Information security Visma Engage

Appendix 6.4
Service Description

Version: May 2022

Description

This appendix describes information security requirements regarding Visma Engage.

Visma Enterprise A/S (herafter Visma) carries out an annual follow-up where we ask the supplier to confirm that they continue to comply with the requirements.

ISO 27001 Annex A reference	Information Security requirement
Clause 8.2	The Supplier shall provide risk mitigation and monitoring of risks to ensure that risk management is satisfactory
A.5.1.1	Supplier must have a comprehensive information security policy supporting technical and organizational measures implemented by the Supplier and its Sub-processors
A.7.1.1	The Supplier must perform Pre-employment checks including reviewing criminal records for all where possible
A.7.2.2	All relevant employees handling Visma data shall follow a security training program about relevant security procedures applicable to their respective roles.
A.8.1.1	The Supplier shall have an asset management policy and maintain an inventory of all assets holding Visma data including hardware, software, electronic documents and physical documents/media.
A.8.1.3 A.8.2.3 A.8.3	The supplier shall implement measures to ensure protection against accidental, unauthorize or unlawful loss, destruction, alteration or damage of data processed
A.12.2.1	Servers must be protected by hardening equipment, installing security patches, maintaining virus protection software, and controlling access to prevent unauthorized access and service disruption.
A.10.1.1	Visma data must be encrypted when at rest and/or in transit using best practice and industrial standards. This includes data storage on servers, workstations, mobile medias and backup medias.
A.9.1.1 A.9.2 A.9.3.1 A.9.4	There must be procedures handling User Access Management
A.9.1.2	Supplier's access to Visma data shall be restricted to authorized personnel only.
A.9.2.1 A.9.2.2 A.9.2.5	All supplier personnel's access to Visma data shall be logged and audited on a periodic basis.

A.9.4.2	Repeated attempts to gain access to the information system using an invalid password shall be monitored and appropriate action shall be taken in the case of suspected attempts of abuse.
A.9.2.2	Procedures shall be in place to deactivate passwords that have been corrupted or inadvertently disclosed.
A.9.2.4 A.9.4.3	Passwords must be protected in order to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.
A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.4	In areas where there is access to- and processing of Visma data, the following requirements apply: (a) Access only to identified authorized individuals. (b) All access to the production area shall be logged. (c) Cameras and alarms should be located in relevant areas of the datacenters e.g. entries to datacenters. (d) The area should employ a combination of proximity access control systems, biometric scanners, or escorted access to secure the Suppliers equipment and other equipment for processing Visma data. (e) Fire protection and suppression: Fire extinguishers, alarms, and emergency buttons shall be installed to protect the facilities and IT systems. (f) Uninterruptible Power Supply: Uninterruptible Power Supplies (UPS) shall be installed on the Suppliers network and servers to protect the facility and computer equipment from electrical power fluctuations and outages.
A.12.1.1 A.12.1.2	Operations must follow formal and documented procedures. Such procedures and verifications shall be subject to audit.
A.12.1.2 A.12.5.1 A.12.6.2 A.14.2.2 A.14.2.3	All changes to production systems shall be quality assured and follow a formal and documented change management procedure.
A.12.2.1 A.12.6.1	DDoS: The Supplier must use best industry standards for protection against DDoS attacks. The effectiveness of such protection shall be tested at least bi-annually.
A.12.3.1	Data backup and recovery: The supplier shall ensure that procedures are in place for backup and recovery of data. Conducted backup and recovery must be documented
A.12.3.1	Backup: The Data Processor must perform regular backups at least daily of data and system configurations when changed. Backup copies must be stored in a separate location from the production system or in a fire and water-proof container.
A.12.3.1	Restore test: The Data Processor must test a full restore of data from the backup media at least once a year.
A.12.4.1 A.12.4.2 A.12.4.3	Supplier will implement audit logging that will record activity in information systems that store, process or display Data Logging can be implemented using device, operating system or application processes and/or procedural methods Logging methods must capture privileged and administrative users access to devices, systems or applications and those logs must be reviewed on a regular basis.

	Logs must be available during an incident investigation involving Data. Logging must be kept for 90 days
A.12.2.1 A.12.5.1 A.12.6.1	The Supplier shall have a process for the adoption, testing, and deployment of patches relevant for the systems related to the services provided to Visma in a timely manner
A.13.1.1 A.13.1.2 A.13.1.3 A.13.2.1 A.13.2.2 A.13.2.3	Security are handled accordingly to a Network Security Policy or according to established security procedures
A.8.3.2 A.11.2.7	Procedures for and verification of destruction Of Media And Hardware
A.131.1 A.13.1.2	Firewalls: The supplier shall have firewalls in place to isolate the production services from the public internet and other unsecure zones.
A.16.1.1	Procedures for Security Incident management and reporting
A.17.1.1 A.17.1.2 A.17.1.3	Business continuity plans, including disaster recovery plans, must be established and updated and tested regularly
A.17.1.1 A.17.1.2 A.17.1.3	Disaster/Recovery test: The data processor must implement disaster/recovery plans such that the agreed service level if applicable – including recovery time objective (RTO) and recovery point objective (RPO) – can be met. The plan must be tested at least once a year.
A.12.6.1	Vulnerability Scanning must be conducted regularly on systems supporting Visma data. Supplier must ensure that corrective action is taken for vulnerabilities that result in risk of loss, alteration or access to Visma data
A.18.1.2	License management
A.12.1.4	Separation of development, testing and operational environments
A.7.1.2	All employees with access to Visma data must sign a non disclosure agreement
A.8.2.1 A.8.2.2	A policy or procedure to ensure classification of all Visma/customer data as confidential, must be implemented.