SECURITY AND PRIVACY WHITE PAPER

Polycom Pano

Part 3725-85466-001

Version 1.2

September 2018

INTRODUCTION

This white paper addresses security and privacy related information for Polycom Pano and describes the security features and access controls in the processing of personally identifiable information (PII) or personal data and customer data in conjunction with Pano. Poly uses such data in a manner consistent with the Poly Privacy Policy and this white paper (as 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 Polycom's website.

Pano is designed for sharing and interacting with content using mobile devices, computer systems, and the Pano App. Pano is an on-premises device that can further integrate with the Polycom Cloud Service.

SECURITY AT POLY

Security is a critical consideration in the deployment of any network-connected device, such as Pano. Poly aligns with ISO/IEC 27001:2013 practices for our Information Security Management System (ISMS). ISO/IEC 27001 is the most widely accepted international standard for information security best practices and a tangible measure by which existing and potential customers can be reassured that Poly has established and implemented best-practice information security processes. ISO/IEC 27001:2013 explicitly includes the product development process, which reinforces the commitment of Poly to information security best practices and controls.

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 for the implementation of specific security technologies, such as controls related to cryptographic ciphers, protocols, storage and web services, and intended 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 process. Every development phase establishes security requirements alongside functional requirements. 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. Additional testing, in the form of standards-based Static Application Security Testing and patch management, is a cornerstone 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 monitor the data processing while also enabling the data controller to create and improve security features.

Poly considers the right to data protection with due regard to ensure that data controllers and processors can fulfill their data protection obligations. This is true across all phases from developing to designing to selecting and using applications, services, or products that are based on the processing of, or which process, personal data.

If you are an individual user and the purchase of Pano has been made by another party as the customer, all the privacy information relating to

personal data is subject to the privacy policies of the Pano customer, as controller of such personal data.

SECURE DEPLOYMENT

Deployment of Pano is designed to support a variety of scenarios and work environments. Please consult the Pano Administrator Guide and Pano Deployment Guide for further details regarding deployment configurations and options.

POLYCOM CLOUD SERVICE INTEGRATION (OPTIONAL)

Pano can be integrated with the Polycom Cloud Service. The service is hosted in a datacenter in the United States within the Microsoft Azure cloud to leverage the scalability, availability and geographic redundancy offered of such an environment.

Each Polycom Cloud Service customer is provided at least one tenant account that is created when the customer activates their Polycom Cloud Service. These accounts use an email address as the user ID. The email address is verified via an email that contains an activation link, allowing the user to configure a password for the account. Once signed in, users then can manage their passwords as needed, with the ability to reset their password if it is forgotten or change it at their discretion. All local passwords are stored in 1-way encrypted format using SHA256 hashing.

It is also possible to federate the Polycom Cloud Service to the customer's enterprise authentication service. Polycom Cloud Service supports federation via OAuth 2.0 to both Microsoft Office 365/Azure AD and to Microsoft Active Directory (via Active Directory Federation Services 3.0). This allows users to sign in with their enterprise user account credentials to the Polycom Cloud Service by entering them into the federated authentication provider's own sign-in page and thus enjoy whatever level of single sign on (SSO) integration has been configured within their organization.

The Polycom Cloud Service uses access tokens from the authentication provider that grant it limited and controlled access to resources owned by a user.

- Access tokens are not stored by the cloud service. They are discarded after being uses to obtain basic user profile information (user email address, user display name).
- Access tokens have limited lifetimes controlled by the authentication provider.

For details on Microsoft Azure's underlying security mechanisms upon which the Polycom Cloud Service is built, see BLANK.

CRYPTOGRAPHIC SECURITY

Pano uses secure communication channels for all connections with content sharing devices, over data networks, and with integration to cloud services.

Modules and TLS cipher suites implemented in the Pano and Polycom Cloud Service are open (i.e., publicly disclosed) and have been peer reviewed. Cryptographic libraries are regularly updated.

Pano App implements OpenSSL cryptographic libraries on the system where the application is installed. Pano App will encrypt the HTTPS data stream to Pano over port 443, using TLS 1.2 and symmetric encryption algorithms.

Secure communication channels also underpin the optional integration of Pano and Pano App to Polycom Cloud Service.

HTTPS (443) using TLS 1.2:

- Compression: disabled
- RFC 5746 renegotiation
    - Client-initiated: disabled
- Ciphers:
    - AES 128/256
    - Key Exchange: ECDHE 256
    - SHA, SHA256, SHA384 hashing

Customer access to Polycom Cloud Service administration, through the tenant web portal, will support HTTPS over port 443 using either TLS 1.1 or TLS 1.2. Otherwise, as noted above, with the following ciphers:

- AES 128/256 (CBC, GCM)
- Key Exchange: DHE 2048, ECDHE 256
- SHA, SHA256, SHA384 hashing

DATA PROCESSING

Pano collects and processes data related to sharing and annotating content:

- Content shared to the device
- Annotations made to the content
- Device and room names
- Device IP and MAC addresses, and serial numbers
- Pairing configuration with Polycom RealPresence Group Series (when configured) including IP address, administrator name and password of paired devices
- Pano App, when used, collects, and processes the following additional data related to sharing and annotating content, and to serve connectivity and troubleshooting:
- Shared document filenames and types
- Content shared to the device
- Annotations made to the content
- User actions including login type, pairing details and duration, PIN usage, exception messages
- Platform details including OS and version, system language, hardware specifics such as CPU, GPU, memory size, manufacturer, and model

Additionally, with Polycom Cloud Service integrated:

- Pano device information including device and room names, IP and MAC addresses, and serial numbers
- Microsoft tenant information including tenant domain, name, GUID, and e-mail (global IT admin)
- Authentication provider (if enabled) including name, client ID, client secret, tenant, tenant ID

Personal Data Category	Type of Personal Data	Purpose of Processing
Pano Administration	• Device and room names • Connecting IP addresses	• Configure device access • Data logged for troubleshooting
Shared Content	• Content shared to Pano devices • Annotations made to shared content	• Content and annotations may be saved to facilitate collaboration
Pano App	• User email address • Pano IP address • Document names • System details including: OS & version, system language, and hardware specs	• If "Remember me" option selected when signing in to Cloud Service • To connect to previously used devices • For logging and debugging
Tenant User Profile	• Name • Email address • Password • Organization name	• Authenticate and authorize administrative access to the Polycom Cloud Service

PURPOSE OF PROCESSING

Pano processes information for the following purposes:

Manage Pano Access

Configuration of device administration, content sharing rules, and integration with Polycom Cloud Service can be performed via an administrative web interface.

Share and annotate content
Pano primarily serves to allow users to collaboratively share data and annotate the shared content with a feature to save the shared and annotated content.

Personal data is processed, only as it is relevant to the configuration of Pano and sharing of content and annotations.

HOW CUSTOMER DATA IS STORED AND PROTECTED

The Polycom Cloud Service is hosted in the Microsoft Azure Cloud, in a data center located in the United States region of the Americas geography. Access to servers is limited to only authorized staff members. The servers are not directly accessible from outside the data center. They are accessed only via a secure 'bastion' server, with access limited to a small cohort of authorized Polycom Cloud Service personnel.

Poly may change the location of the Polycom Cloud Service in the future; details of any such change shall be set forth in the latest copy of this white paper available on the Poly website.

For transferring personal data of E.U. customers to the U.S., Poly uses an Intragroup Data Transfer Agreement incorporating the E.U. Standard Contractual Clauses as the transfer mechanism.

Each Polycom Cloud Service customer's data resides in the data center in a multi-tenant system and is compartmentalized using access controls to provide data isolation between Poly customers. All customer data is encrypted both at rest and in transit using strong cryptography.

All customer data is backed up daily. 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.

DATA PORTABILITY

Pano administrators can download the following customer data from the Pano:

- System logs (as generated)

Pano users connected with Pano App can download the following customer data, during an active session, with content saving enabled:

- Saved content and annotations
- Pano App logs (as generated)

THIRD-PARTY PROVIDERS (SUB-PROCESSORS)

Poly shares customer information with service providers, contractors, or other third parties to assist in providing and improving the service. All sharing of information is carried out consistent with the Poly Privacy Policy.

DATA DELETION AND RETENTION

For customers who integrate with the Polycom Cloud Service, Poly may retain customer tenant data for as long as needed to provide that customer the service. After a customer's Cloud Service subscription terminates or expires, Poly will delete personal data within one year of termination or expiration of the service. When a customer makes a request for deletion, Poly will delete the requested data within 30 days, unless the data is required to be retained for Poly's legitimate interests of if needed to provide the service to the 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 (such as name, site information, and IP address) with randomly generated alphanumeric characters.

CHANGE MANAGEMENT

A formal change management process is followed by all teams at Poly. All changes implemented to RealPresence DMA go through vigorous QA testing where all functional and security requirements are verified.

SECURITY INCIDENT RESPONSE

The Poly Security Office (PSO) promptly investigates reported anomalies and suspected

security breaches on an enterprise-wide level. You can 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 at the Poly Security Center.

ADDITIONAL RESOURCES

To learn more about Polycom Pano, visit our website.

DISCLAIMER:

This document 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.