Voxpopme Information Security Policy

Contents

Voxpopme recognizes the trust our clients place in us when we work together. We invest heavily in our Information Security processes, and our solutions are built with data security as our highest priority. Our Information Security team is managed by our CTO, VP of Operations and Compliance Manager.

Voxpopme will maintain administrative, physical, and technical safeguards to protect the security, confidentiality, availability and integrity of data within the Software as a Service we provide. An overview of these measures is provided below:

Managing Risk

- Voxpopme manages and controls risk by ensuring that we maintain a robust program of auditing, monitoring and reviewing our systems and logs

- We conduct third-party Remote Penetration Testing on an annual basis, and we are happy to provide the output report of this process to our clients

- We implement internal vulnerability scanning on an ongoing basis, and manage any identified vulnerabilities quickly, remediating these based on their risk severity

Standards and Certifications

- Voxpopme is ISO 27001 and ISO 9001 Certified. Our Information Security processes, policies and controls are based on the ISO 27001 framework, with internal and external audits taking place on a regular basis to confirm our ongoing compliance with this globally-recognized standard

Privacy Policy

- Voxpopme implements additional policies regarding Personal Data. Our Privacy Policy provides information on how Personal Data is handled and protected: https://www.voxpopme.com/video-question/privacy-policy

Software Development Life Cycle

- A Software Development Life Cycle (SDLC) is implemented to ensure that security is considered and optimized at each stage of the development process. Voxpopme's Engineering Team prioritize secure development and are experienced in best practice in industry standards including OWASP
- Voxpopme employs a code review process to increase the security of the code used to provide the applications in production environments

Vulnerability Testing

- We utilize a number of web-based scanning and monitoring functionalities to identify security vulnerabilities. Where these are identified, they are prioritized and remediated by our engineers
- Vulnerability analysis is an established element of our code review process

Patch Management

- Applications are patched frequently as part of our build process, and systems are frequently brought up to date with new security patches. Critical vulnerabilities are patched as a high priority as soon as a patch becomes available
- Non critical software patches are also subject to business monitoring using our endpoint management solutions to avoid any vulnerabilities or shadow software issues

Data Centers

Voxpopme has engaged Amazon Web Services (AWS) to provide Data Center/Hosting services. AWS security information may be accessed or requested by Customers, as applicable, directly from AWS (https://aws.amazon.com/security/).

- Infrastructure: Voxpopme utilizes geographically distributed data center and stores all production data in physically secure data centers

- Redundancy: Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. Data Center services are designed to allow Voxpopme to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have industry standard preventative and/or corrective maintenance procedures. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to industry standard procedures

- Power: The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. A primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center

- Data Center Business Continuity: Voxpopme replicates data over multiple systems to help protect against accidental destruction or loss. Voxpopme has designed and periodically tests its business continuity planning/disaster recovery programs

- Data Transmission: Data centers provide secure data transfer mechanisms that are 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. Voxpopme transfers data via Internet standard protocols

Network Security

- Access to the production environment: Access is granted following the principle of least privilege, must be approved by the CTO and is via an enforced VPN

- External Attack Surface: Voxpopme employs multiple layers of network devices and web access firewalls to protect its external attack surface. Voxpopme considers and risk-assesses potential attack vectors and incorporates appropriate purpose built technologies into external facing systems

- Network Incident Response: Voxpopme monitors a variety of communication channels for security incidents, and our staff will react promptly to known incidents

- Encryption Technologies:

  We encrypt data at rest using AES256. We encrypt all data over public networks using HTTPS. We encrypt in transit with TLS 1.2 where the client communicating supports it.

  We use WPA-PSK/WPA2-PSK network authentication with TKIP +AES data encryption for wireless transmissions.

Anti Virus Controls

- The term “virus” means any computer code intentionally designed to (a) disrupt, disable, harm, or otherwise impede in any manner the proper operation of a computer program or computer system or (b) damage or destroy any data files residing on a computer system without the user’s consent. Voxpopme will use industry standard methods, designed to reduce the possibility of the existence of a virus

- Anti-virus software scans our systems on an ongoing basis to detect any suspicious activity. Signature files, patches, and updates are automatically uploaded and implemented on an ongoing basis

Access Control

- Voxpopme’s internal data access processes and policies are based on the least-privilege methodology, and designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data
- Voxpopme designs its systems to allow only authorized persons to access data. We employ a centralized access management system to control access to production servers, and provide access to only authorized staff. The granting or modification of access rights is based on the authorized staff job responsibilities; job duty requirements necessary to perform authorized tasks and a need to know basis. All access must be in accordance with Voxpopme’s internal data access policies and training
- Privileged access is limited to only to approved staff and on the strict approval of the CTO or VP of Operations
- System administrator and system operator activities are logged and the logs protected and regularly reviewed

- Customer's administrators and end users must self-authenticate. Passwords can be routinely reset according to industry standards

Data Storage, Isolation, and Authentication

- Voxpopme stores data in a multi-tenant environment. Data, the services database, and file system architecture are replicated between multiple data centers. Voxpopme logically isolates data on a per customer basis at the application layer. Voxpopme logically separates Customer's data, including data from different end users, from each other. Data for an authenticated end user will not be displayed to another end user (unless the former end user or administrator allows the data to be shared)

Change Management

- Any code changes are reviewed for security and vulnerability considerations and signed off through a process of peer review and manager approval before they are implemented
- Any business changes that affect or impact business processes, information processing facilities and systems are subject to risk-assessment prior to the changes being implemented

Backups

- Backups are taken at least daily of our critical databases. We automate and document the creation of our critical infrastructure and application deployments in order to minimize MTTR (Mean Time to Repair) in the event of a disaster

Data Destruction

- Secure and permanent deletion of data is conducted according to the principles established in our Retention and Deletion Policy
- All items of equipment containing storage media or data shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use

Employee Security

- Voxpopme employees are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards
- Employees are required to execute confidentiality clauses within their employment contracts and must acknowledge receipt of, and compliance with, Voxpopme' confidentiality and privacy policies
- Voxpopme utilizes a third party platform to provide regular, mandatory security training to our employees. Topics include clear desk policy, password security, GDPR, anti-phishing and data handling
- All staff are subject to pre employment checks as part of the employment process
- Employee access to systems and information is based on the least-privilege methodology. Access is reviewed and revoked as appropriate in the event of role change or termination
- Voxpopme has, and maintains, a security policy for its staff and requires security training as part of the training package for all staff

Subprocessor Security

- Voxpopme requires Subprocessors to provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide

Business Continuity

- Voxpopme has a Business Continuity Plan, which ensures that we can maintain service and support to our customers in the event of an incident or disaster. The system is based on our ISO27001 framework, and includes full and frequently tested system back-ups

Incident Management

- Voxpopme implements an ISO 27001-based security incident management process to respond to any suspected security incident. Under this process, incidents are raised to Voxpopme's Executive Team to ensure that incidents are managed quickly and efficiently, and that appropriate support and resources are allocated to resolve them

Supporting Documentation Available on Request:

- ISO Certifications
- Software Development Lifecycle
- Network Diagram
- Retention and Deletion Policy
- Remote Penetration Management Report
- AWS SOC3 Certification

For additional information about Voxpopme's security, data or compliance policies and processes, please contact security@voxpopme.com