Version June 2018

General Security Measures

1. Data Centers

Voxbone data centers are located in enterprise-class data centers at top-tier data center providers in Brussels (BE), New-York (US), Frankfurt (DE), Los Angeles (US), Sydney (AU) and Hong-Kong (HKG). All data centers provide the full range of hosting facility features such as fully redundant power as well as the highest levels of security.

Facilities are unmarked to help maintain a low profile. All visitors have to go through a security check-in before accessing the facility. Access is available only to data center personnel and a subset of Voxbone employees, who know and acknowledge Voxbone's privacy and security requirements. Data center access is logged and monitored. 24x7 onsite staff provides additional protection against unauthorized entry.

Multiple levels of power redundancy are provided at the highest level of availability. Battery and UPS backup power sources prevent power spikes, surges and brownouts. If a total utility power outage ever occurs, all of the data centers' power systems are designed to run uninterrupted, with every server receiving conditioned UPS power. The UPS power subsystem is N+1 redundant, with instantaneous failover if the primary UPS fails. If an extended utility power outage occurs, routinely tested, on-site diesel generators can run indefinitely.

Heating, ventilation and air conditioning (HVAC) systems provide appropriate and consistent airflow, temperature and humidity levels. Every data center HVAC system is N+1 redundant. This ensures that redundant systems immediately and automatically come online should there be an HVAC system failure. Advanced fire suppression systems are designed to stop fires from spreading in the unlikely event ones should occur.

Voxbone replicates data over multiple systems to help to protect against accidental destruction or loss. Voxbone has designed and regularly plans and tests its business continuity planning and disaster recovery programs.

2. Network and transmission

Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Voxbone transfers data via Internet standard protocols.

Our data centers contain redundant network connectivity with multiple Internet Service Providers, and employs robust routing to allow network traffic to take the best path. Voxbone makes HTTPS encryption (also referred to as SSL or TLS connection) available.

3. Access controls

Network access to and from Voxbone applications is controlled by dedicated firewall devices, Intrusion Detection/Prevention Systems (IDS/IPS), Access Control Lists (ACLs). Employee access to Voxbone production servers require use of a secure channel.

4. Data storage and transport

Customer data in transit is encrypted using high grade TLS encryption.

Voxbone uses effective and efficient storage-based technologies that enable daily "snapshot" backups. These can be used within a data center for quick data recovery. For offsite backups, we mirror all production data to DE data centers at least once every 24 hours or less.

Voxbone
Avenue Louise 489
1050 Brussels
Belgium

Tel: +32 2 808 00 00
Fax: +32 2 808 00 01

5. Decommissioning

Certain disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes before leaving Voxbone premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Disk Erase Policy.

6. Business Continuity Plan and Disaster Recovery (DR)

Voxbone's data protection measures, high availability and built-in redundancy are designed to ensure application availability and protect information from accidental loss or destruction.

- Our data centers have redundant power, fire prevention, network paths and generators to survive moderate disaster scenarios
- We have local and offsite backups for all data centers
- All Voxbone networking, storage, servers and databases, power and network paths are redundant within a data center and can survive hardware failures
- Recovery Point Objective (RPO) from onsite backups is 1 hour. RPO from offsite backups is 24 hours.

Voxbone load-balances at every tier in the infrastructure, from the network to the database servers. Application server clusters are enabled to ensure that servers can fail without interrupting the user experience. Database servers are clustered for failover. DR plan incorporates geographic failover between US data centers and European data centers.

Voxbone
Avenue Louise 489
1050 Brussels
Belgium

Tel: +32 2 808 00 00
Fax: +32 2 808 00 01