

# Recording and Video Content Storage and Encryption

Here's what RP1Cloud holds on to: recordings made by meeting hosts, and the login data including time-stamps for meeting attendees. This information is stored, with full redundancy and security, at an automated SAS 70 II cloud datacenter. RP1Cloud uses role-based Access Control mechanisms that restrict access to specific objects containing ePHI.

During a call, RP1Cloud does not record any part of the meeting itself. The only time a meeting is recorded is when the meeting host uses the recording feature. That recording is encrypted and held in our secure datacenter. It is ONLY available for download (no streaming) after the proper authentication procedure.

Uploaded shared video content is also stored in secure containers. The video content sharing stream is encrypted (AES-128bit) when shared in a meeting. Users may also choose to delete their uploaded video content from our service as well.

Recordings are only accessible to the recording originator. Hosts can upload and share full-motion video content in your meetings. They can choose to record and share meetings.

Recordings may be downloaded to an on-premise media server or storage device. Users may choose to delete their recordings at any time using the web user interface.

## Application-Level Security

### User Account Security

- Each RP1Cloud account is secured with a standard username and password
- Authentication requests are always sent over HTTPS
- Passwords are never sent via email or any other form of electronic transmission (the "Forgot Password" feature only allows for resetting the end-user's password)

### In-Meeting Security Features

**Meeting access** is protected by unique personal authenticators – email, conference ID and multi-tiered passwords, even when RP1Cloud is in emergency mode.

RP1Cloud meetings come with optional security capabilities that users may set as default or enable when required:

- **Encrypt Meeting Option** – an option that forces an RP1Cloud meeting to only allow end points with sufficient encryption capabilities enabled.
- **Expel Participant** – during a meeting, any participant can be removed from the meeting with a click of a button.
- **Lock Meeting** – The host can mute and remove attendees, and can lock meetings so that no one else can join.
- Meetings are **private** by default, and require an invitation and the above info to get in.
- There's an **auto-logout** if meetings haven't been properly ended, and meeting hosts can terminate sessions in progress.
- Only meeting hosts can **start and stop recording** a meeting and all presented content.

# Application-Level Security (Cont'd)

## Global Facilities Security

The RP1Cloud service is powered by Polycom and consists of software that runs on cloud-compute clusters from a leading global server vendor. It is deployed and managed across multiple Tier-1 co-location data centers around the world. They are equipped with the following security features:

- **Physical Security:** 24x7x365 onsite monitoring and physical security, including biometric identification mechanisms.
- **Power:** two or more power supplies from different power providers; Onsite generators and reserve fuel supplies
- **Bandwidth:** redundant 1-Gpbs (minimum) connections to the public internet supplied by Tier 1 bandwidth vendors
- **Fiber connectivity:** Data centers feature numerous and diverse points of entry (POE) into the building, offering pathway diversity and total flexibility in terms of service providers
- **Cooling:** redundant cooling (air conditioning) systems
- **Diesel fuel farm:** environmentally-compliant diesel fuel storage facilities, which house fuel for generators to ensure 7x24x365 operation during any emergency
- **Water:** redundant cooling water supplies
- **Fire Suppression:** redundant automated fire suppression systems
- **Diverse Rise Systems:** secure, diverse and redundant pathways which run through the building offering diversity for network security. The riser systems have 2-hour fire ratings and all riser rooms are under CCTV 24/7/365 surveillance, with alarmed door entry. Access is restricted, regulated and fully secure
- **Data Replication:** data is stored redundantly within the center, and/or offsite depending on deployment

## Infrastructure and Network Security

RP1Cloud employs a wide range of security management practices to provide a secure and reliable service to customers. This includes network firewalls throughout the infrastructure to create security zones for different applications and services. RP1Cloud also deploys proxy servers that terminate all 3rd party / customer traffic at a proxy layer. All web traffic passes through industry-leading load balancers to protect against a suite of application attack vectors.

Beyond the firewall, proxy servers and load balancers, RP1Cloud also periodically scans for network, port, and application-level vulnerabilities. Furthermore, all of the 3rd party applications and operating system software is checked for security advisories and is patched periodically.

Routers, firewalls, load balancers, and proxy application servers are all configured to mitigate numerous types of DOS attacks.

# Security assurances and controls

The RP1Cloud service is delivered and maintained with an infrastructure (i.e. **Data Centers**) boasting the following certifications or specifications:

- SSAE 16
- ISAE 3402
- CSAE 3416
- SOC 1 Type II
- SOC 2 Type II
- ISO 27001
- NIST 800-53
- SP 800-53
- PCI DSS
- COBIT
- Industry-leading, high average uptime track record of >99.999% globally

Should you require more information, please contact us at [privacyoffice@rp1cloud.com](mailto:privacyoffice@rp1cloud.com).

## Media Handling & Encryption

We use a three-tiered AES encryption system which encrypts data on the user's computer, again in transit and finally when at rest in our storage datacenters.

## Privacy and Customer Data Storage

### User Profile Details

RP1Cloud stores the following user information:

- Username
- Password
- Email address
- First name
- Last name
- Company name

### Billing Details

RP1Cloud does not allow for the handling or processing of billing transactions.