum.
- Performing daily work that does not require privileged access rights on an account with these rights is prohibited.
- Accounts with assigned privileged access rights must be separate from the accounts used for daily work.
- If the use is associated with an assigned and approved task, it is considered an approved action.
- Daily technical support actions performed by Internal IT or their counterparts are considered approved actions.
- If possible, the implementation of a Multi-Factor Authentication mechanism is required for accounts with privileged access rights.
- Permissions for accounts with privileged access rights should be limited to the minimum necessary for performing their tasks.
- The use of privileged access rights must be logged by systems and monitored by system administrators, Product Owners, their equivalents or other individuals delegated for monitoring.
- Duties that require privileged access, especially in sensitive areas, should be divided among multiple people if possible, so no single person has control over all aspects of any critical process.

3.3. Asset management

Effectively managing the lifecycle of information-processing assets is fundamental in maintaining the confidentiality, integrity, availability, and authenticity of the information processed with these resources.

In LINK Mobility, the following categorization of assets, along with the departments (or roles) responsible for managing them throughout their lifecycle, has been adopted:

CATEGORY
Employee Workstation
Handheld Devices
Accessories
Servers & Systems
Physical Documents
Other

Note: In the internal version of LINK Mobility Information Security Policy the table above consist of two additional columns describing asset types for each category and responsibility.

In the above table, the "Responsibility" columns [**Note:** Not included in the public version of the Information Security Policy] also refer to local counterparts of the mentioned departments or roles.

- All LINK Mobility assets must have an assigned Asset Owner. The Asset Owner is the individual responsible for managing assets throughout their lifecycle:
  - An Asset Owner may or may not be a member of the departments listed in the table above [**Note:** Departments not listed in the public version of the Information Security Policy].
  - Asset Ownership may be transferred if needed.
- Assets must be assigned to individuals who use them for their daily work with the exception of:
  - All assets that cannot be assigned to a single person due to their use by more than one individual in daily work. Examples of such assets include those in the Servers and systems category. In such cases, only an Asset Owner should be assigned.
- Creating and maintaining records of assets used in LINK Mobility is required. The asset registry must include at least:
  - The name of the respective asset.
  - A unique identifier in the form of an internal inventory number or serial number.
    - Assigned numbers should (if possible) be located on the assets.
  - The first and last name of the individual assigned to the asset.
  - The current status in the asset's lifecycle (e.g., in use, retired, in stock).
  - Asset Owner.

- Files and paper documentation under this Policy are considered assets and information. Following applies:
  - They are subject to information classification described in section 2.4 of this Policy, not asset classification.
  - The creator of the file/document is considered the Asset Owner, and all copies are treated as separate assets.
  - They fall under the exception to the rule of assigning individuals to assets.
  - Acceptable use of these assets is described in section 2.4.2 of this Policy.
  - They are not required to be recorded in the asset registry.

LINK Subsidiaries may implement their asset management policies as long as they remain aligned with this Policy.

3.3.1. Acceptable use of assets

For all LINK Mobility assets, the following applies:

- All employees are expected to apply good judgment in their use of company assets and information.
- All company assets as defined in section 3.3 must be used for legitimate business purposes. Personal use should be minimal and should not interfere with work responsibilities.
- Employees should assess the risk in the usage of company assets, considering the classification metrics in section 2.4
- If a physical device is lost, stolen, or used in an unauthorized manner, or any of these activities are suspected to have occurred, this must promptly be reported to Internal IT.
- Any loss, theft, or unauthorized use of any other corporeal or intangible assets should promptly be reported to the asset owner
- Employees are obliged not to share allocated assets with unauthorized individuals without the consent of the Asset Owner.
- Assets need to be secured in a way to prevents loss, damage, and unauthorized access.

It is strictly prohibited to:

- Intentionally download, transmit, or otherwise introduce malware onto assets.
- Use assets for harassment, discrimination, or otherwise illegal activities.
- Share assets or information of an **Internal**, **Restricted,** or **Confidential** nature with unauthorized individuals or entities
- Engage in activities that result in excessive consumption of resources or disrupt network services.
- Reveal user credentials to others, which could give others access to LINK's assets.

For assets in the Employee Workstations, Handheld Devices, and Accessories categories, the following policies and procedures apply:

- **Group IT Policy** – Acceptable use of assets
- **Asset Management Process** – Procedure for asset management

For all other assets, the responsibility to create acceptable use policies lies with the Asset Owner. Acceptable use policies for assets must comply with the Information Security Policy.

3.3.2. Asset Classification

Assets are classified to determine critical assets for business operations and to adjust the priority and level of security measures for these assets. All assets within LINK Mobility must be identified, documented, and classified using the provided asset classification.

The classification of assets at LINK Mobility involves distinguishing assets between **KEY ASSETS** and regular assets.

Assets must be identified as **KEY ASSETS** whenever at least one of the following conditions is met:

- The asset is the LINK Mobility production system.
- The asset is a system that creates/stores backup copies of information for key assets.
- The asset is critical for ensuring LINK's business continuity.
- The asset is a system processing information classified as **RESTRICTED**.
- A breach of confidentiality, integrity, availability, or authenticity of the asset could lead to critical consequences for LINK Mobility, such as:
  - Grave damage to LINK's operations.
  - Major financial losses, revenue reduction, or cost raise.
  - Significant customer implications.

Examples of **KEY ASSETS** could be main application (production) servers processing customer data, or financial systems where data loss would result in legal penalties.

Asset owners may adjust the level of security measures for their assets according to their classification. The security measures must comply with this Policy, and any changes should only introduce measures that enhance security.

It is required that **KEY ASSETS** be taken into consideration when creating the "Business Continuity Plan" and "Disaster Recovery Plan".

3.3.3. Return of assets

Return of assets refers to the process of returning LINK Mobility-allocated assets from employees in the event of:

- Termination of employment.
- Termination of asset usage.
- Exchange of allocated assets (e.g., changing assigned phones).
- Other LINK Mobility business needs.

In all of the above cases:

- Assets allocated to an employee must be promptly returned to LINK Mobility following established procedures for the respective types of assets.
- Any records of issued assets must be updated upon their return to LINK Mobility.
- Further actions with the returned assets must comply with the requirements outlined in section 3.3.4 of the Information Security Policy.

3.3.4. Secure disposal or re-use of equipment

After returning assets to LINK Mobility, they can either reach the end of their lifecycle and be withdrawn from the organization or be reused. For both of these processes, the Asset Owner holds the responsibility, and additional procedures that comply with this Policy must be created.

3.3.4.1. Secure disposal

Secure disposal is the final part of the asset lifecycle. It occurs when LINK Mobility discontinues the use of an asset, and its removal from the organization is required.

LINK Mobility requires that the asset disposal process include:

- Backup critical data before erasing memory drives.
- Erasing and obstructing the recovery of any LINK Mobility-owned information by overwriting memory drives:
  - if overwriting is not feasible due to technical issues, physical destruction of the disks is required, either through shredding, degaussing, or drilling holes in hard drives to render them unusable.
- Destruction of memory drives by authorized companies specializing in media disposal.
- Documenting information regarding retired assets, including information about the responsible individual and the date of secure decommissioning of the media.

Secure decommissioning of server media is often performed by the service provider:

- It is required to ensure that the provider employs appropriate information removal methods.
- LINK Mobility does not require the physical destruction of hard drives by the provider.
- The methods for decommissioning media at suppliers must be verified as part of the Supplier Due Diligence process following section 3.11 of the Information Security Policy

3.3.4.2. Re-use of equipment

The assets returned to LINK Mobility may be reused if LINK deems it appropriate. In this case, the returned assets are assigned to another person.

Before being reused, assets must be properly prepared through:

- Backup critical data before erasing memory drives.
- Erasing and obstructing the recovery of any LINK Mobility-owned information by overwriting memory drives.
- Documenting information regarding preparing assets for being reused, including information about the responsible individual and the date of secure wipe of the media.
- Changing the records in asset registers.

3.3.5. Equipment maintenance

Devices used in LINK Mobility may require servicing related to malfunctions or other issues. In the first instance, any corrective actions should be taken by individuals in the appropriate roles at LINK Mobility, such as Internal IT or System Administrators.

- All internal repair actions must be carried out following the manufacturer's recommendations and internal procedures.
- Extra care must be taken to ensure that repair actions do not exacerbate the issue or void the manufacturer's warranty.

If internal repair actions are not feasible or have proven unsuccessful, authorized service providers, manufacturer warranties, or service providers from the supplier should be engaged.

If possible, repair actions should be performed on LINK Mobility premises.

- External service providers conducting services within LINK Mobility facilities are subject to guest policies described in section 3.6.5 of the Information Security Policy.
- If it is necessary to send a device to a service provider for repair, the following steps must be taken:
- Sent devices must have their hard drives removed.
- Before removing the hard drive, it is required to contact the manufacturer to confirm that this action will not void the warranty.
- If removing the hard drive is not possible due to technical reasons or warranty concerns, overwriting the disk's contents is required.
- If overwriting the contents of the hard disk is not possible, and removing it would void the warranty, the option of relinquishing the manufacturer's warranty should be considered, followed by the removal of the disk against the manufacturer's recommendations, or utilizing a different service.
- The shipment of the device must be duly recorded in the asset registers.
- If devices are located at the service provider's premises by default (e.g., servers), the option of repair by the service provider should be utilized. This option must be specified in the agreements between LINK Mobility and the service provider.

3.3.6. Bring Your Own Device

Bring Your Own Device (BYOD) policy pertains to situations where an employee wishes to use personal devices to provide services for LINK Mobility.

The use of personal devices is allowed, provided the following requirements are met:

The employee has submitted a request to their supervisor for the use of a personal device and obtained their approval.

The device has been configured following section 3.7.1 of the Information Security Policy.

The use of the employee's device has been recorded in the appropriate registers;

- The device will not be used by anyone other than the employee, including the employee's family, friends, or roommates.
- The device will be stored appropriately to prevent unauthorized access.
- The use of Mobile Device Management / Mobile Application Management solutions for BYOD is highly recommended.
- The employee submitting a request to use their device to provide services to LINK Mobility accepts the risk of potential loss of data in case a device wipe is necessary and agrees to adhere to this Policy requirements on their device.
- LINK Mobility is not responsible for private data stored on an employee's device.
- An employee is obliged not to use the devices in a manner contrary to the law. In the event of a breach of this obligation, LINK is not liable for any criminal actions committed by the employee.
- Loss or theft of the device must be reported to Internal IT immediately.

3.4. Business continuity

LINK Mobility is committed to maintaining the confidentiality, integrity, and availability of its information assets, even during crisis situations or business disruptions.

To fulfil these commitments, the implementation of appropriate organizational and technological measures is required to ensure the security of information in situations that may disrupt LINK's operations.

3.4.1. Business continuity planning

LINK Mobility requires the creation of two types of plans related to business continuity and key assets:

- **Business Continuity Plan:**
  - This plan focuses on ensuring that business operations can continue in the event of various types of disruptions or failures. It includes measures and procedures that allow LINK Mobility to maintain its ability to provide services in non-standard conditions.

- **Disaster Recovery Plan:**
  - This plan focuses on the recovery of services and systems in the event of a major disaster or failure that could impact the availability of key assets. It includes measures and procedures aimed at quickly restoring systems and data in the event of a complete shutdown of operations.

Both of these plans are crucial for ensuring the continuity of LINK Mobility's operations in the event of various emergency scenarios and must be tailored to the company's key assets.

3.4.1.1. Identification of key assets

Information Assets must be classified following section 3.3.2 of this policy to prioritize protection measures during business continuity situations.

Key assets must be included in the Business Continuity Plan and Disaster Recovery Plan.

3.4.1.2. Threats, Vulnerabilities, and Risk Assessment in Business Continuity

- For key assets, it is necessary to conduct the identification of threats, vulnerabilities, and risks generated by them to determine the potential impact of risk realization on the continuity of LINK Mobility's operations.
  - The identified risks must be taken into account during the business continuity planning, and actions aimed at their reduction must be documented.
  - Risk Assessment has been described in section 2.5 of this Policy.
- It is required to conduct vulnerability scans and penetration tests for critical assets to identify weaknesses and threats to LINK's operational continuity.
  - Vulnerability management has been described in section 3.9.3 of this Policy

3.4.1.3. Access Control in Business Continuity

In the event of an incident related to business continuity, there may arise a need to grant additional access to systems to ensure personnel are able to perform remedial actions. It is essential to ensure that in such a scenario, only the minimum necessary access required for task execution is granted, and appropriate security measures are implemented.

- Access Control to LINK assets has been described in section 3.2 of this Policy,
- Access Control must be adequately integrated with Business Continuity Plans and Disaster Recovery Plans.
- Identification of key accesses to systems allowing for incident and disaster handling is required.
- Access Control must take into account situations where extraordinary (emergency) access is required as part of incident or disaster-related activities.
- Implementation of time-limited access for personnel involved in business continuity tasks is highly recommended,
- All accesses granted for incident-related tasks or tasks related to maintaining business continuity must be monitored.

- Strong authentication mechanisms for personnel accessing information remotely or in alternative locations must be implemented.
- Remote access to systems must be secured by requiring the use of an approved VPN and additional connection authorization.
- An equal level of Access Control must be maintained for any redundant systems, tunnel connections, etc.
- Multi-factor authentication for accessing critical systems and applications must be enforced if possible.
- The lack of personnel availability must be taken into account for access controls in continuity planning. Access allowing for corrective actions must be provided to at least two individuals.
- The use of NPA is permitted in extreme scenarios, as outlined in section 3.2.8 of the Information Security Policy.

3.4.1.4. Incident Response Planning

- Incident Response in LINK Mobility utilizes the following procedures and policies:
  - NOC Incident Management procedures for platforms monitored by NOC Team.
  - Information Security Incident Management following section 3.5 of this Policy.
- Incidents must be thoroughly analyzed in terms of their source, incident management, and required corrective actions.
- Post-mortem meetings must be conducted and documented following section 3.5.5 of this Policy.
  - Conducting these meetings and analyzing incidents is crucial for LINK Mobility to decrease the likelihood of recurrence in the future.

3.4.1.5. Communication and Coordination

- Communication and coordination play a crucial role in maintaining information security during disruptions. To ensure proper communication, plans must include information about:
  - System owners – these are individuals who need to be informed in case of a disruption.
  - Contact persons for specific systems – these are individuals responsible for the proper functioning of systems and ensuring corrective actions. This also includes contact points with service providers for specific systems.
  - Communication escalation process – defining the communication flow based on the impact.
  - Relevant stakeholders – internal or external individuals who need to be informed with specified when to inform them.
  - Incident Response Team – individuals responsible for conducting the incident management process (e.g. Incident Manager, Technical Expert, Logbook Keeper). These roles can be taken over by the NOC team in the case of incidents related to availability.
  - Legal authorities – it is required to identify appropriate contact points, depending on local legislation.

3.4.2. Redundancy

- The infrastructure and systems related to critical assets of LINK Mobility must be analyzed to identify bottlenecks and single points of failure.
- Key assets of LINK Mobility must enable operational continuity in case of failures.
- For key assets, it is required to consider:
- Providing additional power sources.
- Providing additional network connections.
- Ensuring additional servers to take over the main server's tasks in case of failure.
- Ensuring backups.
- It is required to ensure an appropriate physical distance for backup systems. The creation of backup systems in primary locations is prohibited.

3.4.3. Data Backup

Creation of appropriate backup management processes and procedures for LINK Mobility systems is required.

- It is required to specify and document the following indicators for systems:
  - Recovery Time Objective (RTO) – targeted duration within which a system or service needs to be recovered and brought back to full functionality after a disruption or outage.
  - Recovery Point Objective (RPO)– the maximum tolerable amount of data loss that a system or organization can afford in the event of a disruption or outage. It is measured in terms of time, indicating how much data can be lost between the last backup or data synchronization and the occurrence of an incident.
- The RTO and RPO metrics must be approved by the Product Manager.
- Backups of information must be made at specified, regular intervals that meet the defined RTO and RPO indicators for a given system.
- Backups of information must be stored in separate locations.
- Backup data must be encrypted at rest and during transmission in accordance with section 3.9.2.2 of the information security policy.
- Access to backup data must be secured in accordance with the access control described in section 3.2 of the information security policy.
- The implementation, testing, and documentation of the backup restoration process are required.
- The backup data must be checked for data integrity.
- Retention of backup files must follow the LINK Retention Policy.
- Backups should be immutable.

Note: In the internal version of LINK Mobility Information Security Policy this section includes information about required distance between backup locations.

3.4.4. Capacity management

Capacity management refers to the process of planning, monitoring, and optimizing resources to meet the demands of LINK Mobility's infrastructure and systems.

To ensure effective capacity management, LINK Mobility requires Product Owners and System Administrators to:

- Monitor system performance regularly to identify potential capacity issues:
  - Monitoring of systems and applications has been described in section 3.9.4 of the information security policy.
- Taking into account the growing needs resulting from the expansion of systems, businesses, or applications during capacity planning,
- Optimize resource allocation to maximize efficiency through the analysis and assessment of IT resource utilization, such as:
  - CPU usage
  - Memory usage
  - Storage usage
  - Network bandwidth usage
- Implementing scalability to accommodate increased workloads and system expansion. This involves designing systems and infrastructure to handle growing demands and ensuring that additional resources can be easily added as needed to maintain performance and availability,
- Evaluate and select appropriate hardware and software upgrades to handle growing demands,
- Ensure that capacity planning aligns with business objectives and service level agreements (SLAs),
- Utilizing load balancing methods to evenly distribute traffic and workloads.

3.4.5. Testing

Ensuring operational continuity at LINK Mobility must undergo regular testing to identify any issues, discrepancies, or risks related to continuity of operations. Personnel responsible for ensuring continuity of operations are required to be familiar with the relevant plans to ensure appropriate responses to incidents and disasters.

- LINK Mobility requires Product Owners and Product Managers to ensure proper testing of Business Continuity and Disaster Recovery Plans.
- These plans should be tested at least once a year, and the results of these tests must be taken into account for creating new plans or improving existing ones.

Additionally, testing of systems and infrastructure for load capacity is also required to identify bottlenecks and other potential issues that may affect the continuity of operations.

It is required that the results of these tests be documented in the form of test reports.

3.5. Information security incident management

3.5.1. Security events and incidents

- **Event:** In the context of information and network security, an event typically refers to any observable occurrence in an asset, system, or network. Events can be safe or malicious. For instance, a user logging into a system is an event, as is an attempt to access a file.
- **Incident:** An incident usually refers to an event or series of events that lead to a breach of information security, a compromise of the confidentiality, integrity, authenticity, or availability of data, or any unauthorized access or attempts to access information systems. For the NIS2 Directive, the focus is primarily on incidents that have a significant disruptive effect on the continuity of the essential service.
  - According to Article 6(6) NIS2: *"'incident' means an event compromising the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data or of the services offered by, or accessible via, network and information systems;"*
- **Significant Incident:** Within the NIS2 framework, a "significant incident" usually implies a higher threshold of impact or disruption. An incident would be considered "significant" if it meets certain criteria established by the NIS2 Directive, which might involve factors like the number of users affected, the duration of the incident, or its geographic spread. A significant incident would trigger specific requirements in terms of reporting and response.
  - According to Article 23(3) NIS2: "An incident shall be considered to be significant if:
    - *it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;*
    - *it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage."*

3.5.2. Incident qualification

Incidents at LINK Mobility are assessed based on estimating the potential consequences caused by the event. To facilitate communication between the LINK NOC department, and LINK Information Security, a four-level classification is used, tailored to the specific department's requirements.

Note: In the internal version of LINK Mobility Information Security Policy this section includes table with incident qualification and assigned risk consequences.

3.5.2.1. NIS2 Incident qualification

The NIS2 Incident qualification is used by LINK Information Security to assess a specific incident in accordance with the requirements of the NIS2 Directive. The qualification takes into account the level as per section 3.5.2 of the Information Security Policy and the type of security breach.

Note: In the internal version of LINK Mobility Information Security Policy this section includes table aligning NIS2 Incident qualification with LINK Mobility Incident qualification mentioned in section 3.5.2. The table consist of information about NIS2 qualification for each type of breach (Confidentiality, Availability, Integrity, Authenticity).

3.5.2.2. NOC Incident qualification

LINK NOC team works according to ITIL 4. In ITIL 4 an incident is an unplanned interruption to a service or reduction in the quality of a service. This means that an availability incident in LINK is an unplanned interruption to a service or the failure of a component of a service that hasn't yet impacted the service. In order to be considered an incident in LINK, it must cause a disruption in service — and it has to be unplanned.

Note: In the internal version of LINK Mobility Information Security Policy this section includes table with NOC incident qualification and assigned risk consequences.

3.5.3. NIS2 authority reporting obligations

All significant incidents must be reported to appropriate authorities as noted in the Information Security Incident Handling Guidelines.

3.5.4. Incident levels in relation to GDPR – Personal Data Breaches

Information security event, incident, or significant incident if the scenario includes processing of personal data, may become also a "Personal data breach": as defined in Art 4 of GDPR: "a 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".

Handling and responding to GDPR personal data breaches are described in separate Data Breach and Crisis Management policies.

3.5.5. Incident response

- Confidentiality, Integrity, or Authenticity Incident – Incident response is the responsibility of local teams. LINK Mobility Information Security Team must be informed of the incident occurrence.
- Availability Incident:
- LINK Mobility Information Security Team or LINK Mobility NOC Team must be informed of the incident occurrence.
- Personal Data Breaches – Incident response lies on the local teams, or LINK Mobility NOC, depending on the type of incident. Handling and responding to GDPR personal data breaches are described in separate Data Breach and Crisis Management policies.
- All types of incidents follow Information Security Incident Handling Guidelines.

Note: In the internal version of LINK Mobility Information Security Policy this section includes more information about availability incident response.

For incidents and significant incidents, the following steps are required:

- **Identification:** Assessment of the incident according to the table in section 3.5.2 of this Policy. Depending on the type of incident, the Crisis Management policy may be invoked.

- **Communication:**
  - Notifying the relevant LINK Mobility teams, individuals, or stakeholders of the incident occurrence.
  - Escalating the incident to the relevant teams or individuals based on the incident level, escalation matrix, or other procedures.
  - Setting up communication channels.
- **Containment:** Taking immediate actions to mitigate the impact of the incident on LINK Mobility. This may involve isolating affected systems, disabling compromised accounts, or blocking malicious network traffic.
- **Collection of evidence:** Done according to section 3.5.6 of this Policy.
- **Eradication:** Identifying the root cause of the incident and eliminating it. This may involve removing malware, patching vulnerabilities, and addressing any weaknesses in the environment that contributed to the incident.
- **Recovery:** Restoring systems and data to normal operation. This may involve restoring the system from backup and implementing additional security measures to prevent a recurrence.
- **Lessons Learned:** Conduct a post-incident review or debrief to assess the incident response process and plan future actions to mitigate the risk of recurrence. This involves evaluating incident response in search of points to improve on, updating procedures, and policies, or providing additional security measures.
- **Documentation:** Preparing a final incident report that provides a detailed description of the incident, individuals involved, actions taken, lessons learned from the incident, and plans for further improvement.

The above steps can be expanded based on incident management procedures for individual systems or teams within LINK Mobility.

3.5.6. Collection of evidence

In the event of an incident, it is crucial to gather evidence to facilitate more efficient incident management, draw lessons from the incident, identify the source of the incident, or hand them over to the authorities in case of legal actions taken as the consequences of the incident.

- The collected evidence should include:
- Exported event logs are described in section 3.9.4.1 of the Information Security Policy.
- Binary copies of disks and systems if required.
- Email conversations in the form of .msg files.
- Surveillance footage if required.
- Screenshots of conversations using electronic communication channels other than email.

All collected evidence must be available only in read-only format. Any interference or modification of the collected evidence is prohibited.

The evidence material is treated as information classified as RESTRICTED and must be appropriately secured.

Note: In the internal version of LINK Mobility Information Security Policy this section includes an example of electronic communication channels used in LINK Mobility.

3.5.6.1. Log files

- All systems must produce event logs as described in section 3.9.4 of this Policy.
- Event logs must collect actions described in section 3.9.4.1 of this Policy.
- Event logs must be monitored as described in section 3.9.4.2 of this Policy.
- Access to log files must be managed according to section 3.2 of this Policy.
- Access to log files is only possible in read-only mode.
- Log files must be protected against unauthorized change.

3.5.7. Communication on incidents

Communication regarding incidents is differentiated between internal and external communication.

- Internal communication refers to communication within LINK Mobility and its subsidiaries.
- External communication refers to communication that extends beyond the company.

All internal and external communication must be described in the relevant incident response procedures and policies and must be in compliance with this Policy.

- **Internal communication:**
  - Incidents with a defined severity level must be reported immediately to the LINK Mobility Information Security Team.
  - Incidents and events with a defined severity level may be reported to the LINK Mobility Information Security Team after the incident response process is concluded.
  - Personal Data Breaches must be reported immediately to the Data Protection Officer and the LINK Mobility Information Security Team.
  - It is required to document internal points of contact within the company for incident management for individual systems.
  - It is required to notify stakeholders of the incident occurrence and keep them informed of the current progress.

Note: In the internal version of LINK Mobility Information Security Policy this section includes information about specific severity levels and requirements for internal communication.

- **External communication**:
  - External communication must always adhere to the established procedures and policies within LINK Mobility.
  - Unauthorized personnel are prohibited from engaging in external communication regarding incidents.
  - Significant incidents must be reported in accordance with section 3.5.3 of this Policy.
  - Communication-related to Personal Data Breaches is conducted in accordance with the Data Breach and Crisis Management policy.

3.5.8. Incident report

Every incident in LINK Mobility must be documented in the form of an incident report. To ensure proper incident management, the incident report must include the following information:

- The start date of the incident along with the exact (or approximate if not possible) time.
- The date of incident identification along with the exact time.
- The composition of the team responsible for incident management, in particular:
  - Incident manager
  - Logbook keeper
  - Technical expert (if possible)
- Detailed description of the incident along with timestamps. The description must include:
  - Actions were taken to contain the incident.
  - Actions were taken to eradicate the incident.
  - Meetings, and key conversations related to incident management.
  - Actions taken to restore systems.
- The end date of the incident along with the exact time.
- Lessons learned from the incident.
- Risk assessment of a recurrence of the incident.
- Attached are evidence materials.

Handling of incident reports must adhere the following:

- All incident reports must have the appropriate information markings. Incident reports are treated as information classified as **RESTRICTED**.
- The final incident report must be protected from unauthorized access and modification.
- Incident reports must be presented to individuals accountable for the respective system or process.
- Incident reports must be stored for at least 5 years.

3.6. Physical and environmental security

LINK has several physical offices around the world. Local management is encouraged to create relevant physical security policies and/or procedures, considering their specific context including perimeter(s), assets and physical segregation thereof, and environmental factors. All offices should implement controls to address deterrence, detection, access control, and security personnel. Unauthorized entry to any LINK office is prohibited.

Each LINK premise is obligated to secure:

3.6.1. Physical Access Control

- All access must be physically secured requiring individual identification.
- Physical access must be registered according to section 3.2.1, and adhere to all relevant access principles including segregation of duties.
- Considering local legislation, 24/7 video surveillance could be implemented to monitor entry- and exit points:
- Implementation must be done following a documented Legitimate Interest Assessment per office location, subject to DPO consideration and approval.
- Deter access to all entries, exits, and windows where reasonably reachable with alarm systems, fencing, and/or barred glass.

Note: In the internal version of LINK Mobility Information Security Policy this section includes examples of individual identification methods.

3.6.2. Server Rooms

All server rooms must:

- Be locked at all times to avoid access to unauthorized employees and visitors.
- Each door in conjunction with the server room must have an alarm system.
- Be protected against environmental threats:
- Have sufficient and redundant temperature controls to ensure appropriate cooling at all times.
- Have no windows (where impossible, windowed environments are to have sufficient protection of sunshine and heat).
- Be protected against flooding.

When using Data Centers the following requirements outlined in section 3.11.2 must be met.

3.6.3. Employee Awareness

- Employee Awareness training should take into account physical security threats, addressing
- Social engineering attacks such as tailgating,
- Lock devices when unattended,
- Facilitate and enforce the use of personal lockers for safe keeping of equipment,
- Other relevant topics following this Policy, other LINK Policies, and any local procedures,
- Clean desk policy as described in section 3.6.8 of the Information Security Policy
- Employees should be encouraged to stay vigilant.

3.6.4. Employee responsibilities

Employees are the first line of defence by ensuring the awareness of, understanding, and commitment to upholding physical security principles.

All employees must:

- Display proactive security behaviors, such as reporting lost access cards immediately or identifying potential security risks.
- Be introduced to the idea that physical security is everyone's responsibility.
- To provide feedback on physical security measures as this can reveal potential vulnerabilities or areas for improvement.

3.6.5. Visitors

A visitor is any individual seeking access to a LINK office who doesn't hold permanent access via their employment with LINK. All visitors must be accompanied by the inviter or an approved employee.

Logs should be kept for all visitors. These logs should include:

- name
- purpose
- date
- time of arrival
- time of departure

3.6.6. Waste management

Waste management is a critical aspect to consider in information security. Improper waste disposal can lead to unauthorized access to sensitive information or materials:

- Secure decommissioning of IT assets must be done according to the Asset Management Process.
- Any paper containing labeled information must be disposed of according to the Handling of information.

- Disposal perimeters should be secured for unauthorized access to deter dumpster diving.

3.6.7. Remote work

Any information or equipment that is taken out of LINK premises should follow strict security measures as described in this policy, Asset Management Process, and Handling of Information.

3.6.8. Clean desk

The following "clean desk policy" applies to all LINK employees and consultants:

- Employees are required to ensure that all restricted/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Employees are prohibited from using copy machines or other copying techniques (e.g. scanners, digital cameras) without authorization.
- Computer workstations must be locked when the workspace is unoccupied.
- Computer workstations must be shut completely down at the end of the workday.
- Computer workstations must be locked after a defined period of inactivity.
- Any **Restricted** or **Confidential** information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
- File cabinets containing **Restricted** or **Confidential** information must be kept closed and locked when not in use or when not attended.
- Keys used for access to **Restricted** or **Confidential** must not be left at an unattended desk.

Note: In the internal version of LINK Mobility Information Security Policy includes information about defined period of inactivity for locking workstations.

3.7. Internal IT

It is essential to integrate security practices in the management of end-user devices (workstations, handheld devices) to protect sensitive information, prevent security incidents, and comply with relevant regulations and standards.

3.7.1. User devices management

- Asset management in the form of user devices is carried out in accordance with section 3.3 of this Policy.
- Use of personal devices for work purposes is carried out in accordance with the Bring Your Own Device Policy described in section 3.3.6 of this Policy.
- Equipment maintenance has been described in section 3.3.5 of this Policy.
- All user devices in LINK Mobility must be configured by Internal IT or their equivalents.
- All user devices in LINK Mobility must be centrally managed by Internal IT or their equivalents.

- All user devices must be configured to be compliant with:
  - Section 3.2 of this Policy for user accounts.
  - Section 3.2.10 of this Policy for use of privileged access rights.
  - Section 3.9.2 of this Policy for encryption.
  - Section 3.2.9 of this Policy for remote access.
  - Section 3.9.1.1 of this Policy for clock synchronization.
  - Section 3.9.4.1 of this Policy for event logging.
  - Section 3.3.5 of this Policy for maintenance.
  - Section 3.6.8 of this Policy for clean desk, screen lockout
- The configuration of LINK Mobility user devices must:
  - Prevent users from using external memory storage devices.
    - Configuration allowing the reading of the contents of the storage device is permitted, provided that writing to the device is prevented unless the storage medium is encrypted.
  - Enforce the installation of system updates and security patches.
  - Prevent users from software installation.
    - Installation of software on user devices must be done according to section 3.7.2 of this Policy.
  - Disable all unused or unnecessary ports, protocols, services, and features.
  - Deactivate, change passwords and rename local system and built-in accounts.
- All user devices must have installed an approved antivirus/antimalware solution.
- Internal IT and their counterparts have the right to verify the configuration of user devices at the request of the Asset Owner or Information Security Team.

3.7.2. Software management

- Installation of software on LINK devices and systems can only be done through the use of privileged access rights.
- The configuration must prevent users from independently installing software.
- The installation of software must be approved by the Asset Owner or a delegated person.
- The software can only be installed by Internal IT, system administrators, Asset Owners, their counterparts, or delegated individuals.
- Software may only be used in compliance with applicable license and purchasing agreements:
  - Each employee is individually responsible for reading, understanding, and adhering to all licenses.
  - The usage of unlicensed software is prohibited.
- All software installed on LINK devices or systems must be approved by the Asset Owner:
  - Only software from legal sources is allowed to be installed.

- Only work-related or productivity-enhancing software can be installed.
- Installation of unsolicited and not work-related software is prohibited.

- The default software required for LINK Mobility systems and devices must be identified and documented:
  - The installation of software from this list does not require additional approval from the Asset Owner.
  - An employee can request the installation of software not on the list from the Asset Owner.
- Use of any privileged utility programs must require privileged access rights and is prohibited if not allowed by the Asset Owner.
- Internal IT, system administrators, Asset Owners, their counterparts, or delegated individuals have the authority to conduct software audits on devices and systems within LINK Mobility.

3.7.3. E-mails

- Employees are required to use LINK Mobility email accounts for both external and internal communication. Usage of personal e-mail accounts is prohibited.
- Employees are required to use LINK approved clients for mailboxes.
- It is required to use secure protocols for mail communication.
- The sender of the e-mail must make sure the receiving address is correct:
  - In case of sending an e-mail to the wrong recipient where personal data is involved the Data Breach Policy must be invoked.
  - Company e-mails should not be forwarded to personal e-mail addresses.
- When using e-mail, all employees must be aware of “phishing”. All employees must be careful about opening attachments and following links embedded in the content:
  - In case of finding suspicious e-mails, those must be reported to Internal IT.

Note: In the internal version of LINK Mobility Information Security Policy this section specifies mailbox clients approved by LINK Mobility.

3.7.4. Remote work

Employees are allowed to work remotely subject to compliance with:

- Section 3.10 of this Policy for network security / remote access.
- Section 3.6.8 of this Policy for physical security / clean desk
- Devices used for remote work must be configured according to section 3.7.1 or according BYOD policy in section 3.3.6.

3.7.5. Cloud storage

When using personal computers (LINK-owned and BYOD), all proprietary information of LINK should be stored on LINK approved cloud storages. Usage of other cloud solutions is not permitted.

Note: In the internal version of LINK Mobility Information Security Policy this section specifies cloud storages approved by LINK Mobility.

3.8. Project Management & Secure Development Life Cycle

It is essential to integrate security practices throughout the project life cycle to protect sensitive information, prevent security incidents, and comply with relevant regulations and standards.

3.8.1. Information security in project management

Information security must be integrated into the project management process. Individuals responsible for project management need to adhere to the following practices in their processes.

3.8.1.1. Risk Management

Risk management must be incorporated during all phases of the project:

- The process must include:
  - Identifying risks.
  - Assessing their potential impact and likelihood.
  - Executing measures to mitigate these risks.
- The separate document named Project Security Controls Checklist can be used to fulfill the above requirements.

Note: Project Security Controls Checklist includes a list of required security controls and possible risks that may be identified.

3.8.1.2. Security requirements

Projects must meet the minimum security requirements of LINK Mobility:

- Minimum requirements are defined in this policy, and a separate document named Project Security Controls Checklist,
  - If the project involves the processing of personal data it must also follow minimum requirements from Privacy and Security by Design Guidelines,
- Additional security requirements can be defined by Product Owner, Product Manager, or designated personnel.

3.8.1.3. Secure design and development

Security must be also integrated into the design and development phases.

- To ensure proper integration of security, one must follow secure practices

Note: In the internal version of LINK Mobility Information Security Policy this section lists more secure practices required by LINK Mobility.

3.8.1.4. Secure design and development

Change management must be implemented following requirements from section 3.8.2. of this Policy. It is required that every change must be documented, tracked, and approved.

3.8.1.5. Training and Awareness

Individuals holding roles as developers, administrators, or other roles actively involved in the development of software or systems at LINK Mobility must complete training on information security and GDPR available on the internal platform.

The competence of individuals actively involved in software or system development must be continuously enhanced through training, courses, or participation in conferences to ensure that these individuals possess sufficient knowledge to maintain information security in the systems.

3.8.1.6. Security testing

Systems and applications must be tested for information security following section 3.8.8 of this policy.

3.8.2. Change control and versioning

To ensure proper change control for the software development process, LINK Mobility requires the use of secure source control systems that support versioning. Product Owners may choose a tool that meets their requirements as long as they comply with this policy, at their discretion.

Tools used by Product Owners must at the very least support:

- Versioning
- Tracking changes
- Reverting changes

3.8.3. Access to source code

The Product Owner is responsible for authorizing access to source code and maintaining an access control register. Granting access should reflect the employee's role in the organization. Access to source code must be protected by strong authentication mechanism.

Note: In the internal version of LINK Mobility Information Security Policy this section includes information and requirements about one authentication mechanism that may be used in LINK Mobility.

For LINK Mobility policy on the use of NPA refer to section 3.2.8 of this Policy.

- A Product Owner is responsible for maintaining an access control register to NPA that has access to source code.
- Source code should be accessed only from workstations and systems approved by LINK Mobility and using a secure connection.

3.8.4. Issue tracking

Product Owners are required to use an issue tracking system in their projects and that:

- Every change to the system should be reflected through an appropriate task in the issue tracking system.
- Commits should include the issue number from the issue tracker system.
- Every issue being selected for development has an assigned employee.
- Tasks must be approved before they can be initiated by the developer.

The Product Owner is the one responsible for approving these changes. Product Owners can designate the responsibility to others but still be held accountable.

3.8.5. Software development methodology

Product Owners must adopt a software development methodology that:

- Meets specific project requirements and information security requirements.
- Supports issue tracking throughout the whole software development lifecycle.

Software development must always follow an adopted methodology to ensure the proper functioning of the process.

3.8.6. Environment separation

- It is required to separate development, test, and production environments.
- It is required to at least logically separate LINK customer data/information in any environment.

3.8.7. Automated build and deployment

- LINK Mobility systems should use automatic build and deployment tools. These tools should be fully automated and deliver a complete setup, including any configurations, etc.
- Deployments must be approved by the Product Owner, using Continuous Deployment mechanisms is an exception from this rule.
- Deployment should follow the section “Release” from Privacy and Security By Design guidelines.

3.8.8. Test and reviews

To ensure an adequate level of information security, all changes should (if possible) be tested through:

- Code Review process
- Automated testing
- Performance testing
- Manual testing

During testing the following rules must be observed:

- During testing, the use of production data (real data) is strictly prohibited.
- Tests should be conducted in appropriate environments, and no changes should be deployed to the production systems before completing all tests.
- Additionally, it's highly recommended to use any kind of Static Code Analysis Tool & Software Composition Analysis tool to perform security checks before or immediately after committing changes.
- The test must demonstrate that the application or system meets the minimum requirements of LINK Mobility. To achieve this, the document named **Project Security Controls Checklist** can be utilized.

3.8.9. Use of libraries or SDKs

Use of libraries or Software Development Kits ("SDK") should follow the section "Use of libraries or SDKs" from Privacy and Security by Design guidelines. External software may only be used in compliance with applicable terms and conditions. The usage of unlicensed libraries and SDKs is prohibited.

3.8.10. Outsourced development

Outsourced development is allowed under this Policy, but if the development is to be carried out by an external vendor, the vendor must follow the SDD process following section 3.11 of this policy.

All development done by external parties must follow the Secure Development Life Cycle "SDLC" from this section of this policy.

3.9. Operations

3.9.1. Configuration management

All LINK Mobility devices must be configured to ensure their security and compliance with this Policy. First and foremost, it is required that:

- LINK Mobility systems and devices must be configured in a standard manner, following established configuration procedures:
  - System administrators are responsible for creating configuration procedures for LINK Mobility systems. These procedures must be approved by the Product Owner or their equivalent.
- Access to LINK systems and devices must be configured in accordance with the access control requirements described in section 3.2 of this Policy.
- The cryptographic protections of LINK systems and devices must be configured in accordance with the cryptography requirements described in section 3.9.2 of this Policy.
- Default accounts and passwords for LINK systems and devices must be disabled or changed.
- Disabling all unused and unnecessary protocols, ports, and services is required.
- Only systems that require access to the Internet should have it.
- Access to administrative privileges for LINK Mobility systems and devices must be restricted to adequate roles.
- LINK Mobility systems and devices are required to have antivirus protection installed.
- Event logging in LINK Mobility systems and devices must be carried out in accordance with section 3.9.4.1 of this Policy.
- The installation of software on LINK Mobility systems and devices must require elevated privileges.
- Installation of software on the operating systems of LINK Mobility systems must comply with section 3.7.2 of this Policy.
- The configuration of LINK Mobility systems and devices must prevent users from using external drives. If it's not possible to configure the system/device in this way, physical security measures should be applied to directly secure the ports (using port covers) or prevent physical access (using locked server cabinets).
- The time synchronization configuration for LINK Mobility systems and devices must adhere to section 3.9.1.1. of this Policy.
- The use of privileged utility programs must follow the software management in section 3.2.10 of this policy.
- Using hardening guidelines should be considered.

Note: In the internal version of LINK Mobility Information Security Policy this section includes an additional recommendation regarding configuring systems and devices in a standard manner.

Note: In the internal version of LINK Mobility Information Security Policy this section includes a requirements for restricting connections.

Note: In the internal version of LINK Mobility Information Security Policy this section specifies roles that could have access to administrative privileges for LINK Mobility systems.

Note: In the internal version of LINK Mobility Information Security Policy this section specifies exact hardening guidelines that should be used.

3.9.1.1. Clock synchronization

Time synchronization is important in the context of information security because it prevents discrepancies between timestamps recorded from different systems during the collection of evidence, for example, in the event of an incident.

When feasible it is required that:

- All systems must utilize defined time protocols to synchronize time from trusted and centrally placed time servers.
- LINK Mobility time sources should not be lower than defined Stratum.
- The sources used must be documented in the configuration procedures.

Note: In the internal version of LINK Mobility Information Security Policy this section specifies time protocols used for LINK Mobility systems.

Note: In the internal version of LINK Mobility Information Security Policy this section specifies the lowest stratum that can be used for LINK Mobility systems.

It is recommended that LINK Mobility systems support the ability to query them about the used time server to verify the time sources used for different LINK systems. Clock synchronization should be verified by system administrators at least once a year and is required when implementing a new system.

3.9.2. Encryption

Encryption and data masking are among the fundamental methods for maintaining the confidentiality of information used in LINK Mobility and are required for all information processed by LINK.

3.9.2.1. Data at rest

Data at rest refers to data that is stored on a physical medium, such as a hard drive, flash drive, or backup tape, as opposed to data that is actively moving or being processed. Encrypting data at rest involves applying encryption to protect data when it is stored in databases, file systems, or other storage repositories.

All LINK devices must have encrypted disks according to the operating system.

Note: In the internal version of LINK Mobility Information Security Policy this section specifies encryption solutions assigned to operating system.

In general, development must choose the strongest possible measures for cryptography, according to performance requirements on the solution level.

Note: In the internal version of LINK Mobility Information Security Policy this section specifies encryption solutions that may be used by LINK Mobility systems.

It is preferred that RSA is used as an algorithm for encrypting keys and similar assets which do not require immediate heavy computational force, as asymmetric key generation is a slow and CPU-intensive process.

Note: In the internal version of LINK Mobility Information Security Policy this section specifies recommended key sizes.

3.9.2.2. Data in transit

Data in transit refers to information that is currently moving from one location or device to another over a network or communication channel. This data is vulnerable to interception and eavesdropping if it's not properly protected through encryption and other security measures.

- LINK Mobility requires all data to be encrypted in transit, by:
- Utilizing secure protocols for communication such as:
- Transport Layer Security (TLS) – The lowest possible version is TLS 1.2, while 1.3 is recommended
- Hypertext Transport Protocol Secure (HTTPS)
- Utilizing secure sockets.
- Implementing end-to-end encryption.
- Utilizing SSL/TLS certificates.
- Utilizing Virtual Private Networks.

Note: In the internal version of LINK Mobility Information Security Policy this section specifies more secure protocols used for communication and VPN solutions that may be used by LINK Mobility.

3.9.2.3. Key management

Key management refers to the processes and procedures involved in generating, storing, distributing, and disposing of cryptographic keys used for encryption and decryption. It is a critical component of data security and is essential for maintaining the confidentiality and integrity of encrypted data.

- Product Owners are required to document key management procedures that include information on key generation, storage, transmission, and destruction.
- Keys must be stored in a secure location with limited access to prevent unauthorized access, modification, or loss of keys.
- Access to these locations must follow section 3.2 of this Policy.
- Storing keys in plain text is prohibited. Keys must be adequately protected through hashing/ encryption following section 3.9.2 of this Policy.
- Compromised keys must be immediately destroyed, and this process must be described in the procedures for the respective systems.

- Keys should be only transmitted using secure protocols described in section 3.9.2.2 of this Policy.
- "Bring Your Own Key" approach is permitted whenever this is technologically feasible and in accordance with the local legislation.

3.9.3. Management of technical vulnerabilities

Vulnerability means a weakness, susceptibility, or flaw of ICT products or ICT services that can be exploited by a cyber threat. The purpose of vulnerability analysis is to identify, quantify, and prioritize vulnerabilities in a system to determine two key indicators: exposure/impact & severity. It is also a means to indicate if safeguards in place are sufficient in terms of confidentiality, integrity, authenticity, and availability.

LINK Mobility subsidiaries may use different tools and methods to achieve vulnerability analysis (vulnerability scans and penetration testing).

3.9.3.1. Overall Vulnerability Rating

All vulnerabilities detected through vulnerability scans or penetration tests should undergo additional analysis, comparing the severity of the vulnerability (usually expressed as a CVSS score) with the potential for exploitation and its consequences on LINK Mobility systems. This analysis must be performed by the Product Owner or a person designated by them.

The severity of vulnerabilities is most commonly expressed as a CVSS score. If, for any reason, a CVSS score has not been assigned to a vulnerability, the Product Owner is required to conduct their own assessment of the vulnerability's severity.

For each vulnerability, it is required to assess the likelihood of its exploitation and its consequences.

Both indicators are combined to get a "Vulnerability Rating".

Note: In the internal version of LINK Mobility Information Security Policy this section includes tables for severity rating, exposure/impact score and a matrix for vulnerability rating.

The final step in vulnerability analysis is to determine the Overall Vulnerability Rating (OVR) based on the calculated Vulnerability Rating and the classification of the asset to which the vulnerability pertains.

Note: In the internal version of LINK Mobility Information Security Policy this section includes tables for Overall Vulnerability Rating based on asset classification.

3.9.3.2. Vulnerability remediation

After completing the vulnerability analysis, the Product Owner is required to create and implement a vulnerability remediation plan.

This plan must include:

- One of three actions that can be taken towards the vulnerability:
  - **Mitigate** – Implementation of corrective actions aimed at patching the vulnerability. It is required to provide information on how the vulnerability will be remedied.

- **Accept** – No corrective actions will be taken. A declaration of vulnerability acceptance is required from the Product Owner and Product Manager, and approval from the individuals accountable for the respective system/platform. Reasoning must be provided.
- **Avoid** – The vulnerability will not be fixed; however, measures will be taken to hinder its exploitation, such as concealing it, modifying access, or other actions. It is required to provide information on how the vulnerability will be avoided.

- Estimated implementation time for the remediation actions for each vulnerability.

It is required that the remediation plan be presented no later than the end of the week following the presentation of the penetration test or vulnerability scan report.

The estimated implementation time for the remediation actions should meet the requirements from the table below:

OVR	IMPLEMENTATION TIME
CRITICAL	2 weeks
HIGH	1 month
MEDIUM	3 months
LOW	Nice to have within 6 months

Mitigation must also be offset by the following:

- Cost-benefit analysis.
- Operational impact.
- Feasibility.
- Applicable regulations.

3.9.4. Logging and monitoring

Collecting information about actions taken on LINK Mobility systems or by these systems allows for tasks such as monitoring anomalies or gathering evidentiary material in case of an incident. Logging activities are crucial for the incident management process and must be properly implemented for all LINK Mobility systems. Logs should be kept as long as there is a business need and no longer than specified in the **LINK Retention Policy**.

3.9.4.1. Event logs

Collecting information about actions taken on LINK Mobility systems or by these systems in the form of event logs is required.

Systems, if applicable, must log the following actions:

- Authentication and Authorization Events.
- Access Control Events.

- Network Activity.
- System and Application Errors.
- Security Logs.
- Privilege Escalation and Elevation Events.
- File and Data Changes.
- Account Management.
- Audit Logs actions.
- Database Activity.
- External Device Connections.
- Web Application Logs.
- Email and Messaging Logs.
- Backup and Recovery Logs.
- Event logs must contain:
- Timestamp.
- Event source.
- Event ID.
- User or Process information.
- IP Address or Hostname.
- Description/Message.
- Event Result or Status (e.g. Authentication Failed/Successful).
- Raw Data/Payload.
- When logging personal or sensitive data, event logs must respect privacy laws and regulations. Personal data should be appropriately masked or protected.
- It is recommended to send logs to a centralized log collection system.
- It is required that system configurations include time synchronization from a single source as per section 3.9.1.1 of this Policy - Lack of time synchronization can lead to conflicting information.

Note: In the internal version of LINK Mobility Information Security Policy this section specifies events to be logged for each activity.

3.9.4.2. Monitoring and threat intelligence

LINK Mobility key assets must, and LINK Mobility systems should, be monitored for threats to the confidentiality, integrity, availability, and authenticity of information. Information about potential threats must be analyzed to be able to facilitate informed actions to prevent the threats from causing harm or reduce the impact of such threats.

Monitoring must send appropriate alerts to administrators in case of events, (including correlations of more events), indicating anomalies.

Note: In the internal version of LINK Mobility Information Security Policy this section includes examples of anomalies.

3.10. Network security

The networks managed by LINK Mobility must be secured against unauthorized access. Only devices belonging to LINK Mobility or compliant with the Bring Your Own Device policy are allowed to access the network.

- LINK Mobility requires network administrators to create network diagrams to provide an overview of the utilized solutions, connections, and their security.
- Network diagrams are treated as either Confidential or Restricted classified information depending on their level of detail.
- It is required to document and store information about the used IP addresses to prevent address conflicts when using static addressing.
- Remote access to networks has been described in section 3.2.9. of this Policy.

General access to the Internet, through the LINK Mobility network is permitted only for business purposes. LINK Mobility employees are responsible for ensuring that they and not violate any LINK Mobility policies and do not perform illegal/malicious activities.

3.10.1. Wireless connection

- All devices serving as access points for the wireless network must be configured in accordance with section 3.9.1 of this Policy.
- All devices serving as access points for the wireless network must be physically secured in accordance with section 3.6 of this Policy
- Wireless networks must meet the requirements for data encryption in transit as described in section 3.9.2.2 of this Policy
- Wireless networks should be segregated as described in section 3.10.5 of this Policy.
- Access to the wireless network must:
  - Require user authentication using a password in accordance with section 3.2.7.1 of this Policy
  - Utilize authentication protocols and encryption methods specified by LINK Mobility.
  - In the case of using authentication protocols not supporting unique authentication details for each user, it is required to change the password periodically following LINK Mobility requirements and in the event of an employee's departure.
  - The above-mentioned restrictions do not apply to the guest network.
- MAC Address whitelisting is highly recommended.

Note: In the internal version of LINK Mobility Information Security Policy this section specifies authentication protocols for wireless networks and time of periodical password change.

3.10.2. Wired connection

The cabling used to connect devices to LINK Mobility's network must be secured in accordance with section 3.10.6 of this Policy.

- Network devices such as routers, switches, and hubs must be properly configured in accordance with section 3.9.1 of this Policy.
- Network devices such as routers, switches, and hubs must be physically secured in accordance with section 3.6 of this Policy.
- Access to the network must be restricted through:
  - MAC address filtering allows access only to specified devices.
  - It is highly recommended to use network access authentication via LINK Mobility approved protocols.
  - It is highly recommended to utilize any other Network Access Control solutions that provide greater security than MAC address filtering.
- Network segmentation is recommended in accordance with section 3.10.5 of this Policy.
  - Guest access to the wired network is prohibited. Guest access should only be provided through the wireless network.

Note: In the internal version of LINK Mobility Information Security Policy this section specifies authentication protocols approved by LINK Mobility.

3.10.3. Networks not managed by LINK

LINK Mobility allows employees to work remotely. For this form of work, the following applies:

- Employees are responsible for properly configuring wireless network access devices while working remotely.
  - Employee's wireless networks must be configured in a way that requires password authentication for access.
  - Utilization of LINK Mobility approved protocols is required.
  - An employee lacking sufficient knowledge of network configuration should seek assistance from the local Internal IT or their equivalent.
  - Employees are responsible for the physical security of access points in the private network.
  - LINK Mobility does not require employees to adhere to specific physical security measures for their private access points. Only physical protection of the device against unauthorized access is required.
- Employees are required to connect only to known networks and verify network names before connecting.

Note: In the internal version of LINK Mobility Information Security Policy this section specifies authentication protocols approved by LINK Mobility.

3.10.4. Using publicly available wireless networks

Using any unsecured public wireless networks available in places such as hotels, shopping malls, airports, or restaurants is prohibited.

LINK Mobility also considers situations such as business trips, and on-site visits to customer or supplier locations. In such cases, employees are required to:

- Exercise particular caution when connecting to available networks.
- Do not connect to networks that have not been password-protected and are publicly available.
- Refrain from using remote access to LINK Mobility's resources unless it is necessary.

In a scenario where no secure networks are available LINK Mobility recommends to use cellular network. Employee needs to ensure that enabled hotspot is password protected.

3.10.5. Segregation of networks

Segmenting networks is one of the fundamental methods to prevent unauthorized access to information. This division aims to limit access to resources for visitors to LINK Mobility premises or those gaining access to the network in any other way.

- It is required that LINK Mobility networks be divided into at least the LINK internal network and the guest network.
- The guest network must not have any access to LINK Mobility's internal resources.
- Guest access should be limited to wireless networks only. Wired network access for guests should be prohibited.
- Further network segmentation between departments or specific server access is recommended.

3.10.6. Cabling security

Cables and Ethernet sockets used in LINK Mobility networks must be adequately protected against damage, interference, and unauthorized access.

- The Ethernet cables used in LINK Mobility must be located in closed conduits or technical ceilings/ floors.
- Ethernet cable parameters required by LINK Mobility include:
  - Minimum category: 5e according to EN 50173 standard.
  - Shielding Type:
    - U/FTP at least.
    - S/FTP recommended.
    - SF/FTP is highly recommended.
  - Compliance with industry standards and regulations.

- If possible, to avoid electromagnetic interference and signal disruption, it is required to:
  - Avoid running Ethernet cables near potential sources of electromagnetic interference, such as high-power devices, radio equipment, microwave devices, etc.
  - Maintaining a distance of 15-30 centimeters between Ethernet cables and power cables is required to minimize the risk of electromagnetic interference.
  - Avoid running Ethernet cables and power cables in parallel or at right angles to minimize the risk of electromagnetic interference.
  - Avoid excessive sharp bends or sags in Ethernet cables.
  - Run Ethernet cables in separate channels to isolate them from other types of cables.
- The use of proper cable management is required to facilitate the troubleshooting process.
- All ports associated with unused sockets must be deactivated.
- Tampering with cabling by unauthorized personnel is prohibited. All actions on Ethernet cables must be carried out only by network administrators or technical support personnel.

3.10.7 Web filtering

The LINK Mobility network can only be used for work-related purposes; therefore, it is highly recommended to implement various types of web filtering solutions aimed at protecting users from accessing harmful content that could compromise LINK Mobility's information security.

3.11. Supplier Relations / Supplier Due Diligence

Supplier Due Diligence (SDD) is a process through which LINK identifies, prevents, mitigates, and accounts for the adverse impacts in relations with suppliers and business partners.

3.11.1. Suppliers management

Onboarding new suppliers should be managed according to the Supplier onboarding manual. LINK defines the supplier relationship based on different criteria as described in the SDD process, however for Information security purposes all Data Centers are considered key suppliers.

For each supplier, there must be a dedicated person (business owner) named who is responsible for the contractual relationship with the supplier. Before any new supplier is onboarded the SDD process must be completed if any information is shared between LINK and supplier. Business owners must document the scope of the information that is shared between LINK and the supplier.

As part of the SDD process, the supplier is required to return filled LINK SDD questionnaires that cover information security and business continuity.

- If personal data is shared with the supplier the supplier needs to follow stipulations made in the Processor section of the **Personal Data Protection Policy**.
- If this is not possible the responsible person should gather enough information to satisfy the need for an initial audit.
- The filled-out questionnaire or other documentation needs to be reviewed and approved by a qualified person, either someone from the Information Security department or a technical expert.

Appropriate legal agreements or contracts between LINK and its suppliers must be in place.

These agreements should specify the terms of the relationship, including:

- The right for LINK to conduct audits.
- Policies related to the retention of personal data or other relevant information.
- Technical and organizational measures concerning security.
- Service Level Agreements (SLA) stipulate the expected quality of service, uptime, and other pertinent metrics.

Specific requirements for key suppliers:

- Suppliers, especially the key ones, should undergo a follow-up audit at a minimum of once a year. Moreover, if there's a major change in their operations, services, or any other significant factor, an audit should be conducted irrespective of the yearly schedule.

3.11.2. Management of the ICT supply chain

Each data center must be audited at least once a year. Documentation of the audit should be stored for at least 3 years.

Data centers that host critical LINK production environments must:

- Be at a third level of data center tier classification
- Have ISO 27001 or SOC2 Type 2 certification. If ISO 27001 certification is present, the business owner should request a statement of applicability from the data center.
- Documented and tested BCP plans that can be shared with LINK on request

3.11.3. External audit

To conduct audits LINK may hire external auditors. External auditors are considered suppliers and must undergo the SDD process. External auditors can access LINK information only if an appropriate Non-Disclosure Agreement is in place and it is not prohibited by law.

Conducting audits by external auditors can’t have an adverse impact on LINK’s operations and should not lead to interruptions in operation continuity.

External penetration tests must follow the Penetration testing procedure. Audit tests should only be carried out on “read-only” access to software and data, preferably in a separate audit environment

3.11.4. Cloud services

In its operations, LINK Mobility can utilize cloud vendors. Many cloud vendors have standardized agreements that are offered on a "take it or leave it" basis. This means that customizations or negotiations of the terms are limited or non-existent. LINK is aware of this limitation when entering into contracts with such vendors.

Each cloud vendor must undergo the SDD process. This process might sometimes rely only on the public information provided by the vendor. The goal is to understand the system's design, architecture, and interactions to ensure compatibility and security.

Before finalizing a contract with a cloud vendor, LINK must ensure that the agreement aligns with its internal requirements. These requirements might include:

- LINK expects cloud vendors to base their services on recognized industry best practices and standards when it comes to system design and infrastructure setup.
- In the case of a security breach or other information security events, LINK requires that the cloud vendor provide the necessary support to address and mitigate the incident.
- The vendor must specify when and how they remove LINK's data from their systems. This includes details about data deletion methods to ensure that once deleted, the data cannot be recovered.
- If cloud vendors offer the option to choose where the data is stored geographically. LINK always opts to have its data stored within Europe. This could be due to regulatory requirements, latency concerns, or other strategic reasons.
  - LINK Mobility subsidiaries located outside of the EU/EEA area may choose a geo-location based on their location.

Ultimately, the use of cloud services by LINK should be approached with the same rigor and security scrutiny as the deployment of any other system. Specific security guidelines might be available in other sections of LINK's policy. However, any engaged cloud vendor must allow LINK to implement its security controls. While not explicitly listed here, these controls could encompass encryption methods, access control policies, network security monitoring, vulnerability scanning, data backup and recovery, protection against DDoS, documented BCP plans, incident response, and more.

3.12. Exceptions

An exception to this Policy requirement allows for non-compliance with the policy based on accepted risk.

An exception to an information security policy, standard, procedure, instruction, or practice may be granted in any of the following situations:

- Compliance would cause a major adverse financial impact that would not be offset by the reduced risk occasioned by compliance (i.e., the cost to comply offsets the risk of non-compliance).
- Immediate compliance would disrupt critical operations.
- Another acceptable solution with equivalent protection is available.
- Compliance is not possible due to technological or organizational limitations.
- Individual assessment of the situation, is not listed above.

An individual must present an exception request to the Information Security Team.

Exception requests must consist of:

- The specific policy/procedure/other documents from which exception is being requested.

- The specific device, application, service, process, or activity for which the exception is being requested.
- Data classification category of the associated device, application, or service (if eligible)
- The type of data that will be affected, either directly or indirectly by the exception.
- The nature of the non-compliance i.e. specific deviation from the policy.
- Why an exception is required, e.g., what business need or situation exists, what alternatives were considered and why are they not appropriate?
- Assessment of potential risk posed by non-compliance.
- Plan for managing or mitigating those risks, e.g. compensating controls, and alternative approaches.
- Anticipated length of non-compliance.
- Additional information as needed, including any specific conditions or requirements for approval.

Exception requests must be reviewed by the Information Security Team to assess the risk and forwarded to a top management for an approval.

Once a particular type of exception has been granted, future requests of the same type may not receive the same ruling.

If a certain type of exception is constantly being requested and approved Information Security Team should verify if the policy/procedure/other documents need to be adjusted to include the exception as a norm.

Exceptions must be reviewed during internal audits and documented in the audit report but will not be marked as non-compliance.

Approved requests for exception may be revoked in the event of a security incident or policy violation.

3.13. Non-compliance

Non-compliance refers to the failure to meet the requirements of this Policy or international standards to which LINK Mobility declares compliance. It can be detected during compliance audits conducted by LINK Mobility or external audits.

All non-compliances must be:

Documented.

Analyzed for:

- Source of non-compliance.
- Possibility of non-compliance in other areas or the possibility of similar non-compliances.
- Generated risk
- Further action with non-compliance.

The risk generated by non-compliance must be documented and monitored during risk assessment or subsequent audits.

Corrective actions related to non-compliance must be documented and monitored during control assessments and subsequent audits.

All non-compliances must be described in the audit report and presented to top management.

4. Enforcement

Strict compliance with this Policy is expected and required from all LINK Mobility Managers and Employees. Violation of this Policy may result in disciplinary action, up to and including termination of employment.

4.1. Implementation

The implementation of the Policy is conducted both at the Group and country level in LINK Mobility. It is the responsibility of every LINK Mobility manager to implement this Policy within his or her area of functional responsibility, lead by example, and provide guidance to the Associates reporting to him or her. LINK Mobility's managers, with Human Resources functions, must also seek to structure incentives and conduct performance assessments accordingly. All employees are responsible for adhering to the principles and rules set out in this Policy.

4.2. Reporting potential misconduct / non-retaliation

Any LINK Mobility Manager or Employee with knowledge of suspected misconduct must report his or her suspicion promptly in accordance with LINK Mobility's Whistleblowing Procedure. Reporting potential misconduct in good faith providing information or otherwise assisting in any inquiry or investigation of potential misconduct will be protected against retaliation.


linkmobility