Polycom Device Management Service for Enterprise
Introduction
This white paper addresses security and privacy related information for Polycom Device Management Service for Enterprise (PDMS-E). 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 PDMS-E, 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.

If someone is an individual user and the purchase of PDMS-E has been made by their employer as the customer, all the privacy information relating to personal data is subject to their employer’s privacy policies as controller of such personal data.

PDMS-E is a cloud-based device management service for Poly and Polycom audio endpoints (both personal and conference-based).

Security at Poly
Security is always a critical consideration for a cloud-based service such as Polycom Device Management Service for Enterprise. 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.

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 Device Management Service for Enterprise service 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 Device Management Service for Enterprise collects and processes data related to the provisioning, configuration, and management of supported devices including:
- Site names, descriptions, and locations
- Site device counts
- Device names and group lists
- Device configuration profiles
- Device software updates

Additionally, with Polycom Cloud Relay deployed:
- Line registration status and URI
- Call status
- Device uptime and last reboot time
- Scheduled tasks

Purpose of Processing
The primary purposes of processing information by the Polycom Device Management Service for Enterprise are:

*Manage site provisioning*
Sites are a collection of customer-defined networks that can be configured for management and deployment of devices.

*Enable device provisioning*
View your devices and manage important information like software versions and device configurations.

Personal data is processed only as it is relevant to the configuration and provisioning of audio devices.
How Customer Data Is Stored and Protected
The Polycom Device Management Service for Enterprise is hosted in the Microsoft Azure Cloud or Amazon Web Services (AWS), in a data center located in the United States region of the American geography. Poly has implemented technical and physical controls designed to prevent unauthorized access to, or disclosure of customer content. In addition, we have systems, procedures, and policies in place to prevent unauthorized access to customer data and content by Poly employees.

Poly may change the location of PDMS-E in the future. 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.

All customer data is stored within the data center(s) on which the service is deployed encrypted at rest using 256-bit AES encryption.

<table>
<thead>
<tr>
<th>Source of Personal Data</th>
<th>Categories of PI Processed</th>
<th>Business Purpose of Processing</th>
<th>Disclosed to the following Service Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative user profile</td>
<td>• Name&lt;br&gt;• Email address&lt;br&gt;• Password&lt;br&gt;• Organization name</td>
<td>• Authenticate and authorize administrative access to the service</td>
<td>• Azure, AWS</td>
</tr>
<tr>
<td>Device information</td>
<td>• Device name&lt;br&gt;• Device public IP&lt;br&gt;• Device private IP&lt;br&gt;• MAC address&lt;br&gt;• SIP URI&lt;br&gt;• SIP user&lt;br&gt;• Far site name&lt;br&gt;• Far site number</td>
<td>• Configuration of devices&lt;br&gt;• Monitoring of devices (only available when deployed with Cloud Relay)</td>
<td>• Azure, AWS</td>
</tr>
</tbody>
</table>

Data Portability
Polycom Device Management Service for Enterprise administrators can download the following customer data from the PDMS-E Portal:
- Export user-defined configuration profiles.
- Export device lists and attributes as CSV files.

Data Deletion and Retention
All information collected from the customer is stored in the database with the tenant information configured as the access control mechanism. Nothing is transmitted outside of the Polycom Device Management Service for Enterprise. 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 for which they have subscribed 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
Servers are in a secure data center, with only authorized staff members having access. The servers are not directly accessible from outside the data center – they are accessed only via a secured ‘bastion’ server, with only authorized Poly personnel granted access to it.

Each customer’s data resides in the data center in a multi-tenant system and is compartmentalized using access controls to provide data isolation between Polycom Device Management Service for Enterprise customers.

For details on Microsoft Azure’s underlying security mechanisms upon which PDMS-E is built, see here.

For details on AWS underlying security mechanisms upon which the PDMS-E is built, see here.

Poly has implemented technical and physical control designed to prevent unauthorized access to or disclosure of customer content or customer personal data. In addition, we have systems, procedures, and policies in place to prevent unauthorized access to customer data and content by Poly employees.

Cryptographic Security
Polycom Device Management Service for Enterprise uses secure communication channels for all connections between its cloud services and the devices it manages. All customer data is encrypted both at rest and in transit using strong cryptography including AES-256 and TLS up to v1.2.

Polycom Device Management Service Portal:
- HTTPS (443) using TLS 1.2
  - Compression: disabled
  - RFC 5746 renegotiation
    - Client-initiated: disabled
  - Ciphers
    - AES 128/256
    - Key Exchange: ECDHE 256
    - SHA, SHA256, SHA384 hashing

Polycom Cloud Relay to Polycom Cloud Service:
- HTTPS (443) using TLS 1.1, TLS 1.2
  - Compression: disabled
  - RFC 5746 renegotiation
    - Client-initiated: disabled
  - Ciphers
    - AES 128/256 (CBC, GCM)
    - Key Exchange: DHE 2048, ECDHE 256
    - SHA, SHA256, SHA384 hashing

Polycom Cloud Relay Device Connections (to local on-premise devices):
- HTTPS (443) using TLS 1.1, TLS 1.2
  - Compression: disabled
  - RFC 5746 renegotiation
    - Client-initiated: disabled
  - Ciphers
    - AES 128/256 (CBC, GCM), Camellia 128/256 (CBC)
    - Key Exchange: ECDHE 256, RSA
    - SHA, SHA256, SHA384 hashing

TLS cipher suites and modules implemented in the Polycom Cloud Service are open (i.e., publicly disclosed) and have been peer reviewed. Cryptographic libraries are current and regularly updated.

Authentication
User authentication for the Polycom Device Management Service for Enterprise is provided by the Polycom Cloud Service, which offers two different methods.
The first method is to use the built-in “local” Polycom Cloud Service user accounts. Each Polycom Cloud Service customer gets at least one “local” account that is created when the customer activates their Polycom Cloud Service. These accounts use a user’s email address as the user ID. The email address is verified via an email that contains an activation link, which, when followed, allows the user to configure a password for the account, at which time they can sign in. Users then can manage their passwords as needed, with the ability to reset their password if it is forgotten or change it at their discretion. All local passwords are stored in 1-way encrypted format using SHA-256 hashing.

The second method is to federate the Polycom Cloud Service to the customer’s enterprise authentication service. Polycom Cloud Service supports federation via OAuth 2 to both Microsoft Office 365/Azure AD and to Microsoft Active Directory (via Active Directory Federation Services 3.0). This allows users to use their enterprise user account credentials when signing into the Polycom Cloud Service, entering them only into the federated authentication provider’s own sign-in page and enjoying whatever level of Single Sign On (SSO) integration has been configured in their organization. The Polycom Cloud Service then receives access tokens from the authentication provider that grant it limited and controlled access to resources owned by a user.

Note:
- Access tokens are not stored by the cloud service – they are discarded after being used to obtain basic user profile information (user email address, user display name).
- Access tokens have limited lifetimes controlled by the authentication provider.

Role-Based Access Control (RBAC) allows the Polycom Cloud Service administrator to tailor access control to each user based on their specific access needs. For PDMS-E specifically, both a ‘Device Admin’ and ‘Device Operator’ role can be selected for users – the former provides full access to device management functions; the latter provides a ‘viewing-only’ access level. See the Polycom Cloud Service Administration Guide for more details on user roles.

Disaster Recovery and Business Continuity
Polycom Device Management Service for Enterprise is architected to provide high reliability, resiliency, and security. The service is hosted in multiple Microsoft Azure or Amazon AWS data centers in the United States. Normal low impact outage due to loss of power or connectivity is already handled by the cloud hosting providers —Microsoft Azure or 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 Device Management Service for Enterprise, 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.