SECURITY AND PRIVACY WHITE PAPER

# Poly Workflow Suite and Poly Clariti Workflow Lite

Part: 3725-87283-001

Version 02

August 2021

**Introduction**

This white paper addresses security and privacy related information regarding Poly Workflow Suite and Poly Clariti Workflow Lite and their feature sets. For Workflow Suite these include One Touch Dial (OTD), Easy Schedule (EZY) and Meeting Director. For Clariti Workflow Lite, the reduced feature set includes One Touch Dial (OTD) and Easy Schedule (EZY).

This paper 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 provisioning and delivery of the Workflow Suite and Clariti Workflow Lite and their feature sets including One Touch Dial (OTD), Easy Schedule (EZY), Meeting Director 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 which 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.

The One Touch Dial feature enables an endpoint device to join a meeting by simply clicking a "join" button on the device without the need to dial a potentially long string of digits or a URL.

The Easy Schedule feature enables a user to schedule a meeting within Outlook or G Suite which populates details to join a Poly on-premises video meeting room (VMR).

Meeting Director enables a user to control elements of their Poly on-premises conference from a web browser.

The Workflow Suite feature sets can each be used as standalone with existing Poly platforms or are often paired with Poly Clariti solution and Poly RealConnect cloud service.

**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 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 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.

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.

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 Poly Workflow Suite and Poly Clariti Workflow Lite 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**
Poly does not access any customer's data except as required to enable the features provided by Poly Workflow Suite and Poly Clariti Workflow Lite. If someone is an individual user and the purchase of Workflow Suite or Clariti Workflow Lite 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**
- Calendar invites for resource mailboxes are attached to customer endpoints in order to provide a simplified click to join experience for the user.
- Meeting join details are inserted into an Outlook or G Suite invite as a simple booking mechanism for Poly core meetings.
- Meeting control is used to empower a user to control their conferences from within the web portal.
- Only the minimum required data is collected in

| Source From Where PI Collected | Categories of PI Collected | Business Purpose for Collection | Disclosed to the following Service Providers |
|---|---|---|---|
| Device Identifier Information | • Device name<br>• Resource Mailbox name<br>• IP address | • Help customer diagnose technical issues | None |

logs for trouble shooting potential customer problems.

**How Customer Data is Stored and Protected**
All customer data resides in the on-premises or Microsoft Azure/AWS hosted installation of Poly Workflow Suite and Poly Clariti Workflow Lite. Critical information including log files, device information and passwords are encrypted using AES-256.

**Data Portability**
Log data can be exported from Poly Workflow Suite and Poly Clariti Workflow Lite into a compressed file with .zip extension.

**Data Deletion and Retention**
All information collected is stored in the configuration and log files which reside on the customer's on-premises deployment or the customer's tenant within the Microsoft Azure/AWS installation of Poly Workflow Suite or Poly Clariti Workflow Lite. Nothing is transmitted outside of the customer's network back to Poly.

Poly may retain customer data for as long as needed to provide the customer with any Poly 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.

**Secure Deployment**
The Poly Workflow Suite supports three deployment feature sets provided either individually or together in the Suite.

*Poly Workflow Suite / Poly Clariti Workflow Lite One Touch Dial (OTD)*
In support of Poly endpoints, Exchange on-premises or Web Services is used to provide the calendar to the endpoint. The endpoint accounts are validated with Workflow Suite over NTLMv2. For supported third party endpoints, OTD pushes calendar events to the endpoint through the endpoint's native API over HTTPS.

Calendar connections over Exchange on-premises or Web Services support TLS v1.3. Older versions of TLS are available to support legacy endpoint models. Consult the Administrator's Guide for detailed information about configuration options.

*Poly Workflow Suite / Poly Clariti Workflow Lite Easy Schedule (EZY)*
EZY can integrate with Outlook, as a plugin, Outlook web Add-in and G Suite calendar (Chrome extension) communicates over HTTPS with Workflow Suite and the data channel is encrypted with TLS1.3

*Poly Workflow Suite Meeting Director*
Meeting Director authenticates a user with their

Microsoft Active Directory account using LDAP over TLS1.3. The application collates the meetings scheduled with Exchange and active meetings on the Poly Core infrastructure.

Workflow Suite and Clariti Workflow Lite ensure that your communications are secure and does not record calendar events. As stated above, calendar events that are transported between the service and the customer's endpoint are encrypted using TLS 1.3.

All traffic transported is always encrypted between Workflow Suite and Clariti Workflow Lite and Microsoft O365, Microsoft Exchange on-premises, and Google as calendar providers.

**Server Access and Data Security**

When deployed on customer's premises, server level access is the customer's responsibility as this is an on-premises application installed on a customer provided Microsoft Windows server. The minimum requirements for the server are as follows:

To Support up to 500 Devices:

- Windows Server 2012R2, 2016, or 2019 for hosting the Workflow Server application
- 2 CPU's or better
- 8GB RAM or better

To support up to 1000 Devices:

- Windows Server 2012R2, 2016, or 2019 for hosting the Workflow Server application
- 4 CPU's or better
- 16GB RAM or better

**Cryptographic Security**

All communication with the Poly Workflow Suite and Poly Clariti Workflow Lite portal is encrypted over an HTTPS connection that uses TLS 1.3 with 128 or 256-bit encryption and a 2048-bit key exchange mechanism. Cryptographic cipher suites and modules implemented in Workflow Suite and Clariti Workflow Lite 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 and SHA-384. All passwords are encrypted using AES-256.

Workflow Suite and Clariti Workflow Lite ensure that your communications are secure and do not record or capture video or audio streams. This solution is for scheduling call setup and control only.

All traffic transported between Workflow Suite and Clariti Workflow Lite and Microsoft is always encrypted.

**Key Management**

During the installation, the customer installs a public or private certificate along with private key for secure communication. This key is encrypted and stored within the Poly Workflow Suite and Poly Clariti Workflow Lite application and is used for all external communication.

Workflow Suite and Clariti Workflow Lite generate a 256-bit key for configuration encryption. They use CBC mode for symmetric encryption of configuration.

**Password Management**

Strong passwords are supported. More details can be found here.

**Access Controls**

Poly Workflow Suite has 2 areas for access each with a different access portal:

1. Administrative access to Workflow Suite
2. User access to the Meeting Director portal

Poly Clariti Workflow Lite only has Administrative access to Workflow Suite.

Account authentication to both these portals is managed using the customer's Active Directory environment over LDAP and TLS1.3.

Workflow Suite and Clariti Workflow Lite address access control by using roles within the application so access is narrowed by only allowing administrators, auditors or users based on the principles of need to know and least privilege. It does this by assigning a Microsoft Active Directory group to one of the roles within Workflow Suite.

SSO is supported for both administrative access to the Workflow Suite and Clariti Workflow Lite portal and the Poly Workflow Suite Meeting Director user portal which is also controlled by the customer's Microsoft Active Directory.

This is a private installation either on-premises or may be deployed into the customer's tenant within Azure or AWS which Poly does not have direct access (unless provided as a Poly Managed Service).

**Authentication**

Poly Workflow Suite and Poly Clariti Workflow Lite support integration of enterprise authentication providers via the OAuth2 standard in Graph API.

With OAuth2, Workflow Suite and Clariti Workflow Lite can securely integrate with enterprise authentication providers and thereby authenticate enterprise users without ever having access to their credentials. The administrator enters credentials only into the authentication provider's own sign-in page and grants limited and controlled access to the Graph API application owned by the administrator. Workflow Suite and Clariti Workflow Lite then receive access tokens from the authentication provider using the ID and secret from the Graph application.

Note:

- Access tokens are not stored by Workflow Suite or Clariti Workflow Lite
- Access tokens have limited lifetimes controlled by the authentication provider
- Workflow Suite and Clariti Workflow Lite support the following authentication provider:
    - Microsoft Office 365 (Azure AD) via OAuth2

**Administration**

Administrative access to Poly Workflow Suite and Poly Clariti Workflow Lite uses LDAP and TLS1.3 to connect to the customer's Microsoft Active Directory which is assigned to an administrator role within Workflow Suite or Clariti Workflow Lite for administrative or audit purposes.

**Security Monitoring and Logging**

Poly Workflow Suite and Poly Clariti Workflow Lite log critical events in an active log file viewable within the administrator's portal. These logs are downloadable. These logs may be needed by Poly support teams if working on a potential problem. Log files and device information are encrypted using AES-256.

**API**

Poly Workflow Suite and Poly Clariti Workflow Lite use OAuth2 with the Microsoft Graph API in order to access Microsoft APIs for Exchange online meetings to enable One Touch Dial to access the endpoint's resource mailbox and pass joining details to the authenticated endpoint. Administrators must consent to the terms and conditions for the Azure Active Directory (AAD) Application. The following API is used:

- ***Read online meeting details***
  Allows the app to read online meeting details in your organization, without a signed-in user.

Alternatively, a service account with Reviewer rights, impersonation rights, or a passthrough account is

also supported for integration with Microsoft Exchange and is encrypted with TLS1.3.

**Disaster Recovery and Business Continuity**
When Poly Workflow Suite or Poly Clariti Workflow Lite are deployed on customer premises, the primary responsibility for Disaster Recovery and Business Continuity resides with the customer.

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. 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 Poly Workflow Suite, visit our product website.

For more information on Clariti Workflow Lite please also see this site.

**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.