Planview Projectplace™

DATA SHEET

Security, Trust, and Assurance

A closer look at Planview Projectplace 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 network containing the Planview Projectplace™ ("Projectplace") production servers (the service) is protected by redundant firewalls, intrusion detection systems and load balancers. The Projectplace service is on a physically segregated network that requires two-factor authentication for administrative access from its office network. Planview® proactively monitors and analyzes firewall and system logs to identify unusual traffic patterns, potential intrusion attempts and other security threats. Planview also uses reliable network monitoring services for its co-location facilities.

Role-based access control

Access control is native at every level in Projectplace. As an example, workspace administrators can create user groups and assign access rights at the folder level, restrict access to workspace administrative tools, lock documents, or hide boards to ensure confidentiality.

World-class Security

Planview uses TLS protocol with 256-bit AES encryption to protect data in transit in Projectplace. No user data (including login information) is ever sent through unencrypted public channels. Furthermore, all documents stored in Projectplace are automatically encrypted with a unique key, using the AES-256 encryption algorithm, which is saved anonymously in order to prevent identification. The encryption keys are stored separately, and precautions taken to prevent unauthorized access both to the encrypted document and its corresponding encryption key.

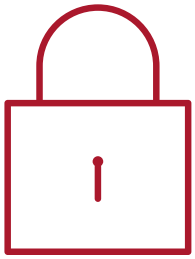
All user passwords are stored in a one-way encrypted format which is invisible to Planview employees thereby eliminating the ability to retrieve lost or forgotten passwords.

Strong passwords and unique user names

Each Projectplace user is identified with a unique user name and authenticated with a personal password in the system. The required minimum length of a password is six characters. Policies with more stringent password requirements can be implemented either at the enterprise level for all projects under that enterprise account or at the workspace level by the workspace head administrator.

This policy includes external members of enterprise projects. If a user's password does not comply with the policy, access to the workspace 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.

Two-step verification



With two-step verification users' accounts are protected by both their password and their mobile. We encourage all Projectplace users to enable this extra layer of user login security.

Integration with Single Sign-On (SSO)

No need to remember multiple passwords. Projectplace supports single sign-on (SSO) and utilizes SAML and active directory federation service for its enterprise clients.

Integrity

Physical and environmental measures

The Projectplace production environments are currently hosted in Ohio, USA for our U.S./Latin America customers and in Stockholm, Sweden for all other worldwide customers. Projectplace 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

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

Availability

System status and performance

The availability of the service and uptime status is monitored by Pingdom®, an independent third-party. This information is published daily on the Projectplace website. Why publish information about system performance and status? Because Planview believes in transparency of system usage and system performance. When evaluating Planview or using the Projectplace service, users may want to know how well the service performs over time and how fast the service is.

Multi-layer redundancy

The Projectplace network infrastructure is designed with complete redundancy and maximum availability. In the event of failure, all operation-critical equipment, including routers, firewalls, web, application and database servers, as well as storage and network arrays, has been deployed and configured for seamless transition.

Web acceleration and content delivery

Through collaboration with Content Delivery Networks, one of the world's leading, distributed, computing platforms, the Projectplace service realizes improved performance for our customers around the world.

Disaster recovery and business contingency

The Projectplace production system is run on a multi- site cluster at two geographically dispersed locations; U.S. data center reside in Ohio, U.S. while EU data centers are in Sweden. In the event of a major disruption or disaster at one or both production sites, an emergency response team of selected Planview staff is summoned to activate the disaster recovery plan.

Backup and restoration

Planview has put into effect multi-step mirroring and backup routines for its production databases and document storage systems. In the unlikely event of multiple server failure, the backups serve the sole purpose of restoring the whole production system. Planview employees are unable to restore individual projects or documents from backups. All data stored on the primary database servers is mirrored on secondary servers in real time. The secondary servers are located at the second data center provider's co-location facility and are configured to automatically take over production tasks if a primary server fails.

Trust: Your Data is Yours

Data ownership

All user data stored in Projectplace is owned solely by the account the user belongs to. Users can download their files at any time during the workspace lifecycle. When no longer using the service, archiving can be done offline. The service also features data portability, which provides users with tools to facilitate easy data exports; needless to say, access control rules apply.

Data retention

Once a user initiates the deletion of workspace data – e.g. emptying a project's wastepaper basket or terminating a workspace – the object referrers and its associated encryption keys are deleted from the Projectplace database. This initiates the garbage collection process: removal of the encrypted file from the data vault and overwriting of the data within 30 days. The process is identical for both primary and secondary data centers. User data is never stored on removable storage systems or backup media.

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.

Projectplace 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 workspace 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

Projectplace.com and Planview.com use cookies to optimize the user experience. Cookies help make Projectplace work according to user expectations. Planview does not collect any personally identifiable or sensitive information without written consent and permission. More information about Cookies can be found on the Planview website here: https://www.planview.com/trust/privacy/statement/.

Assurance: Tested and Approved

ISO-certified service

Projectplace 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 Projectplace has well-established structures for information security that run throughout the organization – from top to bottom.

Cloud Security Alliance – STAR

The Security, Trust & Assurance Registry (STAR) of the Cloud Security Alliance® (CSA) is a publicly accessible registry, documenting the security controls provided by various cloud computing offerings, which help users assess the security of cloud providers they currently use or are considering using. It is a simple but powerful idea: cloud providers post self-assessments of their cloud services, which CSA makes publicly available so that cloud consumers can make more informed purchasing decisions. Planview's participation with Projectplace in this initiative and openly publishes information about its security controls in place.

Independent audits

Planview commits considerable resources to continually assessing security threats, as well as developing its infrastructure and system's security functions. The Projectplace 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.