SECURITY AND PRIVACY WHITE PAPER

Poly Rove

Part 3725-88227-001

Version 01

March 2023

Introduction

This white paper addresses security and privacy related information for the Poly Rove DECT 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 Rove DECT 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.

The Poly Rove DECT product family offers a scalable and secure wireless communication for any small, medium, or large business. Built for on-site employees, the Poly Rove wireless IP Phone solution delivers the freedom to move. 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 Rove DECT products are capable of being configured to integrate with the following optional Poly products:

Optional configuration	Provisioning	Other Services
Poly PDMS-SP	No	Analysis & Reporting Device Management & Monitoring

Security at Poly

Security is always a critical consideration for 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.

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.

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

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 Poly to minimize any impact on the services provided to the customers. All changes implemented to Poly Rove DECT 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.

Data Collection

If someone is an individual user of these products, 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 Rove DECT Base Station devices:

- MAC address
- Serial number
- Display name
- System name
- IPv4 addresses
- Admin ID and password
- System log files

By default, the following information is processed and stored locally on the Poly Rove Base Station devices:

- Serial number
- System name
- 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 Poly device management solution, the cloud service may process this data. The server or cloud service may also process device network information 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

For the set of usage data sent to PDMS-SP, 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 to any services not required by Poly is blocked.

Data Deletion and Retention

For clearing of local device call log information, please refer to the Privacy Guide in the product documentation for Poly Rove DECT. For the set of usage data sent to the PDMS-SP 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.

Secure Deployment

Poly Rove 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 User Guides in the product documentation for the Poly Rove for further details regarding deployment configurations and options.

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.

Cryptographic Security

Poly Rove DECT products use 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 Poly is protected with encryption as indicated.

Authentication

The customer's administrator can access Poly Rove DECT 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 over HTTPS.

NOTE: If you have elected to use PDMS-SP, please review the table below for details about the personal data processing that Poly will perform.			
Source from Where PI Collected	Categories of PI Collected	Business Purpose for Collection	Disclosed to the following Service Providers
Device Identifier Information	• Admin ID • Password • Device ID • Device display name • IP address • MAC address • Serial number • 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 PDMS-SP)
Device User Information	• Log files	• 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 PDMS-SP)

Disaster Recovery and Business Continuity

Poly Rove DECT products are deployed on customer premises. Primary responsibility for Disaster Recovery and Business Continuity resides with the customer.

Additionally, these products are designed 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. 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 Rove DECT products, 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.