SECURITY AND PRIVACY WHITE PAPER

Poly Studio G9 Base Kit Plus

Part 3725-88833-001

Version 1

June 2024

Introduction

This white paper provides security and privacy related information for the Poly Studio G9 Base Kit Plus product. The Poly Studio G9 Base Kit Plus is a Microsoft Teams Rooms on Windows device.

This paper also describes the security features and access controls in HP | Poly's processing of personally identifiable information or personal data ("personal data") and customer data in connection with the Poly Studio G9 Base Kit Plus when used with the Poly Lens cloud service, and the location and transfers of personal and other customer data. HP | Poly will use such data in a manner consistent with the HP Privacy Statement and this white paper which 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.

Poly Studio G9 Base Kit Plus provides video conferencing solutions for small, medium, and large conference rooms. It is deployed on-premises within the customer's environment. As this system is deployed in the customer's environment, it is the responsibility of the customer to protect data that resides on the system.

Optional Integrations Available

Your device natively supports the optional integration with Poly Lens. Poly Lens provides an enrolled customer with access to a dedicated web portal which includes device management of Poly conferencing endpoints and basic reporting capabilities. Reports are based on data (including certain personal data of a customer as described below) collected from a customer's Poly Studio G9 Base Kit Plus when configured to send data to HP | Poly. Customer data is automatically uploaded to Poly Lens and accessed via the Poly Lens web portal application using an encrypted tunnel and software module embedded on Poly Studio G9 Base Kit Plus. For security and privacy details related to Poly Lens, please refer to the Poly Lens Security and Privacy White Paper located here.

Security at HP | Poly

Security is always a critical consideration for HP | Poly 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 with 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 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 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 are cornerstones 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

Microsoft Teams Rooms on Windows Security Practices

Please refer to Microsoft's documentation for Teams Rooms security.

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 the Poly Studio G9 Base Kit Plus product 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 Collection

By default, Poly Studio G9 Base Kit Plus devices *do not* automatically send data to the HP | Poly cloud for use with the Poly Lens service. See the Poly Studio G9 Base Kit Plus Solution Guide for details on registering the product with Poly Lens. Once the product is onboarded to Poly Lens, data collected will be used for the purposes identified in the table below. For details about this data processing, please refer to the Security and Privacy White Paper for Poly Lens located here.

If someone is an individual user of this product, 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.

Data Processing

By default, the following information is processed and stored locally on the Poly Studio G9 Base Kit Plus device:

- MAC address

- Serial number
- Display name
- System name
- IPv4/v6 addresses
- Admin ID and password
- System log files

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

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 HP | Poly device management solution, the cloud service processes configuration files and their overrides to aid the management of the devices in the deployment. The cloud service may also process device network information, media statistics and device asset information to aid in device analytics, which enables device performance validation and visibility into customer quality of experience and service performance.

Source From Where PI Collected	Categories of PI Collected	Business Purpose for Collection	Service Providers (when onboarded to Lens)
Device Identifier Information	• Device ID • Device name • MAC address (for both primary device and IP peripherals) • Serial number • IPv4/v6 address • Domain name • Device geolocation data including time zone • Network identifiers	• Present product inventory to customer in Poly Lens • Internal research (product improvement, development, and analytics) • Activities to verify or maintain quality (Product and Sales Engineering Support) • Detecting security incidents • Debugging • Serial number for entitlement	Azure, AWS
Device User Information	• Log files	• Debugging • Detecting security incidents	Azure, AWS

How Customer Data is Stored and Protected

If the Poly Studio Base Kit G9 Plus device is configured to send 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 HP | Poly receives data from the customer's device, it is verified for integrity, processed, and saved in a database. HP | Poly may change the location of the database and details of any such change shall be set forth in the latest copy of this white paper available on HP | Poly's website. The HP | Poly database and application servers reside in the AWS/Azure data center behind a fully patched firewall that is also managed. Access for any services not required by HP | Poly is blocked.

Data Deletion and Retention

For clearing of local device call log information, please refer to the Privacy Guides in the product documentation for the Poly Studio, Poly Studio P15, and Poly Studio R30.

For the set of usage data sent to the Poly Lens 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

The Poly Studio G9 Base Kit Plus product 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 Studio G9 Base Kit Plus Solution Guide and the Microsoft Teams Rooms for Windows documentation for further details regarding deployment configurations and options.

Server Access and Data Security

All customer data sent to the HP | 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 HP | Poly cloud is backed up daily in digital form. 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 is not accessible to the Cloud Service Provider.

Cryptographic Security

The Poly Studio G9 Base Kit Plus product uses secure communication channels for all connections with content-sharing devices and over data networks. These 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.

Data sent to HP | Poly are protected with encryption as indicated.

Authentication

The customer's administrator can access the Poly Studio G9 Base Kit Plus product for management and configuration by using the device's Windows accounts as described here.

Disaster Recovery and Business Continuity

The Poly Studio G9 Base Kit Plus product is deployed on customer premises. Primary responsibility for Disaster Recovery and Business Continuity resides with the customer. Additionally,

these products are 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 the Poly Studio G9 Base Kit Plus product 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 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.