SECURITY AND PRIVACY WHITE PAPER

Poly Pano

Part 3725-85466-001

Version 06

March 2024

Introduction

This white paper addresses security and privacy related information for Poly 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. HP | Poly uses such data in a manner consistent with the HP Privacy Statement and this white paper (as may be updated from time to time). This white paper is supplemental to the HP Privacy Statement. The most current version of this white paper will be available on HP | Poly'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 HP | Poly Cloud Service.

Security at HP | Poly

Security is always a critical consideration for all products and services. HP | 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 HP | Poly is managed through the HP Cybersecurity team, which oversees secure software development standards and guidelines. The HP | 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 HP | Poly Product Security Standards.

Secure Software Development Life Cycle

HP | 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 HP | Poly also includes a significant emphasis on risk analysis and vulnerability management. To increase the security posture of HP | 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.

Privacy by Design

HP | 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, HP | Poly considers the right to data protection with due regard.

Security by Design

HP | 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 HP | Poly uses – both on-premises and in the cloud as well as to the development, delivery, and support of HP | Poly products, cloud services, and managed services.

The foundational principles which serve as the basis of HP | 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

Security Testing

Both static and dynamic vulnerability scanning as well as penetration testing are regularly performed for production releases and against our internal corporate network by both internal and external test teams.

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 HP | Poly to minimize any impact on the services provided to the customers. All changes implemented to Poly Pano and related HP | 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.

Data Processing

Poly 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, MAC addresses, and serial numbers
- Pairing configuration with Poly 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, and exception messages
- Platform details including OS and version, system language, hardware specifics such as CPU, GPU, memory size, manufacturer, and model

Additionally, with HP | Poly Cloud Service integrated:

- Pano device information including device and room names, IP, 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, and tenant ID

Purpose of Processing

Poly Pano processes information for the following purposes:

Access Management

Configuration of device administration, content sharing rules, and integration with HP | Poly 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.

Source of Personal Data	Categories of PI Processed	Business Purpose for Processing	Disclosed to the Following Service Providers
Pano Administration	• Device and room names • Connecting IP addresses	• Configure device access • Data logged for troubleshooting	• None
Shared Content	• Content shared to Pano devices • Annotations made to shared content	• Content and annotations may be saved to facilitate collaboration	• None
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	• None
Tenant User Profile	• Name • Email address • Password • Organization name	• Authenticate and authorize administrative access to the HP | Poly Cloud Service	• Azure

How Customer Data is Stored and Protected
The HP | Poly 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 HP | Poly Cloud Service personnel.

HP | Poly may change the location of the HP | Poly 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 HP | Poly website.

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

Each HP | Poly 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 HP | 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
Poly 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)

Data Deletion and Retention

For customers who integrate with the HP | Poly Cloud Service, HP | Poly may retain customer data for as long as needed to provide the customer with any HP | Poly cloud services for which they have subscribed and for product improvement purposes. When a customer makes a request for deletion to HP's Chief Privacy and Data Protection Officer form, HP | Poly will delete the requested data within 30 days, unless the data is required to provide the service to customer.

HP | 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.

Secure Deployment

Deployment of Poly 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.

Cryptographic Security

Poly 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 HP | Poly 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 the HP | Poly 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, and SHA384 hashing

Customer access to HP | Poly 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, and SHA384 hashing

HP | Poly Cloud Service Integration (Optional)

Poly Pano can be integrated with the HP | Poly 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 with such an environment.

Each HP | Poly Cloud Service customer is provided at least one tenant account that is created when the customer activates their HP | Poly 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 can then 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 SHA-256 hashing.

Authentication

It is also possible to federate the HP | Poly Cloud Service to the customer's enterprise authentication service. The HP | Poly 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 HP | Poly 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 HP | Poly 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 used to obtain basic user profile information (user email address, user display name).
- Access tokens have limited lifetimes controlled by the authentication provider.

Disaster Recovery and Business Continuity

Poly Pano is deployed on customer premises. Primary responsibility for Disaster Recovery and Business Continuity resides with the customer.

Additionally, the Poly Trio conferencing system is architected to provide high reliability, resiliency and security.

HP | 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. HP | 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 HP Cybersecurity team promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. You may contact them directly at informationsecurity@hp.com

The HP Cybersecurity team works proactively with customers, independent security researchers, consultants, industry organizations, and other suppliers to identify possible security issues with HP | Poly products and networks. HP | Poly security advisories and bulletins can be found on the HP Customer Support website.

Subprocessors

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

The subprocessor list here identifies HP | Poly's authorized subprocessors and includes their name, purpose, location, and website. For questions, please contact HP's Chief Privacy and Data Protection Officer form.

Prior to engagement, suppliers that may process data on behalf of HP | 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 Pano, visit our website.

Disclaimer

This white paper is provided for informational purposes only and does not convey any legal rights to any intellectual property in any HP | Poly product. You may copy and use this paper for your internal reference purposes only. HP | 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 HP | POLY FROM TIME TO TIME. To review the most current version of this white paper, please visit our website.