SECURITY AND PRIVACY WHITE PAPER

Poly Solution for

Microsoft Teams on Windows

Part 3725-87952-001

Version 02

May 2022

Introduction

This white paper addresses security and privacy related information for the Poly Solution for Microsoft Teams on Windows.

This paper also describes the security features and access controls in Poly's processing of personally identifiable information or personal data ("personal data") and customer data in connection with the delivery of the Poly Solution for Microsoft Teams on Windows features, including the location and transfers of personal and other customer data. Poly will use such data in a manner consistent with the Poly Privacy Policy, and this white paper which may be updated from time to time. This white paper is supplemental to the Poly Privacy Policy. The most current version of this white paper will be available on Poly's website.

The Poly Solution for Microsoft Teams on Windows is deployed on-premises within the customer's environment. As these systems are deployed in the customer's environment, it is the responsibility of the customer to protect data that resides on the systems.

Solution

Poly and Microsoft are long-term partners committed to making your meetings work through high-quality voice, video, and video-interop solutions that work seamlessly with Microsoft Teams. Poly solutions enable existing video and voice conferencing equipment to work easily with your current and future Microsoft collaboration platforms for complete communication.

Poly Room Kits for Microsoft Teams Rooms on Windows deliver a simple, clutter free user experience with brilliant video and audio features for focus rooms all the way up to large boardrooms. All-in-one video bars free up the conference table surface especially in smaller rooms, while the tabletop touch controller connects to the dedicated collaboration PC securely stowed in the cabinet or on the wall with a single cable.

Poly A.I.-driven technologies such as Poly DirectorAI equalizes physical distances in the meeting room and ensures that everyone in the room is seen clearly with automatic camera framing technology. Audio innovations such as Poly NoiseBlockAI and Acoustic Fence technology ensure that distracting noises inside and outside the room are intelligently blocked out, so your voice is heard clearly.

Poly Room Kits for Microsoft Teams Rooms on Windows transform any room into a high-impact collaboration space.

Security at Poly

Security is always a critical consideration for Poly products and services. Poly's Information Security Management System (ISMS) has achieved ISO 27001:2013 certification. ISO/IEC 27001 is the most widely accepted international standard for information security best practices.

Product security at Poly is managed through the Poly Security Office (PSO), which oversees secure software development standards and guidelines. The Poly Product Security Standards align with NIST Special Publication 800-53, ISO/IEC 27001:2013, and OWASP for application security. Guidelines, standards, and policies are implemented to provide our developers with industry approved methods for adhering to the Poly Product Security Standards.

Secure Software Development Life Cycle

Poly follows a secure software development life cycle (S-SDLC) with an emphasis on security throughout the product development process. Every phase of the development process ensures security by establishing security requirements alongside functional requirements as part of initial design.

The S-SDLC implemented by Poly also includes a significant emphasis on risk analysis and vulnerability management. To increase the security posture of Poly products, a defense-in-depth model is systematically incorporated through layered

defenses. The principle of least privilege is always followed. Access is disabled or restricted to system services nonessential to standard operation.

Standards-based Static Application Security Testing (SAST) and patch management are cornerstones of our S-SDLC.

Privacy by Design
Poly implements internal policies and measures based on perceived risks which meet the principles of data protection by design and data protection by default. Such measures consist of minimizing the processing of personal data, anonymizing personal data as soon as possible, transparently documenting the functions and processing of personal data, and providing features which enable the data subject to exercise any rights they may have.

When developing, designing, selecting, and using applications, services and products that are based on the processing of personal data or process personal data to fulfill their task, Poly considers the right to data protection with due regard.

Security by Design
Poly follows Security by Design principles throughout our product creation and delivery lifecycle which includes considerations for confidentiality, integrity (data and systems), and availability. These extend to all systems that Poly uses – both on-premises and in the cloud as well as to the development, delivery and support of Poly products, cloud services, and managed services.

The foundational principles which serve as the basis of Poly's security practices include:
1. Security is required, not optional
2. Secure by default, Secure by design
3. Defense-in-depth
4. Understand and assess vulnerabilities and threats
5. Security testing and validation
6. Manage, monitor, and maintain security posture
7. End-to-end security: full lifecycle protection

Vulnerability Management
Patches are evaluated and applied in a timely fashion based on perceived risk as indicated by CVSSv3 scores.

Change Management
A formal change management process is followed by all teams at Poly to minimize any impact on the services provided to the customers. All changes implemented to the Poly Solution for Microsoft Teams on Windows go through vigorous quality assurance testing where all functional and security requirements are verified. Once Quality Assurance approves the changes, the changes are pushed to a staging environment for UAT (User Acceptance Testing). Only after final approval from stakeholders, changes are implemented in production. While emergency changes are processed on a much faster timeline, risk is evaluated, and approvals are obtained from stakeholders prior to applying any changes in production.

Hardware Security
We bundle our Poly Room Kits for Microsoft Teams Rooms on Windows with either a Dell Optiplex 7080 XE or Lenovo ThinkSmart Core (you can, alternatively, choose your own computing appliance).

The Dell Optiplex 7080 XE or Lenovo ThinkSmart Core both run on Microsoft Windows 10 Enterprise. They both ship with TPM 2.0 (Trusted Platform Module 2.0), which protects the data used to authenticate the Teams Room resource account using encryption.

Kernel Direct Memory Access (DMA) Protection is a Windows 10 setting that is enabled on Teams Rooms. With this feature, the OS and the system firmware protect the system against malicious and unintended DMA attacks for all DMA-capable devices:

- During the boot process.
- Against malicious DMA by devices connected to easily accessible internal/external DMA-capable ports, such as M.2 PCIe slots and Thunderbolt 3,

during OS runtime.

Teams Rooms also enables Hypervisor-protected code integrity (HVCI). One of the features provided by HVCI is Credential Guard. Credential Guard provides the following benefits:

- **Hardware security** - NTLM, Kerberos, and Credential Manager take advantage of platform security features, including Secure Boot and virtualization, to protect credentials. A Kensington lock prevents unauthorized access to the GC8 touch controller.
- **Virtualization-based security** - Windows NTLM and Kerberos derived credentials and other secrets run in a protected environment that is isolated from the running operating system.
- **Better protection against advanced persistent threats** - When Credential Manager domain credentials, NTLM, and Kerberos derived credentials are protected using virtualization-based security, the credential theft attack techniques and tools used in many targeted attacks are blocked. Malware running in the operating system with administrative privileges can\'t extract secrets that are protected by virtualization-based security.

Data Collection

If someone is an individual user of the Poly Solution for Microsoft Teams on Windows, and their employer has purchased and configured the system on their behalf, all the privacy information relating to personal data in this white paper is subject to their employer's privacy policies as controller of such personal data

Purpose of Processing

Information that is processed is used for enhancing the user experience, allowing configuration of settings required for proper delivery of services and easy access to frequently used data.

When configured to use an optional Poly device management solution, the on-premises server processes configuration files and their overrides to aid the management of the devices in a given deployment. The server may also process device network information, media statistics and device asset information to aid in device analytics, which enables device and service performance validation.

Data Processing

By default, some information is processed and stored locally on the Poly Solution for Microsoft Teams on Windows server. These details can be found at https://docs.microsoft.com/en-us/microsoftteams/teams-privacy

As these devices and systems are deployed in the customer's environment, it is the responsibility of the customer to protect the data processing.

How Customer Data is Stored and Protected

These details can be found at https://docs.microsoft.com/en-us/microsoftteams/rooms/security

Data Portability

An administrator can login to Windows and export log data and configuration settings using standard Windows functionality.

Data Deletion and Retention

These details can be found at https://docs.microsoft.com/en-us/microsoftteams/rooms/security

Software Security

Microsoft Teams Rooms App

After Microsoft Windows boots, Teams Rooms automatically signs into a local Windows user account named Skype. The Skype account has no password. To make the Skype account session secure, the following steps are taken:

- The Microsoft Teams Rooms app runs using the Assigned Access feature found in Windows 10 1903 and later. Assigned Access is a feature in Windows 10 that limits the application entry points exposed to the user. This is what enables single-app kiosk mode.

Using Shell Launcher, Teams Rooms is configured as a kiosk device that runs a Windows desktop application as the user interface. The Microsoft Teams Rooms app replaces the default shell (explorer.exe) that usually runs when a user logs on. In other words, the traditional Explorer shell does not get launched at all. This greatly reduces the Microsoft Teams Rooms vulnerability surface within Windows.

- Additionally, lock down policies are applied to limit non-administrative features from being used. A keyboard filter is enabled to intercept and block potentially insecure keyboard combinations that aren't covered by Assigned Access policies. Only users with local or domain administrative rights are permitted to sign into Windows to manage Teams Rooms. These and other policies applied to Windows on Microsoft Teams Rooms devices are continually assessed and tested during the product lifecycle.

Account Security

Teams Rooms devices include an administrative account named "Admin" with a default password. We strongly recommend that you change the default password as soon as possible after you complete setup.

The Admin account is not required for proper operation of Teams Rooms devices and can be renamed or even deleted. However, before you delete the Admin account, make sure that you set up an alternate local administrator account configured before removing the one that ships with Teams Rooms devices. For more information on how to change a password for a local Windows account using built-in Windows tools or PowerShell, see the following:

- Change or reset your Windows password
- Set-LocalUser

You can also import domain accounts into the local Windows Administrator group. You can do this for Azure AD accounts by using Intune. For more information, see Policy CSP -- RestrictedGroups.

Network Security

Generally, Teams Rooms has the same network requirements as any Microsoft Teams client. Access through firewalls and other security devices is the same for Teams Rooms as for any other Microsoft Teams client.

Specific to Teams Rooms, the categories listed as "required" for Teams must be open on your firewall. Teams Rooms also needs access to Windows Update, Microsoft Store, and Microsoft Intune (if you use Microsoft Intune to manage your devices).

Teams Rooms is configured to automatically keep itself patched with the latest Windows updates, including security updates. Teams Rooms installs any pending updates every day beginning at 2:00am using a pre-set local policy.

To understand more on Network Security, please refer to https://docs.microsoft.com/en-us/microsoftteams/rooms/security

Disaster Recovery and Business Continuity

The Poly Solution for Microsoft Teams for Windows is deployed on customer premises. Primary responsibility for Disaster Recovery and Business Continuity resides with the customer.

Additionally, the Poly Solution for Microsoft Teams for Windows is architected to provide high reliability, resiliency, and security.

Poly has a Business Continuity and Disaster Recovery Plan reviewed and approved by management to ensure that we are appropriately prepared to respond to an unexpected disaster event. Poly tests disaster recovery processes and procedures on an annual basis. We use the results of this testing process to evaluate our preparedness for disasters and to validate the completeness and

accuracy of our policies and procedures.

Security Incident Response

The Poly Security Office (PSO) promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. You may contact the PSO directly at informationsecurity@Poly.com

The PSO team works proactively with customers, independent security researchers, consultants, industry organizations, and other suppliers to identify possible security issues with Poly products and networks. Poly security advisories and bulletins can be found on the Poly Security Center.

Subprocessors

Poly uses certain subprocessors to assist in providing our products and services. A subprocessor is a third-party data processor who, on behalf of Poly, processes customer data. Prior to engaging a subprocessor, Poly executes an agreement with the subprocessor that is in accordance with applicable data protection laws.

The subprocessor list here identifies Poly's authorized subprocessors and includes their name, purpose, location, and website. For questions, please contact privacy@poly.com.

Prior to engagement, suppliers that may process data on behalf of Poly must undergo a privacy and security assessment. The assessment process is designed to identify deficiencies in privacy practices or security gaps and make recommendations for reduction of risk.

Suppliers that cannot meet the security requirements are disqualified.

Additional Resources

To learn more about the Poly Solution for Microsoft Teams for Windows, visit our product website.

Disclaimer

This white paper is provided for informational purposes only and does not convey any legal rights to any intellectual property in any Poly product. You may copy and use this paper for your internal reference purposes only. POLY MAKES NO WARRANTIES, EXPRESS OR IMPLIED OR STATUTORY AS TO THE INFORMATION IN THIS WHITE PAPER. THIS WHITE PAPER IS PROVIDED "AS IS" AND MAY BE UPDATED BY POLY FROM TIME TO TIME. To review the most current version of this white paper, please visit our website.