



Public Information Security Policy for the Leschaco Group

Version: 2.3

Release status: released

Release date: 07.07.2023

Review cycle: annually

Document classification: Public

Contents

1.	Preamble	3
2.	Intent and Objectives of the Public Security Policy	4
3.	Key Aspects of our Information Security	4
4.	Implementation	5
5.	Management Responsibility	5
6.	Security Officer	5
7.	Scope/Area of Application	5
8.	Approval and Communication Channels	6
9.	Final Clause	6

1. Preamble

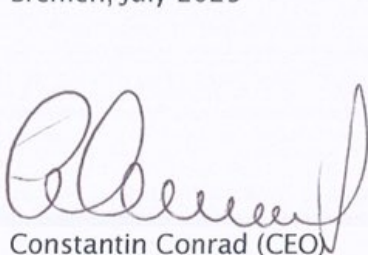
As a competent worldwide acting logistic service provider, security is an integral part of our company philosophy. An indispensable prerequisite for long-term and sustainable success is the trust of our customers in a high-performance and secure information technology, which must ensure the constant availability of our IT systems and the protection of customer data. It is security which contributes to the trust our customers feel when relying on our worldwide services. Therefore, the business of the Leschaco Group depends on a secure and properly working IT supporting its processes, employees and customers. To maintain a secure and reliable working environment, every person needs to know and honour the Leschaco security standards. This public representation of our Corporate Information Security Policy and its underlying documents are providing a comprehensive guide which needs every one of us to follow in order to contribute to the success of the Leschaco Group.

Educating and sensitizing our own employees to existing and potential security risks is also part of our holistic, security strategy approach.

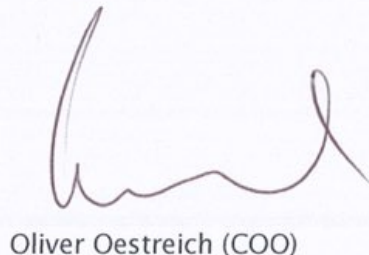
Information security is an important component in ensuring the continued existence of our company and accordingly has a high priority in our company. Our employees are required to observe and comply with the specifications and guidelines on information security.

This Public Information Security Policy is a public representation (stripped from internal information) of Leschaco's Corporate Information Security Policy.

Bremen, July 2023

Handwritten signature of Constantin Conrad in black ink.

Constantin Conrad (CEO)

Handwritten signature of Oliver Oestreich in black ink.

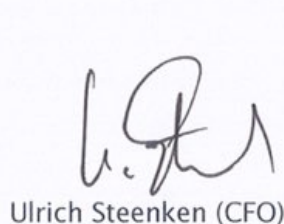
Oliver Oestreich (COO)

Handwritten signature of Nils Fahrenholz in black ink.

Nils Fahrenholz (iCOO)

Handwritten signature of Steffen Küpper in blue ink.

Steffen Küpper (CPO/CCO)

Handwritten signature of Ulrich Steenken in blue ink.

Ulrich Steenken (CFO)

2. Intent and Objectives of the Public Security Policy

The ideas and expertise of our employees are the foundation of our success. The availability of our operating facilities and systems reflects our reliability towards customers and business partners and contributes significantly to the reputation of Leschaco. In order to protect these values, our company creates an appropriate level of protection for the confidentiality, integrity and availability of our processes, information and systems.

The declared corporate objective is effectively protecting central business processes together with the information assets and systems. This is achieved by creating globally applicable security standards and integrating these security standards into our processes. The defined information security objectives help to achieve the company's goals.

Every employee is expected to maintain an awareness of information security in all daily activities. Every supervisor is obligated to ensure that his or her employees comply with the information security regulations by his or her employees and to monitor compliance with them. Any employee who identifies information security weaknesses is required to report them to his or her supervisor or the Security Officer.

3. Key Aspects of our Information Security

Least Privilege Principle

Authorizations and information are assigned restrictively and only to those persons and departments who need them. It MUST be clear to the persons involved how confidential information is and for whom it is intended. This also applies to authorizations in IT systems and physical access rights.

Proper Handling of Documents and Data Storage Media

Handling documents and data carriers with confidential content is a key issue in protecting information. The sparingly use of printouts of sensitive information, the secure storage of documents and storage media in locked areas and proper disposal are the responsibility of each employee.

Technical Security

The level of security can be significantly strengthened by technical means. Targeted investments in security and the secure design of our IT and infrastructure are therefore also part of our security strategy.

Continuous Improvement Process

The ISMS follows the recommended continuous improvement process based on the PDCA model. (Plan, Do, Check, Act). The aim is to demonstrably and regularly ensure the appropriateness, completeness, sustainability, effectiveness and efficiency of the implemented information security processes and protective measures.

Personal Responsibility

Every employee has a responsibility to report vulnerabilities, suspicious situations and incidents. The knowledge and compliance of guidelines by our employees is seen as a prerequisite and expected from every employee.

4. Implementation

To ensure the implementation of information security requirements, Leschaco employs an information security management system (ISMS) based on the international standard ISO/IEC 27001:2013 and the relevant legal and industry-specific requirements.

5. Management Responsibility

The Leschaco Group Management Board is accountable for information security within the company and is committed to providing the necessary human, organizational and financial resources to establish, maintain and further develop an appropriate level of information security.

As part of their management duties and role model function, all managers are particularly responsible for promoting the existing security awareness of their employees regarding information security and IT security.

6. Security Officer

The Security Officer of Leschaco is responsible of implementing and maintaining the ISMS. The Security Officer is our single point of contact for all our security related questions and issues. He is responsible for periodic reporting the effectiveness and efficiency of the implemented security measures to the Leschaco Group Management Board.

7. Scope/Area of Application

The principles and rules of all components of the Security Policy are binding for all units of Leschaco Group, if this is compatible with applicable corporate, labour and regulatory law.

With the publication of the Information Security Policy, all levels and areas of the target groups MUST be aware of the security requirements of the Information Security Policy for their area of activity and act accordingly. This also means that policies which are subordinate to this Information Security Policy MUST be applied.

In addition to complying with the requirements set out in this Information Security Policy, the units/sites/branches MUST consider and comply with the applicable site-specific legal and regulatory requirements as defined by the relevant local regulatory authorities and equivalent security standards.

Compliance may be part of internal and external audits.

8. Approval and Communication Channels

Approval of this security policy SHALL be made by the board of directors. Communication SHALL be done in an appropriate manner according to the corresponding stakeholders. The public security policy SHALL be publicised on the Leschaco homepage. The internal security policy and all underlying documents SHALL be publicised in Leschaco's internal guidelines directory.

9. Final Clause

Despite all due care, deviations from the specifications of other standard setters cannot be completely ruled out. In such a case, the target groups concerned are requested to comply with the stricter regulation. On the other hand, the standard-setting units are required to reach agreement on overlapping regulations / areas of responsibility.