Vocal Video Security Statement

Last updated: January, 2024

Vocal Video values the trust that our customers place in us by letting us act as custodians of their data. We take our responsibility to protect and secure your information seriously and strive for complete transparency around our security practices detailed below.

Our Privacy Policy and Data Processing Addendum also further details the ways we handle your data. We are certified under the EU-U.S Data Privacy Framework, UK Extension to the EU-US Data Privacy Framework, and Swiss-U.S. Data Privacy Framework (listing here). As a result, the European Commission has ruled DFP certified companies are safe and trusted for EU-US data flows (link).

Physical Security
Vocal Video's information systems and technical infrastructure are hosted at an Amazon Web Services (AWS) data center located in Northern Virginia, USA. The datacenter is a world-class, SOC 2 accredited data center. Physical security controls at their data centers include 24x7 monitoring, cameras, visitor logs, and entry requirements.

Certifications and Attestations
AWS has achieved the following relevant certifications and attestations that apply to the Vocal Video service:

- ISO 9001 (Global Quality Standard) - public link
- ISO 27001 (Security Management Controls) - public link
- ISO 27017 (Cloud Specific Controls) - public link
- ISO 27018 (Personal Data Protection) - public link
- AICPA SOC1 (Audit Controls Report)
- AICPA SOC2 (Security, Availability & Confidentiality Report)
- AICPA SOC3 (General Controls Report) - public link
- Cloud Security Alliance Controls Level 2 - public link

Data Retention
We retain your customer data while you are an active customer of our service. After your subscription expires, we purge all your customer data from our systems within 30 days.

Payment Processing
Vocal Video uses Stripe to accept and process credit card payments securely. Stripe has been audited by a Payment Card Industry (PCI)-certified auditor and is certified as a PCI Service Provider Level 1. Stripe can therefore accept and process credit card information securely in accordance with these standards on behalf of Vocal Video. Vocal Video stores no credit card information on its systems.

Access Control
Access to Vocal Video's technology resources is only permitted through secure connectivity. Production data is only accessible via secure keys and multi-factor authentication where applicable. Vocal Video grants access on a need to know basis of least privilege rules, reviews permissions quarterly, and revokes access immediately after employee termination.

Security Policies
Vocal Video maintains and regularly reviews and updates its information security policies, at least on an annual basis. Employees must acknowledge policies on an annual basis and undergo additional training such as HIPAA training, Secure Coding, and job specific security and skills development and/or privacy law training for key job functions. The training schedule is designed to adhere to all specifications and regulations applicable to Vocal Video.

Personnel
Vocal Video conducts background screening at the time of hire (to the extent permitted or facilitated by applicable laws and countries). In addition, Vocal Video communicates its information security policies to all personnel (who must acknowledge this) and requires new employees to sign non-disclosure agreements, and provides ongoing privacy and security training.

Vulnerability Management and Penetration Tests
Vocal Video maintains a documented vulnerability management program which includes periodic scans, identification, and remediation of security vulnerabilities on servers, workstations, network equipment, and applications. All networks, including test and production environments, are regularly scanned using trusted third party vendors. Critical patches are applied to servers on a priority basis and as appropriate for all other patches.

We also conduct regular internal and external penetration tests and remediate according to severity for any results found.

Encryption
We encrypt your data in transit using secure TLS cryptographic protocols.

Development
Our development team employs secure coding techniques and best practices, focused around the OWASP Top Ten. Developers are formally trained in secure web application development practices upon hire and annually.

Development, testing, and production environments are separated. All changes are peer reviewed and logged for performance, audit, and forensic purposes prior to deployment into the production environment.

Asset Management
Vocal Video maintains an asset management policy which includes identification, classification, retention, and disposal of information and assets. Company-issued devices are equipped with full hard disk encryption and up-to-date antivirus software. Only company-issued devices are permitted to access corporate and production networks.

Information Security Incident Management
Vocal Video maintains security incident response policies and procedures covering the initial response, investigation, customer notification (no less than as required by applicable law), public communication, and remediation. These policies are reviewed regularly and tested bi-annually.

Breach Notification
Despite best efforts, no method of transmission over the Internet and no method of electronic storage is perfectly secure. We cannot guarantee absolute security. However, if Vocal Video learns of a security breach, we will notify affected users so that they can take appropriate protective steps. Our breach notification procedures are consistent with our obligations under applicable country level, state and federal laws and regulations, as well as any industry rules or standards applicable to us. We are committed to keeping our customers fully informed of any matters relevant to the security of their account and to providing customers all information necessary for them to meet their own regulatory reporting obligations.

Information Security Aspects of Business Continuity Management
Vocal Video's databases are backed up on a rotating basis of full and incremental backups and verified regularly. Backups are stored within the production environment to preserve their confidentiality and integrity and are tested regularly to ensure availability. Furthermore, Vocal Video maintains a formal Business Continuity Plan (BCP). The BCP is tested and updated on a regular basis to ensure its effectiveness in the event of a disaster.

Your Responsibilities
Keeping your data secure also requires that you maintain the security of your account by using sufficiently complicated passwords and storing them safely. You should also ensure that you have sufficient security on your own systems. We require TLS to secure the transmission of video and audio responses.

Logging and Monitoring
Application and infrastructure systems log information to a centrally managed log repository for troubleshooting, security reviews, and analysis by authorized Vocal Video personnel. Logs are preserved in accordance with regulatory requirements. We will provide customers with reasonable assistance and access to logs in the event of a security incident impacting their account.