Technical and Organizational Measures
GoTo Meeting, GoTo Webinar, GoTo Training and GoTo Stage

Executive Summary

This Technical and Organizational Measures (TOMs) document outlines GoTo's commitments to privacy, security, and accountability for GoTo Meeting, GoTo Webinar, GoTo Training and GoTo Stage. GoTo upholds comprehensive global privacy and security programs, along with organizational, administrative, and technical safeguards designed to:

- Ensure the confidentiality, integrity, and availability of Customer Content.
- Protect against threats and hazards to the security of Customer Content.
- Prevent any loss, misuse, unauthorized access, disclosure, alteration, and destruction of Customer Content.
- Maintain compliance with applicable laws and regulations, including data protection and privacy laws.

These measures include:

- **Encryption**:
  - *In Transit* - Transport Layer Security (TLS) v1.2 or higher.
  - *At Rest* - Advanced Encryption Standard (AES) 256-bit for Customer Content.
- **Compliance Audits:** GoTo Meeting, GoTo Webinar and GoTo Training holds SOC 2 / SOC 3 Type II, BSI C5, PCI DSS, TRUSTe Enterprise Privacy certifications, Internal controls assessment as required under a PCAOB annual financial statements audit, Global CBPR and PRP certifications, and APEC CBPR and PRP certifications.
- **Legal/Regulatory Compliance:** GoTo maintains a comprehensive data protection program with processes and policies, designed to ensure Customer Content is handled in accordance with applicable privacy laws, including the GDPR, CCPA/CPRA and LGPD.
- **Penetration Testing**: In addition to in-house testing, GoTo contracts with external firms to conduct penetration testing.
- **Logical Access Controls:** Logical access controls are implemented and designed to prevent or mitigate the threat of unauthorized application access and data loss in corporate and production environments.
- **Data Segregation**: GoTo employs a multi-tenant architecture and logically separates Customer accounts at the storage layer.
- **Perimeter Defense and Intrusion Detection**: GoTo employs advanced perimeter protection tools, techniques, and services to prevent unauthorized network traffic from accessing its product infrastructure. The GoTo network is safeguarded by externally facing firewalls and internal network segmentation to ensure robust security.
- **Data Retention**:
  - GoTo Meeting, GoTo Webinar, GoTo Training and GoTo Stage Customers may request the return or deletion of Customer Content at any time, which will be fulfilled within thirty (30) days of Customer's request.
  - For GoTo Meeting, GoTo Webinar and GoTo Training, Customer Content will automatically be deleted between ninety and one hundred (90-100) days after expiration of a customer's then-final subscription term.

Contents

1 Product Introduction

GoTo Meeting, GoTo Webinar, GoTo Training and GoTo Stage (together, the "Service") are online communication solutions that enable individuals and organizations to interact using various features, depending upon service offering, including desktop screen sharing, video conferencing, chat, and integrated audio. GoTo Meeting, GoTo Webinar, GoTo Training, and GoTo Stage share infrastructure and are delivered via a CDN to web browsers or installable applications.

- GoTo Meeting, GoTo Webinar and GoTo Training enable organizers to schedule, convene, and moderate online sessions including audio, webcam, screen sharing and more using the GoTo web, desktop and mobile applications.
- GoTo Training provides specific features applicable to web-based training, such as online access to tests and materials and a hosted course catalog.
- GoTo Webinar provides special support to conduct one-to-many information presentation events reaching local and global attendees over the internet.
- GoTo Stage is an extension of GoTo Webinar where GoTo Webinar organizers can create customizable channels and publish their webinar recordings. Published recordings are showcased on the GoTo Stage homepage, organized by business categories. At any point, organizers can unpublish their recording through GoTo Webinar, which removes the video from their channel page and the GoTo Stage ecosystem.

1.1 Conference Management and Registration

Organizers can schedule sessions directly within the Service. They can adjust various settings of upcoming sessions and prepare their content and attendees.

1.2 Audio

Integrated audio conferencing for GoTo Meeting, GoTo Webinar and GoTo Training sessions is available through Voice over Internet Protocol (VoIP) and the public switched telephone network (PSTN).

1.3 Video

All products offer high quality webcam video that adjusts to a user's bandwidth and latency.

1.4 Content Uploading (Webinar and Training only)

Organizers can upload files and media for use during sessions, either ahead of a session or once the session has started.

1.5 Session Reporting

Organizers can see participation statistics and other session statistics in their session history.

1.6 Recording and Transcripts

Sessions can be recorded locally and to the cloud. Account administrators and session organizers can choose to enable cloud recordings in addition to or instead of local recordings. Local recordings are stored on the organizer's system and are not subject to GoTo's retention limits.

When this feature is enabled by the administrator and the organizer, cloud recordings are automatically available directly in the organizer's session history and transcripts are automatically created. Session recording transcripts are created using GoTo hosted models For **GoTo Meeting**, an account administrator can choose to enable recordings and decide whether those are stored locally or in the cloud. If cloud recordings are enabled, the meeting organizer can choose to record a given meeting and store it in the cloud. Transcripts are automatically created for cloud recordings.

For **GoTo Webinar**, organizers can choose to auto-transcribe all cloud recordings. Only an organizer can start a recording and if their auto-transcribe setting is enabled, a transcript will be created.

For **GoTo Training**, account administrators can control whether organizers are able to save recordings to the cloud. Account administrators are not able to prevent organizers from recording sessions locally. Trainings cannot be transcribed.

1.7 Business Messaging (Meeting only)

An extension of GoTo Meeting, business messaging allows GoTo Meeting users to see the presence status of other users within their account, exchange instant messages and share files. The account administrator defines the scope for visibility and discoverability of various users.

Business messaging users can see the presence status of any other user within their account once they are included in their contact list. Messages can be exchanged with all members of a team and with external users if they have been explicitly included via an invite by email. External users are business messaging users who are not members of a Customer's internal team (e.g., customer, prospect, or partner). Messages can be direct (between two participants), in a private group or in a public group.

Users can also share other content within business messaging by uploading and downloading files. The shared files are available for download by all users with access to the messages in a given conversation or group.

1.8 Webcast (Webinar only)

GoTo Webinar webcasts use broadcast gateways, third-party streaming engines and content delivery networks designed to reliably deliver screen sharing, audio, and video media to attendees joining from a web browser. The gateways receive media data from the media servers and transcode them into standard codecs. The streaming engine produces HTTP Live Streaming (HLS) at multiple bitrates to enable adaptive delivery for users with sub-optimal network connections.

1.9 GoTo Stage (Webinar only)

Videos published to GoTo Stage are available for discovery on the GoTo Stage homepage and in search engine results, unless the organizer restricts discoverability using the administrative settings on their channel page. Undiscoverable recordings can be accessed by anyone registered to GoTo Stage using a direct URL to the channel or to the video's unique "Watch Now" page. Visitors register for GoTo Stage using their name and email address or may connect via select social media accounts such as LinkedIn, Facebook, and Gmail. The URLs for visitors to access videos are live for a limited amount of time to limit unwanted sharing.

2 Product Architecture

GoTo Meeting, GoTo Webinar, GoTo Training, and GoTo Stage are Software as a Service (SaaS) solution designed for high performance, reliability, scalability, and security. These Services are supported by high-capacity servers and network equipment with appropriate security controls in place and redundant infrastructure designed to preclude single points of failure. Clustered servers and backup systems are in place to support application processes in the event of a heavy load or system failure.

Application/server sessions are load balanced across geographically distributed clusters designed to ensure performance and adequate latency.

The Service infrastructure and data are hosted by cloud hosting providers.

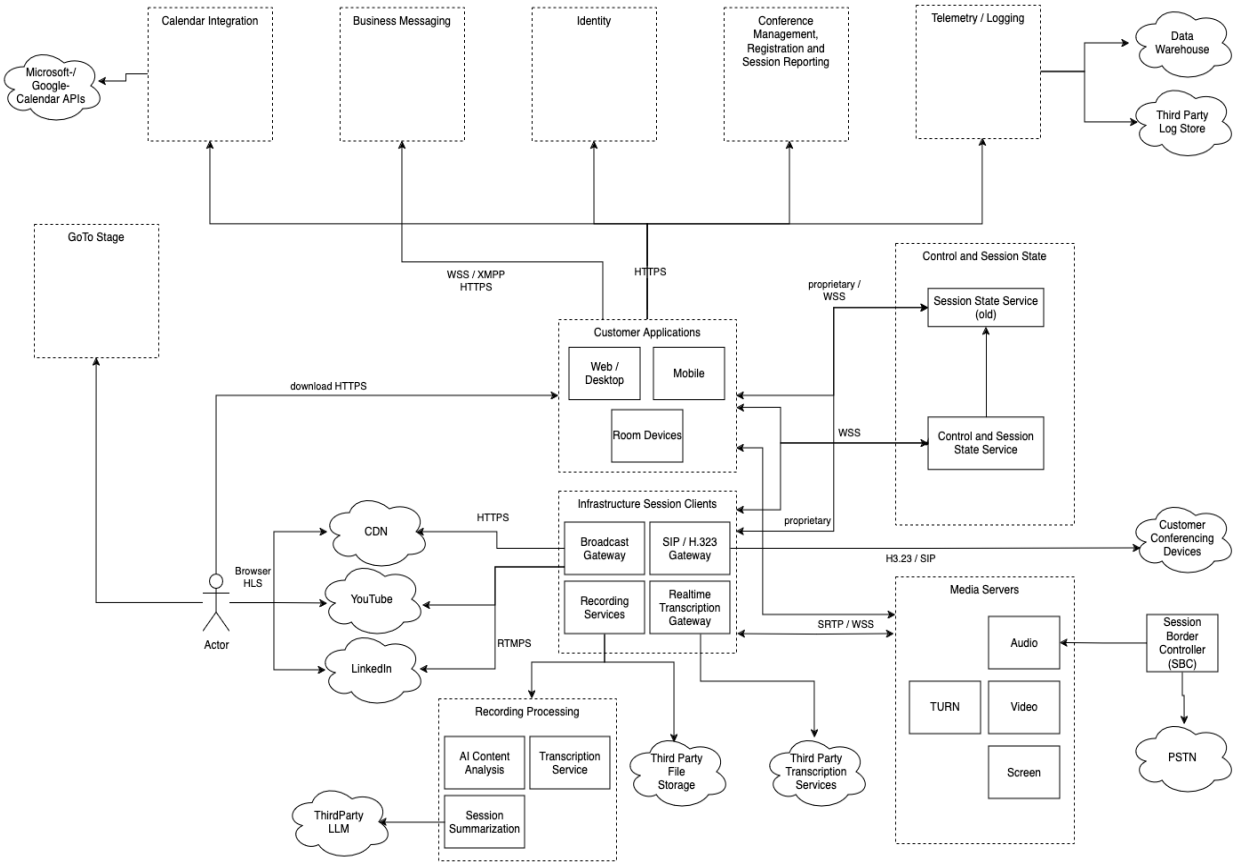

Figure 1: Central Architecture

Customer Applications (GoTo web, desktop and mobile applications or "clients"; a device called GoTo Room (Meeting only)): The Customer Applications provide the Service functionality as described above in Section 1 (Product Introduction).

Identity Services: Manages user accounts and enables secure and standardized account authorization and login.

Conference Management, Registration and Session Reporting Services: Conference Management provides information about scheduled sessions and enables scheduling new sessions and adjusting existing sessions. Registration Services enable registration for sessions where this is required. Session Reporting provides information on past sessions including recordings, transcriptions, attendance and more.

Business Messaging: Management of channels as well as sending, receiving and storage of messages and attachments; used for out of session messaging only.

Calendar Integration: Allows users to synchronize their Microsoft Outlook or Google calendars to get notifications about GoTo sessions.

Telemetry/Logging: Sending of telemetry probes or log statements to help gather usage statics and diagnose issues.

Control and Session State Services: Provide functionality used by client applications to initiate and receive non-media related changes to the session state.

Media Servers: Responsible for receiving, converting and distributing audio, video, and screen sharing content.

PSTN: Public switched telephone network allows users to dial into sessions via physical or IP telephones.

Session Border Controller: Connects GoTo's Voice over Internet Protocol (VoIP) with commercial telephony providers.

Recording Services: Enables recording of session audio, video, screen sharing and business messaging content.

Broadcast Gateway: Used for GoTo Webinar Webcasts and supports layout, transcoding, and packetizing the media streams into HLS streams, which are distributed via CDN to browser-based clients or pushed to RTMP-enabled streaming platforms like YouTube or LinkedIn.

H.323-/SIP-Gateway: Enables connection to session audio via SIP or H.323 conferencing devices.

Realtime Transcription (RTT) Gateway: Provides live transcription of session participants' speech.

GoTo Stage Services: Management of GoTo Webinar video content by organizers; provides viewing experience to visitors.

3 Technical Security Controls

GoTo employs technical security controls that are designed to safeguard the Service infrastructure and data residing therein.

3.1 Encryption

GoTo regularly reviews its encryption standards and may update the ciphers and/or technologies used in accordance with the assessed risk and market acceptance of new standards.

3.2 Encryption In Transit

GoTo implements security measures for data in transit that are designed to protect against passive and active attacks on confidentiality, integrity, and availability. Communications security controls are implemented for screen and video sharing, VoIP, webcam video, keyboard/mouse control, text-based chat information and other session data.

GoTo uses Internet Engineering Task Force (IETF)-standard TLS protocols to protect TCP communication between endpoints.

HTTPS and WSS are used to protect non-media data, while in-session media data is protected by SRTP, WSS, or DTLS.

Internally, GoTo also uses mutual certificate-based authentication (mTLS) on servers that handle media data.

3.2.1 Audio and Video Security

An SRTP-based protocol using standard encryption mechanisms that leverage AES128 at a minimum is used to protect the confidentiality and integrity of VoIP connections between the endpoints and servers.

3.2.2 Website, API, and Internal Web Service Security

All connections to the Service websites, APIs and internal web services are protected using TLS. This includes Content Uploading, Session Reporting, Recordings and Transcripts, and others.

3.2.3 Business Messaging

Presence updates, messages, and files are transferred via a TLS-secured channel to chat services and onward to users. File content is made available through cryptographically signed URLs that link to the content.

3.2.4 Webcast Security (Webinar only)

Webcast streaming gateways forward traffic to the streaming engine over SRTP, all within GoTo's secure internal network. CDNs pull data from the streaming engine securely over HTTPS. The clients also pull data securely from CDNs over HTTPS.

3.3 Encryption at Rest

3.3.1 Profile Data

The content is stored in a relational database with AES 256-bit encryption.

3.3.2 Conference Management, Registration and Session Reporting

The content is stored in a relational database with AES 256-bit encryption.

3.3.3 Content Uploading

Uploaded content and related metadata are stored in AWS S3 and Amazon Dynamo DB, all with AES 256-bit encryption. Additionally, metadata is stored in Apache Cassandra and Amazon Aurora without encryption at rest.

3.3.4 Recordings and Transcripts

Cloud recordings are stored in AWS S3. Files are encrypted at rest using server-side encryption with AES256. Audio files for transcription are encrypted using AES256.

3.3.5 Business Messaging Security

Messages are stored in an AWS Aurora database, and shared files are stored in AWS S3, both with AES 256-bit encryption at rest.

3.3.6 GoTo Stage

This uploaded content and related meta data is stored in AWS S3 with AES 256-bit encryption. The metadata is stored in Apache Cassandra and the search index in Elasticsearch, both not encrypted at rest.

3.4 Firewall and Proxy Compatibility

The installable clients include built-in proxy detection and connection management logic to help automate software installation, avoid the need for complex network (re)configuration and maximize user productivity. Firewalls and proxies already present in a user's network generally do not need any special configuration to enable use of the Service.

For more details, and the exact domains, IPs and ports used, please visit the respective support pages for Meeting, Webinar and Training.

3.5 Installable Client Security Features

The installable clients are designed with appropriate security features and employ strong cryptographic measures, including signed endpoint software and "client-only" connections.

3.5.1 Signed Endpoint Software

The Service's executables are digitally signed for integrity protection and authenticity. GoTo's client application software follows appropriate quality control procedures, configuration management procedures, and a Secure Development Lifecycle (SDL) model during development and deployment.

3.5.2 "Client-only" Connections

To reduce the risk that remote systems can target them with malware and viruses, the installable clients are not configured to receive inbound connections. This helps protect users participating in a session from being infected by a compromised host used by another attendee.

3.5.3 Cryptographic Subsystem Implementation

Cryptographic functions and security protocols implemented in the installable clients use the open source BoringSSL or OpenSSL cryptographic libraries. No external APIs are exposed that would allow other software to access the cryptographic libraries bundled in the client.

The web application uses the browser's cryptographic libraries. There are no end-user-configurable cryptographic settings that allow for accidental or intentional misconfiguration.

3.6 User Authentication

Role-based authorization and appropriate access controls depend upon the ability to identify and authenticate users. To ensure that organizers and attendees have the right privileges, account and session authentication features are incorporated into the Service.

3.6.1 Account Login

The Service websites offer the following login methods:

- Direct sign-in with username and password;
- Sign-in through a social or other account provider using LastPass, Google, Facebook, LinkedIn, Microsoft, or Apple. (https://support.goto.com/meeting/help/connect-your-social-or-other-account-for-sign-in); and
- SAML-based single sign-on.

For direct sign-in, all passwords have minimum character and complexity requirements. Mechanisms are in place to protect against brute-force login attacks and unusual login activity.

GoTo does not store account passwords in plaintext. Rather, passwords are stored using a salted cryptographic hash function designed to be resilient to dictionary and brute force attacks. Passwords are transmitted over secured connections (TLS).

3.6.2 Authentication of Session Attendees

Authentication of session attendees in a meeting is not supported. Through password protected meetings we can enforce only attendees with a known password can join the session. Additionally, once all attendees have joined a meeting session, it can be locked to prevent unauthorised attendees.

Authentication of session attendees in a webinar is not supported. Attendees get a unique link to join, and they need to use the same for joining the webinar. The unique link is not easy to guess and should not be shared with others. Also, we now support allowing or blocking users using specific email domains from registering for your event.

Authentication of session attendees in a training is not supported. Attendees get a unique link to join, and they need to use the same for joining the training. The unique link is not easy to guess and should not be shared with others.

3.6.3 Role-Based Access Control

Application-defined roles can be assigned to Service users and support Customers in enforcing company access policies related to Service and feature use. Users can access controls and privileges based on their assigned role:

Organizers (or trainers for GoTo Training) are authorized to schedule meetings, webinars, and/or training sessions. An organizer sets up each session, invites attendees, initiates and ends the session and designates the current presenter.

Attendees are people invited to participate in sessions. Attendees can view the presenter's shared screen, chat with other attendees and view the attendee list.

Presenters are attendees that can share their screen with other attendees. Presenters can also grant other attendees shared control of their keyboard and mouse.

Administrators are individuals authorized to manage a multi-user account. Administrators can configure account features, authorize organizers, and access a variety of reporting tools.

GoTo internal administrators are GoTo staff members authorized to manage GoTo Meeting, GoTo Webinar, and GoTo Training services and accounts on behalf of our Customers.

3.7 Recordings Access Control

Organizers can easily share recordings with attendees after a session through unique, direct links, and attendees can view the recording playback from within their web browser.

For GoTo Webinar, the sharing URLs do not expire as long as the recording is available. To disable access to a recording, organizers can delete the recording at any time.

For GoTo Meeting, recordings can be shared via URLs that use a random token with limited validity. Sharing can be restricted to defined parts of the content, and either be available to everyone with the URL or only to users with configurable email addresses. These restrictions can be adjusted even after the URL is shared.

4 Hosting Workloads

The GoTo infrastructure is designed to increase service reliability and reduce the risk of downtime from any single point of failure using cloud hosting data centers.

Hosting locations may vary (i.e., depending on data residency election), for detailed information, please refer to the GoTo Connect Sub-Processor Disclosure available in the Product Resources section of the GoTo Trust and Privacy Center.

4.1 Cloud hosted Workloads

Physical security is the responsibility of the Cloud provider (AWS, Azure, OCI). Reference to their documentation:

- https://aws.amazon.com/compliance/data-center/controls/
- https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security
- https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html

Other than physical security, all cloud providers operate with some form of a shared responsibility model where the cloud provider is responsible for protecting the infrastructure (hardware, software, networking) that runs all the services the provider offers. The customer is responsible for the configuration of the services they are using.

5 Customer Content Retention Schedule

Unless otherwise required by applicable law, Customer Content shall automatically be tagged for deletion within ninety (90) days and successfully deleted within one hundred (100) days of the termination, cancellation, or expiration and, in each case, deprovisioning of Customer's then-final subscription. Upon written request, GoTo may provide written confirmation/certification of Content deletion.

The above timelines are applicable for all Services, and additional Service-specific deletion timelines are set out below:

GoTo Meeting

During subscription term: GoTo Meeting session history and cloud recordings shall be deleted automatically on a rolling one (1) year basis during a Customer's active subscription term, for both paid and free accounts.

After subscription term: Upon the conclusion of a paid subscription to GoTo Meeting, Customer's accounts that contain a free license will revert to a free account and Content will be retained. For accounts that do not contain a free license or are explicitly cancelled or terminated, Content shall automatically be tagged for deletion within ninety (90) days and successfully deleted within one hundred (100) days of the termination, cancellation, or expiration and, in each case, deprovisioning of Customer's then-final subscription. Further, free GoTo Meeting accounts shall automatically be deleted after two (2) years of user inactivity (e.g., no logins).

Removal of user from paid account: If a user is deleted or otherwise removed from an active paid account, scheduled sessions are automatically tagged for deletion after ninety (90) days and successfully deleted within one hundred (100 days) of user removal.

GoTo Stage: GoTo Stage users with an active GoTo Webinar subscription may unpublish/remove any published webinars at any time via self-service through the GoTo Webinar services environment and/or by submitting a support request to GoTo.

6 Revision History

Version	Month/Year	Description
Version 3.2	July 2024	Updated and published by Legal
Version 3.3	June 2025	Standardized the document to include Product Specific sections only.
Version 3.4	August 2025	Added Privacy verbiage under Compliance Audits in Executive Summary, and aligned TLS version in Executive summary with document text.