2022

Information Security Policy

dated December 2022

TABLE OF CONTENTS

1 Introduction

1.1 Importance of information security and basic principles

The protection of information is a particular concern of the Management Board of Westwing Group SE, which hereby issues the present Information Security Policy.

Information of all kinds is the backbone of our business activity and therefore represents valuable working capital. Any loss, manipulation, or impermissible disclosure of business-critical information, personal data or customer data can quickly lead to significant financial losses or damage to the company's image.

Compliance with legal requirements and regulations, as well as the observance of internal security regulations, are fundamental cornerstones of the Westwing Group. Data protection and the protection of company assets in the form of information are two of the most important factors for the compliance goals of the Westwing Group. In their business processes, all legally independent entities (business units) must fulfill the statutory and legal conditions of the respective country.

The adequate security of business processes, IT, infrastructures, and critical information is a strategic factor for the competitiveness and continued existence of Westwing. As a publicly listed company this is also an inherit demand from our shareholders. Information and all components involved in the production, processing, storage, and deletion of information – including IT, internal and external employees, business partners, business processes, and communications equipment – must be protected in a way commensurate with their value.

It is the goal of the Westwing Group to protect its proprietary, confidential, and privileged information, regardless of the way it is produced, processed, transmitted, stored or used.

An important factor for assuring comprehensive and effective information security is not only compliance with this Information Security Policy and the related directives, but also the situation-appropriate observance of all other relevant guidelines and organizational instructions, of the Westwing Group, including the Code of Conduct of Westwing, the specifications of Internal Audit and data protection, and other regulations published on intranet (Workplace by Facebook) as well as on Westwing websites.

This Information Security Policy (referred to hereinafter as the "Policy") will be regularly updated every three years or as needed by the Security Tribe.

1.2 Strategic goals of information security and data protection

The strategic goals of data protection and information security are:

- To maximize business continuity
- To minimize business losses
- To protect customer, business partner and employee personal data

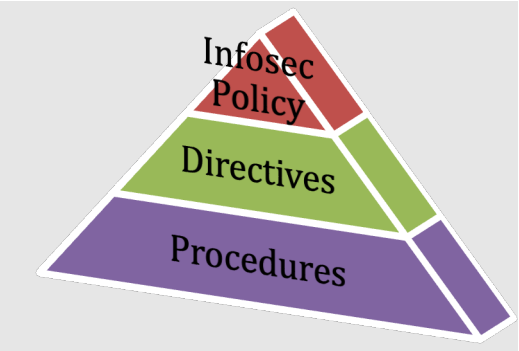
- To prevent, as well as to minimize the effects of security incidents
- To take precautions to ensure the authorized use of systems and information

Because information security and data protection serve the business interests of the Westwing Group, these strategic goals are foundational in business requirements.

1.3 Westwing Information Security Management System

At Westwing we use the ISO27000 framework as a guiding principle. A key element according to this standard is an Information System Management System (ISMS). The ISMS can be considered as a systematic approach for managing and protecting a company's information. The ISMS represents a set of policies, procedures, and various other controls which comprise the information security rules in an organization.

The Westwing Information Security Management System (ISMS) is divided into three parts:



1.3.1 Westwing Information Security Policy

This is the present document and represents the highest level of the Westwing ISMS and is defined as the "*company-wide definition of the strategy, guiding principles, goals, mandate, requirements, and responsibility for protecting the information assets of the Westwing Group*." As it is the north star for all other levels, it is released and signed by the management board.

1.3.2 Directives

This level is defined as "*binding, technology-neutral standards for specific areas and target groups of information security that specify detailed measures in fulfillment of the information security policy*." They are also often referred to as "Level 2 policies" or short "policies"

1.3.3 Procedures

This level is defined as "*binding technical and organizational implementation rules of defined scope for the implementation of the directives and standards."* At Westwing, these include publications in Westwing intranet "Workplace", published guidelines and standards in

Confluence and consists of security concepts, organizational instructions, technical concepts, handbooks, forms, etc.

2 Goals and scope of application

2.1 Scope of application

This Policy applies to all affiliated subsidiaries in which the Group holds a majority equity interest, including all business units and segments worldwide, and their employees. In addition, this Policy applies to all internal and external service providers, business partners, and other third parties that record, process, or use the corporate information of the Westwing Group and have undertaken to comply with this Policy.

Country- or company-specific variations of directives (generally should not happen) must be approved by the Chief Information Security Officer (CISO, see 3.1.1) and adopted by the responsible CEO/Founder/managing director. Information security must be assured in all stages of the lifecycle of business process, products and services, from the feasibility study to development, introduction, operation, and decommissioning or termination.

The Data Protection Officer (DPO) or the Data Protection Law team must be consulted prior to the implementation of this policy in companies that belong to the Westwing Group but are not subject to the jurisdiction of the Federal Republic of Germany.

2.2 Definition of information security and data protection

Information security is the result of the entire process of ensuring secure and continuous business processes through the protection of information and information systems. The goal of information security management is to monitor and minimize information security risks by analyzing vulnerabilities and threats and implementing appropriate protection measures.

IT Security is an integral aspect of information security and is focused on implementing appropriate protection measures and providing support in the analysis of the vulnerabilities and threats to the company's information systems.

Data protection means compliance with all applicable laws and regulations, including the General Data Protection Regulation (EU) 2016/679 ("GDPR") as well as national data protection laws, ("data protection law") and the company's internal regulations applicable to the processing of personal data by companies of the Westwing Group.

Effective information security is an indispensable prerequisite for data protection. The confidentiality of personal data is the interface between information security and data protection. The Data Protection Officer and the Data Protection Law team advise the CISO on the implementation of the information security requirements of data protection law.

2.3 Goals of information security

The overarching goal of information security is the risk-adequate protection of the company's assets. This is achieved in accordance with the standards of the ISO 27000 series through the implementation of technical, organizational, and personnel-related measures during business activity. The participation rights of the employee representatives are to be honored in the implementation of personnel-related measures.

The following fundamental goals of information security are to be achieved:

2.3.1 Confidentiality

Assurance that data and information can be accessed only by authorized persons in permissible ways.

2.3.2 Integrity

Intactness of information and data. In electronic communications, this means that data is not modified during transmission and storage in unauthorized ways.

2.3.3 Availability

Assurance that information and services can be retrieved and used by authorized persons within the intended time.

2.3.4 Authenticity

Assurance that the communication partner (technical and non-technical) is truly the person whom he claims to be, and that the information on hand was produced by the stated source.

2.3.5 Non-Repudiation

Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.

Nonrepudiation provides proof of the origin, authenticity and integrity of data

2.4 Goals derived from business requirements

Information security management must take the original business requirements of the Westwing Group into account and must be implemented in concordance with those requirements.

To ensure the consistency and efficiency of security processes, they should be organized and implemented in such a way that they fulfill both the business requirements and the principles of this Policy, as well as the applicable statutory provisions and the supporting directives and instructions.

The goal of “non-repudiation” must be designed in such a way that such actions are only done by authorized persons and systems according to an authorization concept.

2.5 Participation rights of employee representatives

This paragraph applies only in countries and companies with a labor union.

To the extent that employee representatives have participation rights, such rights must be honored without exception and represent a prerequisite for the validity of the implementation of this policy in relation to employees.

3 Roles and responsibilities

The tasks and responsibilities for information security are hereby defined to ensure that employees, business partners, or other persons or companies that have access to the information or systems of the Westwing Group comply with this Policy.

3.1 Organization of information security management

The Chief Information Security Officer (CISO) is responsible for the information security of the Westwing Group.

3.1.1 Chief Information Security Officer (CISO)

The Executive Board of the Westwing Group appoints a Chief Information Security Officer (CISO). In the performance of his duties, the CISO leads the Security Tribe and works closely together with other corporate functions. He reports to the CTO of the Westwing Group.

The tasks of the CISO are as follows:

- Specification of the information security strategy and introduction and operation of an Information Security Management System (ISMS).
- Publication of information security directives and implementation instructions.
- Definition and assignment of information security-related tasks, projects, and budgets in the Security Tribe.
    - Institution of a risk management process for information security that accords with the guidelines of corporate risk management.
    - Promotion of security awareness through training courses and other security initiatives.
    - Support and enablement of the business units and segments to improve local security.
    - Monitoring and reporting of the information security status to the Management Board and the Audit Committee of Westwing.
    - Analysis of status reports and results, and derivation of measures in the GRC.

3.1.2 Information Security Officer (ISO)

This is an optional role and might be introduced for larger subsidiaries or to ensure compliance with country-specific legal requirements. The Westwing Group appoints, to the necessary extent, Information Security Officers (ISOs) who report functionally and/or organizationally to the CISO. The ISO performs the following tasks:

- Structured and systematic improvement of regional information security in accordance with business risks, in cooperation with other security departments.
- Continual conduct of security audits, tests, and spot checks to verify and report on the effectiveness of security measures and regulations.
- Implementation of the information security reporting procedures adopted by the CISO.
- Support and advising of the business units on the secure implementation of information security measures in processes and applications.
- Coordination of the implementation of information security regulations, standards, and directives, and the corresponding processes and mechanisms in his area of responsibility.
- Direct and regular communication with and reporting to the CISO.

3.1.3 Security Board

The Security Board is the decision-making body of the Westwing Group's security organization. The central duties are:

- Approval of directives within the Information Security Regulations
- Analysis and coordination of risk analysis results and the status of information security
- Coordination, prioritization, and adoption of measures and initiatives for implementing the information security strategy and for enhancing information security

The CISO and CTO (Chief Technology Officer) make up the decision-making body within the Security Board. Other departments (Extended Security Board), including (for example) VP Legal and Director GRC, Data Protection Officer (DPO), Human Resources, Internal Audit, Heads of IT of the countries, and the competent employee representatives, will be purposefully consulted as needed.

3.2 Information security management, processes, and mission

To ensure effective, lasting, and risk-based information security, it is necessary to implement an information security management process that is oriented to the internationally recognized standards for security management (particularly including the ISO 27000 series). Supporting directives, standards, and instructions describing the requirements for the respective area of information security in detail must be issued and maintained.

Information security management consists of several processes that build on one another, which are executed by the Westwing Group security organization under its responsibility within

the scope of the security regulations. The following fundamental processes of information security management are to be implemented:

Risk analysis and risk management are indispensable prerequisites for the protection of information assets and are therefore the main drivers of all other security management processes.

The **management of information security incidents** minimizes losses and analyzes incidents for the sake of prevention.

Continuing education and development of security awareness to enhance the level of security through appropriate training courses, security initiatives, and measures.

Monitoring and reporting to identify and react to potential vulnerabilities and security violations, including extensive reporting.

Audit and review to ensure and measure the effectiveness of the information security management system.

Business continuity management based on predefined criteria to protect against interruption and disasters and to ensure the continuity of business processes.

The processes of information security management are to be carried out in coordination with the Westwing Group's data protection processes and compliance management guidelines, Quality Management, Technology Department, Risk Management, Internal Controls, Human Resources, the employee representatives (if applicable) and Internal Audit. They are to be structured and organized in such a way as to support the fulfillment of statutory and legal obligations.

3.3 Responsibility for information security

It is the responsibility of everyone covered by this policy to support information security initiatives and to follow the Westwing Group's Information Security Policy, guidelines, directives, standards, and instructions.

It is the duty and responsibility of every manager of the Westwing Group SE and its subsidiaries to ensure information security in their area of responsibility. As part of this responsibility, they must ensure that all persons (internal/ external) who work with sensitive data are properly instructed or professionally trained (awareness training). In addition, suppliers, business partners, and service providers must be contractually obligated to implement/ comply with the security standards of the Westwing Group.

Every individual must take responsibility for ensuring the attainment of the Westwing Group's goals and the protection of corporate information.

It is the responsibility of the business units and entities to identify and document security-relevant processes, systems, and information that must be protected. To achieve this, they consult the directives and guidelines issued in the ISMS and collaborate proactively with the security team.

3.4 Contact partners

Employees who have questions about this policy, the directives or security procedures should first contact their supervising manager.

Managers may contact the CISO or the security tribe with regards to this policy.

For detailed operational security questions, the security service desk (https://westwing.me/security) should be used to contact the security tribe.

4 Principles / guidelines

The following guidelines describe the fundamental rules and principles of information security in the Westwing Group.

4.1 Compliance with laws and regulations

Obligation to comply with all relevant laws and regulations related to information security, particularly the information security requirements of data protection laws.

4.2 Cost-effective protection

Corporate information, processes, and systems must be protected against known threats in an economically efficient manner.

4.3 Security needs of our customers

Consideration of the security needs of our customers and assurance that the security requirements of the Westwing Group are fulfilled by customers, business partners, and suppliers.

4.4 Introduction and effective implementation of security standards

Introduction of appropriate directives, standards, instructions, and measures to protect the confidentiality, integrity, availability, and authenticity of information.

4.5 High level of security awareness

Attainment of a high level of security awareness by all employees, managers, customers, and business partners through consistent security management, training courses, and the application of security standards.

4.6 Access only by authorized persons

Only authorized persons may be allowed to access corporate information and systems. For all requested permissions, the “Need to know” and “Least privilege” principle must be applied.[1]

4.7 Disclosure of information

Information is disclosed only in the company’s interest or to fulfill statutory, legal, or collective bargaining requirements or company instructions.

4.8 Investigation of security violations

Institution of a process for monitoring, reporting, and investigating possible violations of information security. Such a process is to be instituted in observance of the participation rights of the employee representatives.

4.9 Compliance with the Westwing Group’s corporate regulation

Compliance with all the Westwing Group’s corporate regulations and company-wide directives.

4.10 Integrated information security

Integration of information security measures into the day-to-day operations to ensure the effective protection of corporate assets in the form of information.

4.11 Protection of the entire information process

The entire information process (generation, use, processing, storage, dissemination, and destruction) for all physical and logical information objects must be protected against loss, damage, and abuse.

4.12 Formal process for exceptions

Institution of a formal risk approval process for necessary exceptions to information security directives, to achieve a controllable process.

[1] https://en.wikipedia.org/wiki/Principle_of_least_privilege

5 Compliance

All business units and entities are required to comply with this Policy and the directives and instructions derived from it (“Westwing Security Policies”). The business units are required to institute programs to ensure compliance and progress.

In compliance with laws and regulations, all Westwing business units and entities are required to follow the information security processes within the country-specific legal systems, as well as all other applicable guidelines and standards.

Exceptions to this Policy and the Westwing Group’s Information Security Regulations require coordination with the CISO and formal approval by the responsible CEO/MDs, to ensure a controllable, risk-based approach (see 4.12).

Non-compliance may lead to consequences under employment law or criminal law or other consequences. The regulations of the Westwing Group like “Code of Conduct”, “Capital Market Compliance Guideline”, “Westwing Risk Management manual” and the provisions of individual contracts apply.

6 References

Code of conduct

Capital Market Compliance Guideline

Westwing Risk Management manual