Rev Information Security & Privacy Program Overview

The following document provides an overview of Rev's Information Security & Privacy program. We advise reviewing this document in its entirety.

Rev.com's advanced platform is a multi-tenant, multi-user, on-demand service providing unbeatable quality, speed, and value to clients and freelancers alike.

Rev.com may be securely accessed 24×7 through any Internet-connected computer with a standard browser, an application program interface (API), or mobile applications.

Objectives

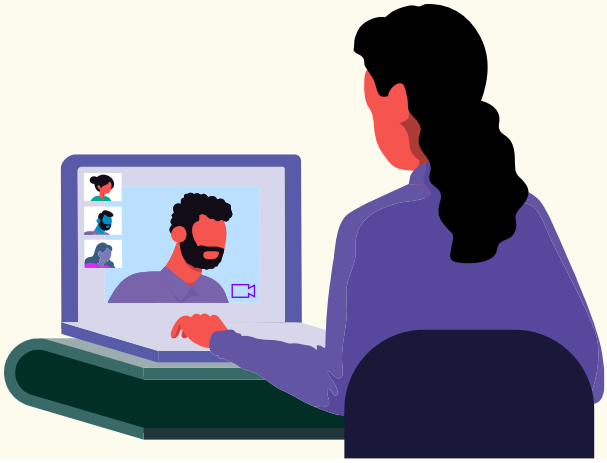
Security is a critical part of our business. With our security & privacy program, we strive to

1. Ensure that customer data is encrypted and inaccessible to other customers and the public.
2. Ensure that customer data is accessible to staff only to the extent necessary to perform the required work.
3. Prevent loss or corruption of customer data.
4. Maintain a redundant infrastructure with 99.9% uptime.
5. Provide timely notification in the unlikely event of downtime, data corruption or loss.
6. Provide continuous training for our staff on proper operation of our systems and best practices for security and privacy.

Our security policies and procedures are reviewed on an ongoing basis by the Rev security team, which is also responsible for their enforcement. All our staff have signed confidentiality agreements.

Information Security

Rev.com uses appropriate technical, organizational and administrative security measures to protect any information in its records from loss, misuse, unauthorized access, disclosure, alteration and destruction. Rev.com uses National Institute of Standards and Technology (NIST) guidelines as a foundation for its security program including



Privacy

Please see the Rev Privacy Policy (https://www.rev.com/about/privacy) for details on how Rev.com treats personal information and complies with privacy regulations.

Personally Identifiable Information

Rev follows best practices handling Personally Identifiable Information (PII) with guidance from the published General Data Protection Regulation (GDPR).

Rev never stores credit card information. Rev maintains a PCI certification for payment processing. Rev works with PayPal to ensure that all payments are secure and encrypted.

Employees

Employees are restricted to handle data required to perform their job. Our staff is trained on proper use of our systems and best practices for security & privacy. All employees have completed background checks and have signed confidentiality agreements.

Transcriptionists & Captioners

Revvers (our transcriptionists, captioners, etc.) are vetted through a rigorous screening process and receive training. All Revvers have signed NDAs and strict confidentiality agreements.

While actively working on a file, Revvers are required to use our secure and proprietary tools, only accessible through a web-based portal.

Revvers cannot download audio, video or transcript files as a general rule (configuration can be modified regarding audio/video download if the customer requests it). They are required to have a valid username and password.

Technical controls exist to block Revvers from accessing Rev.com while using VPN technology. If their account is deactivated, they are locked out of all platform customer resources including forums. All Revver account modifications and customer data access are logged.

Third Party Marketers

We do not share or sell information we collect to third party marketers.

Secure Infrastructure

All Rev.com services are hosted by Amazon Web Services (AWS). AWS maintains strict physical access policies that utilize sophisticated access control mechanisms.

Environmental controls such as uninterruptible power and non-destructive fire suppression are integrated elements of all data centers.

Secure Infrastructure (cont.)

Rev.com's infrastructure spans multiple AWS availability zones for high availability and utilizes amazon S3 for storage of data (https://docs.aws.amazon.com/AmazonS3/latest/dev/DataDurability.html). AWS provides Distributed Denial of Service (DDoS) services.

Storage & Transmission

All customer files are encrypted both at rest and in transit. Communications between you and Rev servers are encrypted via industry best-practice protocols TLS 1.2 and AES-256. TLS is also supported for encryption of emails.

Backup & Recovery

Rev backs up data constantly to prevent any loss or corruption. All Rev & customer data is hosted at Tier IV or III+, SSAE-16, PCI DSS, or ISO 27001 compliant facilities in the United States.

Data Control & Deletion

Customers can purge video, audio, and/or document data from Rev systems at any point via the User Interface (UI) and can set up automated deletion policies via a support ticket.

Software Development Lifecycle

As a cloud service company, Rev.com releases software frequently so that clients may benefit from on-going development of new service and security capabilities. Rev.com follows a defined Software Development Lifecycle (SDLC) that includes the application of security-by-design principles. Rev operates using an agile development methodology under which software development teams and management are tasked with ensuring that the SDLC process and design principles are followed.

Secure Service Operations

Access to production infrastructure is managed in keeping with Role Based Access Controls (RBAC) and "Least Privilege". Access is limited to the Rev.com operations team. Sensitive product service data stored in service databases never leaves the production system.

Firewall rules are maintained so that production systems can only be accessed for maintenance from defined Rev.com locations using secured access mechanisms. Systems are maintained in a hardened state with defined baselines for all host and network equipment. All changes to systems are tracked and managed according to well-established change management policies and procedures. The patch level of third-party software on systems is regularly updated to eliminate potential vulnerabilities.

Availability & Access

We maintain a redundant infrastructure with 99.9% uptime. All customer data is accessible to staff only to the extent necessary to perform the required work. And just like our customer support, our Security Team is on call 24/7 to respond to security alerts and events.

Breach Detection and Response

Rev.com utilizes network Intrusion Detection Systems (IDS) and network integrity management tools to continuously monitor the state of the system. Availability is continuously monitored using external monitoring tools. Application and infrastructure logs are aggregated and archived centrally, facilitating both analysis for suspicious access patterns and future forensic analysis. Regular external vulnerability scanning is also performed.

In the event of a breach, Rev.com has the ability to isolate components of the system for containment and maintain ongoing operations. Rev.com's incident response team is at the ready to notify customers of security impacting events