Google Meet

Meet Security

Secure meetings for your organization

Take advantage of the same secure-by-design infrastructure, built-in protection, and global network that Google uses to secure your information and safeguard your privacy. Our array of default-on anti-abuse measures keep your meetings safe.

Privacy

- Meet adheres to the same robust privacy commitments and data protections as the rest of Google Cloud's enterprise services.
- We do not use customer data for advertising or sell customer data to third parties.
- We undergo regular rigorous security and privacy audits for our Cloud services, including Meet.
- Meet does not have user attention-tracking features or software.

Encryption

- All data in Meet is encrypted in transit (IETF Standard) by default between the client and Google for video meetings on a web browser, on the Android and iOS apps, and in meeting rooms with Google meeting room hardware. If you join a meeting by phone, audio is carried by the telephone network and might not be encrypted.
- Meet recordings stored in Drive are encrypted at rest by default.

Counter abuse

- We employ a vast array of counter-abuse measures to keep your meetings safe. These include anti-hijacking measures for both web meetings and telephony dial-ins.
- Our meeting codes are 10 characters long, with 25 characters in the set. This makes it harder to brute force "guess" meeting codes.
- External participants can join directly, only if they are on the calendar invite or if they have been invited by in-domain participants from within the Meet session.
- Any other external participants must request to join the meeting, which must be accepted by a member of the host organization.

Google Cloud

For more information visit **g.co/gsuite/meet**

Google Meet

Secure Deployment & Access

- For users on Chrome, Firefox, Safari and new Edge we don't require or ask for any plugins or software to be installed, Meet works entirely in the browser. This limits the attack surface for Meet and the need to push out frequent security patches on user machines. On mobile, we recommend that you install the Meet app from the App Store or the Play Store.
- Meet users can choose between multiple 2-step verification options or enroll their account in Google's Advanced Protection Program (APP). APP provides our strongest protections available against account hijacking.

Controls

- We offer Access Transparency as part of G Suite Enterprise - a feature which logs any Google Admin access to 'Meet recordings' stored in Drive, along with the reason why that access happened.
- Meet recordings in Drive can be stored in specific regions via Data Regions (video transcodes, processing, indexing, etc. are not covered)
- With Google Vault, admins can set retention policies for Meet recordings. This can be useful to help fulfil legal obligations.

Compliance

- Our products, including Meet, regularly undergo independent verification of their security, privacy, and compliance controls, achieving certifications, attestations of compliance, & audits against standards around the world.
- Our global list of certifications and attestations can be found here. They include SOC 1/2/3, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, FedRAMP Moderate ATO, HIPAA compliant use, HITRUST CSF, GDPR, Privacy Shield Framework (EU-U.S. & Swiss-U.S.), BSI C5 (EMEA), ENS High (Spain), MTCS Tier 3 (Singapore), OSPAR (Asia Pacific), and CSA STAR.

Reliability

- Google's network is engineered to accommodate peak demand and handle future growth. Our network is resilient and engineered to accommodate the increased activity we've seen on Meet. By leveraging Google's global infrastructure, Meet can scale quickly and efficiently to satisfy demand.