Otter.ai SECURITY

Security is first priority for Otter.ai. We understand that you have entrusted us with sensitive data, and we protect it accordingly. This page describes the security measures we take to protect your data.

Physical Security

Otter.ai uses Amazon Web Services (AWS) for storage and compute services. AWS has globally recognized certifications including ISO 27001, CSA, SOC 1 and SOC 2. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state-of-the-art intrusion detection systems, biometric locks, and other electronic means. Only authorized personnel have access to the data centers.

Cloud Security

Otter.ai uses Amazon Web Services (AWS) as their cloud provider. AWS consistently achieves the security standards required for our hosted platform and our customer's needs. AWS is committed to protecting the security and confidentiality of its customers' content.

Database Security

Otter.ai hosts your data in a secure database. Only two administrators have access to this database as required by their job function. This database can only be accessed via VPN servers and via secure remote connection enforced by multi-factor authentication.

Communications Security

All communications with Otter.ai via our web application or APIs are transmitted over secure encrypted connections.

All server-to-server communications within Otter.ai infrastructure are encrypted using TLS 1.2.

Otter.ai Security

Perimeter Security

To block unauthorized system access we utilize firewall controls available natively via our cloud provider, Amazon Web Services.

Data Security and Backups

We use Amazon Simple Storage Service (S3) for backups. All data is written to multiple disks instantly across our US-based AWS datacenter. Additionally, this data is encrypted at rest with (AES) 256.

Business Continuity & Disaster Recovery

Otter.ai services are highly available and fault-tolerant, providing resiliency against a multitude of adverse impacting events. Otter services are hosted on Amazon Web Services (AWS) and are designed using clustered services, allowing us to provide you with assurance that our services will be available when you need them.

FAQ's

Can we get our data out of your service?

Upon cancellation of our services, you may request a return of Customer Personal Data up to 90 days after termination of the Terms outlined in the Data Processing Attachment listed in the Appendix of our Terms of Service. If requested, we can provide information assets and user company data (recordings, transcripts).

How do you protect your services from external attacks?

We have implemented information security best practices to protect our services. We mitigate unauthorized access, conduct logging and monitoring, and manage vulnerabilities. These protective measures are audited by external firms.

Is our data backed up? How often?

Your data is fully backed up using automation.

How can I report incidents?

We encourage users to report incidents to support@otter.ai.

Are you transparent with the way you use and access our data?

The usage of your data is outlined in the Privacy Policy. While the Privacy Policy goes into more detail, here is a quick summary of the data that we or our trusted vendors collect:

Name
Billing Address
Payment Information
IP address
Device IDs
Carrier Type
Device Model
Brand
Web Browser Used
Operating System

Please note payment information is not shared with us and is maintained by our payment processing vendor.

Access to customer data is strictly controlled and logged via the usage of access control policies and monitoring our Security Operations Center provides. We exercise the utmost diligence to ensure access to customer data is only for business purposes.

How will I be notified if there is an incident involving our data?

We will notify any impacted customers as soon as we become aware of a personal data breach involving customer personal data. We utilize documented internal procedures to ensure that impacted clients are provided continual updates until the issue is rectified.

Are other vendors used to provide services to customers?

To provide our customers with high service levels and a high-quality solution, we utilize a select group of vendors. The list of vendors that we currently use can be found here.

How do you ensure your services are reliable?

We deploy best-in-class architecture design of our services that incorporate redundancy and resiliency concepts. Amazon Web Services provides us with an additional layer of assurance that the best-in-class architecture that we deploy resides on highly dependable infrastructure with proven uptime of 99.99%.

Do you align with a cybersecurity framework to minimize the risk of a data breach?

Otter.ai's security program aligns with the NIST Cybersecurity Framework (NIST CSF, or CSF).