SECURITY AND PRIVACY WHITE PAPER

Poly Trio Conferencing Series

Part 3725-86468-001

Version 02

May 2020

Introduction

This white paper addresses security and privacy related information for the Poly Trio conferencing series.

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 Poly Trio conferencing series 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.

Whether it's by audio, video, or content sharing, give your teams the ability to clearly express their ideas with a Poly Trio. It delivers many best-of-breed capabilities from a single, sleek device. People can connect with a touch, on almost any platform, to get amazing sound on a phone optimized for their room size.

The Poly Trio conferencing system is the smart conference phone that delivers Poly's world class audio, video and content sharing capabilities in a single device that can connect to a variety of different platforms including Microsoft Room Systems, Microsoft Teams and Zoom Rooms.

The Poly Trio 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 system.

Optional Integrations Available

The Poly Trio conferencing system is capable of being configured to integrate with the following optional Poly products and services:

Optional configuration	Provisioning	Other Services
Poly Lens	No	Analysis & Reporting
Zero Touch Provisioning (ZTP)	Yes	Not applicable
PDMS-E (cloud service)	Yes	Device Management & Monitoring
PDMS-SP (cloud service)	No	Device Management & Monitoring
Poly RealPresence Resource Manager System (on customer premises)	Yes	Device Management & Monitoring

Note: By default, certain personal data is sent to Poly for use by the Poly Lens cloud service even if you have not yet registered for access to the Poly Lens cloud service. For security and privacy details related to Poly Lens, please refer to the Poly Lens Security and Privacy White Paper located here.

For security and privacy details related to the other optional products and services, please refer to here.

For security and privacy details related to the RealPresence Resource Manager System, please refer to the Privacy section of the Operations Guide for Poly RealPresence Resource Manager System.

Poly Trio devices support integration with certain third-party applications which may result in one of these applications processing personal data. Please carefully review all security and privacy information that is provided by the applicable vendor prior to using their applications with Poly Trio.

Poly Trio supports Poly Trio Visual+ and Poly Trio Visual Pro devices to provide additional video and content sharing capabilities. For more information, please see Poly Trio Visual+ and Poly Trio

VisualPro.

Security at Poly

Security is always a critical consideration for any product which is a network-connected device such as the Poly Trio conferencing system. Poly aligns with ISO/IEC 27001:2013 for our Information Security Management System (ISMS). 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 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 processes. Every phase of development process ensures security by establishing security requirements alongside functional requirements as part of initial design. Architecture reviews, code reviews, internal penetration testing, and attack surface analysis are performed to verify the implementation.

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 is a cornerstone of our S-SDLC.

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 for the Poly Trio conferencing system 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.

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.

Cryptographic Security

The Poly Trio conferencing system uses secure communication channels for all connections with content-sharing devices and over data networks. The Poly Trio conferencing system implements cryptographic libraries locally on the system and will encrypt all data being transmitted. Data transfers use HTTPS data stream over port 443, using TLS 1.2 and symmetric encryption algorithms AES-128 and AES-256.

Modules and TLS cipher suites implemented in the Poly Trio conferencing system are open (publicly disclosed) and have been peer reviewed. Cryptographic libraries are regularly updated.

Data sent to Poly, as well as data sent to any optional products or services, are protected with encryption as indicated.

In addition to the standard Ethernet port, certain Poly Trio systems also support NFC-assisted Bluetooth and wireless network connectivity (Wi-Fi). Both interfaces are disabled by default. When using Bluetooth, device and audio data is sent using HFP and AADP profiles. When using Wi-Fi, Poly Trio devices can be configured using one of several security modes including WEP, WPA PSK, WPA2 PSK or WPA2 Enterprise.

Secure Deployment

The Poly Trio is deployed and administered on-premises within the customer's environment. Deployment options are available to support a variety of scenarios and work environments. Please consult the Poly Trio Administrator Guide for further details regarding deployment configurations and options.

Authentication

Users can access Poly Trio devices using the phone's LCD menu display or the device's web interface. A separate password is required to be entered to access the administrator settings menu. Access to the device's web interface requires a username and password to be entered via a web browser. Accessing the device through the LCD menu requires an unlock PIN to be entered manually (when the phone lock feature is enabled).

Data Processing

By default, the following information is processed and stored locally on the Poly Trio conferencing devices:

- MAC address
- Serial number
- Display name
- System name
- IPv4/v6 addresses
- SIP username
- SIP URI
- Obi number
- Local contacts
- Admin ID and password
- Full Call detail record (CDR)
- System log files
- Directory entries

This information is used by the device to provide basic functionality, device pairing operations, enable the REST API functionality, and to enhance the user experience by providing easy access to call history and frequently used contacts.

If you elect to use the Poly Trio with optional products or services, for security and privacy details related to these optional products and services, please refer to Poly's website located here.

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

Data Collection

By default, the Poly Trio conferencing system automatically sends product usage data, device data, call detail records and quality of service data to the Poly Cloud for use with the Poly Lens service. Data collected will be used for the purposes identified in the table following this section. For details about this data processing, please refer to the Security and Privacy White Paper for Poly Lens located here.

To turn OFF data collection, please see the

"Turn off the System Usage Data Collection" section in the Poly Trio Privacy Guide.

If you are an individual user of a Poly Trio conferencing system, and your employer has purchased and configured the system on your behalf, all the privacy information relating to personal data in this white paper is subject to your employer's privacy policies as controller of such personal data.

Source From Where PI Collected	Categories of PI Collected	Business Purpose for Collection	Disclosed to the following Service Providers
Device Identifier Information	• Device ID • Device display name • IP address • MAC address (for both primary device and paired/ unpaired IP peripherals) • Wi-Fi MAC address • Bluetooth address • Serial number • PCS Number • PCS Account Code • System name • Device geolocation data including Time zone	• Internal research (product improvement, development and analytics) • Activities to verify or maintain the quality (Product and Sales Engineering Support) • Detecting security incidents • Debugging	Azure (used by Poly Lens)
Device User Information	• User ID • SIP username • SIP address • SIP alias name • Admin name and password (hashed) • Local contacts • Log files • Tenant ID • Email address • Organization name	• Internal research (product improvement, development and analytics) • Activities to verify or maintain the quality (Product and Sales Engineering Support) • Detecting security incidents • Debugging • Short-term, transient use (login)	Azure (used by Poly Lens)

Local and Remote Call Participant Information	• Full Call detail record (CDR) • Dial string number • Call ID • Participant names (local and remote) • Participant IP addresses (local and remote)	• Internal research (product improvement, development and analytics) • Activities to verify or maintain the quality (Product and Sales Engineering Support) • Detecting security incidents • Debugging • Short-term, transient use (login)	Azure (used by Poly Lens)

How Customer Data is Stored and Protected
By default, data is stored securely on the Poly Trio conferencing system and is only accessible via the LCD menu or the device's web interface (when using certain Trio base profiles).

Poly Trio conferencing systems save all local contacts to the local database residing on the device file system from which the .xml file is generated. When a user adds/deletes/modifies contacts in the local contact directory, those details are stored in a contact directory file. It is possible to configure the phones to hide the contact directory and favorites options from all screens in the user interface on all Poly Trio conferencing systems. It is also possible to set the local directory as read-only and restrict users to modifying the speed dials only. There is also a configurable option for the user to stop uploading of the local contacts and call logs to a provisioning server (if configured) through a menu item accessible from the phone's LCD interface.

Poly Trio maintains a local call detail record (CDR). The local CDR is enabled by default but can be disabled if desired. The local CDR is saved automatically to the local database residing on the device file system. Access to the phone file system is restricted to administrator access only.

For the set of usage data sent to Poly, data is stored in a database server that is in an SSAE 16 Type II certified data center in the United States that runs dedicated databases and application servers. When the Poly database server receives data from the customer, it is verified for integrity, processed, and saved in the database.

Poly may change the location of the database server and details of any such change shall be set forth in the latest copy of this white paper available on Poly's website.

The Poly database and application servers reside in the Azure data center behind a fully patched firewall that is also managed. Access for any services not required by Poly is blocked.

Server Access and Data Security
All customer data sent to the Poly cloud is encrypted both at rest and in transit using strong cryptography including AES-256 and TLS up to v1.2.

All customer data sent to the Poly cloud is backed up daily in digital form using the Azure data factory. Normal access controls of authorized users and data security policies are followed for all backup data. No physical transport of backup media occurs. The backup data during rest and while in transit is encrypted using AES 256.

Servers are in a secure data center, with only authorized staff members having access. The servers are not directly accessible from outside the data center.

Data Deletion and Retention

For clearing of the contacts, there is an option presented to the user under the settings menu in the Poly Trio conferencing device's LCD interface. A user can select this option to clear all the local contacts saved locally on the device or an optional Poly device management solution (if configured). For clearing of CDR information, please refer to the Poly Trio Administrator's Guide and Poly Trio Privacy Guide.

All contact and call log data are deleted (but not overwritten) when the phone is reset to factory default settings.

As stated above, the same also applies to all data stored on the Poly Trio conferencing system by third-party applications. This data will be deleted when the system is reset to factory settings or when changing from one base profile to another. The rest of security related aspects of third-party applications should be covered by each application's documentation available directly from the applicable vendor.

For the set of usage data sent to Poly, Poly may retain customer data for as long as needed to provide the customer with any Poly cloud services for which they have subscribed and for product improvement purposes. When a customer makes a request for deletion to privacy@poly.com, Poly will delete the requested data within 30 days, unless the data is required to to provide the service to customer.

Poly may "anonymize" personal data in lieu of deletion. The anonymization process is irreversible and includes but is not limited to searching and sanitizing all customer-specific data (e.g., name, site information and IP address) with randomly generated alphanumeric characters.

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 Trio conferencing series, 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.