SECURITY AND PRIVACY WHITE PAPER

Poly Private Hosted Infrastructure Services Overview

Part 3725-86318-001

Version 01

August 28, 2019

INTRODUCTION

This white paper addresses security and privacy related information regarding Poly Remote Managed Services for Poly UC&C infrastructure, which are hosted by Poly. 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 provisioning and delivery of the Managed Services, 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 (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 is available on Poly's website.

The following managed services are discussed in this white paper:

MANAGED SERVICES POLY HOSTED SOLUTIONS

- Private Hosted for Business (PHfB)
- Private Hosted for Enterprise (PHfE)

OVERVIEW OF MANAGED SERVICES

There are two (2) options for these types of solutions: Private Hosted for Business and Private Hosted for Enterprise. The options are chosen based on size, location, and features required. These solutions all include RealPresence Platform (RPP) hardware, service, and maintenance as part of the service. Poly retains ownership of all provided service components and data center engagements. If edge traversal functionality is included in the solution, endpoint access is provided over the internet. Network sizing is determined by concurrent users, call rate, signaling, and overhead. Customer can provide up to 4U and 350W of equipment in Poly DC space for network termination. Customer handoff to Poly Service is via a Poly provided switch and/or firewall.

Poly will provide a secured managed services environment consisting of the appropriate systems to provide the supporting services for the DMZs, user authentication, and secure customer connections. The monitoring and management DMZ systems consist of a bespoke jump server, a monitoring probe, and file storage dedicated to the engagement. Each solution is created using multiple logically separate DMZs to host the monitoring and management, call platform, and internet facing systems. IP addressing (RFC 1918/24) is provided by the customer making the solution a virtual extension of the customer's network. The customer must ensure that there are no IP conflicts on their network.

For connectivity from internal corporate network, an MPLS or private line is required.

PRIVATE HOSTED FOR BUSINESS

The Private Hosted for Business service is designed to provide RealPresence Platform (RPP) services to customers requiring a small to medium sized video solution. The solution is hosted in the Poly primary data center, located in the United States. The features and capacities of these solutions are limited.

PRIVATE HOSTED FOR ENTERPRISE

The Private Hosted for Enterprise service is designed to provide RealPresence Platform (RPP) services to customers requiring a large-scale video solution. The solution is hosted in a Poly-acquired data center to meet customer regional and usage expectations. Geographic redundancy can be designed and provided using multiple data centers around the globe.

SECURITY AT POLY

Security is a critical consideration in the deployment of any network-connected device, and even more so for managed services.

Poly Managed Services practices the ITIL framework.

Poly has been awarded ISO/IEC 27001:2013 certification for our Information Security Management System (ISMS).

ISO/IEC 27001 is the most widely accepted international standard for information security best practices and a tangible measure by which existing and potential customers can be reassured that Poly has established and implemented best-practice information security processes.

ISO/IEC 27001:2013 certification not only reinforces our commitment to information security best practices and controls, but it explicitly includes the product development process.

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 for the implementation of specific security technologies—such as cryptographic controls related to ciphers, protocols, storage, and web services—are intended 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 while also enabling the data controller to create and improve security features.

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 to make sure that data controllers and processors can fulfill their data protection obligations.

SECURE DEPLOYMENT

The RealPresence Platform (RPP) functionality and hardware are installed within Poly's environment. Ownership and environment responsibility is retained by Poly. Poly is responsible to procure and secure the public internet access and public IP addresses for the service to use.

Customer information obtained during onboarding is used to create the DMZs. The DMZs are encapsulated by firewall security zones.
No unnecessary network ports are opened between zones. The DMZs have the following specific functionality to support the service.

Monitoring uses a collector in a customer specific DMZ allowing for gathering of alert information (e.g., SNMP, API, Ping, etc.) from the customer and isolation of the internal managed services network. Externally, all traffic to the customer will traverse customer provided MPLS or dedicated private line. Internally, monitoring information is sent to the monitoring database, within the managed services environment, to generate alerts and dashboards for the Customer Management Center (CMC), technical support team.

Management is performed on a jump server. This serves as a bastion host for authorized users. No internet accessible Poly systems directly access customer systems, except for operating system updates through a proxy. Management traffic (e.g., HTTPS, SSH, Telnet, Ping, etc.) is generated from the customer specific DMZ to systems covered under the Remote Management and Monitoring Service. Configuration backups of managed devices are taken monthly for recovery. Backups and support information (e.g., system logs, CDRs, network traces, etc.) are temporarily stored on the jump server. Backup information on jump servers is encrypted (See Cryptographic section for details). Support information is to be removed from the DMZ immediately upon being moved to support systems.

Poly uses its own change management policies and procedures, aligned with ITIL, to document and review changes for viability and necessity.

PRIVATE HOSTED FOR BUSINESS (PHFB)

All servers required to run RPP applications are supplied, hardened and accessed by Poly only. Poly will procure the public internet access for the service to use. This solution is currently only located in one (1) data center in Aurora Colorado, USA. Poly will provide the network equipment required to integrate the solution within the data center.

PRIVATE HOSTED FOR ENTERPRISE (PHfE)

All servers required to run RPP applications are supplied and configured by Poly. Poly will procure the public internet access for the service to use. Poly does not provide any back-bone network connections between regionally diverse implementations. The customer is required to provide the IP address space for solution, it is therefore best that the routing between data centers be provided over the customers network. Poly will provide the network equipment required to integrate the solution within the DC space. Customer/service provider is required to bring their private network connection or MPLS to the Poly DC space. If shared facility, then customer can supply a cross connect to the Poly space. Customer network handoff to Poly Service are via a Poly switch and firewall. The public internet access provided by Poly is used for the following purposes:

- Poly Remote Monitoring and Management
- External users using H323/SIP endpoints to dial into solution
- Any optional integrations that are configured

USER AUTHENTICATION

Poly personnel use certificates on Poly managed assets for their software VPN connection to the Poly Managed Services network. From the Poly laptop, administrators access the specific jump server required using unique AD credentials. The Managed Services network has a separate active directory server for providing unique credentials and logging user activity on the jump server dedicated to the customer. Poly Managed Services personnel initially access the customer’s managed devices using local administrator credentials provided during onboarding. These credentials are changed when Managed Services goes operational and are required to follow Poly’s own strong password configuration policy which complies with industry standard security practices.

Managed device credentials are stored in an encrypted password manager which is assigned, managed, and logged per user.

Customer user access is provided requiring unique identifiers and passwords which must be changed per Poly policy. Business Relationship Manager (BRM) can facilitate requests and will follow up on password changes. All customer user traffic will stay within the customer’s network. Customer will not be allowed administrative access to the managed solution.

DISASTER RECOVERY AND BUSINESS CONTINUITY

The solution's core network leverages hardware redundancy on all routers, switches and firewalls. Depending on the chosen customer solution, the Poly data center can supply single or redundant MPLS or leased line connectivity to the customer. Each core DC has multiple routes to the internet. The monitoring solution leverages a distributed application to request and receive SNMP information. The monitoring application's core databases and app servers are virtualized on separate hardware. Management tools are also virtualized, baselined using snapshots, and backed up on a regular and recurring basis using standard virtualization toolsets.

Solutions for each customer will have service level objectives or service level agreements designed around their specific solution design and documented in the service agreement.

CRYPTOGRAPHIC SECURITY

Managed Services Connections

- Certificates per Poly asset used for administrative access
  - Encryption algorithm: SHA-256
  - Authentication algorithm: RSA
- IPsec VPN connection minimums
  - Encryption algorithm: AES-256
  - Authentication algorithm: SHA-2

Managed Services Data Storage Encryption

- Password storage
  - Encryption algorithm: AES-256
  - Local authentication: SHA-512
- Support ticket information
  - Encryption algorithm: AES-256
- Reporting server (BRMs)
  - Encryption algorithm: SHA-256
- Backup server (application backup data)
  - Encrypted by individual application (please see individual application Security White Paper for details)

DATA PROCESSING

Monitoring data continuously flows between sensor and internal database. This does not contain personally identifiable information.

Backups are stored encrypted for 61 days on the customer's jump server.

System logs and call detail records are collected through the IPsec VPN for troubleshooting and reporting for the service. These may contain names, emails, IP addresses, locations.

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

If you are an individual user and the purchase of a Poly managed service has been made by your employer as the customer, all the privacy information relating to personal data in this white paper is subject to your employer's privacy policies as controller of such personal data.

Personal Data Category	Type of Personal Data	Purpose of Processing
Support and reporting services	- Endpoint display name - User email address - User ID - User phone number - User address/location	- Troubleshooting and support remediation - Provide required reporting for managed services
Configuration backups	- Display name - User email address - User ID - Phone number - Organization address/location	- Ability to recover from system failure

PURPOSE OF PROCESSING

The primary purposes of processing information by the managed service are to:

Provide support and reporting per agreement requirements and to provide recovery of system failure.

HOW CUSTOMER DATA IS STORED AND PROTECTED

Poly may change the location of the Poly Managed Service 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.

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.

When Poly managed services needs to store customer or personal data to provide basic services, the data is processed as follows:

CATEGORY	WHERE IT STORED AND HOW PROTECTED	HOW LONG
Data backups	Stored encrypted in customer DMZ (refer to cryptographic security for encryption details)	61 days
Reporting data	Encrypted server in Poly IT environment	12 months or the conclusion of the engagement
Technical support	Stored in customer DMZ, stored in Poly CRMs, stored on sftp	Temporarily held until 90 days after ticket is closed

SERVER ACCESS AND DATA SECURITY

Poly is responsible for physical and data security for all systems in their environment up to the customer connection at the edge of the network.

All servers created for the use of managed services follow hardened templates for deployment. Firewall ports are opened only as necessary and changes are documented through change management.

Backend and management servers that are the foundation for the Managed Services Network and DMZs are in secure data centers. Only authorized staff members may access the facility with their badges. Access to the equipment for these systems is established via secure and bidirectional tunnel, or in the case of Private Cloud for Business, over direct internal network only.

THIRD-PARTY PROVIDERS (SUB-PROCESSORS)

Poly shares customer information with service providers, contractors, or other third parties to assist in providing and improving the service. All sharing of information is consistent with the Poly Privacy Policy.

DATA DELETION AND RETENTION

Poly may retain customer data for as long as needed to provide that customer with the RMM managed service. When a customer makes a request for deletion, 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.

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. https://support.polycom.com/content/support/security-center.html

ADDITIONAL RESOURCES

To learn more about Poly Managed 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.