SECURITY AND PRIVACY WHITE PAPER

Plantronics Manager Pro

Part 3725-86321-001

Version 02

December 2019

INTRODUCTION

This white paper addresses security- and privacy-related information regarding Plantronics Manager Pro. It 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 Plantronics Manager Pro, 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 (as updated from time to time). The most current version of this paper will be available on the GDPR website.

Plantronics Manager Pro is an internet-based subscription service (i.e., Software as a Service—SaaS) powered by Amazon Web Services (AWS), which provides the ability to manage, monitor, and configure a variety of Plantronics audio devices. It supports managing headsets, viewing policy compliance status, locking settings, managing by user groups (LDAP/manual), IT troubleshooting, and analysis reporting of assets, usage, conversation, and acoustics. When used with Plantronics Hub client application, Hub policy can also be set and updated using Plantronics Manager Pro.

Note: Although Plantronics Manager Pro is powered by AWS and can be used with Plantronics Hub, the scope of this white paper is limited to Plantronics Manager Pro. Please see here for more details about Plantronics Hub and for AWS security details see here.

SECURITY AT POLY

Security is a critical consideration in the deployment of any network-connected device, and even more so for enterprise integration with a cloud-based service such as Plantronics Manager Pro.

Poly aligns our security practices with ISO/IEC 27001, the most widely accepted international standard for information security best practices.
Poly services are also compliant with these security-related audits and certifications.

- Sarbanes-Oxley (SOX) Compliance: Poly is SOX compliant.
- Plantronics is ISO 9000 certified.
- Plantronics Manager Pro is hosted in the AWS environment. AWS maintains multiple certifications for its data centers, including ISO 27001 compliance, PCI Certification, and SOC reports. For more information about their certification and compliance, visit the AWS Cloud Security, Identity and Compliance website.

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 for the implementation of specific security technologies—such as cryptographic controls related to ciphers, protocols, storage, and web services—are intended 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 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 and services, 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.

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 Plantronics Manager Pro go through vigorous QA testing where all functional and security requirements are verified. Once QA approves the changes, they are pushed to a staging environment for user-acceptance testing (UAT). Only after final approval from stakeholders are changes implemented in production. All customer impacting changes are applied during regularly scheduled maintenance periods or during upgrade windows communicated to customers in advance. While emergency changes are processed on a much faster timeline, risk is evaluated and approvals are obtained from stakeholders prior to application.

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, transparently documenting the functions and processing of personal data, 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 process personal data to fulfil data controllers' and processors' tasks, Poly considers the right to data protection with due regard to making sure that they are able to fulfil their data protection obligations.

SECURE DEPLOYMENT

Plantronics Manager Pro is an internet-based subscription service hosted entirely in AWS. The customer enterprise IT admin and user computers are required to make outbound connections to the Manager Pro tenant instance. All traffic transported between the customer computers and Plantronics Manager Pro is always encrypted. The customer admin is responsible for managing the Manager Pro tenant. Customer admin can access, view, and manage application audit logs for their tenant and run various reports if the reporting features are enabled but is not able to access any tenant data directly as it is stored in AWS using encryption at rest. Data can potentially be made visible via third-party partner apps but only if the customer has provided access.

From a Poly administrative perspective, administrators are required to use strong password authentication and the Poly Dev Ops team is required to use multi-factor authentication whenever logging into AWS to manage all deployments of the Plantronics Manager Pro service. Certificate based SSH is used to access AWS instances supporting Plantronics Manager. SSH certificates are rotated on a regular basis. Any remote access required by Poly is directly into the AWS instance, not the customer's internal network.

USER AUTHENTICATION

Plantronics Manager Pro supports the integration of enterprise authentication providers via SAML 2.0. Once configured, Plantronics Manager Pro can be accessed by selecting the single sign-on (SSO) button in the Plantronics Manager Pro login dialog (service provider-initiated) or can be accessed by selecting Plantronics Manager Pro from your list of identity provider applications (IDP-initiated). Both IDP-initiated SSO via SAML 2.0 and SP-initiated SSO are supported. Supported IDPs that have been tested and confirmed include Ping, Okta, and ADFS. Other IDPs may work but have not been tested and therefore are not officially supported. Contact your Poly account representative or your Plantronics reseller to request support for a specific IDP.

CRYPTOGRAPHIC SECURITY

While processing all Plantronics Manager Pro data, industry standard HTTPS over TLS 1.2 is used for data encryption in transit and hardware based AWS EBS volume encryption with Advanced Encryption Standard (AES-256) for data at rest. Encryption keys are managed by the AWS KMS service.

DISASTER RECOVERY

Plantronics Manager Pro is architected to provide high reliability, resiliency, and security.
Annual disaster recovery tests are performed and stakeholders are engaged to make updates to the plans as needed.

Our infrastructure runs on fault-tolerant systems for failures of individual servers or even entire data centers. Our operations team tests disaster recovery measures regularly and an on-call team is ready to quickly resolve any incidents in the event of such occurrence. Additionally, Poly DevOps manages and maintains the service under the Plantronics Manager Pro Standard Operating Guidelines.

For Plantronics Manager Pro, customer data is stored across multiple AWS availability zones within region specific data centers. We have well-tested backup and restoration procedures, which allow recovery from a major disaster.

For Plantronics Manager Pro, when a system outage occurs, we will post notification on the Plantronics Manager Pro System Status page along with the expected resolution time.

DATA PROCESSING

Poly does not access any customer's data except as required to enable the features provided by the service. If you are an individual user and the purchase of the Plantronics Manager Pro 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.

PURPOSE OF PROCESSING

Personal data collected and the purposes for which it is collected are listed in the table below.

In general, the data collected by Plantronics Manager Pro is directly related to the level of subscription. For example, if you are not subscribed to the Call Quality and Analytics Suite, then the
data required to populate these reports will not be collected.

While using our mobile apps, we ask to collect your location information for the purpose of enabling features in the Plantronics Hub for Android/iOS mobile app such as the BackTrack™ feature.

PLEASE NOTE: The ability to pseudonymize network username, end user display name, computer hostname, and domain was added as of version 3.13, not 3.9. It is only enabled by default for new tenants. Tenants that were created prior to 3.13 will need to enable the feature manually. Versions of Hub prior to 3.13 do not support this functionality so in that case the pseudonymization is only performed on the server side.

.

DATA CATEGORY	SUBSCRIPTION LEVEL	WHAT WE COLLECT	WHY WE COLLECT IT
Tenant Administration	All	First name, last name and email address of the IT Administrator(s) for the tenant	Required for tenant creation and used by Poly for customer communication
		Access events (log in/out)	These events can be monitored by Poly at an individual (customer) level or in aggregate for understanding administrative behaviors.
Plantronics Hub for Desktop in a Plantronics Manager Pro Environment	All (version 3.9 and higher)	Client instance ID, System ID	Poly-assigned identifiers for ensuring a system and an instance of Hub can be associated to a user.
		Network username, end user display name, computer hostname, and domain	Associates a unique user to a device and the device to a system. Note: These data elements are pseudonymized by default beginning in version 3.13.
		LDAP user attributes including LDAP group membership, user name, account name, city, company, country, department, department number, division, employee type, office, state, zip code, display name, telephone number, street address, and title	LDAP attributes are entirely under the control of the administrator. These LDAP attributes are completely optional and are not collected by default. Your company may choose to enable these attributes in the Plantronics Hub collection criteria.
		Plantronics device information including model ID, product ID, serial number	Required for proper update selection, troubleshooting, and reporting.
	All (prior to version 3.9)	End user email address, local IP address, network IP address	Versions of Hub prior to 3.9 may send these pieces of data. Plantronics Manager Pro does not keep or store this information. Update to the latest version to ensure this data is not sent.
		Call ID	Required for Radio Link Quality report (Data sent only with subscription of Call Quality and Analytics Suite or better)
Plantronics Hub for Mobile in a Plantronics Manager Pro Environment	All	Client instance ID	Poly-assigned identifiers for ensuring an instance of Hub can be associated to a user
		Network username, mobile device hostname, and domain	Associates a unique user to a device and the device to a system. Note: These data elements are pseudonymized by default beginning in version 3.13.
		Plantronics device information: model ID, product ID, serial number (IMEI)	Required for proper update selection, troubleshooting, and reporting

HOW CUSTOMER DATA IS STORED AND PROTECTED

All customer data is stored within the AWS data centers on which the service is deployed using hardware-based AWS EBS volume encryption with Advanced Encryption Standard (AES-256) for data at rest.

Customer data is automatically backed up nightly in digital form. Normal access controls of authorized users and data security policies are followed for all backup data. No physical backup media is used.

The operations team is alerted in case of a back-up system failure so that such failure is remediated. Backups are fully tested at least every 90 days to ensure that they work as expected.

All customer data is stored solely within the Plantronics Manager Pro system where the tenant resides, and within the aggregated reporting data warehouse. Tenant-specific MySQL data are stored in separate DB schemas. Mongo (NoSQL) documents are stored with tenant-specific IDs.

Data flow within Plantronics Manager Pro can be controlled and will only exist within a defined geographic residency. Data center locations are determined based on customer location and may include USA, Ireland, Australia, and Singapore.

Data is not replicated across regions. Backups are stored in the same AWS region as where the tenant is hosted.

Note: The use of third-party apps or APIs should be carefully considered as they may process data in or transfer data to different geographies.

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.

We use a combination of administrative, physical, and logical security safeguards and continue to work on features to keep your information safe. Your data may be accessed by Poly as required to support the service and access is limited to only those within the organization with the need to access data in order to support the service.

DATA DELETION AND RETENTION

Poly will only retain customer data for as long as needed to provide that customer with Plantronics Manager Pro services. After a customer's subscription terminates or expires, within a reasonably practicable period of time after the 30-day post-termination period ends, Poly will disable an end customer's account and use reasonable efforts to delete and/or destroy the data and issue a Certificate of Destruction. All encryption keys are destroyed at time of deletion. Tenant cannot specify deletion method. Upon customer request, a certificate of data destruction will be issued once all data has been deleted and all data backups have expired and been purged.

SERVER ACCESS AND DATA SECURITY

Plantronics Manager Pro is hosted on AWS.
Only authorized staff members with proper access permissions have access to the production servers.

Poly also 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 corporate infrastructure uses a suite of cloud native and optimized tools to secure the Plantronics Manager Pro environment. These include but are not

limited to native Amazon security constructs such as VPC security groups and functionally isolated application tiers. Rather than actively scanning instances for running malware processes, Poly utilizes our SDN tool to block unauthorized outbound network traffic. Any instance attempting unauthorized outbound connections is terminated by Poly.

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. The list of our sub-processors is available online here.

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.

ADDITIONAL RESOURCES
To learn more about Plantronics Manager Pro, and the Terms of Use and Privacy Policies that apply to your use of the service, visit our website.

This white paper is intended to describe Plantronics security policies and procedures related to Plantronics Manager Pro Software-as-a-Service offering.

The terms and conditions of the Terms of Use and Privacy Policies control and supersede this white paper to the extent there is any inconsistency.

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.