Information Security Policy

Kastelo Group

Management Board
2020-03-23

Contents

1 Introduction

This document is created and enacted for Kastelo Holding AB and subsidiaries, collectively "Kastelo Group" or "Kastelo".

Kastelo provides services that affect our customers most valued and critical asset: information. Thus, both our customers, partners, and employees must be able to rely on Kastelo to conscientiously assume responsibility for conducting our business in a way that ensures the security of their data. For us, providing comprehensive security and extensive data protection is more than just an obligation to meet statutory and regulatory requirements; it is also an explicit mark of quality of our services.

To ensure a sufficiently high level of data protection Kastelo has implemented an Information Security Management System, ISMS, governed by this policy. The aim of the ISMS and policy is to provide continuous risk-based information security management encompassing processes and controls for reducing or eliminating risks and threats to ours or our customers information assets. The ISMS and the policy are based on international standards such as ISO 27002, ISO 27005 and the EU General Data Protection Regulation. Topic specific standards and best practices are also applied in the different sections of the ISMS.

The ISMS and this policy are directed at all employees, subcontractors and partners to set the standard of how security is to permeate the business and workings of Kastelo. They are also aimed at our customers and shareholders to offer a transparent testimony to how Kastelo protects their assets and interests.

Violations of the policy may lead to disciplinary actions.

2 Principles of Data Protection

The following principles govern all security provisions and requirements within Kastelo.

2.1 Principle: Lawful conduct

Lawful conduct provides the basis for all actions conducted within the Group.

We respect the rights of the individuals and uphold the right to freedom of opinion and freedom of speech. Any security measures controls or contractual requirements that infringe such rights shall only be implemented within the legally admissible framework, with due regard to appropriateness.

2.2 Principle: Data Protection and Data Security

We work actively to ensure a sufficient level of data protection in regards to:

- *confidentiality* – that information is not made available or disclosed to unauthorized individuals, entities or processes;
- *integrity* – that information is kept accurate and complete and not altered by unauthorized individuals or entities;
- *availability* – that information is accessible and usable by authorized individuals, entities or processes when needed; and
- *traceability* – that activities can be derived to an identifiable individual or entity.

2.3 Principle: Customer Trust

We shall provide secure and reliable products and services to our customers.

2.4 Principle: Security Culture

Integrity and security awareness shall permeate the way we act and the way we conduct ourselves and our business throughout all levels of the company.

2.5 Principle: Need to Know

Knowledge and access to information shall only granted where needed. All access authorizations are controlled, and granted accesses are reviewed on a regular basis.

2.6 Principle: Leaning on Expertise

We lean on best practices and internationally recognized standards and regulations.

2.7 Principle: Risk-based Approach

Implementation of security measures and controls are based on systematic risk management:

- *identification of threats* to security protection goals;
- *investigation and assessment* of current security situation;
- *identification of resulting risk*, including *potential consequences* and *likelihood of occurrence*;
- identification of *appropriate countermeasures* or *consciously accepted risk*;
- *documentation* of evaluation process and decisions on security controls; and
- *long term management* of risk.

Risk-based security management demands a comprehensive view of key corporate assets and their correlation to critical business processes.

3 Security Management

To achieve our security goals, ensure proper implementation of security measures and maintain a continuous and long-term effective management of security Kastelo has implemented an Information Security Management System, ISMS. The ISMS encompasses organizational, administrative and technical elements throughout the whole business and applies to information in all its forms.

The ISMS, and this policy, applies to all employees using the company assets or partaking in business projects and deliveries, regardless of geographical location. This includes external parties such as contractors and partners.

The ISMS and this policy will be revised continuously and at the least annually.

4 Security Culture

Responsibility for information security management is incorporated in the organizational structure and every member of the organization, including contractors, are responsible for compliance with policies and instructions. Ultimate responsibility for communicating and promoting the ISMS and this policy throughout their organizations, and for encouraging a security culture throughout every aspect of the business, lies with management.

Employees shall be given the required security competence and shall also be encouraged to learn about security on their own initiative. They shall question any requirements which they feel to be ambiguous or unintelligible, and are encouraged to oppose any instructions which may be considered unethical or are evidently unlawful without having to fear any negative consequences.

Employees shall also notify the company of any relevant security risks and incidents of which they are aware.

5 Structure of Information Security Management System

The Information Security Management System is structured into several tiers.

Figure 1: ISMS Tiers

Each tier successively expands on and concretizes the tier above. This policy defines the overarching goals and principles; the Handbook defines how these principles are put into practice; the Standards, Processes and Guidelines describe the specifics of each practice; and finally, Instructions and Checklists define the individual steps to be taken in certain processes.

6 Monitoring and Reviews

Security Management shall monitor implementation of and compliance with the ISMS and Group Security Policy as well as review the applied security measures and take appropriate actions to ensure continuous improvement of the ISMS. Business units shall also perform their own reviews of compliance and implemented controls.