Planview Projectplace™

INFO SHEET

Planview Projectplace: A Secure Collaborative Work Management Solution

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

How does Planview Projectplace support your needs? Just ask.

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

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. In addition, annual penetration tests are carried out by independent third parties. We also have these tests repeated whenever we make significant changes to the Projectplace environment.

Projectplace has an established information security management system, which was awarded ISO 27001 certification by Intertek, an independent auditor. A copy of this certificate can be requested by customers or prospected with an NDA in place.

2. How do I request to have a penetration test of Projectplace conducted?

We have an open policy that allows our clients to perform penetration tests of our service. The pen test may be performed either by you or a third party whom you appoint, provided that relevant non- disclosure agreements have been completed and testing pre-conditions including such items as dedicated time frames and defined test types, have been met.

3. 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 network containing the Projectplace production servers (the service) is protected by redundant firewalls and load balancers. The Projectplace service is located on a physically segregated network that requires two-factor authentication for administrative access.

We proactively monitor and analyze firewall and systems, using our internal system for security information and event management to identify unusual traffic patterns, potential intrusion attempts, and other security threats. Industry-leading network monitoring services deliver another line of defense.

4. 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 the exposing of client data, you would be informed promptly.

"The security of your data is our priority. Projectplace is ISO27001 certified with role-based access controls, 99.5% uptime, and 256-bit AES encryption both in transit and at rest."

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

5. What processes are in place to make Projectplace less vulnerable to known web-application attacks?

The Projectplace 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.

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

We achieve logical separation of user data through object level access controls and encryption. In the Projectplace solution, each object links to a file individually encrypted, using an AES-256 algorithm. Access controls are implemented at the object level to prevent unauthorized users from accessing data.

Production or user data is not used in the Projectplace 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.

7. How is confidential data stored and transmitted by the Projectplace service protected? Which encryption methods are used?

Data in transit is encrypted with 256-bit AES ciphers and TLS protocols, using a 2048 bit RSA public key for key exchange. User data (including login information) is not sent through unencrypted channels.

All documents stored in the Projectplace solution are automatically encrypted with a unique key, using the AES-256 encryption algorithm. Documents are saved anonymously, rendering identification impossible. Encryption keys are stored separately, with precautions taken to prevent unauthorized access both to encrypted documents and their corresponding encryption keys.

User data is not stored in the Projectplace database; only the objects which refer to the encrypted files are stored in the data vault.

8. 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 semiannually and requires multi-factor authentication.

9. Which of my data stored in the Projectplace solution can be viewed by Projectplace staff?

Only a client's contact information and project membership can be viewed by support and sales staff. Planview administrators can see project names and associated team members; however, this information is never shared with anyone, nor sold or marketed to any third party, per our Privacy Statement.

Planview staff is prohibited from accessing your project data or uploaded documentation, and given our strong encryption, is effectively unable to do so within normal daily operations or using existing tools.

To obtain access to project data and to recover project files, an administrator must retrieve the encryption key for each individual object and decrypt each file. To prevent unauthorized retrieval of your data, mechanisms for access control through two-factor authentication, logging, and monitoring have been implemented.

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

For U.S. customers, Projectplace is hosted in Ohio, U.S.. For customers outside of the U.S., Projectplace is hosted in Stockholm, Sweden.

The ISO 27001-certified service organization provides server hall facilities with 24-hour physical security.

This includes comprehensive identification, access control and monitoring systems, automatic fire protection, redundant climate control, and fail-over power supply. All physical access to Projectplace data centers is logged and monitored in real time.

11. What data-backup and data-retention policies apply to the information stored on Projectplace production servers?

Multi-step mirroring and online backup routines for production databases and document storage systems have been put into effect. These mirrored data vaults are subject to security control identical to that of the production system. User data is not stored on removable backup media (i.e. tapes).

The backups serve the sole purpose of restoring the whole production system in the unlikely event of multiple server failure. Employees are unable to restore individual projects or documents from these backups.

Upon contract termination, procedures are in place to remove and securely dispose of user data.

Procedures for this include deleting encrypted files from the data vault, removing the referrer object and encryption key from Projectplace databases, and overwriting the allocated memory space in the data vault to prevent restoration.

Projectplace retains user data as long as clients remain members of the service. Projectplace can retain user data indefinitely for active project members.

12. What is the backup schedule for Projectplace servers? How much data could my organization potentially lose?

We operate a fully redundant system with real- time database mirroring. All data generated on the Projectplace primary site is continuously backed up to its secondary site via dual fiber connections. Our disaster recovery tests indicate zero data loss.

Further, in the event of an actual disaster, we commit to keeping recovery time objective ("RTO") and recovery point objective ("RPO") to minimum levels that would not have an adverse effect on users.

13. What are the RTO and RPO of the disaster recovery solution for the Projectplace service?

The Projectplace production server system is run on a multi-site cluster at two geographically dispersed locations. All critical servers and applications are installed at both locations, which, in the case of a major disruption or disaster, ensure business continuity.

All data stored in the primary database servers is mirrored to secondary servers in real time.

Secondary servers are configured to automatically take over production tasks. In the event one of the locations fails, the second site is configured to take over all production tasks with minimal service disruption and capacity loss (estimated RTO less than 30 minutes and RPO of approximately 5 minutes).

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.

14. How long are backups and operating data retained?

Unless data is explicitly deleted by the project user, all project information is retained for the duration of the project. Once you initiate project data deletion – by emptying a project's waste paper bin or terminating a project – that information is no longer retained. Object referrers and their associated encryption keys for deleted objects are deleted from the Projectplace database, which then initiates the garbage collection process, removing the encrypted file from the data vault and overwriting the data.

Projectplace does not use backup tapes or other removable media to store user data. Once the data is purged from both primary and secondary systems, it is no longer available.

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

Once a user initiates deletion of project data, object referrers and their associated encryption keys are deleted from the Projectplace database. This initiates the garbage collection process, which removes the encrypted files from the data vault and overwrites the data.

The process is identical for both primary and secondary data centers. User data is not stored on any removable storage systems or backup media.

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

All Projectplace 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 Projectplace 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.

17. Does Projectplace support Single Sign On ("SSO") for the login procedure?

Yes, Projectplace 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 Projectplace solution without having to log in separately, with authentication federated from the Active Directory. This reflects the industry's standard procedure for SSO that is widely in use.

18. Can we mitigate our security risk by limiting access to the Projectplace solution through filtering IP addresses?

Currently, we do not enable source IP-based access restriction as the Projectplace solution is intended for global access. With nearly a million users worldwide, IP source-address filtering is not a manageable access control for the Projectplace solution.

19. Is Projectplace a PCI DSS-certified merchant/service provider?

Payment Card Industry Data Security Standard ("PCI DSS") is a set of security requirements and guidelines for merchants who store, process, or transmit cardholder data. Payment processing is outsourced to DIBS Payment Services. Cardholder data is not stored, transmitted, or processed by Projectplace. Users are directed to the DIBS secure payment page for online purchasing, and returned to Projectplace upon transaction completion. Since we never touch payment card data, Projectplace is not subject to PCI DSS. DIBS, however, is a PCI DSS-validated service provider for online payment processing.

20. Is Projectplace HIPAA compliant?

Planview personnel (including administrators) have no access to the information stored in Projectplace databases by our clients and as such we do not store, process, and transmit patient records. It is our Customers who are HIPAA compliant, not the solution (Projectplace).

21. Does Projectplace support two-step verification (aka two factor authentication)?

Yes, for added login security, Projectplace supports two step verification via SMS based TOTPs as well as an authentication app like Google Authenticator or via hardware security device like Yubikey.

22. What security measures are in place for the Projectplace Mobile Apps?

The Projectplace mobile apps are available for Android version 6.0 and Apple iOS version 10 and later. The same privileges and access abilities apply for logging in to the mobile app as for the Projectplace browser version. Full disk encryption is applied to all downloaded data.

In addition to the username/password or SAML login, an optional PIN code login can be enabled for increased security. This feature is enabled upon request submitted to the Customer Care team.

The option to prevent Account users from using the mobile apps can be provided upon request submitted to the Customer Care team.

Once a user logs out of the mobile Projectplace app, all download data (cache) is deleted.

Note: The Android app does not work on rooted devices.

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

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