Recapped

Your security is our top priority

We take your security seriously. Recapped is built for the enterprise and has been focused on enterprise-grade security since day one.

We're cognizant of the fact that far too often, too little thought has been given in enterprise sales organizations around data privacy and security with regard to the mutual plans your team is sending via email today.

Recapped is built to not only accelerate your deal cycles, but also drastically improve security and communication channels in place with clients. Recapped enables end-to-end admin, end-user, and client controls. We have full access logging, content security, and secure all data and information with the following core policies below.

Core Infrastructure and Data Security Overview

Physical Security

Recapped is hosted on AWS (Platform as a Service) providing customers with robust data center security and physical environment controls.

Data Encryption

Recapped ensures your sensitive data is fully segregated and encrypted on AWS using AES-256 industry standard encryption.

Data Usage

Recapped does not sell or otherwise utilize your data for third party advertising purposes in any way.

Data Privacy

We only use customer data to provide you and your clientele the service. We have access controls in place, and do not look into your account without your permission.

Data Recovery

Your data is automatically and routinely backed up in our AWS hosted databases for up to 7 days.

Data Ownership

Your data belongs completely to you. Recapped never deletes data in your account without your permission, and without giving you reasonable time to export it first.

Database Security

Recapped stores your data in its own secure database hosted on AWS, which is managed according to security best practices and security compliance standards.

Integrated Services

Recapped does not access or store or access any of your passwords. We leverage OAuth2 to securely authorize your third party SaaS services with your explicit permission.

Privacy and Safety Features

We are always working to include new privacy features to allow our users to have control over what information is shared with Recapped or with their clients.

Security Operations

Recapped is proud to never have had a security incident in our history. But if an incident were to occur, Recapped is committed to reacting and remediating the issue immediately.

System Security

Recapped is consistently monitoring and updating our systems to ensure your data is protected and that our images, application infrastructure and configurations are up to date.

Restricted Access

We restrict access to key personnel. Our production system access is limited to key members of the Recapped engineering team.

Logging

We log all interactions with our application in AWS and are commited to constantly improving the way we store and track issues in our application.

Application Level Security

Recapped leverages containerized technology, allowing us to act quickly to resolve any issues with our instances in case of failure. In addition, our databases and servers are separated to prevent and avoid single points of failure.

Network Security

In addition to our infrastructure, we take multiple steps to prevent eavesdropping between your systems and ours. All network traffic runs over SSL and HTTPS.

Internal IT Security

We take maximum precautions to protect our own systems. Recapped offices are protected behind mandatory network firewalls from well-known security vendors and premises access is secured by keycards.

Additional Enterprise-Level Features

Engagement Tracking

To ensure the right end-users are accessing your workspaces, users are notified in real-time whenever content is engaged. All customer engagement is tracked and logged.

Unique Generated Hashed Links

Access to Recapped workspaces are not searchable on the internet, and workspaces are protected with uniquely generated hashes to ensure security.

Content Timeout Policy

Your content is only accessible via the Recapped platform and access to uploaded resources is limited to 15 minute session timeouts.

Password Protection

To ensure further access to workspaces, users will be able to set and manage unique passwords.

Administrative Access Controls

Recapped provides company-wide team permissions and admin user controls including creation, modification, and deletion of data and users.

User Access and Content Controls

Recapped enables users to fully control external client access to your content, comments, and activity trails.

Single Sign-On (SSO)

Easily manage user login and sessions through Okta SSO, ensuring only authorized employees have access to Recapped platform.

Regulatory Compliance and Legal

GDPR Complicance

We are taking continuous steps to uphold General Data Protection Regulation (GDPR) standards. Please contact us if you plan to use Recapped in the EU or UK.

CCPA Compliance

Recapped is fully committed to be compliant with guidelines outlined in the California Consumer Protection Act (CCPA)

Privacy Policy

Recapped takes the privacy of our customers very seriously. Access our full privacy policy here

Account Cancellation

In the event that we part ways, we'll make sure your data is safe. To cancel or delete your data, please contact your account manager or the Customer Success team. Cancelling your account will grant access to historical data within Recapped. Recapped can delete your data upon request.

Have additional questions? Simply reach out to your Account Manager or email security@recapped.io