PIantronics Manager Pro Security Overview

January 2017

Plantronics Manager Pro Security Overview

Plantronics takes security seriously. We understand how important the responsibility of safeguarding data is to our customers, and we take comprehensive measures to protect them. For more information on our commitment to providing secure services, please see our Privacy Policy and Terms of Service.

SECURITY PRACTICES

Hundreds of our customers trust Plantronics with their data. We implemented enterprise-class security policies to ensure their confidence. We offer full transparency about the way we handle security and their data, so our customers' information is safe, their interactions are secure, and their business is protected.

If you have additional questions regarding our security practices, we are happy to answer them. Please write to feedback@plantronics.com.

CONFIDENTIALITY

Our IT employees' access to Plantronics Manager Pro customer data is limited to those who need it. Plantronics Manager Pro requires limited employee access to the systems which store and process customer data.

PERSONNEL PRACTICES

Plantronics conducts background checks on all employees before employment, and our IT employees receive cyber security training during onboarding as well as on an ongoing basis. All employees are required to read and sign our information security policy, code of conduct, and the electronic use policy.

COMPLIANCE

Plantronics services are compliant with these security-related audits and certifications.

- Sarbanes-Oxley (SOX) Compliance: Plantronics is SOX compliant
- PCI: Plantronics is a PCI-certified Level 4 Merchant and has completed the Payment Card Industry Data Security Standard's (SAQ-D) allowing us to use a third party to process customer credit card information securely.
- TRUSTe: Plantronics is currently pursuing TRUSTe certification
- ISO 9000 and 27000: Plantronics is currently ISO 9000 certified and plans to pursue ISO 27000 certification in 2017.

The environment that hosts the Plantronics Manager Pro services maintains multiple certifications for its data centers, including ISO 27001 compliance, PCI Certification, and SOC reports. For more information about their certification and compliance, please visit the AWS Security website and the AWS Compliance website.

DATA RETENTION

Customer data is retained as long as required to support the functionality of Plantronics Manager Pro.

DELETION OF CUSTOMER DATA

Plantronics will delete customer data within 30 days of cancellation of services. A certificate of data destruction will be issued once all data has been deleted and all data back-ups have expired and been purged.

CUSTOMER DATA EXPORT

Customers can run reports from Plantronics Manager Pro to preserve data elements and metrics.

DATA ENCRYPTION IN-TRANSIT

Plantronics Manager Pro services uses industry-standard HTTPS/TLS for Data Encryption in-transit.

AVAILABILITY

Plantronics Manager Pro is a highly-available service that you can count on. 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 quickly resolves any incidents.

DISASTER RECOVERY

Customer data is stored at multiple locations in our hosting provider's data centers to ensure access and protection. We have well-tested backup and restoration procedures, which allow recovery from a major disaster. Customer data and our source code are automatically backed up nightly. The operations team is alerted in case of a systems failure. Backups are fully tested at least every 90 days to ensure that they work as expected.

NETWORK PROTECTION

In addition to sophisticated system monitoring and logging, we have implemented two-factor authentication for all server access across our production environment. Firewalls are configured according to industry best practices and unnecessary ports are blocked by configuration.

HOST MANAGEMENT

We perform automated vulnerability scans on our production hosts and remediate any findings that present a risk to our environment.

LOGGING

Plantronics monitors and analyzes access, security and availability logs for production Plantronics Manager Pro deployments. Logs are subject to the same security measures as all other application information.

INCIDENT MANAGEMENT AND RESPONSE

In the event of a security breach, Plantronics will promptly notify the customer of any unauthorized access to their data. Plantronics has incident management policies and procedures in place to handle such an event.

EXTERNAL SECURITY AUDITS

We contract with respected security firms who perform regular audits of the Plantronics Manager Pro services to verify that our security practices are sound, and to monitor our services for new vulnerabilities discovered by the security research community.