Maestro Cloud Security

Last updated: 02.05.2023

Content

Purpose

Maestro Soft (Provider) is a software provider of business applications for accounting, auditing and electronic trust services. The purpose of this document is to provide transparent information on security- and operational management data related to Maestro Soft Cloud services (Maestro Cloud). Maestro Cloud is a Software As A Service (SAAS) enabling the customer to login to a secure environment and work online with Maestro Soft applications.

Technical environments

The Maestro Cloud Development and Test life cycle includes three separated environments:

I. Production environment
II. Pre-production and integrational test environment
III. Test and development

The technical environments comprise the following technology components:

- Web servers
- SQL database server
- File storage server
- Backup storage
- Power and network infrastructure

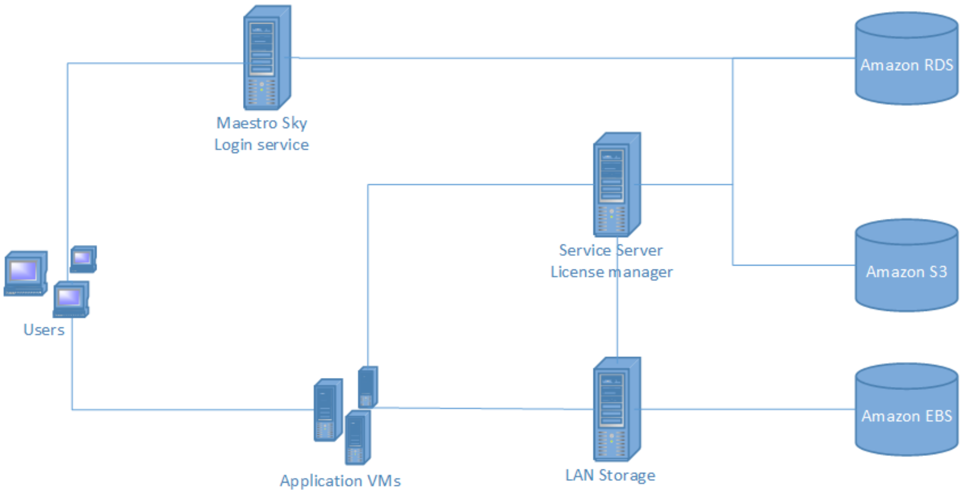

Figure 1Technical system overview

Production environment

The production environment is the environment in which the Maestro Cloud services is performed and that meets all the specified requirements for performance, durability and security. The production environment is exposed to public usage and interacts with the client's web browser.

Location:	Amazon Webservices region Frankfurt
Data backup:	Amazon Webservices region Stockholm

Pre-production and integrational test environment

The pre-production and integrational test environment is the environment in which the service is made available to integrational customers and 3-party vendors to test their integrated functionality. This environment is exposed to public usage and interacts with the client's web browser.

Location:	Amazon Webservices region Frankfurt
Data backup:	Amazon Webservices region Stockholm

Test and development

The test and development environment is the environment in which the service is developed and tested with new functionality. This environment is only available to the Maestro development team.

Location:	Datacenter in Oslo

Security

Internal organization

The security organization consist of the Board, Administration & Management, Development and Operation staff members, and Development & Quality Assurance.

The Board of Directors is ultimately accountable for corporate governance as a whole. The management and control of information security risks is an integral part of corporate governance. In practice, however, the Board explicitly delegates executive responsibilities for most governance matters to the Executive Directors, led by the Chief Executive Officer (CEO).

The Executive Directors give overall strategic direction by approving and mandating the information security principles and axioms but delegate operational responsibilities for physical and information security to the Security Committee (SC) chaired by the Chief Security Officer (CSO).

Security objectives

Perspective	Objective	Location
Operations	Production environment containing • Customer documents and data • Customer meta data • Customer user information	Stockholm, Frankfurt
Operations	Backup of customer documents and data	Stockholm, Oslo

Security description

Internal operational security

The security objectives are secured by means of physical, digital and organizational control mechanisms. The production environment is both physically and digitally isolated from unauthorized personnel.

Authorization to the production environment
Only Maestro DevOp staff members are granted access to the production environment.

Authentication to the production environment
Digital access to the production environment is controlled by means of two factor authentication.

External operational security

All communication with Maestro Cloud is secured by means of SSL Evident encryption connection (HTTPS). This protects data and documents to and from the production environment database and file server.

All customer user access and login to Maestro Cloud requires PKI authentication from the supported e-ID providers.

Confidentiality, data integrity and availability

Data and personal data are only available to the operations personnel. All user access and operations are logged. All Maestro employees and operations personnel are subject to a Non Disclosure Agreement.

Access recovery, and recovery of data after an incident

The provider restores availability and access to data and service in line with the Service Level Agreement. The provider maintains traceability of events and the ability to re-construct data from backup. Backup is performed on a daily basis to a geographical separated location from the production environment.

Testing and evaluation of technical and organisational measures:

The provider conducts testing and evaluation of its own technical and organisational measures. Tests and review of security policy and security organization are carried out regularly and at least once annually.

Physical security and Environmental Protection

Physical security and environmental protection of the production environment is defined by controls provided by the cloud provider. For Amazon Web Services see the System and Organization Controls Reports (AWS SOC).

Data durability, backup and deletion in the production environment

Documents and data committed to the service is stored in the production environment in order to be made available for day to day business operations by the customer. The data is controlled and can be deleted by an authorized customer user. Deleted data will be removed from production database and file storage but will remain in backup storage for a retention period. The current time to delete from backup storage is 30 days.