VOIP\STUDIO

Secure global communications

Overview

At VoIPstudio we consider our customers' data to be a customer asset entrusted to us that requires VoIPstudio to treat each element of data with a high level of security. We consider every element of customer data equally private and have designed our security envelope with that in mind.

Internal and human resource security

All our employees adhere to company-defined security processes and audit trails to ensure account integrity. Our website is McAfee protected. A comprehensive privacy policy is also available on our website for all to read. We perform monthly security scans, and an infrastructure audit for PCI compliance, which is performed by an external party. We continually perform vulnerability testing against threat and attack vectors to detect any security vulnerabilities in payment processes, to avoid ransomware, and other threats.

In addition, VoIPstudio is certified by the UK Government Ombudsman, under the Information Commissioner Office. It will also meet the upcoming requirements of the EU General Data Protection Regulation (GDPR), meaning that our customers can rest assured we adopt and meet not just current requirements, but also regulations as they evolve. VoIPstudio has the following security and compliance monitoring standards and procedures:

- Defined and documented organizational security standards and procedures.
- All employees and contractors required to sign a confidentiality agreement.
- Background checks for all employees that have access to customer data.
- Restricted access to only those employees that need to manage customer data or manage servers hosting customer data.
- Process for the timely removal of access to customer data from any employee or contractor that leaves the company or who no longer requires access. Access is revoked within 24 hours of employee or contractor departure or reassignment.
- Ongoing staff training on all internal security policies and general security awareness.

"VoIPstudio is certified by the UK Government Ombudsman, under the Information Commissioner Office. It will also meet the upcoming requirements of the EU General Data Protection Regulation (GDPR), meaning that our customers can rest assured we adopt and meet not just current requirements, but also regulations as they evolve."

Data centres, encryption and hosting

In terms of security, our calls are routed via our three data centres - UK, US and Japan. All data centres are ISO 27001 certified, which ensures the highest possible standards in data security. All our physical storage devices employ the highest standards of data encryption, using AES-256 to encrypt data. We also use TLS-encrypted SIP signalling and ZRTP for encrypted voice streams.* Physical security for data centres hosting the servers containing customer data meets the following requirements:

- Rooms are secured by at least two access mechanisms (e.g., building key-card, man traps, security guard, and computer room badge-in).
- Only authorized employees are allowed physical access to the servers hosting customer data.
- The vendor maintains 24/7 security at the location.
- All backups of customer data are either stored on-site with controlled access or at a secure vendor controlled or commercial off-site location.
- The site supports additional levels of protection such as uninterruptible power and fire suppression.
- Failed storage components in the data centre undergo a MoD-approved “erase” or “wipe” procedure (if functionally possible) prior to destruction.

“All data centres are ISO 27001 certified, which ensures the highest possible standards in data security. All our physical storage devices employ the highest standards of data encryption, using AES-256 to encrypt data”

Technical controls

VoIPstudio contains sophisticated technical controls that provide protection to its network, systems, and applications.

- VoIPstudio utilizes a top tier hosting provider that protects customer data from external threats.
- VoIPstudio maintains individual accountability for employees and contractors that access systems that host customer data. VoIPstudio has documented user account/password management system for these employees and contractors.
- VoIPstudio ensures that individual access to customer data is controlled (i.e., a separate user name and password is required for each individual administrator). Customer data is compartmentalized to prevent unauthorized access to the data of other customers.
- Data is protected by ‘hardened’ passwords rotated on a 90 day basis.
- Wireless connectivity to networks or servers hosting customer data is protected using security mechanisms such as EAP, TTLS, TLS, or PEAP.
- VoIPstudio has formal security policies and procedures to deal with viruses, malware and related threats. Anti-virus software programs are active on all Windows-based machines. These systems have automated periodic full scans and use updated virus signature files.

** Only applicable to WebRTC calls*

Usage Criteria

In order to protect the confidentiality, integrity, and availability of customer data, VoIPstudio meest the following usage criteria:

- Each user is assigned a unique ID. User IDs and passwords meet the following requirements:
    - Users may change their password at any time.
    - Passwords must be at least 6 characters long.
- Access to data in the VoIPstudio database has permission based controls restricting access to authorized customer users as determined by the customer data owner.
- Each change of user login status is logged within VoIPstudio. All logs are treated as confidential information and access to reports can be restricted using the permission system. Reporting of this information is available within the VoIPstudio administration interface.
- If confidential data, personal data (e.g., names, addresses, phone numbers), or authentication information (e.g., passwords) is transmitted, VoIPstudio supports and recommends the implementation of the optional 256-bit SSL encryption between each component of the communications path.
- By implementing VoIPstudio, users agree to be bound by the Acceptable Usage Policy.
- VoIPstudio's security policy assumes customer data retention is permanent and is designed to that standard. Customers retain the ability to implement their own data retention policy.

Gable House
18-24 Turnham Green Terrace
London W4 1QP
United Kingdom