SECURITY AND PRIVACY WHITE PAPER

Polycom RealPresence Collaboration Server

Part 3725-87951-001

Version 01

March 2022

Introduction
This white paper addresses security and privacy related information for Polycom RealPresence Collaboration Server (RPCS or RMX). It 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 running of RPCS, as well as the location and transfer of personal and other customer data. 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 Poly's website.

Overview
Polycom RealPresence Collaboration Server is a Unified Communications infrastructure product that provides audio/video multipoint call conferencing service for Poly and non-Poly audio and audio/video endpoints. It supports connection of endpoints to its conferencing service via POTS, ISDN and IP (SIP/H.323) network connections. The following platform variants are supported for RPCS: RMX 2000, RMX 4000, RMX 1800 and RPCS Virtual Edition (VE). While RMX 2000/4000 and RMX 1800 are custom hardware-based appliances, RPCS VE can be installed on a virtual machine (VMWare or Hyper-V). RPCS systems can interface with a variety of Poly as well as third-party devices and entities.

The Linux-based operating system running on RMX 2000/4000 and RMX 1800 and the CentOS operating system running the RPCS VE software have been hardened with the latest security patches, best practices for software configurations, and the removal of unnecessary services. Additionally, the OS security has been verified using several industry-leading security and vulnerability scan tools, as well as manual testing.

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.

Secure Software Development Life Cycle
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 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 for the Polycom RealPresence Collaboration Server 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.

Security Settings

The Polycom RealPresence Collaboration Server software may reside within the customer enterprise network and/or in the DMZ. It communicates and responds to other devices and services on the network using specific ports (as configured by the customer). When communicating with any device, service, and/or the management interface, you can configure RPCS to use encrypted communication. RPCS provides fine-grained security settings in its user interface so that customers can harden the security of RPCS as required. RPCS provides several configurable security settings that the user can set to enabled or disabled.

Certificates

Certificates are used between devices within the video conferencing environment (such as servers and endpoints) to authenticate the devices and to support encryption.

Polycom RealPresence Collaboration Server provides certificate management capabilities which enable the user to load new certificates for use by the system.

Network Intrusion Detection System

Polycom RealPresence Collaboration Server uses the iptables utility for access control on network interfaces. For each different kind of packet processing, there is a table containing a chain of rules for the handling of packets. Every network packet arriving at or leaving from the Collaboration Server must pass the rules applicable to it. Depending on the nature of the suspect packets, the

rules may reject, drop, or throttle their arrival rate (by dropping the rest). RPCS maintains a log that includes all non-permitted access attempts blocked by the firewall, such as access to ports that are not open.

Device, Call, and Conference Security
Polycom RealPresence Collaboration Server provides different security features for call signaling and conference management that the user can enable or disable from the RMX Manager UI.

Management Access
Polycom RealPresence Collaboration Server is designed to use multiple network interfaces, which allows different services like signaling, control, management, media etc. to run on different networks. For example, management traffic can be limited to the internal network to prevent possible intrusion from outside the local network.

For management access to the RMX Manager UI or XML APIs exposed by RPCS, local as well as Active Directory users are supported. Users are assigned specific roles like Administrator, Auditor, Chairperson and Operator. Based on the role assigned, users can view and modify specific settings.

The administrator can create and delete other users, and can also perform all configuration and maintenance tasks on RPCS, including enforcing strong passwords, defining password ageing rules, change frequency etc., configuring user lockout, session lockout, and controlling the maximum number of active sessions per RPCS, the number of active sessions per user, the session timeout interval for the RMX Manager UI and XML API logins.

As RPCS runs the Linux operating system, users can change the Linux Root (root) user password for console and SSH access if enabled.

Ultra Secure Mode (USM)
If the Polycom RealPresence Collaboration Server needs to be deployed in a maximum security environment, then it can be configured to operate in Ultra Secure Mode through a system flag. In Ultra Secure Mode all enhanced security features of RPCS are activated and enforced, including network security, user and session management and strong password enforcement.

Data Processing
Polycom RealPresence Collaboration Server does not access any customer's data except as required to enable the features provided by the application. As these systems are deployed in the customer's environment, it is the responsibility of the customer to protect data privacy.

RPCS collects and processes the following types of information:

- Device information (such as type of device, device name, MAC address, IP address, serial number etc.)
- Call and conference data (includes call connection information such as IP addresses, SIP addresses/URIs, calling numbers, and some other caller personal data like user ID or caller name/alias)
- Users' contact and access information (such as contact name, alias name, access credentials)

If someone is an individual user and the purchase of RPCS 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 the controller of such personal data.

Source of Personal Data	Categories of PI Processed	Business Purpose of Processing	Disclosed to the Following Service Providers
Administrative user and Management interface	• Contact Name • Admin and other users' access credentials (login id and password) • System name (used by Admin or other user) • IP address • SIP URI / Tel-URI • MAC address • E164 number • H.323 alias name	• Authenticate Admin and other users for login to RMX • Dialing out calls to participants (stored in Address Book) • Store contact information for ease of use	None
Call participant personal data (including Call Detail Records)	• Calling number • IP address • Display name • SIP URI / Tel-URI • H.323 alias name • H.323 ID	• Deliver audio/video conferencing service • Maintaining call history • Troubleshooting call/connection errors, or performance issues	None
Device information	• Device name • IP address • SIP address/URI • MAC address • Serial number	• Investigate RMX technical issues involving endpoints • Respond to customer support requests	None
Audit and Operational log files	• Admin and other users' login id • System name (used by Admin or other user) • Admin and other users' actions • Call status and statistics of the participants	• Track and audit user activities • Maintain record of configuration changes • Analysis and troubleshooting of RMX issues	None

Data Portability

A data subject has the right to receive a copy of all personal data in a commonly used, machine-readable format. CDRs can be downloaded in plain text or XML format, while the Address Book can be exported in CSV format. Audit Log files and operational logs can be downloaded in plain text format.

Data Deletion and Retention

Poly may retain customer data for as long as needed to provide the customer support for the Polycom RealPresence Collaboration Server product. Any personal data made available while working with Poly Support, specific to a support incident, is retained until the information is requested to be removed by the customer. When a customer makes a request for deletion (privacy@poly.com), Poly will delete the requested data within 30 days, unless the data is required to be retained for Poly's legitimate interests or if needed to provide the service to customer.

Disaster Recovery and Business Continuity

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 but are sometimes conducted more frequently when there are changes to our infrastructure that warrant new tests. 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 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.

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.

Additiona Resources
The *RealPresence Collaboration Server Privacy Guide,* the *RealPresence Collaboration Server Getting Started Guide,* the *RealPresence Collaboration Server Administrator Guide*, and the *Polycom RealPresence Collaboration Server Technical Reference* have in-depth details about Polycom RealPresence Collaboration Server configuration and capabilities. To access those guides and other information about RPCS, please visit our support site.

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.