APPENDIX C
Security measures

GENERAL

The Data Processor shall take all measures necessary under Article 32 of the Regulation, including planned, systematic, organizational and technical measures, ensuring adequate confidentiality, integrity, and availability of information in the processing of Personal Data. With reference to the technical and organisational measures specified in this section, the Supplier provides the following measures:

- Protection relating to physical access and logical access
- Multifactor authentication for admin purposes
- Daily backup and process for secure restore
- Log of access

ENCRYPTION OF DATA

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

Data encryption for data at rest is protected by the Advanced Encryption Standard (AES) algorithm that uses a 256-bit symmetric encryption key in XTS mode, as defined in the IEEE 1619-2007 standard and NIST Special Publication 800-38E as XTS-AES-256.

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 technical levels. Security is a continuous focus and includes organizational awareness and competence.

Development follow OWASP Secure Coding practices for best application security. Cyber Security and controls are based upon NIST Cyber Security Framework.

THE OPERATING ENVIRONMENT

Orange Business Datacenters are used for customer data and located in Sweden. The Orange Business Datacenters serve as the facility for housing all computer equipment and supporting infrastructure necessary for hosting our applications and storing all customer data.

The data centers are located outside of city centers with redundant communication paths, environmental control and monitoring.

Tribia's services run over 2(3) data centers. Computers run in 2 data centers with master nodes in a 3 data center (witness site). This ensures continued operation in the event of a data center failure. By using test capacity for production, 100% capacity will be quickly restored.

All equipment from the data centers up through physical infrastructure up to software functions is redundant and can withstand faults without the services being affected.

The Orange Business datacenters are internally secured by multiple perimeter walls and doors. Intrusions alarms are in place for all datacenters and are connected to an operations center. All access is recorded by CCTV. All access is controlled by electronic locks and access control. Mantrap is installed at entry points and antipassback is in function.

The Orange Business Infrastructure meets the ISO9001, ISO14001, ISO27001 and SOC 2 standards

FIREWALL

The Orange Business Datacenters are protected by the Cisco ACA firewall in concert with the F5 BIG-IP Load Balancer providing firewall, antivirus, intrusion prevention, virtual private network (VPN) and distributed scalable processing and communications capabilities.

BACKUP & RESTORE

Backup services running on Orange Business Datacenters are using a combination of file, image and snapshot backup. Incremental backup and image backup are utilized whenever possible to ensure a performance system. Redundant off-site location used for storing backup.

The backup systems used are immutable and external from Tribia's solution. This means that the backups cannot be changed after they have been taken.

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.