Accelerated Operations Service

Security Description

Rejlers Finland Oy

February 3, 2021

1 Purpose of the document

This document contains a security description of the Accelerated Operations cloud Service provided by Rejlers Finland Oy. The document describes technical and administrative solutions related to data security and data protection for the systems used to deliver the service.

2 Access and user management

Accelerated Operations is a multi-client environment. Each subscriber governs its user administration using the Admin module within the Accelerated Operations service.

A user has two methods to authenticate to AOS:

- Using a self-registered AOS account with a unique and verified e-mail address and a strong password.
- Using an enterprise Office 365 authentication that will provide a unique e-mail address as an identifier.

An AOS account password must be at least ten characters long, and contain uppercase and lowercase letters and at least one digit. The password is encrypted using the Blowfish algorithm.

Subscribers will have two main access levels to the service:

1. *A user* can view and manage the 360 areas according to account user levels described in Accelerated Operations User Guide.
2. *An organization admin* can also use the admin module to manage subscriber's own isolated organization entity, described in Accelerated Operations Admin User Guide

Rejlers grants an initial organization administrator privilege to subscriber. Subscriber can add more privileges inside their organization. User accesses are maintained by adding and removing e-mail addresses in access lists. A user that is not added to any organization or 360 area access lists cannot view any content in the service.

3 Security of the servers and data communications

The service is produced with a virtual server located in the equipment space in Finland. The virtual server is protected by a separate duplex firewall hardware. Only the communications required to provide services are allowed. Service security has been enhanced by limiting communications from countries identified as risky. All connections to the server are logged in the firewalls. Firewall logs are stored for 3 months.

The server has a local firewall on the operating system. Firewall settings are defined according to service requirements and usage requirements. In addition, the server has enhanced security features turned on. In addition to the local log, the server's system and security logs are also stored on a separate log server.

The service's communications are secured in public network by SSL encryption. Data transfer between systems through public network is always protected by either SSH or IPsec VPN encryption.

4 Colocation protection

The colocation used by Rejlers is located in a cave dug in a rock, in separate computer rooms. The space is equipped with lockable device cabinets suitable for ICT systems.

Access to the colocation facilities requires an access right and a personal access key. Access control registers every visit. Routes are monitored by a recording video surveillance system. Premises are equipped with fire and burglar alarm systems.

The colocation is equipped with a controlled cooling system that maintain the temperature at 18-27 Celsius degrees, the standard temperature required for IT devices. The colocation is equipped with an automated Halotron fire extinguisher system.

The colocation is equipped with a redundant 230V power supply. Redundancy is done with the N+a reduntant UPS device and with two auto-starting diesel-powered backup generators. In order to ensure usability, all possible components of the Service have been duplicated, and the platform designed in such a way that a failure of a single device does not affect the service.

5 Backup

The server is backed up every day for changed data and full backup is performed weekly. Daily changed data is retained for 30 days retrospectively. Monthly backups are saved for the past three months. Backups are cyclically tested according to the test plan.

6 Control

The platform service provider monitors the status of server hardware and communication devices, as well as power supply and cooling equipment, with its own control systems. In addition, Rejlers Finland Oy monitors the state of servers and services with its own control systems.

7 Interfaces

The Accelerated Operations Service is used with a browser on computer or mobile device. The service information is located in a separate database. TCP port 443 is used for communication between the browser and the server. The communication is secured by the SSL protocol.

The Accelerated Operations Service can be integrated into client systems through different interfaces. The interface is implemented on client systems by means of separate traffic modules. Communication between systems is encrypted.