SECURITY AND PRIVACY WHITE PAPER

Poly+ and Poly+ Enterprise Services Overview

Part 3725-88092-001

Version 01

September 2022

Introduction

This white paper addresses security and privacy related information regarding Poly+ Services. This white paper describes the security features and access controls applied to Poly's processing of personally identifiable information or personal data ("personal data") and customer data in connection with the delivery of this Poly+ Service, and 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 is available on Poly's website.

Poly+ is a premium support service for Poly devices. It provides unlimited, global 24x7 technical support, advanced hardware replacement, ecosystem cloud partner support, and other premium features.

Security at Poly

Security is always a critical consideration for all Poly products and services. 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 and you can be reassured that Poly has established and implemented best-practice information security processes.

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.

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.

Security by Design

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

The foundational principles which serve as the basis of 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

Source of Personal Data	Categories of PI Processed	Business Purpose for Processing	Disclosed to the following Service Providers
Support and reporting	• Name • User Email Address • User ID • User Phone number • User address/location • Serial number • IP address • MAC address • Call start and end date/time • Device configuration data • Provisioning information • Device usage and performance data • CDR • Support entitlement information	• Troubleshooting and support remediation • Provide required reporting • Sending replacement products • Entitlement	• Salesforce • Azure, AWS – if Poly Lens is provisioned with Poly+

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.

Data Processing

System logs and call detail records can be collected by or sent to Poly. These may contain names, emails, IP addresses, locations.

Customers who contact Poly for technical support are asked to provide contact information.

If someone is an individual user and the purchase of a Poly+ Service has been made by their employer as the customer, 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.

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 Poly device management solution, the on-premises server or cloud service processes configuration files to aid the management of the devices. The server or 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.

How Customer Data Is Stored and Protected
Entitlement and support ticket data are stored in Poly's support databases. If Poly+ is integrated with Poly Lens, support data will also reside in Lens. All data is encrypted in transit using TLS 1.2. (Please see the Security and Privacy White Paper for Poly Lens).

Support artifacts sent to Poly by the customer to aid in troubleshooting will be deleted 90 days after support ticket closure. This includes system logs, call detail records (CDRs), etc.

Poly may change the location of the business systems used to process customer information. The details of any such change shall be set forth in the latest copy of this white paper available on Poly's website.

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

Data Deletion and Retention
Poly may retain customer data for as long as needed to provide the customer with the support services. 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 be retained for Poly's legitimate business purposes or if needed 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 (such as name, site information, and IP address) with randomly generated alphanumeric characters.

Server Access and Data Security
Computers used to process customer information in the delivery of the Poly+ are protected from malware and viruses and are patched in a timely manner. They adhere to Poly's ISMS requirements for controlled access and follow least privilege and need-to-know principles. When these computers are used remotely, they must authenticate to the Poly network using MFA.

Change Management
Poly's delivery of Poly+ Services utilizes the ITIL framework.

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 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.

Disaster Recovery and Business Continuity
Poly+ Services are architected to provide high reliability, resiliency, and security. 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. 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 Poly Security Office (PSO) promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. Please 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+ Services, please 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 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.