Assetti Service and Security Statement

Assetti – Service Delivery

Assetti is a cloud based service, which follows a software distribution model where the application is hosted by a cloud service provider and made available for customers over the internet. In this model, service delivery continuity responsibility is on the service provider, differing from the traditional on premises installation model, where the customers typically manage the environments.

Service delivery is monitored in various areas, including following categories:

Base service delivery continuity

Assetti offers a cloud based property asset management solution delivering services through a cloud platform of Planeetta Internet Oy - one of the leading internet hosting providers in Northern Europe.

Planeetta Internet's servers are using the data center of Digita Oy for all hosting services. Located in Ilmala, Helsinki this data center is one of the most important locations for internet traffic in Finland. The data center fulfils the highest specifications of Finnish Communications Regulatory Authority (FICORA 54/2008 M: Regulation on priority rating, redundancy, power supply and physical protection of communications networks and services). Regulations of the European Commission are being followed for safety and technical aspects (DciE – Datacenter Infrastructure Efficiency).

The data center is connected to internet network via three independent backbone network operators. Two different power supplies are provided for all server and storage equipment through a separate independent and secured power sources. The track record of the server is approximately 99,96% which equals a total unexpected downtime of 150 minutes per year.

Assetti maintenance breaks are usually done between 21.00 to 24.00 (GMT+2) in business days during which the service is not accessible.

Architecture

Assetti's architecture is built with a server-side framework, where all of the application state, business and UI logic reside on the server. Unlike client driven frameworks, Assetti application never exposes its internals to the browser, thus vulnerabilities cannot be leveraged by an attacker. This architecture follows good security practises and has automatic protection against the most common vulnerabilities in web applications.

The framework which Assetti is using has built-in protection against cross-site scripting (xss) attacks. All communication between the server and customer are included with a user session specific cross-site request forgery (CSRF) token, which minimizes the risk from CSRF attacks. All communication in Assetti application goes through one web service used for RPC requests which limits attack entry points on the application.

Monitoring and reaction

Assetti receives automatic notifications from server provider regarding disruptions on the host service. The server has automatic monitoring system which alarms duty officer when necessary, the system expects to have 30 minutes responses time on a 24/7/365 basis. Assetti is being monitored hourly by the support team on server performance, log activities, unexpected errors and requests.

Notifications are sent promptly to all admin users by Assetti support team in case there is a system-wide disruption.

Authentication mechanism and user identity

Assetti production can only be accessed with an authorised identification of the person accessing system and the valid registered password. Assetti application uses only secure HTTPS connections, where all information is encrypted. Registration emails contain single user tokens, and passwords are encrypted using SHA-256.

The Assetti password policy enforces the following rules: A minimum of 8 characters, containing at least one uppercase letter and one number. To prevent brute force attacks only a limited number of login attempts are permitted per user before a wait period is enforced.

The Assetti application uses role and permission based access control. These are customizable for each customer's environment. User accounts are granted and reset via emails which contain secure links containing SHA-256 registration tokens which are valid for a single a use.

Security and risk management

Assetti provides a separate branch for each customer - referred to as customer environment - to assure high level of data security. One customer's data is not visible to other customers inside Assetti, and the data itself is stored in a separated database schema.

Assetti always ensures customer data is securely protected, with all communication through the cloud being encrypted. Login and access control are enforced on every page in Assetti.

Cross site scripting (XSS), cross site request forgery (CSRF) and external SQL injection are all prevented.

Assetti employees are restricted from accessing customer data, unless given permission by the customer during deployment phase. All employees have signed a non-disclosure agreement restricting their share of information to third parties. Access to data is only given upon customer's requests for assistance during Setup and Training. In case support or application administration is required, only two members of Assetti team will get access to your data: a chosen support person and his/her substitute. All support accounts for individual cases have unique passwords which have 10 or more random characters and are changed on a quarterly basis.

Backups and error recovery

Besides the backup function included as a feature in Assetti, customer's data is backed up automatically in the system. Daily backups are stored and kept for 14 days, while monthly backups remains in the system for 12 months. All backups are converted to tape and stored in a separate secure location once per week.

Assetti offers data recovery services for customers in case there have been accidental changes to the data. Customers are advised to contact Assetti support team via phone or email if the automatically backed up data is wished to be recovered.