SECURITY AND PRIVACY WHITE PAPER

Poly G7500, Poly Studio X50 and Poly Studio X30

Part 3725-86421-001

Version 02

March 2021

Introduction

This white paper addresses security and privacy related information for the Poly G7500, Studio X50 and Studio X30 products.

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 G7500, Studio X50 and Studio X30 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.

Poly G7500, Studio X50 and Studio X30 products provide video conferencing and content-sharing solutions for small, medium and large conference rooms. They are 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.

Optional Integrations Available

Poly G7500, Studio X50 and Studio X30 products are capable of being configured to integrate with the following optional Poly products:

Optional configuration	Provisioning	Other Services
Poly Lens	Yes	Analysis & Reporting
Poly RealPresence Resource Manager System (on customer premises)	Yes	Device Management & Monitoring

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

Security at Poly

Security is always a critical consideration for any product which is a network-connected device such as the Poly G7500, Studio X50 and Studio X30 products. 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 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. 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 are cornerstones 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 to Poly G7500, Studio X50 and Studio X30 products and related Poly cloud services 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.

Android Security Practices

On all Poly video endpoints, the Android operating system is locked down. Android features and functions that are not necessary for standard operation of a given device are disabled.

- Devices run a modified and restrictive implementation of Android which limits the capabilities of the device as compared with commonly available Android phones and tablets.
- Poly removes the ability to side-load APKs or access the Google Play store, and we formally test that these restrictions remain in place across product releases.
- We follow Android recommended guidelines for signature verification of installed applications, and all device software updates are restricted to Poly signed update packages. Ecosystem partner applications enabled on Poly devices may allow over the air updates of the partner application, independent of the device firmware update.
- All devices are tested against known rooting and jailbreaking methods and are hardened against architecture modification.
- Physical ports are hardened to protect the device from common Android attack vectors.
- Endpoints are designed and tested to ensure that a device administrator can configure the security posture according to local needs. Examples of configuration options available to a local administrator include configuration of password policy, encryption strength and responses to failed login attempts. Logging, both internally and remotely, is also configurable.

Partner APKs that are installed on Poly devices are subjected to Poly security review and all installed Poly and partner APKs are tested for common Android vulnerabilities including:

- Data leakage
- Sensitive data storage

- Outside influence
- Malicious modifications

Cryptographic Security

Poly G7500, Studio X50 and Studio X30 products use secure communication channels for all connections with content-sharing devices and over data networks. The Poly G7500, Studio X50 and Studio X30 products implement cryptographic libraries 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 G7500, Studio X50 and Studio X30 products are open (i.e. publicly disclosed) and have been peer reviewed. Cryptographic libraries are regularly updated.

Data sent to Poly, as well as data sent to the optional Poly RealPresence Resource Manager System, are protected with encryption as indicated.

Secure Deployment

The Poly G7500, Studio X50 and Studio X30 products are 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 G7500, Studio X50 and Studio X30 Administrator Guides for further details regarding deployment configurations and options.

Administrator Authentication

The customer's administrator can access Poly G7500, Studio X50 and Studio X30 products for management and configuration by using the device's web interface. Access to the device's web interface requires administrator credentials to be entered via a web browser.

Data Processing

By default, the following information is processed and stored locally on the Poly G7500, Studio X50 and Studio X30 devices:

- MAC address
- Serial number
- Display name
- System name
- IPv4/v6 addresses
- SIP username
- SIP URI
- Local contacts
- Admin ID and password
- Full Call detail record (CDR)
- System log files
- Directory entries
- IP peripheral details
  - MAC address of paired and unpaired devices
  - IP address
  - Serial number
  - Encryption key (remote)
  - MAC address
  - Serial number
  - Display name

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 G7500, Studio X50 and Studio X30 products with the optional Poly RealPresence Resource Manager System, it will send information to that system for the purpose of provisioning and management. For details about this data processing, please refer to the Privacy section of the Operations Guide for Poly RealPresence Resource Manager System.

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 G7500, Studio X50 and Studio X30 devices automatically send 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 G7500, Studio X50 and Studio X30 Administrator's Guide in the product documentation.

NOTE: After the installation to Poly devices of certain 3rd party apps or services via the Poly software promotion process, please be aware that personal data may still be available to those apps or services via the device APIs even if sending data to Poly has been turned OFF. Please refer to the documentation of those 3rd party applications or services for details.

If you are an individual user of a Poly G7500, Studio X50 or Studio X30, 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) • Serial number • PCS Number • PCS Account Code • System name • Device geolocation data including Time zone • Encryption key (remote)	• 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

The Poly G7500, Studio X50 and Studio X30 products 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 local contact directory file.

The Poly G7500, Studio X50 and Studio X30 products also maintain a local call detail record (CDR) which contains call information such as local and remote party identification, number dialed, time and date of the call and call duration. The CDR is enabled by default but can be disabled if required.

The local CDR data is saved automatically to the local database residing on the device file system. Only the administrator has access to the device file system based on the principles of “least privilege” and “need-to-know.”

If the device is configured to use an optional Poly RealPresence Resource Manager System as a provisioning server, the local contacts file, the device logs and the CDR data will be securely sent to the solution for backup. There is also a configurable option for the user to stop uploading of the local contacts through a menu item accessible from the device’s administrative web interface.

For the set of usage data sent to Poly Lens, data is stored in a database server located in a data center in the United States that is SSAE 16 Type II certified and 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 stored on your local device, there is an option presented to the administrator through the web interface. An administrator can select this option to clear all the local contacts. For clearing of local device call log information, please refer to the G7500, Studio X50 and Studio X30 Administrator's Guide and Privacy Guide in the product documentation.

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

For details related to clearing of G7500, Studio X50 and Studio X30 data stored in your organization's RealPresence Resource Manager System, please refer to the Privacy section of the Operations Guide for Poly RealPresence Resource Manager System.

For the set of usage data sent to the Poly Lens cloud service, 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 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 Poly G7500, Studio X50 and Studio X30, 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.