

Technical description of the PowerOffice Go service

Security and accessibility

Security is one of our key values. We accept all security reports, and practice responsible disclosure. Some key features for PowerOffice Go

- We conduct security audits and annual penetration testing assisted by internal and external experts.
- We perform automatic scans for security defects every night.
- We regularly audit our code to find logic flaws that could lead to a vulnerability.
- Passwords are never stored as text and are always "hashed" on the server. This means no one else can find out what your password is.
- We offer two factor authentication (2FA) on login, and mandatory 2FA can be specified on the client.
- Communication between client and server is protected by industry standard SSL encryption.
- Data is stored encrypted at rest.

Data protection

- All our employees have entered into a confidentiality agreement and only have access to systems and features they need to perform their tasks.
- Access to stored information is limited to a few people who works with operation of the services. Other staff cannot access your data unless they are invited as users on the client.
- The service logs all changes that users make in the system so that they are traceable in retrospect.

Backups

- Backups are performed automatically, and we have snapshots every 10 minutes for the last week. Backups are available up to 1 year.
- Backups are stored in a different region from our datacenters.
- We test the process of restoring from backups on a regular basis.

Contingency plan

We have a contingency plan ensuring continuous operation in the event of a fallout of our hosting location or our offices.

Operational Environment

PowerOffice Go uses Microsoft Azure as its operating platform. Data processing takes place in Europe and follows European regulations and protection requirements privacy.

In order to meet national legal requirements, data is also stored in Norway.

Our primary datacenter is in Amsterdam, Netherlands

Datacenters in use is certified with ISO 27001, ISO 27017, ISO 27018, ISO 20000-1, ISO 22301, ISO 9001 and CSA Star, and has the following security measures:

- Locked with alarm and 24/7 monitoring
- Video surveillance and traceability of access to the premises
- Redundant climate control with environmental monitoring of gas, moisture, heat and water
- Fire alarm with automatic fire extinguisher
- Uninterruptible power supply regularly tested against fictional power failure

System changes by user

User of Go have limited access to and options for changing the settings of the client, in terms of accounting and the required reporting. The system is delivered with standard settings, with limited customization. In any case, all user activity is logged, and changes can be identified in full detail.

SAF-T requirements

The system can generate a SAF-T report in compliance with the requirements. The SAF-T reporting in Go have been tested extensively and verified by third parties.