Security Statement

Tribia (hereafter Tribia) has delivered collaboration solutions (hereafter Solution) as a SaaS-solution since 2001 and has long experience with handling business critical information and data security for clients. As a supplier we give you a reliable, secure and flexible Solution. We take the task of providing you with a safe Solution very seriously and place great emphasis on ensuring that your content is always available and secure.

1. APPLICATION SECURITY

ENCRYPTION OF DATA

All data traffic and credentials are encrypted using TLS (Transport Layer Security) to ensure that no unauthorized access to data.

USER IDENTIFICATION

Users are identified by a valid combination of username and password. Authentication is managed with either SSO or built-in user repository. For password encryption, a one-way encryption is run and the password is never visible to any Tribia employees. By login a mechanism is run to prevent brute-force attacks on user accounts.

ACCESS

Users can access per project room and can for example have write permissions in a project, but only read rights in another. In addition, the read and write permissions can be set on all levels. Rights can be set based on individuals or groups.

SAFETY TESTS AND SECURITY

Independent safety tests are done by expert communities to ensure against attacks such as cross-site request forgery (CSRF), cross-site scripting (XSS), SQL injections among other on technical level. Security is a continuous focus and includes organizational awareness and competence.

MICROSOFT AZURE CLOUD HOSTING

Azure Cloud Services offers a rich service catalog and a dynamic allocation of resources. In cooperation with our professional operation partner Basefarm, Azure is utilized to provide a stable and future proof operating environment for our applications and data.

BASEFARM HOSTING

THE OPERATING ENVIRONMENT

There is great emphasis on the safety of the operating environment which is based in Norway and established at our professional operation partner Basefarm (hereafter The Operating Partner). The physical environment is divided into two data centers and information that is stored in the Solution is mirrored in real time for quick recovery in case of an emergency.

The datacenters are facilitated with access control, video surveillance, climate control, fire detection with early warning, emergency power and anything else that characterizes a modern and secure data center.

The operating environment are located in anonymous industrial buildings. Logos or other effects associated with our operating partner does not exist at the building.

The terrain around is shaped so that there is little danger of flooding, and the buildings are solid.

The risk of burglary is considered as small.

The buildings are located behind several massive steel doors that are connected to an alarm system that is monitored 24 hours a day through the Operating Partner`s operating centre.

Access to the data centres is given only to personnel with special needs and when required with prior approval. Access Cards and code is also required at all times. Service technicians and any other personnel granted access only when accompanied by authorized personnel.

All employees of our operating partner sign a standard confidentiality agreement. This also includes any access to customer data. Our operating partner staff have limited access / rights / access to customer data depends on users / user groups, which in turn is determined by the function they provide.

The data centre is monitored 24 hours a day, 365 days a year, through the Operating Partner`s support team. In the support team, there are always highly trained and qualified staff with extensive experience in the areas of networking, operating systems and applications.

Connection to the Internet is robust and consists of redundant connection to the NIX and redundant connections to different providers for general Internet traffic. In addition, we have redundant interconnection against some major players in Norway.

Our Operating Partner has a quality system based on ISO. The processes involved in service delivery is in general based on ITIL.

FIREWALL

The Solutions platform is implemented behind redundant firewall service and load-balancing from reputable suppliers. It is implemented unique rules for the firewall and policies based on the security requirements the Solution demands. The Operating Partner is responsible for all operation, maintenance and monitoring of firewalls.

BACKUP & RESTORE

Backup service for the Solution running on Azure uses reliable Blob storage with in-built security Backup service for the Solution consists of an advanced two-layer architecture with backup to disk and then to the underlying tape or disk storage in a third datacentre. This architecture leads to significantly shorter backup and restore times.

We have the following standard backup:

- Incremental backup is performed twice daily (at. 12:00 and 24:00)
- Deleted / changed files stored on backup for 30 days (retention)

Backup is taken daily in our Operating Partner's backup windows, with guaranteed response to restore in the event of hardware failure or data loss. Backup services are online and do not imply downtime for backup. Only authorized personnel have access to physical copies of backup media.

Involved technicians must sign a declaration of confidentiality.

MICROSOFT AZURE CLOUD HOSTING

Azure Cloud Services offers a rich service catalog and a dynamic allocation of resources. In cooperation with our professional operation partner Basefarm, Azure is utilized to provide a stable and future proof operating environment for our applications and data.

THE OPERATING ENVIRONMENT

Azure Norway is used to ensure that all customer data stay located in Norway. In all Azure datacenters physical access to the areas where data is stored is strictly controlled. Typically, tall fences made of steel and concrete encompass every inch of the perimeter. Cameras are located around the datacenters, with a security team monitoring their videos at all times. Professionally trained security officers also routinely patrol the datacenter and monitor the videos from cameras inside the datacenter at all times.

Controlled access points are located at the facility's perimeter, at the building's perimeter, inside the building, and on the datacenter floor. Physical access to the datacenter is strictly controlled and must be requested and approved before arriving at the datacenter. Permissions are granted on a need-to-access basis and limited to a certain period of time.

Physical security reviews of the facilities are conducted periodically.

The Azure infrastructure meets a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2.

FIREWALL

The Azure platform Firewall is a managed, cloud-based network security service that protects our Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

The Operating Partner in cooperation with Microsoft Azure is responsible for all operation, maintenance and monitoring of firewalls

BACKUP & RESTORE

Backup service for the Solution running on Azure uses reliable Blob storage with in-built security and high availability features. When applicable, snapshots are used for some workloads such as VMs and Azure Files, drastically reducing the time to recover your data to the original storage.

We have the following standard backup:

- Incremental backup is performed twice daily (at. 12:00 and 24:00)
- Deleted / changed files stored on backup for 30 days (retention)

Backup is taken daily with guaranteed response to restore in the event of hardware failure or data loss. Backup services are online and do not imply downtime for backup Access to backups is restricted only to authorized Backup Admins.

All infrastructure is represented as code and can quickly be rebuilt from scratch in case of a disastrous loss of data. Infrastructure code is located in a secure git repository. Infrastructure as code makes it easy to move the entire deployment of services to a different datacenter should the need arise.

CONCLUSION

You can trust that Tribia do what we can to ensure the safety, performance and reliability of your projects. If you have any questions about the Services and its safety, performance or reliability, send us an email to support@tribia.com. We hope that this information has been helpful.