ClickMeeting

Security Policy

ISO 27701
BUREAU VERITAS Certification

ClickMeeting

Introduction

ClickMeeting is an easy-to-use SaaS webinar platform used worldwide. It was built using highend technology, with data security as the highest priority. The platform meets stringent security requirements in the design, deployment, and maintenance of its network, platform, and applications. Businesses and government agencies can use ClickMeeting services routinely and effectively, secure in the knowledge that their sessions are safe and private.

Role-based security features

Each ClickMeeting user is assigned an application-defined role, so account owners can enforce company access policies related to service and feature use.

Host privileges

Hosts have the top level of webinar control and can grant and revoke various privileges for participants.

Host capabilities include the following:

- Invite attendees before or during the webinar, so only authorized participants can join the webinar.
- View an attendee list showing current roles and privileges.
- Start and end the webinar, to prevent others from disrupting it.
- Make any attendee an active presenter.
- Allow or disallow the use of chat by attendees.
- Disconnect or log out attendees.

- Transfer the host role to another attendee so the webinar can continue if the host must leave. (Once an attendee becomes a host, this privilege cannot be revoked.)

Presenter privileges

A presenter shares content with the attendees. Any webinar attendee may be granted the role of active presenter.

Presenters have the following capabilities:

- Upload chosen documents to a webinar room and show them to attendees, without displaying all your files and folders from your computer.
- Grant or revoke remote keyboard and mouse control to another attendee, to facilitate efficient communication through desktop interaction.
- Designate an attendee as a presenter, allowing a flexible, dynamic flow.

The difference between Host and Presenter is that the Host has the ultimate control over the account panel and webinar room. He can invite attendees, presenters, schedule and run webinars or online meetings, and control attendees data and billing details. Presenter, however, can only run an event (after being designated by a Host), with no access to the account panel or billing details.

Attendee privileges

Users with the attendee role have the following privileges:

- Join any webinar they've been invited to.
- View the presentation content unless the presenter has paused or disabled it.
- If granted, remotely control the presenter's keyboard and mouse. (Remote control privileges are automatically revoked whenever the presenter moves his mouse.)
- Use chat to send text messages to all other attendees. (Chat may be disabled or moderated by the host or presenter.)
- Leave a webinar at any time.

With basic access rights and privileges on assigned roles, webinars have the flexibility to facilitate interaction between attendees without compromising control or visibility.

Hosts can easily add attendees or change the presenter as needed throughout the webinar. Presenters remain in complete control of their desktops, and hosts have everything required to manage the webinar effectively.

Multi-user privileges

The multi-user feature allows you to have multiple users on the same account.

With the multi-user feature, the account owner can:

- Enable co-workers, employees, or contractors to log into the account using their own credentials.

- Enable multiple users to create and host many events under one account.
- Grant access to selected employees while staying in control of the company account.
- Ensure the consistency of account credentials and avoid unexpected password changes.
- Control the brand consistency in all customizable elements created by other users.
- Retain sole control of billing decisions to get the company invoices under control.

Multi-user limitations:

- Multiple users of the company webinar account are not allowed to host more than one event at the same time. To be able to do that, the account owner needs to purchase an Additional Room Session in the account add-ons.
- Multiple users cannot handle company invoices on their own.
- To empower a user with privacy and more independence, the account owner needs to purchase a subaccount (or multiple subaccounts). Each person gets their own storage space and recording time allowances. They can also keep their files and information private.

Secured Data Centers

ClickMeeting offers a global infrastructure that includes:

1. Data Centers (which store personal data given to us by clients acting as data administrators, as well as their files and recordings) are located in DE, FR, PL and RU (in the latter case, exclusively within the scope of data and files entrusted to us by Russian customers). For a detailed list of data centers that CM uses, visit: https://knowledge.clickmeeting.com/privacy-security/privacy-security-faq/#where-are-clickmeeting-data-centers-located

2. Other servers (access servers, not storing data) located in PL, DE, FR, NL, US, HG, SG, UK, BR, RU and CA.

We have a number of independent server service providers in order to ensure the best possible performance and safety. These services are delivered from various regions of the world. We monitor our infrastructure and respond to emergencies 24/7. You can check the status at any given moment at status.clickmeeting.com.

At ClickMeeting we maintain security status consistent with industry standards. For detailed information regarding the applied safeguards, visit: https://www.ssllabs.com/ssltest/analyze.html?d=clickmeeting.com

We offer alternative procedures and server rooms in case of attacks and emergencies. In case of an emergency on any of the servers, customers from the defective server are directed to another server in order to ensure the continuity of platform operations.

ClickMeeting periodically carries out automatic penetration tests and conducts a public program called BugBounty.

We also offer an SSO service. It is only available on Enterprise plans, upon contacting the Sales Department.

For more information regarding technical and organizational security measures applied by ClickMeeting, visit:
https://knowledge.clickmeeting.com/uploads/2020/03/2020.02.21.Tech_.and_.Org_.Measures.pdf

Security Personnel

We have a dedicated security department that recommends and implements security procedures for ClickMeeting services and business operations.
Our dedicated security department recommends and implements security procedures for ClickMeeting services and business operations.

Highly qualified security personnel receive ongoing training in all aspects of security to remain at the forefront of security innovation and meet the criteria for security accreditations.

Management of security-related features covers:

- Account management
- User account-management actions
- Account creation
- Security policy
- Account passwords
- Strong account-password criteria
- Webinar passwords – a host can set a webinar password and optionally choose to include or exclude the password in the webinar invitation email.

Webinar room and account security features

Role-based authorization depends on the ability to correctly identify and authenticate every user. ClickMeeting uses robust account and webinar authentication features to verify the identity of each host, presenter, and attendee.

Website account login

To access an account on the ClickMeeting website, users must provide a valid email address and user account password. Passwords must consist of at least eight characters and include letters, numbers and non-alphanumeric characters.

Passwords stored in the service database are encrypted with salted SHA1 and checked using a cryptographically secured verifier that is highly resistant to dictionary attacks.

Authentication of webinar attendees

ClickMeeting provides the following types of access to webinars:

- Password protected – one webinar password for all attendees.
- Token protected – 6-Character password (digits and/or letters) generated by
- ClickMeeting and unique for each participant.
- Registration with manual confirmation – Host approves or declines each registration. Webinar link is sent only to approved participants.

Encryption Technologies/TCP layer security

Data is transported from the client to the cloud-based server using 256 bit Secure Socket Layer Secured by RSA 2048 bits certificate (SHA256withRSA).

ClickMeeting provides the following encryption mechanisms:

Protocols

TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

End-to-end encryption (E2EE)

End-to-end encryption (E2EE) provides an extra layer of security for meetings that require enhanced privacy or data protection. This option can be enabled on certain meetings and limits the functionality of the Event Room.

All transmitted data, including audio, video and text (chat), is encrypted on the sender side and only decrypted on the receiver side using AES-GCM algorithm. This protects against interception and unauthorised access to the information.

ClickMeeting holds compliance certificate PCI Data Security Standard

securityMETRICS

Certificate of PCI DSS Merchant Compliance

Payment Card Industry Data Security Standards Validation

Based on the information provided by the merchant listed below involving its security policies, procedures, and regulations, SecurityMetrics has found the merchant to be compliant with the Payment Card Industry Data Security Standards (PCI DSS), endorsed by Visa, MasterCard, American Express, Discover, and JCB card brands.

ClickMetting Spółka z ograniczoną odpowiedzialnością

ClickMeeting holds a certificate issued by Bureau Veritas Certification confirming compliance with GDPR and ISO/IEC 27001:2022 standards.

BUREAU VERITAS

Bureau Veritas Certification

Certificate

Awarded to

ClickMeeting Sp. z o.o.
al. Grunwaldzka 413, 80-309 Gdańsk,
POLAND

Bureau Veritas Certification certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standard detailed below

STANDARD

ISO/IEC 27001:2022

SCOPE OF CERTIFICATION

INFORMATION SECURITY MANAGEMENT SYSTEM COVERING THE CLICKMEETING PLATFORM DESIGNED FOR ONLINE COMMUNICATION, PARTICULARLY FOR ORGANIZING AND MANAGING ONLINE MEETINGS, AS WELL AS STREAMING OWN AUDIO AND VIDEO FILES OVER THE INTERNET.

Certification Cycle Start Date: **18 October 2024**

Subject to the continued satisfactory operation of the organisation's Management System, this certificate is valid until: **17 October 2027**

To check this certificate validity please call: +48 22 549 04 00
Further clarification regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation.

Issue Date: 18 October 2024

Certificate Number: **PL016747/P**

PCA
POLSKIE CENTRUM AKREDYTACJI
CERTYFIKACJA SYSTEMÓW ZARZĄDZANIA
AC 081

Joanna Waberska
Local Technical Manager

MANAGING OFFICE ADDRESS: Bureau Veritas Polska Sp. z o.o., ul. Migdałowa 4, 02-796 Warszawa, Poland
ISSUING OFFICE ADDRESS: Bureau Veritas Polska Sp. z o.o., ul. Migdałowa 4, 02-796 Warszawa, Poland 1/1