Data sheet

Security, trust and assurance
– A closer look at Projectplace safeguards

Security: Projectplace protects every bit of your data

Trust: Privacy is not dead at Projectplace, your data is yours

Assurance: Tested and approved
Security, trust and assurance

According to a “cloud-computing, market-maturity” survey, conducted jointly by Cloud Security Alliance (CSA) and ISACA* in 2012, top customer concerns about cloud computing include applicable legislation, data ownership, data retention, privacy and integration, as well as the traditional triad of security: confidentiality, integrity and availability.

To address these concerns, Projectplace has established a security, trust and assurance ecosystem and implemented the measures, described in this knowledge document.

Security
- Confidentiality
- Integrity
- Availability

Trust
- Applicable legislation
- Data retention and ownership
- Integration with single sign-on (SSO) Privacy statement
- Cookie information
- Escrow and exit strategies

Assurance
- ISO-27001 certified service
- Cloud Security Alliance- STAR
- Independent audits
Security: Projectplace protects every bit of your data

Confidentiality

Locked-up network perimeter
The network containing the 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.

Projectplace proactively monitors and analyzes firewall and system logs to identify unusual traffic patterns, potential intrusion attempts and other security threats. Projectplace also uses reliable network monitoring services for its co-location facilities.

Role-based access control at folder level
Access control is native at every level in Projectplace. Project administrators can create user groups and assign access rights at the folder level, lock documents or hide boards to ensure confidentiality.

Military-grade encryption
Projectplace uses TLS protocol with 256 bit AES encryption to protect data in transit. 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 Projectplace employees thereby eliminating the ability to retrieve lost or forgotten passwords.

“Security of user data is of utmost importance to Projectplace. This is why some of the biggest businesses in the world and numerous government organizations across Europe entrust Projectplace with their information.”

Erkan Kahraman,
Chief Information Security Officer
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 project level by the project head administrator.

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.

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.
Integrity

Physical and environmental measures

The Projectplace server environment is hosted at two separate co-location facilities. This ISO-certified service organization provides server hall facilities with 24-hour physical security that includes comprehensive identification systems, automatic fire protection, redundant climate control and fail-over power supply. These meet the stringent requirements outlined in the VDMA 24991 international standard.

Protection against malware

Projectplace provides file-integrity monitoring and 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.

“Since its start-up in 1998, Projectplace has been running its service with an average uptime of 99.9 per cent.”
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 Projectplace believes in transparency of system usage and system performance. When evaluating Projectplace or using the service, users may want to know how well Projectplace 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 by Akamai

Through collaboration with Akamai, one of the world’s leading, distributed, computing platforms, Projectplace is now even faster and more reliable.

This network platform increases both response time and performance. The service is faster, not only in non-European countries, but also in rapidly-growing markets, such as Germany and The Netherlands.

“The Projectplace network infrastructure is designed with complete redundancy and maximum availability.”
Disaster recovery and business contingency

The Projectplace production 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 event of a major disruption or disaster, ensure business continuity. If one of the locations fails, the second site is configured to take over all production tasks, guaranteeing minimal service disruption or capacity loss. In the event of a major disruption or disaster at one or both production sites, an emergency response team, consisting of selected Projectplace staff, is summoned to activate the disaster recovery plan.

Backup and restoration

Projectplace 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. Projectplace 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.

“Projectplace business continuity plan ensures minimum disruption to our service with data centers in two geographically dispersed locations and real time data mirroring between them.”
Trust: At Projectplace, privacy is in force. Your data is yours.

Applicable legislation
A significant, competitive Projectplace differentiator is its focus on the privacy and integrity of client data, which includes protection from potential access by overseas legislation, such as, for example, the United States Patriot Act. All its systems are hosted in Stockholm, Sweden, with client data never leaving its private cloud. Most competitors have data centers outside the EU and are therefore not immune to such legislation.

Data ownership
All user files stored in Projectplace are owned solely by the user. Users can download their files at any time during the project’s 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 project data – e.g. emptying a project’s wastepaper basket or terminating a project – 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.

Single Sign-On (SSO) integration via SAML
Projectplace supports Single Sign-On (SSO), using SAML and an active directory federation service for enterprise users. Single sign-on allows network users to access Projectplace without having to log in separately.

“Our service features data portability, we strongly believe in it.”
Escrow and exit strategies

Projectplace has been a trusted service for cloud-based project management software since 1998. Over one million users in more than 160 countries use Projectplace successfully every day. Testimonials can be read on the Projectplace website.

As one of the first SaaS providers, Projectplace is commonly used as an escrow medium for cross-organizational collaboration.

For companies who work together but don’t want the project documents to be hosted by either side, Projectplace is an ideal solution.

While Projectplace does not support escrow agreements by default, it does give its users the technical assurance that all project documents and plans can be downloaded for off-line retention. All data stored on the Projectplace site is solely owned by the client.

Upon deletion of a project or account, Projectplace does not retain any data. Documents can be downloaded if the clients wish to retain documents for a longer period.

Privacy statement

The sole personal information viewable by Projectplace 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. Projectplace does not share this information with anyone, nor does it ever sell or market this information to any third party. Projectplace employees are prohibited access to any user project data or uploaded documentation. In fact, its extensive encryption procedures effectively prevents anyone (including employees) to access this information through normal daily operations or existing tools.

Projectplace has formulated a privacy statement which explains how the company gathers and disseminates user-related information. The statement is available on the Projectplace website: projectplace.com/terms/privacystatement/.

Cookie information

Projectplace.com uses cookies to optimize the user experience. Cookies help make Projectplace work according to user expectations. Projectplace does not collect any personally identifiable or sensitive information without taking permission from the user.
ISO-certified service

Projectplace has been awarded ISO-27001 certification – an international standard for information security. This includes pro-active 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. Projectplace is proud to participate in this initiative and openly publishes information about its security controls in place.

Independent audits

Projectplace 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, Projectplace entrusts external auditors to evaluate its information security practices and general IT controls.
About Projectplace

Projectplace, as a part of Planview, is a global leader in portfolio management and project collaboration. From small teams to large enterprises, leaders in every industry rely on the company’s cloud solutions to empower organizations to reach their goals and drive results by optimizing the capacity of their people and financial resources. Planview’s singular focus fuels a deep commitment to innovation and customer success. For more information, visit www.planview.com and www.projectplace.com.

Contact

Sweden
Projectplace International AB
Phone: +46 8 586 302 75
Email: info@projectplace.se
www.projectplace.se

Denmark
Projectplace Denmark APS
Phone: +45 7020 8490
Email: info@projectplace.dk
www.projectplace.dk

Benelux
Projectplace Nederland BV
Phone: +31-20-889 21 01
Email: info@projectplace.nl
www.projectplace.nl

Norway
Projectplace Norge AS
Phone: +47 21 42 41 40
Email: info@projectplace.no
www.projectplace.no

Germany
Projectplace GMBH
Phone: +49 (0)69 380 7000 00
Email: info@projectplace.de
www.projectplace.de

United Kingdom
Projectplace LTD
Phone: +44 1189 657 736
Email: info@projectplace.com
www.projectplace.com

United States
Phone: (800) 856-8600
Email: info-na@projectplace.com
www.projectplace.com