Information Security Policy

Visma Enterprise A/S
Gærtorvet 3
DK-1799 København V
Company registration number: 41016027
(“**Visma Enterprise**” or the “**Organisation**”)

Table of contents

Executive summary

Visma Enterprise must at all times protect information and information assets. This means that all information or supporting systems must be handled in a secure manner to ensure:

- Confidentiality - protection from unauthorised access
- Integrity - information is kept correct and complete
- Availability - information is available when needed

You and all your colleagues have to conduct your work accordingly - there are no loopholes.

Depending on your role and responsibility you have to deep dive into and comply with topic specific security policies. You need to check appendix A to see topic specific policies especially applicable to you.

Purpose

This policy forms the overall framework for information security at Visma Enterprise based on the requirements and expectations from customers and interested parties.

Continuously maintaining confidence in Visma Enterprise requires that confidential information is protected by measures and controls to ensure a high level of information security.

Our roles as data controller and data processor, processing a large amount of confidential and personal information on a daily basis, are based on three cornerstones:

Confidentiality: Prevent unauthorised access and ensure that only people with a legitimate need have access to information.

Integrity: Information must be consistent, accurate and complete.

Accessibility: Information and supporting systems must be accessible for the right people when they need it.

The guidelines in this Information Security Policy and the guidelines in the supporting topic specific policies[1], reflects requirements from customers, requirements in legislation and from authorities as well as best practices.

Scope

The Information Security Policy covers all of Visma Enterprise's information assets, i.e.:

- Any information belonging to Visma Enterprise
- Any information processed by Visma Enterprise on behalf of our customers
- Any resources to use, process or store information described above

The Information Security Policy applies for:

- All employees without exception, including external consultants and temporary employees.
- Others who use, process, generate or store Visma Enterprise information assets, including suppliers.

[1] Topic specific policies are Visma internal documents maintained within the Information Security Management System (ISMS). A list of established topic specific policies is presented in appendix A.

Principle

Information Security is established and maintained on a risk based approach, customer requirements, legal and regulatory requirements, business needs and best practices.

Policy

Information security defined

Information security at Visma Enterprise is, in its essence, about preserving and protecting the cornerstones (Confidentiality, Integrity and Availability) that make up the foundation of the trust we have from our customers, employees and interested parties. The protection of these cornerstones are also the key information security objectives of Visma Enterprise:

Information security objectives

As a Visma Enterprise employee, or otherwise subject to this Information Security Policy, you are expected to contribute actively and continuously to the protection of information assets. Working with information assets, you will at all times consider, respect and protect:

- **The confidentiality of information and information assets**
  Access to information and information assets is based on a least privilege principle: Only people with a legitimate need must be able to access information or information assets. You will at all times ensure that information that you access or information in your possession or control is protected from unauthorised access. When sharing information, you will ensure that you have the mandate to share the information and you must ensure that you follow the principle of least privilege.
- **The integrity of information and information assets**
  Information and information assets must be consistent, accurate and complete. Working with information or information assets, you will protect integrity by ensuring that all changes are approved, tracked and documented. In other words, you will not do any changes to information or information assets unless based on a documented work instruction or documented procedure.
- **The availability of information and information assets.**
  Information and information assets must be available when needed to anyone who has a legitimate purpose. Working with information or information assets, you will always have

the availability of information or supporting systems as a priority. Any discontingency of availability is, if not planned and communicated, subject to immediate action.

Your compliance to the above mentioned requirements is essential. Any non-compliance will damage the trust we enjoy from our customers and interested parties.

Information security management

Visma Enterprise will maintain an Information Security Management System (ISMS). The ISMS is established to comply with and is certified within the common information security standard, ISO 27001.

The overall direction of the ISMS is set by top management. A Compliance Board is established to support and ensure focus and engagement from top management on information security matters and direction. The daily operation and maintenance of the ISMS is conducted by the Security & Compliance team - the Information Security Officer taking lead. Specific roles and responsibilities for the running of the ISMS are defined and documented within the ISMS manual.

The ISMS will be continuously improved as applicable and when purpose and value is established. Continuous improvement will be documented within the ISMS manual.

Roles and responsibilities

At Visma Enterprise, information security is the responsibility of everyone, including understanding and adherence to policies, following processes and reporting of information security or privacy events or incidents. Managers are responsible for the day-to-day supervision of affairs relating to Visma Enterprise A/S's information security under the authority of the Information Security Board.

Non-compliance

Non-compliance may have a consequence for the employment relationship of the employee being non-compliant.

Information security measures

Visma Enterprise will maintain a number of information security measures. The measures implemented and to what extent a measure is implemented is based on risk assessments conducted on a regular basis. The risk assessments include considerations of impact on data subjects, organisations and the society.
The following overall areas of security measures are implemented.

- Human resource security
- Asset management
- Information protection

- Identity and access management
- Secure configuration
- Physical security
- Threat and vulnerability management
- System, network and application security
- Supplier relationships security
- Information security event management
- Continuity
- Legal and compliance

Together they contain all the controls listed in ISO 27001:2022 Annex A.

Details on the implementation are documented in the ISMS.

Monitoring

Compliance to policies and the effect of implemented security measures are monitored on an ongoing basis. All security measures are subject to independent audit (ISAE 3402 + ISAE 3000 + ISO 27001)

Training and awareness

All employees will be subject to continuous training within security and privacy best practices.

The training will include training in risk management as applicable to role and responsibility.

Exceptions, ownership, review and approval

Exceptions

Exceptions to this policy are permitted in rare instances where the business benefit is deemed greater than the risk involved. The Exception policy is outlining the requirements regarding exceptions to policies.

Ownership

Ownership of this policy is assigned to the Information Security Board, responsible for its accuracy, compliance, and alignment with the company's objectives.

Review and Approval

This policy undergoes an annual review by the Compliance Board and requires final approval from the Managing Director.
Latest review: 14 November 2024
Latest approval: 14 November 2024

Remark: Appendix A may be updated without re-approval of the main policy. Appendix A may be updated by Security & Compliance following an Compliance Board decision on and approval of one or more of the topic specific policies.

Appendix A - topic specific policies

https://space.visma.com/pages/1e77kpc94jksq8vdvu/Informationssikkerhedspolitikker/1f2r32la5msaaa5io7?locale=da

- Exception Policy
- Organization of Information Security
- Human Resource Security Policy - Employment
- Human Resource Security Policy - Awareness
- Asset Management Policy
- Acceptable Use Policy
- Classification Policy
- Access Policy
- Password Policy
- Cryptography Policy
- Physical Access Policy
- Operational Procedures Policy
- Backup Policy
- Logging and Monitoring Policy
- Communications Security Policy
- System Acquisition Policy
- System Development and Maintenance Policy
- Supplier Relationship Policy
- Information Security and Privacy Incident Management Policy
- Business Continuity Management Policy
- Compliance Policy
- Data processing policy
- Data Retention and Deletion Policy
- Information security and privacy risk management policy