SECURITY AND PRIVACY WHITE PAPER

Polycom OBiTALK

Part 3725-85377-001

Version 1.1

September 2018

INTRODUCTION

This white paper addresses security and privacy related information for Polycom OBiTALK. 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 RealPresence DMA 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 OBiTALK is an online portal for managing Poly phones and analog telephone adapters. The portal provides an easy way to add, configure and check the status of the devices. It also provides the following key functionalities:

- Add, delete, or manage Poly phones and ATAs
- View overall status of devices
- Setup wizards for configuring voice services like Google Voice or other VoIP service providers
- Subscribe to additional services such as ObiExtras or Extended Product Warranty
- Quick access to product FAQs, the OBiTALK Community Forum and other documentation

SECURITY AT POLY

Security is always a critical consideration for any product. Poly aligns with ISO/IEC 27001:2013 practices 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 practices not only reinforce 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, 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

Polycom OBiTALK provides HTTP basic authentication using a username and password. The data is transported using HTTPS over TLS.

DISASTER RECOVERY

The Polycom OBiTALK Service is architected to provide high reliability, resiliency, and security. The entire service is hosted on Amazon Web Services (AWS) to leverage the scalability and redundancy offered by such an environment. Normal low impact outage due to loss of power or connectivity is handled by the cloud hosting provider – AWS. During a major crisis or disaster, service will be moved to a different region until the affected region is restored.

CRYPTOGRAPHIC SECURITY

All communication with the Polycom OBiTALK web portal is over a standard secure SSL connection that encrypts all requests and responses. Transport Layer Security (TLS) between components of OBiTALK is mutual for all connections. Protocol version TLS 1.2 is preferred for a secure connection. TLS compression and client-initiated renegotiation also are disabled. Where implemented, secure server renegotiation is compliant with RFC 5746.

Cryptographic cipher suites and modules implemented in the OBiTALK service are open (i.e., publicly disclosed) and have been peer reviewed. Cryptographic libraries are current, regularly updated, and leverage the Advanced Encryption Standard (AES-128 and AES-256) cipher suites. Hash strengths supported include SHA-256, SHA-384 and SHA-512

MANAGEMENT ACCESS

DATA PROCESSING

The OBiTALK Service collects and processes logs containing:

- Device data (includes information like type of device, device name, phone numbers and installed software version)
- Call data (includes call connection information like IP addresses, and other caller personal data like user ID, or caller name).

If you are an individual user and the purchase of OBiTALK has been made by your employer as the customer, all of 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
Call participant device information AND managed device info	• Device name • IP address • Geolocation • MAC address • 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

PURPOSE OF PROCESSING

The primary purposes of processing information by OBiTALK are to:

Enable asset management – View your device information, manage important information like software versions and device data, and to collect and process device and call statistics.

Perform data analytics – Better understand utilization, capacity, and performance. Personal data is processed by display and reporting purposes only.

HOW CUSTOMER DATA IS STORED AND PROTECTED

The OBiTALK service is run on distributed Amazon AWS servers that run dedicated databases and application servers that reside in the United States. When the OBiTALK database server receives data from the customer, it is verified for integrity, processed, and saved in the database.

The OBiTALK database and application servers reside in the data center behind a fully patched firewall. Access for any services not required by OBiTALK is blocked.

Poly may change the location of the OBiTALK 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.

SERVER ACCESS AND SECURITY

Polycom OBiTALK is hosted in the Amazon cloud. Only authorized staff members with proper access permissions have access to the production servers.

Each customer's data resides in the multi-tenant system and is compartmentalized using access controls to provide data isolation between customers. All customer data is encrypted both at rest and in transit using strong cryptography including AES-256 and TLS up to v1.2.

Customer data is backed up daily. Access is restricted to control access only to authorized users and data security policies are followed for all backup Data. No physical transport of backup media occurs. The backup data, both at rest and while in transit, is encrypted using AES 256.

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.

If you subscribe to the optional feature ObiExtras or purchase an extended warranty, you will be redirected to Amazon directly to complete your purchase. Poly does not collect or process your payment information.

DATA DELETION AND RETENTION

All information collected from the customer is stored in the multi-tenant database, in AWS.

Poly may retain customer data for as long as needed to provide the customer the OBiTALK 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 30 days, unless the data is required to be retained for Poly's legitimate interests 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.

CHANGE MANAGEMENT

A formal change management process is followed by all teams at Poly. All changes implemented to RealPresence DMA go through vigorous QA testing where all functional and security requirements are verified.

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 OBiTALK, please 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.

© 2019 Plantronics, Inc. All rights reserved. Poly and the propeller design are trademarks of Plantronics, Inc. All other trademarks are the property of their respective owners.