Introduction
This white paper addresses security and privacy related information for Polycom OBiTALK ("OBTALK"). 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 OBiTALK, 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.

OBiTALK is an online portal for managing Poly phones and analog telephone adapters (ATA). 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 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 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.

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.

Cloud systems are managed by Poly and are updated as needed. 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 OBiTALK 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 Processing
The Polycom 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 someone is an individual user and the decision to use OBiTALK 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 controller of such personal data.

Purpose of Processing
The primary purposes of processing information by Polycom 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 Polycom 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.

Data Deletion and Retention
All information collected from the customer is stored in a single database that supports a user facing multi-tenant structure 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 the customer with any Poly cloud services 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 be retained to provide the service to customer. Poly may “anonymize” personal data in lieu of deletion. In cases where anonymization occurs, the 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.

Server Access and Data Security
Polycom OBiTALK is hosted in AWS. 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.

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.

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

Disaster Recovery and Business Continuity
Polycom OBiTALK is architected to provide high reliability, resiliency, and security. The service is hosted in Amazon AWS data centers. Normal low impact outage due to loss of power or connectivity is already handled by the cloud hosting providers — Amazon AWS.

During a major crisis or disaster, service will be moved to a different region until the affected region is restored.

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 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 the Polycom OBiTALK, 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.