SECURITY AND PRIVACY WHITE PAPER

Polycom Device Management Service for Service Providers

Part 3725-85474-001

Version 01

September 2018

INTRODUCTION

This white paper addresses security and privacy related information for Polycom Device Management Service for Service Providers (PDMS-SP). 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 the Polycom PDMS-SP product, 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 Polycom's website.

Polycom PDMS-SP provides a cloud portal for managing Poly phones and analog telephone adapters (ATA). Service providers can easily add devices and voice services, configure devices and check device status. Below are the key functionalities:

- Add, delete, or manage Poly phones and ATAs
- Troubleshoot issues by capturing system logs or packets
- View overall status of devices
- Manage organizations and user access permissions
- Upgrade firmware and service API
- Quick access to product FAQs, forums, and documentation

SECURITY AT POLY

Security is a critical consideration in the deployment of any network-connected device, and equally so for integration with a cloud-based service such as Polycom PDMS-SP.

Poly aligns with ISO/IEC 27001:2013 practices for our Information Security Management (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 practices not only reinforce our commitment to information 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, standards, and policies are implemented to provide our developers 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. Additional testing, in the form of standards-based Static Application Security Testing and patch management, is a cornerstone 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 monitor the data processing 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 Poly considers the right to data protection with due regard to making sure that data controllers and processors can fulfill their data protection obligations.

USER AUTHENTICATION

User authentication for the PDMS-SP service is performed via email and password. Portal users enter their email address to register at the self-sign-in portal. They then authenticate themselves with the emailed activation link and choose a password. Thereafter, logins to the site require the supplied email and password. Users can update their password securely on the portal. All authenticated web portal customer connections take place over HTTPS encrypted sessions.

CRYPTOGRAPHIC SECURITY

All communication with the PDMS-SP servers and client browsers is over a secure TLS connection that encrypts all requests and responses. This is achieved with an HTTPS connection authenticated over TLS with RSA-2048 (SHA-256) SSL certificates. All customer data is encrypted in transit using strong cryptography up to TLS v1.2.

DISASTER RECOVERY

The PDMS-SP service is hosted on Amazon Web Services (AWS) cloud infrastructure, within a virtual private cloud. All customer data is backed up daily. Automated database backups, also encrypted at rest, reside within the same VPC. Access controls are implemented for authorized users and data security policies are followed for all backup data – both at rest and while in transit – is encrypted using AES-256.

DATA PROCESSING

The PDMS-SP service collects and processes data including:

- Device data (includes information such as type of device, device name and installed software version)
- Call data (includes call connection information such as time, duration and call quality – e.g., MOS, packets dropped, latency).
- Logs (includes logs from portal web server, device logs and packet captures)

If you are an individual user and the purchase of PDMS-SP 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.

PURPOSE OF PROCESSING

The primary purposes of processing information by the PDMS-SP service are to:

Enable asset management

PDMS-SP service providers can maintain individual login credentials and configuration data for devices they have added to the service (e.g., software versions and device configurations) and view current states of managed device connections to PDMS-SP.

Perform data analytics

PDMS-SP collects and processes anonymous call quality statistics for analytics. IP addresses of devices are mapped to approximate geolocations and reported to controllers. This allows service providers to better understand utilization, capacity and performance.

Personal data category	Type of personal data	Purpose of processing
Call participant device information and managed device information	• Device name • IP address • Serial number • MAC address • Geolocation • Time zone	• Understand how the service is used • Diagnose technical issues • Conduct analytics and analysis to improve the technical performance of the service • Respond to customer support requests

HOW CUSTOMER DATA IS STORED AND PROTECTED

The PDMS-SP servers are hosted on distributed AWS servers that run dedicated databases and application servers that reside in the United States. When the PDMS-SP database server receives data from a customer, it is verified for integrity, processed and saved.

Poly may change the location of the PDMS-SP 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 E.U. customers to the U.S., Poly uses an Intragroup Data Transfer Agreement incorporating the E.U. Standard Contractual Clauses as the transfer mechanism.

The PDMS-SP database and application servers reside in a managed data center behind a fully patched firewall. Access to any services not explicitly required by PDMS-SP is blocked.

SERVER ACCESS AND DATA SECURITY

Servers are located in a secure data center with only authorized staff members granted access. The servers are not directly accessible from outside the data center.

AWS hosting security features are employed to limit access to the service, as well as to secure customer data at rest. PDMS-SP deployment makes use of AWS identity and access management (IAM), VPC subnets, security groups, network access control lists, elastic backing store encryption and SSH-based server access, among others.

All customer data 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.

DATA PORTABILITY

Polycom PDMS-SP service providers and their agents can download the following data from the PDMS-SP portal:

- A CSV listing of all devices configured in the system
- Individual phone configuration, troubleshooting logs and network captures

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 carried out consistent with the Poly Privacy Policy.

DATA DELETION AND RETENTION

All information collected from the customer is stored in a multitenant database with email domain information configured as the access control mechanism. All data is self-contained in the database in the data center.

Poly may retain customer data for as long as needed to provide that customer the PDMS-SP service. After a customer's subscription terminates or expires, Poly will delete personal data within one year of termination or expiration of the service. When a customer makes a request for deletion,

Poly will delete the requested data within thirty (30) days, unless the data is required to be retained for Poly's legitimate business purposes or if needed to provide service to the 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.

CHANGE MANAGEMENT

A formal change management process is followed by all teams at Poly to minimize any impact on the services provided to customers. All changes implemented to the Polycom Device Management Service go through vigorous QA testing where all functional and security requirements are verified. Once QA approves the changes, the changes are pushed to a staging environment for User Acceptance Testing (UAT). Only after final approval from stakeholders are changes implemented in production. All scheduled changes are applied during regularly scheduled maintenance periods. While emergency changes are processed on a much faster timeline, risk is evaluated, and approvals are obtained from stakeholders prior to application.

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.

ADDITIONAL RESOURCES

To learn more about Polycom PDMS-SP, visit our website.

DISCLAIMER:

This document 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.