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.
We utilize enterprise-class security practices to ensure our customers' confidence in the Plantronics products.

This document is intended as a summary of Plantronics' security policies and procedures related to Plantronics Manager Pro Software-as-a-Service offering. The terms and conditions of the documents and policies cited below control and supersede this summary to the extent there is any inconsistency
We encourage you to review these sites regularly as the contents may change. Additionally, your Plantronics Authorized Reseller may have other policies and terms that affect your Plantronics Manager Pro subscription. If you have specific questions, please direct them to your Plantronics Authorized Reseller.

These are the terms and policies that govern Plantronics web and email activities as well as the data privacy of people that interact with Plantronics:

- Plantronics Privacy Policy for the United States: http://www.plantronics.com/privacy
- Plantronics.com Terms of Use: https://www.plantronics.com/us/en/legal/terms/terms-of-use

These are the policies and terms of services that govern our software and software-as-a-service:

- Plantronics Manager and Plantronics Manager Pro Service Level Agreement: https://www.plantronics.com/content/dam/plantronics/documents-and-guides/en/legal/pm-pmp-sla.pdf
- Plantronics Terms of Service: https://www.plantronics.com/us/en/legal/terms/software-services
- Plantronics Application End User License Agreement: https://www.plantronics.com/us/en/legal/terms/application-end-user-license-agreement
- Plantronics Manager and Plantronics Manager Pro Supplemental Service Terms: https://www.plantronics.com/content/dam/plantronics/documents-and-guides/en/legal/pm-pmp-supplemental-service-terms.pdf
- Plantronics Software Privacy Policy: https://www.plantronics.com/software-privacy

Plantronics Manager Pro Security Control Questions

Common Questions

1. Do you have a Security Awareness Program?

    - Yes, Plantronics offers a Security Awareness program to ensure that all employees and contractors have the proper training and knowledge on Plantronics' security policies and procedures. Additionally, Plantronics conducts background checks on all employees before employment, and our IT employees receive additional cyber security training during onboarding as well as on an ongoing basis.

Risk Management

2. Describe the processes to identify and remediate vulnerabilities.

    - 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 standard practices and unnecessary ports are blocked by configuration.

    - Host Management: Automated vulnerability scans are performed on our production hosts and findings that may present a significant risk to our environment are timely remediated.

3. Describe the process used to maintain secure configurations on workstations, servers and network elements.

    - Plantronics Manager Pro is an Internet based subscription service and therefore this question is not applicable to the service operation.

4. Describe the security patch process, including the risk assessment process used to prioritize patches and the implementation timeframe associated with each priority.

    - Plantronics Manager Pro is an Internet based subscription service and therefore this question is not applicable to the service operation.

5. Describe, in general, the processes for disposal and reuse of equipment and software, including the removal of end customer information?

- Plantronics Manager Pro is an Internet based subscription service and disposal and reuse of equipment and software is therefore not applicable to the service operation.

- Plantronics will retain Data stored in end customer accounts for at least 30 days after expiration or termination of the end customers' PMP subscriptions. During this 30-day period end customers may access the Website solely for the purpose of extracting their Data. Within a reasonably practicable period of time after the 30-day post-termination period ends, Plantronics will disable an end customer's account and use reasonable efforts to delete and/or destroy the Data, and issue a Certificate of Destruction. Plantronics has no liability for deletion of Data according to its terms. (See the Plantronics Manager Pro Supplemental Service Terms). Plantronics makes no commitments regarding Data retention with respect to free trials or promotions. Note that while the subscription is active Data retention parameters can be customized by the administrator of Plantronics Manager Pro. Current default is to retain the data indefinitely and customers can run reports from Plantronics Manager Pro to preserve data elements and metrics.

6. Describe your processes for detecting and preventing malware infections or detecting unauthorized hardware/software.

    - Plantronics Manager Pro is an Internet based subscription service and therefore this question is not applicable to the service operation.

    - For Plantronics host computers used to manage and operate the Plantronics Manager Pro services, automated vulnerability scans are performed on production hosts and any findings that present a significant risk to our environment are remediated.

7. Describe your processes and controls for ensuring the isolation, confidentiality and integrity of customer sensitive information in your virtual server environments; including any SaaS, PaaS or laaS vendors that you use to provide services.

    - Please see the data privacy information described in more detail in the Plantronics Software Privacy Policy.

    - When a company uses Plantronics Hub in a Plantronics Manager Pro environment, the enterprise (your company) owns the data created and stored (or that is created and stored automatically). With appropriate authorized written consent, the enterprise may allow access to the data by its reseller, Plantronics, or other parties it may designate.

    - As a policy, Plantronics employees do not monitor or view stored data. However, in limited circumstances Plantronics Associates and Contractors may need to access or review your data. The following are some examples of when such a review may be conducted:

- We believe the Terms of Service have been violated and confirmation is required or we otherwise have an obligation to review account data as described in our Terms of Service;
- We need to do so in order to respond to a request for support;
- Where necessary to protect the rights, property or personal safety of Plantronics or its users; or
- In order to comply with legal obligations including, without limitation, responding to warrants, court orders or other legal process. When legally authorized, we will endeavor to provide the authorized representative of the account owner with notice of a request for account data.

8. Is access to information and technology limited to a need-to-know, job function basis?
    - Yes

9. Is customer sensitive data sent, received, or stored on unencrypted mobile devices such as laptops, tablets or smart phones?
    - Plantronics Manager Pro is a service and therefore this question is not applicable to the service operation.

10. Do you remotely delete data from mobile devices such as laptops, tablets or smart phones in the event of loss or theft of the device?
    - Plantronics Manager Pro is a service and therefore this question is not applicable to the service operation.

Logical Access Controls

11. Which group or team authorizes and which group or team implements firewall rule changes?
    - This is not applicable to Plantronics Manager Pro functionality

12. Is the user required to change his or her initial password during first logon to all systems?
    - Yes.

13. Do you have a standard for minimum password requirements and if so, what is it?

- With respect to customer passwords, the customer may use the single sign-on functionality and configure their own password requirements.

- From an administrative perspective, Plantronics requires strong password authentication and the Dev Ops team is required to use multi-factor authentication.

14. Is there an automated screen lock after a period of inactivity?

- Plantronics Manager Pro is a service and therefore this question is not applicable to the service operation.

- Plantronics computers used to manage and operate the service are equipped with automated screen locks.

Communications

15. Describe how confidentiality of sensitive information is ensured during wireless access.

- Plantronics Manager Pro services uses industry-standard HTTPS/TLS for Data Encryption in-transit and hardware based encryption for data at rest.
  .

16. Have only services essential to network devices been enabled and all other services disabled?

- Plantronics Manager Pro is a service and therefore this question is not applicable to the service operation.

17. Describe the controls utilized to protect customer information in transit and at rest.

- As stated in the Plantronics Software Privacy Policy, Section IV, " We use a combination of administrative, physical and logical security safeguards and continue to work on features to keep your information safe. Your data is accessed by Plantronics as required to support the Service and access is limited to only those within the organization with the need to access to support the Service. For Plantronics Manager Pro data we use industry standard HTTPS/TLS for data encryption in transit and hardware based encryption for data at rest.

18. Describe controls implemented to ensure your network infrastructure is secure and available.

- Plantronics Manager Pro is a service powered by Amazon Web Services. Please refer to Amazon Web Services security policies at https://aws.amazon.com/security/ . Plantronics Manager Pro is a highly-available service. 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, Plantronics DevOps manages and maintains the service under the Plantronics Manager Pro Standard Operating Guidelines.

19. Describe the processes for detecting anomalous traffic on your network.

    - Plantronics Manager Pro is a service powered by Amazon Web Services. Please refer to Amazon Web Services security policies at https://aws.amazon.com/security/ .

20. Is customer production data used in Plantronics' development or test environments?

    - Generally no, except when required to respond to a request for customer support.

Vulnerability and Management

21. How often are vulnerability scans and penetration tests performed?

    - Plantronics Manager Pro is a service powered by Amazon Web Services. Please refer to Amazon Web Services security policies at https://aws.amazon.com/security/ .

22. What is the scope and which systems are covered in Plantronics' vulnerability testing?

    - Plantronics Manager Pro is a service powered by Amazon Web Services. Please refer to Amazon Web Services security policies at https://aws.amazon.com/security/ .

23. Describe Plantronics' security incident management procedures.

    - Plantronics Manager Pro is a service powered by Amazon Web Services. Please refer to Amazon Web Services security policies at https://aws.amazon.com/security/ .

    - Plantronics DevOps manages and maintains the service under the Plantronics Manager Pro Standard Operating Guidelines. Section 2.6.1 of this document states, "The Cloud Operations team will monitor Plantronics Manager for security events. If it is determined that a breach has occurred Cloud Operations will report the event to the Information Security Management team. Information Security Management will engage Legal and Engineering to determine next steps to contain and remediate the breach. Legal will determine how the breach will be communicated and to whom."

24. For breaches or loss of confidentiality with respect to customer data, describe Plantronics' procedures for investigation and notification.

    - Plantronics Manager Pro is a service powered by Amazon Web Services. Please refer to Amazon Web Services security policies at https://aws.amazon.com/security/ .

    - Plantronics Software Privacy Policy, Section IV states, "If Plantronics learns of a security system breach, we may attempt to notify you and provide information on protective steps, if available, through the email address that you have provided to us or by posting a notice on our web site and/or via other communication platforms. Depending on where you live, you may have a legal right to receive such notices in writing."

25. What type of DDoS protection strategy do you have in place?

    - Plantronics Manager Pro is a service powered by Amazon Web Services. Please refer to Amazon Web Services security policies at https://aws.amazon.com/security/ .

Backup and Media

26. How is customer information backed up?

    - The Plantronics Manager Pro Security Overview states: "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."

27. How is the backup media containing customer information secured?

    - Plantronics Manager and Plantronics Manager Pro are backed up to a secure offsite backup service.

28. If you store information at an off-site facility, do you utilize bonded carrier services to transfer information to and from the offsite location?

    - Our backup service does not employ the use of physical media.

29. How do you determine what must be recovered and by when?

    - Our operational objective is to restore the operation of Plantronics Manager Pro as quickly as possible during a service outage. The steps we take are dependent on the nature of the outage incident.

30. Are paper records stored in locked containers and/or shredded?

- Plantronics Manager Pro is a service and therefore this question is not applicable to the service operation. No paper records are maintained to operate this service.

31. What are your documented procedures for the safe and secure disposal of electronic/removable media?

    - Plantronics Manager Pro is a service and therefore this question is not applicable to the service operation. Removable media is not used to operate this service.

Disaster Recovery and Business Continuity

32. What efforts does Plantronics employ to ensure continuity of its services?

    - 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 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.

33. When can customers expect service to be restored following a disaster at one of Plantronics' facilities; i.e., what is your Recovery Time Objective (RTO)?

    - When a system outage occurs, we will post notification on the Manager Pro System Status page here: http://www.plantronics.com/us/support/system-status/ along with the expected resolution time.

34. Considering Plantronics' backup schedule, how old might the data be following a recovery; i.e., what is your Recovery Point Objective (RPO)?

    - The Plantronics Manager Pro Security Overview states: "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."

Compliance / Governance

35. What audits and certifications does Plantronics maintain?

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

- Sarbanes-Oxley (SOX) Compliance: Plantronics is SOX compliant

- TrustArc: TRUSTe certification for Trusted Download (Plantronics Hub) & Privacy Shield (Plantronics Manager Pro)

- Plantronics is ISO 9000 certified.

- Plantronics Manager Pro is hosted in the AWS environment. AWS 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 Cloud Security, Identity and Compliance website.

- 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.

36. How long are logs available to assist in forensic reviews or for monitoring purposes?

    - Plantronics Manager Pro is a service powered by Amazon Web Services. Please refer to Amazon Web Services security policies at https://aws.amazon.com/security/ .

    - 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.

37. How is Information Security part of the system development life cycle (SDLC) for new projects/applications?

    - Code is reviewed prior to advancement to production.

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