Information Security

Appendix 6.1

Version: May 2021

VISMA

Contents

Introduction

This appendix gives a description on information security in relation to the Services Visma Løn incl. My Visma, Visma HR and Datahub, developed and maintained by Visma Enterprise A/S (hereafter Visma Enterprise).

The level of information security meets international requirements in ISO/IEC 27001:2013 Information technology – Security techniques – Information management systems – Requirements ISO 27001, which can be documented by an ISO/IEC 27001:2013 certificate.

Information security

Information Security in Visma Enterprise and for Services in scope is based on the framework ISO/IEC 27001:2013 Information technology – Security techniques – Information management systems – Requirements (hereafter ISO 27001). The purpose of our information security management system (hereafter ISMS) is to establish, implement, maintain and continually improve our information security.

The ISMS preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interest parties that risks are adequately managed. The services in scope has achieved an ISO/IEC 27001:2013 certification.
In addition, an yearly independent ISAE 3402 type 2 report is made.

Visma Enterprises Statement of Applicability consist of information security policies, processes and activities for the following annex A areas:

- Information security policies
- 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 aspects of business continuity management
- Compliance.

Visma Enterprises Information Security Policy and ISO/IEC 27001:2013 certificate is available on request.

Information security policies

Based on a risk assessment, a set of information security policies has been established and approved by Management. The policies have been published and communicated to employees and relevant external parties. The policies are reviewed on an annual basis or when required due to significant changes to ensure their continued appropriateness, adequacy and effectiveness.

Organization of information security

Visma Enterprises Management has defined and allocated all information security responsibilities, appointed an Information Security Officer, and established an Information Security Board. Figure 1 below shows the structure of information security.

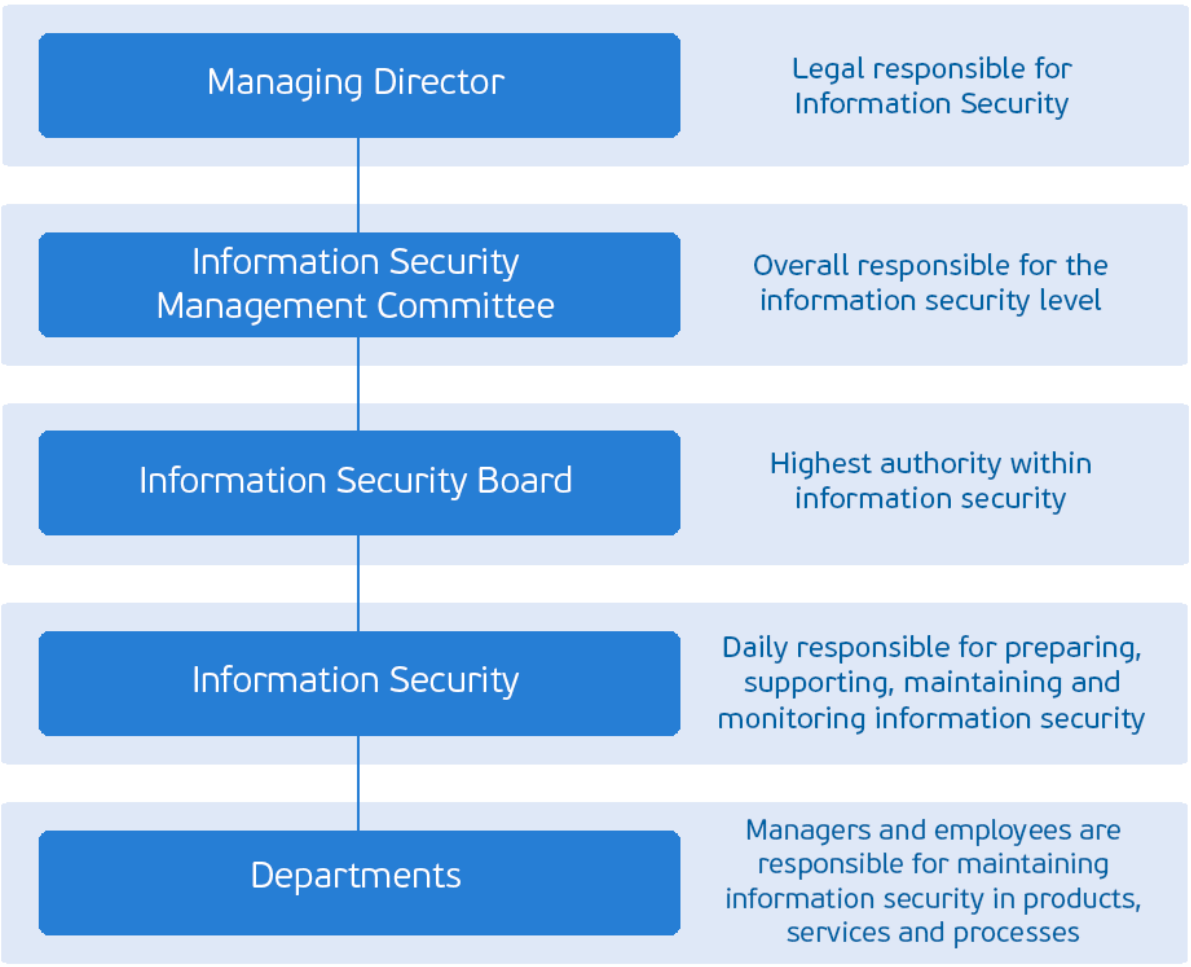

Figure 1: Organization of Information Security

Conflicting duties between critical functions of Visma and areas of responsibility have been segregated. This includes segregation of duties internally between development, test, and production with proper consideration of the use of subservice organizations.
Visma Enterprise addresses information security in its project management.

Human resource security

Prior to employment, Visma Enterprise ensures that employees and external consultants understand their responsibilities and that they are suitable for the roles for which they are considered. This includes screening of criminal records and contractual agreements (including non-disclosure agreement) with employees and external consultants stating their and the organization's information security responsibilities.

During employment, Visma Enterprise ensures that employees and external consultants are aware of their information security responsibilities. This includes information security awareness, training and education.

Asset management

Visma Enterprise has identified organizational assets and defined appropriate protection responsibilities. An asset inventory has been drawn up and is maintained, including acceptable use of information and assets like return, transfer, disposal, etc.

Visma Enterprise ensures that information receives an appropriate level of protection in accordance with its importance to the organization. This includes classification of information in terms of legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification. Procedures for handling assets have been established and implemented.

Procedures for physical media transfer and for disposal of media have been established and implemented to prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.

Access control (user organisation)

The Customer is responsible for adding, changing and deleting access rights for their own employees.

Visma Enterprise ensures that unauthorized access to systems and applications is prevented. Access to information and application system functions is restricted and controlled by a secure log-on procedure (2FA), and password management systems ensure quality passwords.

Access control (Visma Enterprise employees)

Visma Enterprise ensures that access to information and information processing facilities is limited. An access control policy, based on business and information security requirements, has been established and documented and is reviewed on a regular basis. Users are only provided with access to services that they have been specifically authorized to use.

Visma Enterprise ensures authorized user access to prevent unauthorized access to systems and services. A process for user registration, de-registration, and user access provisioning has been established and implemented. Privileged access rights as domain administrators are restricted and controlled. User access rights to restricted information are reviewed at regular intervals. The access rights to information and information processing facilities are removed upon termination of employment.

Visma Enterprise employees are accountable for safeguarding their authentication information. Users are instructed to follow the organization's practices in the use of secret authentication information.

Visma Enterprise ensures that unauthorized access to systems and applications is prevented. Access to information and application system functions is restricted and controlled by a secure log-on procedure (2FA), and password management systems ensure quality passwords.

Cryptography

Visma Enterprise ensures proper and effective use of cryptography on selected areas to protect the confidentiality, authenticity, and integrity of information. A policy on the use of cryptographic controls and the use of cryptographic keys has been established and implemented.
Use of cryptographic controls and cryptographic keys is registered and reviewed on a regular basis.

Physical and environmental security

Visma Enterprise ensures that unauthorized access to the organization's information and information processing facilities is prevented. Security perimeters are defined and offices, rooms, and facilities are secured by physical entry controls.

A policy regarding clear desk, clear screen, and removable storage media has been established and implemented.

Operations security

Visma Enterprise ensures correct and secure operation of information processing facilities. A policy on operational procedures has been established, and a change management workflow has been implemented to ensure the control of changes to the production environments. Development, testing, and operational environments are separated, and changes to production environments must be planned and tested.

Visma Enterprise ensures that information is protected against malware. Visma Enterprise has implemented and communicated an acceptable use policy.

Visma Enterprise ensures the protection against loss of data. Backup and backup-restore tests are performed on a regular basis.

Visma Enterprise ensures logging to record events and generate evidence. Event logs recording user activities, exceptions, faults, and information security events are generated and kept. Logs for reactive use are generated. Log information is protected against tampering and unauthorized access, and a correct timestamp is ensured.

Visma Enterprise minimizes the risk of exploitation of technical vulnerabilities by an effective patch procedure as well as penetration test due to a defined schedule.
A software requisition process has been established in order to limit the installation of software. The number of workstation administrators is limited and reviewed on a regular basis.

Communications security

Visma Enterprise ensures the protection of information in networks and its supporting information processing facilities. Networks are managed and controlled, and groups of information services and users are segregated on networks.

System acquisition development and maintenance

Visma Enterprise ensures that information systems are designed and implemented according to the system development and security life cycle, which ensures a structured and well-controlled environment. A system development and maintenance policy has been established and implemented and is supported by an established system development and security life cycle and by the use of an established change management workflow.

The established system development life cycle provides requirements to:

- review of services after changes to the operating platforms
- restrictions on changes to software packages
- secure system engineering principles
- secure development environment
- outsourced development
- system security testing and system acceptance testing.

Visma Enterprise ensures the protection of data used for testing. An approach to testing as well as strategies and design techniques for testing have been established.

Supplier relationships

Visma Enterprise utilizes subservice organizations for certain purposes.

Visma Enterprise ensures the protection of the organization's assets that are accessible by suppliers. A supplier relationship policy has been implemented. A process for supplier acceptance has been established to ensure classification of suppliers and, if applicable, to ensure supplier acceptance of security requirements.

Visma Enterprise maintains an agreed level of information security and service delivery in line with supplier agreements by monitoring, reviewing, and auditing supplier service delivery on a regular basis. Information security requirements have been laid down for the suppliers. Visma Enterprise reviews the supplier's fulfillment of the information security requirements.

Information security incident management

Visma Enterprise ensures a consistent and effective approach to the management of information security or privacy incidents, including communication on security or privacy events and weaknesses. A process for information security or privacy events or weaknesses has been established and implemented. Reported information security or privacy events and weaknesses are reviewed and classified on a regular basis.

Information security aspects of business continuity management

A business continuity management policy has been established. Business continuity plans and action cards are established and implemented and updated on a regular basis.

Compliance

In cooperation with Visma Enterprises legal department, Visma Enterprise prevents breaches of legal, statutory, regulatory, or contractual obligations related to information security and of any security requirements. Processes for identifying legislative or contractual requirements have been established and implemented, and a register of contractual deviations as well as legislative requirements has been established and is maintained.

Compliance with legislative or contractual requirements regarding intellectual property rights is ensured by Visma Enterprise legal department and is stated in customer contracts and employment contracts.
To ensure the privacy and protection of personally identifiable information, a privacy policy has been established, maintained, and communicated.

Complementary user entity control considerations

Visma Enterprise Services were designed on the assumption that certain controls would be implemented and operated effectively by user organizations. The list below describes additional controls that should be in operation in user organizations to complement the controls at Visma Enterprise.

The list does not represent, and should not be considered, an exhaustive listing of the control policies and procedures which would provide a basis for the assertions underlying clients' financial statements.

- Controls to provide reasonable assurance that physical access to the user organization's premises is restricted to authorized individuals.
- Controls to provide reasonable assurance that access to Visma Enterprises system via terminals/interfaces at user locations is restricted to authorized individuals.
- Controls to provide reasonable assurance that the user organization has proper control over the use of IDs and passwords that are used for accessing and transmitting payroll and HR information, and over preparation of worksheets and that they notify Visma Enterprise of authorized contacts.
- Controls to provide reasonable assurance that the user organization takes action on access in case of resignations, retirements or job rotations.
- Controls to provide reasonable assurance that output reports are reviewed by appropriate individuals for completeness and accuracy.
- Controls to provide reasonable assurance that changes to processing options (parameters) are appropriately authorized, approved and implemented.

User organizations should review the sample payroll transfer (pre-run/test calculation) produced by Visma Enterprise prior to initial payroll processing to determine that all information is complete and accurate or notify Visma Enterprise when there is a change.

--