INFO SHEET

Planview PPM Pro: A Secure Project Collaboration Solution

The security of your information is as critical as your business is dynamic. That's why we built Planview PPM Pro™ on a foundation of the industry's most stringent data security standards.

How does Planview PPM Pro support your needs? Just ask.

1. What third-party audits are performed in the PPM Pro environment?

PPM Pro has an established information security management system (ISMS), which was awarded ISO 27001 certification by Intertek, an independent auditor. Additionally, PPM Pro is independently audited against a rigid set of SOC 2 controls annually.

A copy of this documentation can be requested by customers or prospects with an NDA in place.

In addition to using third-party evaluations of our information security practices and general IT controls, we subject our infrastructure and application to regular vulnerability scans. Finally, annual penetration tests are carried out by independent third parties. We also have these tests repeated whenever we make significant changes to the PPM Pro environment.

2. What steps do you take to protect my information from unauthorized network access, such as malicious internal users, external hackers, viruses, and other types of malware?

The Planview PPM Pro production environment is protected by a robust network infrastructure that provides a secure environment for all customer data. The PPM Pro service is on a physically segregated network that requires VPN access and two factor authentication for administrative access. Planview® also monitors and analyzes system logs to identify unusual traffic patterns, potential intrusion attempts and other security threats. Planview also uses other 3rd party tools and services to provide end-to- end network visibility and protection.

3. How would I be informed were there an incident or breach that could potentially expose sensitive user information?

Planview has developed security incident responses and escalation procedures to ensure timely and effective handling of all situations. If there were ever a security incident that could cause a major service disruption or lead to exposing of client data, you would be informed promptly.

"The security of your data is our priority. PPM Pro is ISO27001 certified with role-based access controls, 99.5% uptime, and encryption of customer data both in transit and at rest."

– Lance Wright, Director of Information Security - Planview, Inc.

4. What processes are in place to make PPM Pro less vulnerable to known web-application attacks?

   The PPM Pro solution is constructed on a multi- tier architecture, consisting of web servers, application servers, and database data storage.

   Planview uses best practice coding standards and an established software development life cycle that incorporates security from the very start; our development team leverages industry guidelines, such as the Open Web Application Security Project (OWASP), Secure Coding Guide, SANS CWE Top 25, and CERT Secure Coding.

5. How is my organization's data segregated from that of other clients?

   Data segregation in the PPM Pro service is managed by utilizing a data access layer (DAL). The DAL is implemented at the database connection layer in the application stack and enforces a connection to set the customer context (CustomerID). This context is then used to enforce security and strictly limit that connection to only the data that is owned by that customer.

   Production or user data is not used in the PPM Pro testing environment. Production and test environments are physically segregated; only dummy user data is used in testing.

   We do not store user data on backup media; instead, we rely on real-time replication of data (through mirroring and online backups) in redundant systems for availability, hosted at co-location sites. Security controls for the segregation of user data are identical in both environments.

6. How is confidential data stored and transmitted by the PPM Pro service protected? Which encryption methods are used?

   Data in transit is encrypted with the TLS v1.2 protocol. User data (including login information) is always sent through encrypted channels.

   All data stored in the PPM Pro solution is automatically encrypted with a unique key, using FIPS-140-2 validated hardware security modules. Encryption keys are stored separately, with precautions taken to prevent unauthorized access both to encrypted data and their corresponding encryption keys.

7. What staff has access to the production databases?

   Only a very limited number of system operation team members have access to the production databases, and access is granted on a least- privilege, need-to know basis. Access is reviewed semi-annually, and requires VPN connection with multi-factor authentication.

8. Which of my data stored in the PPM Pro solution can be viewed by PPM Pro staff?

   Customer data can only be viewed by Customer Care and Customer Success Managers. Access to customer data is only allowed for support purposes.

9. Where are PPM Pro production servers located, and how is access to my assets and/or information controlled, physically secured, and restricted solely to authorized staff?

PPM Pro is hosted as follows: U.S. customers are hosted in Oregon, U.S., Canadian customers are hosted in Montreal, Canada, EMEA customers are hosted in Germany, and our APAC customers are hosted in Australia.

The hosting provider is an ISO 27001-certified service organization that provides 24-hour physical security.

Security measures include comprehensive identification, access control and monitoring systems, automatic fire protection, redundant climate control, and fail-over power supply. No PPM Pro staff have access to the hosting provider's physical sites.

10. What data-backup and data-retention policies apply to the information stored on PPM Pro production servers?

Multiple Read-Only databases are deployed across disparate geographic areas to mirror the master database in real time, enabling database durability, scalability, and resiliency. Point-in-time recovery allows for database restoral during our 35-day retention period.

PPM Pro retains user data as long as clients remain members of the service. PPM Pro can retain user data indefinitely for active project members. Upon customer exit, data persists 125 days after the contract termination date.

11. What is the backup schedule for PPM Pro servers? How much data could my organization potentially lose?

The PPM Pro service is fully redundant with real- time database mirroring. Point-in-time recovery allows for database restoral during our 35-day retention period.

PPM Pro performs quarterly disaster recovery tests to validate the effectiveness of its backup process.

12. What are the RTO and RPO of the disaster recovery solution for the PPM Pro service?

For the PPM Pro service, the RPO (Recovery Point Objective) is 2-5 minutes, and the RTO (Recovery Time Objective) is 4 hours.

In the event of a major disruption or disaster at one or both production sites, an emergency response team consisting of selected Planview staff, is summoned to activate the disaster recovery plan.

13. How long are backups and operating data retained?

Upon customer exit, data persists in the backup system for 125 days after the contract termination date.

14. How is my organization's data disposed of at the time of contract termination?

Customer data is deleted by an automated process 125 days after the end of the customer's term.

15. What controls are implemented and enforced that protect user credentials and ensure a secure login procedure?

All PPM Pro users are required to authenticate with a unique username /password combination. These credentials are encrypted when transmitted over the Internet (HTTPS) and when at rest in the PPM Pro database. A standard combination of password length and complexity is required of all users, but your organization can customize this to enforce your own security requirements.

16. Does PPM Pro support Single Sign On ("SSO") for the login procedure?

Yes, PPM Pro supports Single Sign On ("SSO"), using the Security Assertion Markup Language ("SAML") and Active Directory Federation service for enterprise clients. This allows network users to access the PPM Pro solution without having to log in separately, with authentication federated from Active Directory. This reflects the industry's standard procedure for SSO that is widely in use. Multi-factor authentication can be integrated with SSO if desired.

17. Can we mitigate our security risk by limiting access to the PPM Pro solution through filtering IP addresses?

IP address ranges can be configured by the local administrator, allowing customers to specify the IP addresses that can access their instance of PPM Pro to provide an extra layer of control and security.

18. Is PPM Pro a PCI DSS-certified merchant/service provider?

PPM Pro does not process credit card information, and thus does not require PCI (Payment Card Industry) certification.

19. Is PPM Pro HIPAA compliant?

Because PPM Pro does not store or process any medical related data, the service does not fall under the requirements for HIPAA compliancy.

20. Does PPM Pro support two-step verification (aka two factor authentication)

Yes, PPM Pro supports two step verification for added login security.

Have a question you didn't see answered here? Let us know at **security@planview.com**

For more information about Planview PPM Pro security, visit **Planview.com/Trust**