Information Security Policy

Classification: Public

Applicability

This policy is applicable to the overall organisation of Visma Enterprise A/S including:

- Employees
- External personnel (i.e. consultant) with frequent access to Visma Enterprise A/S's IT systems

---

1. Purpose

The objective of the Information Security Policy is to communicate the direction, expectations, and intentions from the Managing Director concerning the information security at Visma Enterprise A/S (hereafter Visma Enterprise). The policy determines relevant sub-policies, information security requirements, objectives and activities, which are essential for Visma Enterprise's customers' trust and Visma Enterprise's competitive strength.

Visma Enterprise ensures a secure communication and information flow both internally and externally. Visma Enterprise provides secure storage, processing, communication and disposal of information to ensure that no data will be compromised.

Visma Enterprise complies with relevant Danish legislation and regulation and EU regulation that is directly applicable in Denmark.

2. Policy

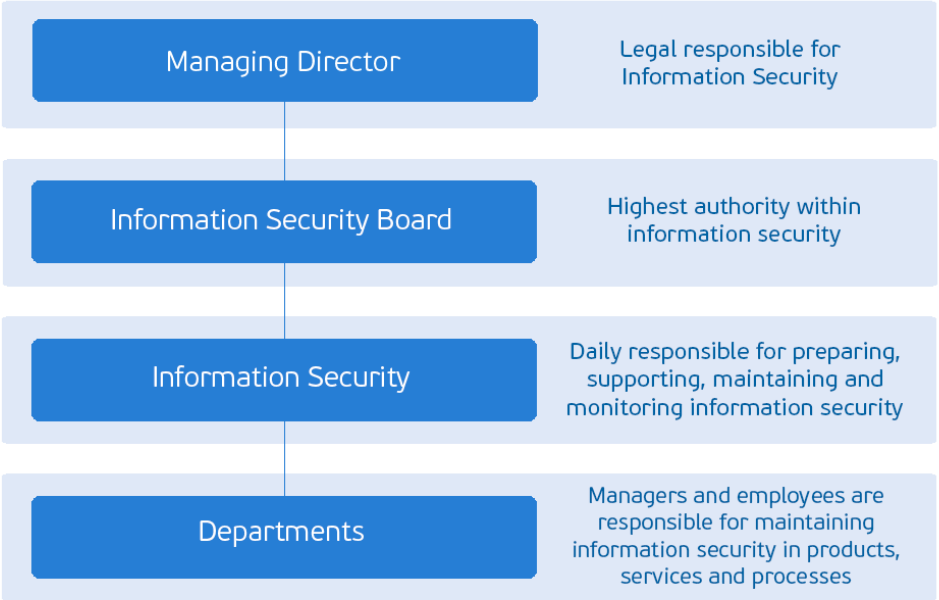
Implementation

The Information Security Policies are based on the standard ISO/IEC 27001:2013 Information technology – Security techniques – Information management systems – Requirements (hereafter ISO 27001).

The standard contains a Statement of Applicability (SOA), which is a part of Visma Enterprise A/S's Information Security Management System (ISMS). The SOA constitutes policies, procedures, processes, organisational decision-making processes and activities within the following information security control areas in Visma Enterprise:

- Organisation of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security continuity (Business Continuity Management - BCM)
- Compliance

Overview



Managing Director

Managing Director (hereafter MD) is responsible for approving

- Information Security Policy
- Business Continuity Management Policy
- Information Security Risk Management Policy
- Business Impact Assessment
- Exceptions

Information Security Board

The Information Security Board is working under a mandate given by the Managing Director.

The Information Security Board approves the level of information security through the acceptance of functional information security policies, strategies and economic dispositions weighted against accepted risks. In addition theInformation Security Board has the authority to make decisions in the following areas:

- Organisation of information security
- Roles and responsibilities
- Priority of security tasks

Information Security Officer

The Information Security Officer is daily responsible for preparing, supporting, maintaining and monitoring information security. This includes adequate information security training for Visma Enterprise's employees and external consultants.

Departments

The individual department is responsible for maintaining information security in products, services and processes.

Managers are responsible for the day-to-day supervision of affairs relating to Visma Enterprise's information security under the authority of the Information Security Board.

Controls

All relevant controls comply with the controls defined in Visma Enterprise’s generic control catalogue.

3. Information Security

To maintain an information security and control level, which corresponds with a commercial trade-off between risk, probability, impact and mitigation costs, Visma Enterprise has implemented policies, controls and processes to cover the information security areas described below.

Visma Enterprise has implemented ISO 27001 as a framework for information security to maintain and improve a high standard in managing security. ISO 27001 addresses actions and measures to preserve:

Confidentiality

Ensure that unauthorised persons cannot gain access to data that can be abused to harm Visma Enterprise's customers, business associates or employees.

Integrity

Ensure that systems provide accurate and complete information.

Availability

Ensure that relevant information and systems are available and systems are stable.

Information security risk management

An information security risk management process is integrated into the work processes and daily tasks of employees and external consultants. Information risk management is continuously monitored and improved.

Information risk assessment is an important part of the information risk management process and product development, and is conducted pursuant to a predetermined plan. For each asset or class of assets, the importance of the asset and its function for the organisation is specified from the point of view of confidentiality, integrity and availability.

Information risk assessment is conducted according to Visma Enterprise's Information Security Risk Management Policy.

Organisation of information security

Visma Enterprise has established a management framework to initiate and control the implementation and operation of information security within Visma Enterprise.

Human resource security

Visma Enterprise has ensured that employees and external consultants understand their responsibilities and are suitable for the roles for which they have or are considered.

Asset management

Visma Enterprise has identified organisational assets and defined appropriate protection responsibilities.

Access control

Visma Enterprise has ensured work-related access to information and information processing facilities.

Cryptography

Visma Enterprise has ensured proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information.

Physical and environmental security

Visma Enterprise has prevented unauthorised physical access, damage and interference to the organisation's information and information processing facilities.

Operations security

Visma Enterprise has ensured correct and secure operations of information processing facilities.

Communication security

Visma Enterprise has ensured protection of information in networks and its supporting information processing facilities.

System acquisition, development and maintenance

Visma Enterprise has ensured that information security is an integral part of information systems across the entire lifecycle. This also includes requirements for information systems, which provide services over public networks.

Supplier relationships

Visma Enterprise has ensured protection of the organisation's assets that is accessible by suppliers, including regularly monitoring, reviewing and auditing of supplier service deliveries.

Information security incident management

Visma Enterprise has ensured a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Information security continuity

Visma Enterprise has embedded information security continuity in the organisation’s Business Continuity Management (BCM).

Compliance

Visma Enterprise has implemented procedures to avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

4. Scope

Governance

The Information Security Officer is responsible for preparing, maintaining, supporting and monitoring the implementation of this policy.

The Information Security Policy is approved on an annual basis. A review of the policy is needed in case of major organisational change, major changes in infrastructure or if critical vulnerabilities arise.

Information security policies and information regarding the information security organisation are available from Space.

Classification

All information security policies are marked with a classification according to their content and the Classification Policy. The classification will prevent unauthorised distribution of restricted information.

5. Enforcement

Responsibility

All employees and external consultants must be aware of and responsible for information security. Every person handling information or using Visma Enterprise A/S's information systems is expected to comply with the information security policies, both during and, where appropriate, after his or her employment in the company.

Non-compliance

Violations of this policy must be reported to the employee's manager, who is responsible for the further handling of the incident.

If an employee overrides its duties within information security, the manager may take the appropriate disciplinary actions, under the supervision of HR.

The responsible host will take immediate action towards non-Visma Enterprise A/S employees.

Exceptions to the policy

Exceptions to this policy are permitted in rare instances where the business benefit is deemed greater than the risk involved.

Exceptions can be granted where:

- clear guidelines are defined for handling of exceptions
- it is work-related (above must also be met)
- declared disaster

Questions

Please direct any questions to the policy to the Information Security Officer.

5. References

- From this page you will find all links related to this area
- Information Security Policies
- Information Security Policies - Developed and maintained by the Visma Group Security

---

Review and approval

This information security policy is reviewed and approved at least yearly by our the Managing Director.

Lates review and approval by Anders Andersen: March 30 2022

Accountable: Managing Director
Responsible: Information Security Board
