NTT

Security and privacy with Microsoft Teams

Over the last few years, video conferencing has become a fundamental part of both daily life and work. But how secure is the solution you use? More than ever, people need to know that their virtual conversations are both private and secure. Luckily, with Microsoft Teams, privacy and security are built into the solution by design.

Microsoft Teams privacy and security controls are built in

Microsoft Teams offers a variety of controls to allow users to manage who participates in their meetings and who has access to meeting information:

- Decide who from outside your organization can join your meetings directly and who must 'wait in the lobby' for someone to add them to the call.
- It is easy to remove participants during a meeting, as well as designate 'presenters' and 'attendees'.
- Add guests from outside your organization but still retain control over your data.
- Use controls to moderate which participants are permitted to post and share content.
- Notify all participants when a recording starts.
- Limit access to recordings to call participants people invited to the meeting.
- Store encrypted recordings in a controlled repository that is protected by permissions.

In addition, advanced artificial intelligence (AI) monitors chats to help prevent negative behaviors like bullying and harassment.

Microsoft is focused on your privacy

When you use a video conferencing service, you are entrusting a third-party with one of your most valuable assets — your data and personal information. With Microsoft Teams, you can feel confident that you are in control of your data, where it is stored and how it can be used.

- Microsoft does not and will never use your Teams data to serve you ads.
- Microsoft does not and will never track participant attention or multi-tasking in Teams meetings.
- With Microsoft Teams, your data is deleted after the termination or expiration of your subscription.
- Microsoft Teams has built in strong measures to ensure access to your data is restricted.
- With Microsoft Teams you can access your own customer data at any time and for any reason.
- Microsoft Teams offers regular transparency reports on their Transparency Hub, detailing how they will respond to third-party and government requests for data.

Learn more at Microsoft's Transparency Hub.

Microsoft’s focus on security and protecting identity

- Microsoft Teams multi-factor authentication (MFA), a feature turned on by your IT administrator, protects your username and password by requiring you to provide a second form of verification to prove your identity.
- Microsoft processes more than eight trillion security signals every day and uses them to proactively protect you from security threats.
- In Teams, Microsoft encrypts data in transit and at rest, storing your data in their secure network of data centers and using Secure Real-time Transport Protocol (SRTP) for video, audio and desktop sharing.
- Teams supports more than 90 regulatory standards and laws, including HIPAA, GDPR, FedRAMP, SOC and Family Educational Rights and Privacy Act (FERPA) for the security of students and children.

> ‘Microsoft processes more than **eight trillion security signals** every day and uses them to **proactively protect you** from security threats.’

NTT is proud to partner with Microsoft, because we believe in their commitment to privacy, security and transparency. As Microsoft’s 2019 Intelligent Communications Partner of the Year, we are experts when it comes to Microsoft Teams and how to best implement it across organizations around the world. Contact us today to learn more about this great collaboration tool.

Learn more about Microsoft Teams and NTT today.

Contact us