How we approach security

“SecureMeeting is on a mission to provide the safest meeting place on the Internet. Our stance is to **never share** any user-identifying data, which includes names, user-profiles, chat-logs, passwords, emails or video-recordings. We are committed to being transparent about our security practices and helping you better understand our approach.”

Organization Security

SecureMeeting’s industry leading security program is based on the concept of defense in depth: securing our organizational and user data at every layer of the stack. Our security program is formulated to help you remain compliant with HIPAA, FINRA, ISO 27000, FedRamp, AIPCA Trust and NIST standards. Our security protocols continuously evolve with updated guidance and industry best practices.

We constantly seek input from advisors, comprising of world renowned experts and scientists, who offer regular oversight and guidance on design, implementation, and management of our security protocols. The internal members of team SecureMeeting focus on security architecture, product security, security engineering and operations, detection and response, and risk and compliance.

Shared Security Model

We do our part. We assume you do yours.

Before covering the details of how we secure our resources, it is important to understand that security is a *shared* responsibility between you and SecureMeeting.

SecureMeeting is responsible for securing the underlying infrastructure that supports video, audio, chat, and at-rest data including passwords and room security. It is your responsibility to take precautions necessary to not broadcast your room link to untrusted parties, and to exercise caution when publishing room credentials on social media, group emails, chat messengers and public forums, where visibility of this information can potentially reach individuals who want to inflict harm. This shared security responsibility model can reduce your operational burden in many ways, and in some cases may even improve your default security posture without additional action on your part.

Not all conversations are made equal. If your conversation is highly sensitive, we urge you to take the extra precautions necessary to secure things on your end.

This includes carefully choosing who you share room names and passwords with, and how you choose to share this information by choosing the right medium. Passwords should be at least 10 characters long, and must include uppercase and lowercase letters, numbers, and special characters to increase the complexity required to second guess. Additionally, we also encourage the host to *change* the password of a room as soon as attendees join the conversation. This further prevents any one of your attendees from potentially compromising room credentials.

Protecting User Data

Securing data at-rest and in-transit

The focus of SecureMeeting's security program is to prevent unauthorized access to user data ("stealing"). Such data includes a live session in progress, participant names, IP addresses, emails, passwords, chat logs and session information.

I. Anonymous by Default

SecureMeeting is built around the central idea that all of our users are anonymous by default, and have the right to remain anonymous throughout the life cycle of interaction with the product. At no point are you *forced* to disclose who you are. In this anonymous mode, you will give up zero data about yourself.

The simplest way to use the product anonymously is to create an ad hoc "room", go live immediately, and invite people to this room using tools *external* to SecureMeeting (e.g., email or encrypted chat applications). When a session is live, we assign random names to all participants based on Pokemon characters. When you are done with your conversation, simply close the browser tab. This form of interaction ensures that no personally identifiable information ever crosses our path, and that there remains nothing to be collected, shared, or stolen. This simple life cycle, which is available to every user on our product, ensures complete anonymity.

Both the host initiating a room, as well as attendees who join a room, have the option of going anonymous. The only time anonymity does not work is when a host invites attendees to their "personal" room – a persistent room owned by the host who requires attendees to announce who they are before being let into the room.

II. Choosing to Sign-Up

Creating an account has longer term benefits beyond the anonymous mode. This could include scheduling meetings for later, viewing all your upcoming meetings in a simple dashboard, adding friends, inviting friends to your room, choosing a persistent display name, having your own persistent room(s) with immutable addresses, choosing background images, and choosing custom caricatures when a session is in progress. This kind of "state" information is only possible if you choose to create an account with us.

This "state" is persistently stored in our backend and constitutes data at rest. We next look at what is stored on our servers, and how we secure data at rest.

III. Minimizing Data "At Rest"

By default, we collect no user identifying data. Even when a user chooses to sign in, our collective goal is to collect as little data as possible.

Anonymous mode: When the host and attendees choose not to sign into the product, no data is retained on our server. All state information is destroyed when the session comes to an end. During a session, however, the following information is stored on the server:

- Temporary names assigned to participants. Default names are randomly generated for every participant from a list of 'Pokemon' characters, which the user can change. This name is tied to every participant and stored on our server for the duration of the session.
- Chat logs from both public and private chat.
- *All of the data pertaining to a session is destroyed when the session comes to an end.*

Sign-in mode: When using a sign-in option, the following credentials are *persistently* stored on our server:

- Login email
- Password
- Upcoming (scheduled) meeting time and associated meeting link
- User selected preferred background image (to hide live background)

Note that we do not store chat logs or any other session generated data like video or audio even when users choose to sign in. We also do not support video recordings on our site for these same reasons.

Session Analytics: We collect bare-bones analytics to help us anticipate trends and site usage across the world. This helps us prepare for unexpected surges, provision our servers and plan future server deployments in different parts of the world. We store trends such as the number of sessions we host, countries of origin, and session durations. *We do not, however, store any personally identifying information on our servers (names, IP-addresses, etc.).*

IV. Securing Data "At Rest"

State information pertaining to sign in and temporary session information in anonymous mode constitute data at rest. On our production network, this data is encrypted using FIPS 140-2 compliant encryption standards.

Our approach to securing this information is to apply three levels of encryption, which we detail below:

- ***Level 1: Securing raw data.*** Login/password and minimal state information is secured as soon as data is generated before they are stored. This data is encrypted using Bcrypt and PBKDF2, in compliance with NIST special publication (NIST SP 800-132).

- ***Level 2: Securing storage.*** Raw encrypted data is further pushed to a secure database (DB). At the DB level, we employ **`AES256-CBC`** (or 256-bit Advanced Encryption Standard in Cipher Block Chaining mode) via OpenSSL using a symmetric key. We also employ this level of storage security for all transient session-specific data, including public/private chat-logs and anonymized user names. Transient data, as previously noted, is destroyed at the end of every session.
- ***Level 3. Server Level Security.*** We employ a collection of cloud hosting platforms, including AWS, Azure and/or Google for redundancy and availability. Each of these platforms provide key management services (KMS) as well as use hardware security modules that are validated under FIPS 140-2.

V. Securing Data "In Transit"

An overwhelming majority of the data generated when using the product is "in transit" (i.e., live on the wire). Specifically, this data comprises video, audio, text, and screen sharing while a session is in progress.

Network Security
Our approach is to secure data at every layer of the networking stack, ranging from application, session, transport, and network.

Data in transit is encrypted in three layers: transport (DTLS), session (SRTP), and application (HTTPS). Much of our video streaming is thanks to WebRTC, which comes with its own layer of end-to-end encryption.

Network Architecture
A network segment is a path between any two end points, and a network path is derived by stitching together relevant segments. Data within a network segment is end-to-end encrypted. A typical live session consists of participating hosts ('end-hosts'), aided by a selective forwarding unit

(SFU). In this mode, a network path comprises of a segment between a source-node and SFU, and then the SFU and destination node. We encrypt data at every layer within each segment. By path stitching segment level encryption, we are able to provide end-to-end encryption and thwart ‘man in the middle’ attacks.

Network Access & Server Hardening

We divide our network systems into separate networks to better protect sensitive data. Systems supporting testing and development activities are hosted on separate networks/servers from our production environment. All servers in the production fleet are “hardened” (i.e., disabling unnecessary ports, removing default passwords, disabling testing accounts, etc.,). Our server images also have a base configuration applied to ensure consistency.

Network access to our production environment from public, open networks (Internet) is restricted, with only a small subset of servers accessible. Only protocols essential for delivery of SecureMeeting’s service to its users are open at our perimeter and there are mitigations against distributed denial of service (DDoS) attacks deployed at the network perimeter. Additionally, for host-based intrusion detection and prevention activities, SecureMeeting logs, monitors, and audits call volumes and has alerting in place for system calls that indicate a potential intrusion.

Compliance

Healthcare, Finance, and Federal Regulations

The focus of SecureMeeting’s security program is to provide a microservice that helps you build compelling, immersive, and video-first solutions in the consumer, enterprise, healthcare, finance, federal, and educational sectors.

If you plan on using SecureMeeting for healthcare, finance, or federal needs, learn how we help you remain compliant by sending an email to compliance@securemeeting.org.

In this section we briefly touch upon our security practices to give you an overview of how we help you remain compliant.

I. HIPPA

The core requirement for HIPPA compliance is to protect all electronic health personal information (e-PHI) of patients, as well as secure their interactions with healthcare providers and insurance companies.

II. FINRA

FINRA recommends that any information transmitted over the internet be encrypted. Since SecureMeeting is a connection between two parties over the internet, it is essential to keep this data in transit encrypted. As mentioned earlier, webRTC mandates encryption using DTLS-SRTP to encrypt media. FINRA recommends these measures for any network that the firm does not manage. In addition FINRA recommends that firms use connections that utilize an HTTPS connection.

III. FedRAMP

We recommend our customers to pursue a tailored authorization from FedRAMP. Our microservice can be configured to store no user data, so it could be classified as a low impact software as a service (SaaS). With this classification we remain compliant by operating in a fully operational cloud environment, being accessible as SaaS, not containing any personally identifiable information (PII), having a low security impact, and being hosted within a FedRAMP authorized platform as a service (PaaS) or infrastructure as a service (IaaS).

IV. Internal Procedures to help you remain compliant

We next talk about internal policies and procedures we have put in place to help you remain compliant while using SecureMeeting for your business needs. This includes endpoint security, access control, system monitoring, data retention, and data disposal.

Access Control
To minimize the risk of data exposure, SecureMeeting adheres to the principles of *least privilege* and *role-based permissions* when provisioning access—employees are only authorized to access data that they reasonably must handle in order to fulfill their current job responsibilities. All production access is reviewed at least quarterly. Employees with access to authorized data who are terminated and/or resign give up access to such data. Typically, passwords and public/private keys are reset and accounts related to parting employees terminated.

Password Management
SecureMeeting requires personnel to use an approved password manager for devices/computers used to write production grade code. Password managers generate, store, and enter unique and complex passwords to avoid password reuse, phishing, and other password related risks.

Data retention and disposal
When using SecureMeeting in the anonymous mode, no data is collected or retained. When customers choose to create accounts, customer data is removed immediately upon deletion by the end user or upon expiration of data retention as configured by the customer administrator. SecureMeeting hard deletes all information from currently running production systems and backups are destroyed with immediate effect.