DATA SHEET

# Security, Trust, and Assurance

## A closer look at Planview PPM Pro safeguards

**Security, trust and assurance**

**Security: Planview® protects all of your data**

- ✔ Confidentiality
- ✔ Integrity
- ✔ Availability

**Trust: Your data is yours**

- ✔ Applicable legislation
- ✔ Data ownership and Data Retention
- ✔ Escrow and exit strategies
- ✔ Privacy statement
- ✔ Cookie information

**Assurance: Tested and approved**

- ✔ ISO-certified service
- ✔ Cloud Security Alliance- STAR
- ✔ Enterprise-ready service
- ✔ Independent audits

## Security: Planview Protects All of Your Data

### Confidentiality

#### Locked-up network perimeter

The Planview PPM Pro™ ("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.

#### Permissions management

Permission management controls all access to PPM Pro entities (projects, resources, tasks, request and so on). Permissions can be granted or revoked based on a User-type, Group-type or profile-based level. This model allows for tight, granular control within the system to ensure data integrity and confidentiality.

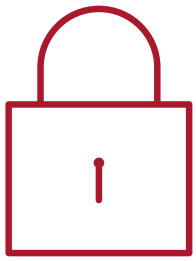
#### World-class Security

Planview uses TLS protocol with 256-bit AES encryption to protect data in transit in PPM Pro. User data (including login information) is always sent through encrypted public channels. Furthermore, all data is encrypted at rest within the primary and databases replicas. The encryption keys are stored separately, and have tightly controlled, restricted administrator-only access.

### Strong passwords and unique user names

Each PPM Pro user is identified with a unique user name and authenticated with a personal password in the system. With strong passwords enabled, the required minimum length of a password is eight characters; one upper case letter, one lower case letter, and one numeric or special character are requirements. Password also can not match previous passwords.

This policy includes external members of enterprise projects. If a user's password does not comply with the policy, access to the project is denied. User-defined password requirements include minimum password length, complexity by means of a combination of upper/lower case characters, numerical digits and maximum password age.



### IP Restrictions

Further security can be realized through the use of IP address restrictions. With IP restrictions enabled, access to the system can be restricted by IP address range.

### Integration with Single Sign-On (SSO)

No need to remember multiple passwords. PPM Pro supports single sign-on (SSO) and utilizes SAML and active directory federation service for its enterprise clients. Multi-factor authentication can be enabled for additional security.

## Integrity

### Physical and environmental measures

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

PPM Pro uses ISO-27001 certified and SOC2/SSAE16 audited co-location facilities, which provide around-the- clock physical security and top-notch environmental protection. It includes comprehensive identification systems, automatic fire protection, redundant climate control and fail-over power supply.

### Protection against malware

Planview provides anti-virus software for all its critical systems commonly affected by malware.

### Audit logging, monitoring and traceability

PPM Pro has comprehensive traceability through object history, with all changes logged and visible. PPM Pro stores all data in a secure manner, with information intact from any changes in any manner.

## Availability

### System status

System availability is monitored by multiple 3rd party applications and / or services. This information is published on the publicly facing, PPM Pro status website. Why publish information about system availability? Because Planview believes system availability transparency provides customers with operational visibility and helps foster a trusting relationship with all of our customers.

### Multi-layer redundancy

The PPM Pro network infrastructure is designed with redundancy and maximum availability. In the event of failure, all operation-critical components, including network, web, application and database servers, as well as storage, has been deployed and configured for near-seamless transition.

### Robust Networking Environment

PPM Pro capitalizes on the reliability, flexibility, security, scalable and high-performant network infrastructure that hosts our service.

The global footprint of our network allows us to deliver our services safely and quickly to all customers regardless of their location.

### Disaster recovery and business contingency

The PPM Pro production systems operate in four geographically dispersed regions. All critical servers and services are installed in at least two data centers within each region. If one of the data center fails, the second data center is configured to take over all production tasks, guaranteeing minimal service disruption or capacity loss. In the event of a major disruption or disaster, an emergency response team of selected Planview staff is summoned to activate the disaster recovery plan.

### Backup and restoration

Planview has put into effect redundancy and backup routines for its production databases. In the unlikely event of multiple server failure, the backups serve the sole purpose of restoring the whole production system. All data stored on the primary database servers is mirrored on secondary and tertiary servers in near-real time. The standby servers are located in geographically disparate locations and are configured to automatically take over production tasks if a primary database server fails.

# Trust: Your Data is Yours

## Data ownership

All customer data stored in PPM Pro is owned solely by the customer. Customers can download their files at any time, provided appropriate permissions are in place. Upon termination of service, customers are provided in-application tools and support to retrieve their data in a timely manner.

## Data retention

Data can be restored to a point-in-time up to the last 5 minutes for the past 35 days. Upon customer exit, data persists 125 days after the contract termination date.

## Privacy statement

The sole personal information viewable by Planview support and sales staff is the user contact information – i.e. name, e-mail address, address, phone number(s), and membership in projects.

PPM Pro administrators are able to view the names of all projects and its members created within the service. Planview does not share this information with anyone, nor does it ever sell or market this information to any third party. Planview employees are prohibited access to any user project data or uploaded documentation. In fact, its extensive encryption procedures effectively prevent anyone (including employees) to access this information through normal daily operations or existing tools.

Planview has formulated a privacy statement which explains how the company gathers and disseminates user-related information. The statement is available on the Planview website: https://www.planview.com/legal/privacy-statement/.

## Cookie information

PPM Pro and Planview.com use cookies to optimize the user experience. Cookies help make PPM Pro work according to user expectations. Cookies are used to keep track of user session information. No other data related to authentication or sessions is stored on the client. Planview does not collect any personally identifiable or sensitive information without written consent and permission.

# Assurance: Tested and Approved

## ISO-certified service

PPM Pro has been awarded ISO-27001 certification – an international standard for information security. This includes proactive management of information security risks and controls. ISO-27001, a high-end certificate, guarantees that PPM Pro has well-established structures for information security that run throughout the organization – from top to bottom.

## Independent audits

Planview commits considerable resources to continually assessing security threats, as well as developing its infrastructure and system's security functions. The PPM Pro infrastructure and application is subject to regular vulnerability scans (on a quarterly basis) with annual penetration tests carried out by independent third parties. These tests are repeated after any significant changes take place in its environment. Additionally, Planview entrusts external auditors to evaluate its information security practices and general IT controls.

## About Planview

As the global leader in work and resource management, Planview makes it easier for all organizations to achieve their business goals. We provide the industry's most comprehensive solutions designed for strategic planning, portfolio and resource management, product innovation, capability and technology management, Lean and Agile delivery, and collaborative work management. Our solutions span every class of work, resource, and organization to address the varying needs of diverse and distributed teams, departments, and enterprises. Headquartered in Austin, Texas, Planview's more than 700 employees serve 5,000 customers worldwide through a culture of innovative technology leadership, deep market expertise, and highly engaged communities. For more information, visit www.planview.com.