IT Security

Appendix 6.1

Security

Version: March 2014

VISMA

Contents

Introduction

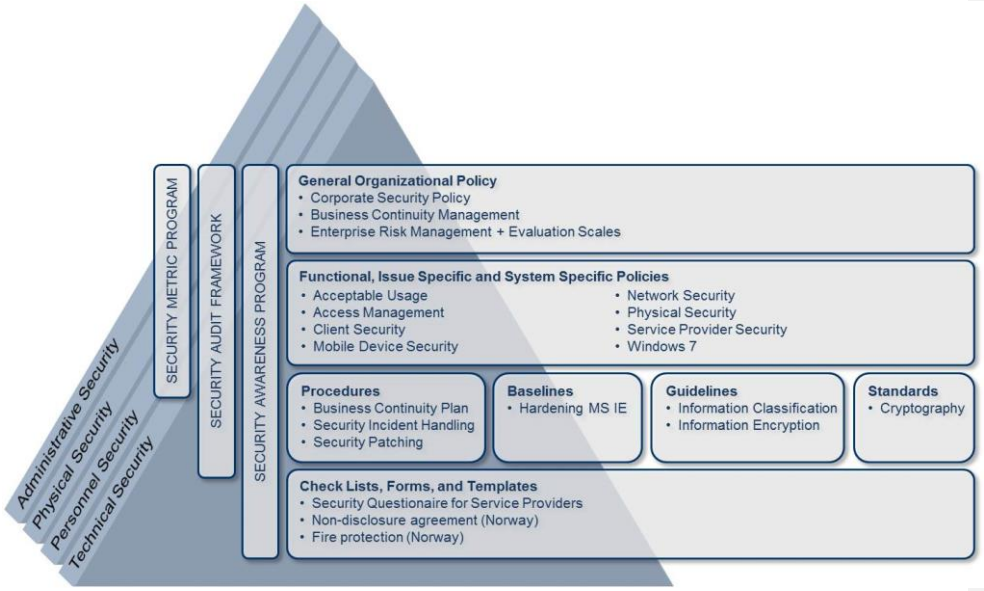
This appendix describes the security elements applicable to Visma Enterprise and its subcontractors.

The operation of Visma Enterprise's IT-solutions is subject to agreements with subcontractors. Those agreements and appendices thereto specify all conditions related to the operation.

The operational centres handle activities in relation to the operation such as installation, upgrades, versioning, backup/restore, support, monitoring and capacity planning. This goes for system as well as application software.

Security Governance

Visma Enterprise has adopted a Security Governance model, in which the security policy forms the upper level.



The security work is based on recognised standards such as the ISO27000-series and ITIL.

With reference to the security policy, functional, topic or system specific policies have been defined. Thus, the Security Governance model includes guidelines for, among others, the following topics:

- User access and passwords
- Protection of data and systems against destruction, theft or unauthorised access
- Contingency plan
- Network security
- Operational security
- Physical security
- Security requirements to operational and subcontractors.

The overall objectives of Visma Enterprises security policy are:

Commented [CRG1]: Her står der stadig Bluegarden

> **2. Security Objectives**
>
> The ability to provide secure handling of information is imperative for Bluegarden's customers' trust and our competitive ability. Therefore it is a prioritised task to ensure a secure and uninterrupted communication and service flow both internally and for our customers. Bluegarden shall provide secure storage, processing, communication and disposal of information, and hence reduce the probability of our own or the customers' information and services being compromised. Bluegarden shall ensure authenticity, confidentiality, integrity, and availability of data and services, and accountability of users for their actions. Security measures shall be correctly implemented, and shall enforce security in an effective and efficient manner.

Development environments and processes

Visma Enterprise has established segregated development, test, and production environments.

The segregated environments contribute to safeguarding the data security in the form of accessibility, integrity and confidentiality of the data that Visma Enterprise stores and processes on behalf of its customers.

Segregation of functions has been established in order to ensure that different persons perform development, test and operation in order to reduce the risk of unauthorised access to data and unauthorised access to make changes to the systems.

Logical access

The customer is in control of access to its data in Visma Enterprise's Payroll and HR-systems, which means that the customer is responsible for the creation of, changes to and deletions of any employee access.

Visma Enterprise will allocate access for its own employees to customer data based on a "need-to-know" principle so only employees with a work-related need have access to customer data.

Request for access requires approval by a superior.

Login method

Access to Visma Enterprise's systems is managed via Visma Enterprise's login-module for customers as well as Visma Enterprise employees.

Authentication

Authentication takes place by means of a two-factor model using user-id and password. Upon entry, a one-time passcode received via SMS must be entered.

Authorisation

Authorisation takes place in each individual system where the individual user for each customer-ID has been allocated a role providing specific access to system functions.

Security in Operational centres

Physical security

Video surveillance is applied in all operational centres.

Measures are taken for protection against:

- Fire
- Water damage
- Lack of supply (e.g. power)

All routing of connections are duplicated.
In addition, guard duty has been established.

Operational set-up

A two-centre operational set-up is used for Visma Enterprises systems.

This means:

- that backup of data is made via dedicated lines between the two centres
- that it is possible to switch to centre 2 if centre 1 is unavailable.

Physical access

Visma Enterprise

Access to domiciles requires a valid access card for opening of the door lock.

Access cards may be limited in time so that they can only be used in certain periods.
(Limitations may be established for calendar periods but also for certain hours of a day).
If a card is lost, it may be blocked.

To persons with a longer lasting relationship with Visma Enterprise, e.g. consultants, sanitary personnel or craftsmen, personal access cards may be issued.

Guests will be given a one-day access card but they are not allowed to walk around in the building unaccompanied. Access cards must be returned to the reception when the guest leaves the domicile.

Operational centres

Access to operational centres requires a valid access card for opening of the door lock.
Access cards are managed by the individual operational supplier.

Access cards may be limited in time so that they can only be used in certain periods. If a card is lost, it may be blocked.

Guests/technicians will be given an access card but are not allowed to walk around in the building unaccompanied.

Staff

Visma Enterprise

Upon employment, all employees must accept a confidentiality declaration and a declaration confirming their compliance with security procedures. Employees are trained to perform their functions within their individual areas of responsibility and, consequently, they are made aware of agreed routines for the individual customer.

Awareness

Visma Enterprise has established an awareness program, which ensures that the employees are aware of the risk associated with the handling of confidential as well as personal and sensitive data.
Processes to support the program have been implemented in the daily routines.

Backup

Visma Enterprise has designated the data that are important in connection with a possible restoration. The operational suppliers perform backups of these data according to Visma Enterprise's instructions. Backups are stored at a secondary operational location and/or backup storage.

Contingency plan and disaster recovery

The operational suppliers have prepared contingency plans that are meant to protect Visma Enterprise's critical business services against serious system failures.

In addition, Visma Enterprise has prepared a contingency plan, continuity plans and recovery plans that are updated at least once a year. A test of all parts of the plans is performed at least once during a three-year period.

Among other things, Visma Enterprise's Business Continuity plan specifies the process for the establishment of a disaster recovery management who will manage the work throughout the disaster recovery situation.

The design of the disaster recovery model is shown below: