

# Security Whitepaper

Revision Date 2010-08-13



## Introduction

Projectplace.com is a secure on-demand service for collaboration and project management. We provide a highly available, responsive and safe environment to ensure that our customers' data is never compromised. Since security is crucial for our customers, we prioritise application and information security highly and devote significant resources to continually develop and improve internal processes as well as information and system security.

The purpose of this document is to provide information on our security measures and ensure that Projectplace.com meets the stringent security requirements of businesses and government agencies. The whitepaper will cover the following security-related topics:

- User Registration and Authentication
- Password Security
- Access Control
- Data Encryption
- Physical and Application Security
- Backup and Data Retention
- Disaster Recovery and Business Contingency
- Internal Procedures

**Projectplace regularly consults professional and experienced security experts for penetration tests and audits of newly developed code prior to its release into production. A copy of the certificate issued after the most recent penetration test can be provided upon request.**

## User Registration and Authentication

### User Account Creation

When creating a user account at Projectplace.com, the user selects a password with a required minimum length of six characters. The registration process is encrypted via Secure Sockets Layer (SSL) to ensure that user data is never transmitted in clear text. Projectplace.com does not issue any system-generated passwords, or send passwords in any email messages to the user.

The user must provide a valid email address as a login ID in order to confirm the user account. If the address is not valid, the registration process cannot be completed, and the user account will not be created.

### Login and Authentication

The user can only access Projectplace.com via an encrypted login page, providing a valid combination of login ID (email address) and password. If the login attempt is successful, a unique session ID cookie is used to identify the user. After a longer period of inactivity, the session ID cookie expires, and the user will have to provide re-authentication in order to continue working with Projectplace.com.

If the combination of login ID and password does not match, Projectplace.com will notify the user of the login failure. The message does not indicate the point of failure to prevent information disclosure to potential intruders.

### Brute Force Protection

Projectplace.com utilises brute force protection preventing exhaustive and dictionary attacks on user accounts and passwords. If a user repeatedly fails to provide a valid combination of login ID and password, the account will be locked for an undisclosed period of time.

## Password Security

### Password Storage

All user passwords are encrypted using the SHA1 algorithm upon creation and cannot be accessed by any Projectplace employees. Projectplace employees do not have any possibility to retrieve lost or forgotten passwords. If a user forgets or loses the password for accessing Projectplace.com, the user has to complete a procedure for password retrieval (see below).

### Password Requirements

The required minimum length of a password is six characters.

Policies with higher password requirements can be implemented on two levels:

- On a per-project basis (by the project's head administrator)
- Enterprise-wide for all projects (by the administrator of the Enterprise Edition). This policy includes external members in enterprise projects as well.

If a user's password does not comply with the policy, access to the project or Enterprise Edition is denied.

The optional password requirements include:

- A minimum password length of eight or ten characters
- A combination of letters and numbers
- A combination of upper case and lower case characters
- A maximum password age of 30, 90, or 180 days (for Enterprise Editions).

For optimal security, a long password containing both upper and lower case characters and numbers is recommended. Furthermore, each user has the possibility to specify a password challenge question and answer for password retrieval.

### Password Retrieval

If a user forgets or loses the password for accessing Projectplace.com, a new password needs to be retrieved through a standardised procedure on the Projectplace.com web site. The user needs to submit the login ID and, if specified, an additional password challenge in order to receive further instructions on how to regain access to Projectplace.com.

The login ID has to be exactly the same as the one provided by the user when creating the user account. If the email address representing the login ID has become invalid, it is not possible for the user to retrieve the password and reactivate the user account.

If the user has specified a password challenge, but fails to complete it successfully, the user must contact the Projectplace.com technical support team for further assistance.

After successful authentication, the user will receive an email message with instructions on how to set a new password for Projectplace.com. The message contains a time-limited one-time token to prevent misuse.

## **Access Control**

In Projectplace.com, a redundant application security model ensures that all information can only be accessed by users with proper credentials. Access control is performed for every user action.

## **Data Encryption**

### **Client-Server Communication**

Projectplace.com uses multi-layer data encryption to guarantee maximum information security. All client-server communication is encrypted via Secure Socket Layer (SSL), thus preventing data in transit from being compromised or accessed by a third party. The Projectplace.com SSL certificate is issued by VeriSign, Inc. or a VeriSign partner.

A lock icon in the web browser's address bar indicates that communication on a web site is encrypted. By clicking on the lock, the user can check detailed certificate information and validate its authenticity.

### **Database Storage**

All documents stored at Projectplace.com are automatically encrypted with a unique key using the AES-192 encryption algorithm and saved anonymously so that they cannot be identified. The encryption keys are stored separately, and precautions have been taken to prevent unauthorised access to both the encrypted document and its corresponding encryption key.

## Physical and Application Security

### Physical Security

The Projectplace.com server environment is hosted in two separate co-location facilities operated by Qbranch 365/24 AB in Stockholm, Sweden. Qbranch AB ([www.qbranch.se](http://www.qbranch.se)) is a profitable, fast-growing co-location provider with AAA-rating. The ISO 20000-certified service organisation provides server hall facilities with 24-hour physical security including comprehensive identification systems, automatic fire protection, redundant climate control, and fail-over power supply. Furthermore, they meet the stringent requirements outlined in the international standard VDMA 24991.

### Network Perimeter

The network containing the Projectplace.com servers is protected by redundant firewalls and intrusion detection systems. We proactively monitor and analyse firewall and system logs to identify unusual traffic patterns, potential intrusion attempts, and other security threats. Projectplace.com also uses network monitoring services provided by Qbranch 365/24 AB for the co-location facilities.

### Internet Connection

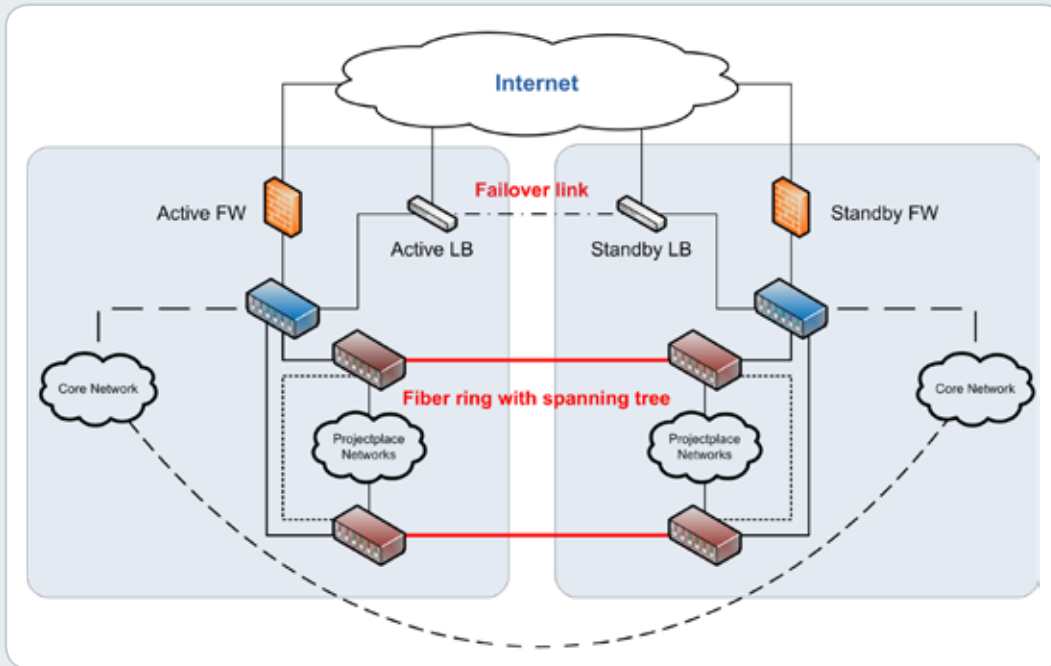
Through Qbranch, Projectplace.com is connected to the Internet via several network providers in a redundant BGP routing environment. If an Internet Service Provider experiences capacity issues or even suffers downtime, the other providers will still guarantee full availability for Projectplace.com.

Currently, the main network providers consist of TeliaSonera International Carrier and IP-only. Furthermore, Qbranch maintains a direct connection to the SOL-IX Internet Exchange in Stockholm, Sweden.

### Multi-Layer Redundancy

The Projectplace.com network infrastructure is designed with the purpose of complete redundancy and maximum availability. All operation-critical equipment, including routers, firewalls, application and database servers as well as storage and network arrays, has been deployed and configured for seamless transition in the unlikely case of a failure.

The following drawing describes Projectplace.com's general system topology:



### **Operating System and Database Security**

All Projectplace.com production servers are hardened at operating system-level. All unnecessary users, services, applications and protocols have been removed, and the systems are maintained at recommended patch levels. Access to servers and production databases is limited to a minimum and protected by strong passwords and other security measures.

### **Server Management**

All information entered or uploaded by a user into Projectplace.com is owned by the user. Projectplace employees do not have any direct server access, except where necessary for system management, maintenance, and backup purposes. Projectplace.com does not utilise any managed service providers. The Projectplace System Operations Team is in charge of all system and network management, maintenance and backups.

## Backup and Data Retention

Projectplace.com has put multistep mirroring and backup routines for the production databases and document storage systems into effect. The backups serve the sole purpose of restoring the whole production system in the unlikely event of multiple server failure. It is not possible for Projectplace employees to restore individual projects or documents from these backups.

All data stored on the primary database servers is mirrored to secondary servers in real time. The secondary servers are located at the second Qbranch co-location facility and are configured to automatically take over production tasks if a primary server fails. Every week, full database backups are performed to an off-site backup server.

Document replication and backup routines follow similar outlines. The file storage consists of several Storage Area Networks (SAN) that are located in separate locations. All data in the primary SAN is replicated to a secondary storage system in real time.

Every night, the system performs an automatic differential backup containing all document files that have been created or modified within the last 24 hours. The nightly backups are kept for seven days before a new backup cycle is started.

In addition to the nightly backups, a backup of the recent week's changes is performed every weekend. The weekly backups are kept for four weeks. All document backups are performed on the secondary SAN. All backups are encrypted, and the encryption of customer data is retained at all steps of the backup process.

Project data is retained in backups for 30 days after a user has initiated its deletion, e.g. by emptying a project's waste basket or terminating a customer project. However, specific deleted data cannot be retrieved since backups are only intended for disaster recovery purposes.

## Disaster Recovery and Business Contingency

The Projectplace.com 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 ensures business continuity in the case of major disruption or disaster. If one of the locations fails, the second site is configured to take over all production tasks with minimal service disruptions and 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.

## Internal Procedures

### Information Security Policy (ISO 27001)

We are committed to the highest possible security standards regarding not only application and system security, but also information security. Therefore we have adopted the rules and recommendations of ISO 27001 for Projectplace. The standard encompasses the whole company and specifies routines for information classification, person,ation of safeguards.

### Threat Evaluation and Risk Assessment

New security risks and threats are continuously evaluated using the Swedish "Miniriskmetod" to ensure that Projectplace.com is securely developed and deployed. For external verification, we regularly consult professional and experienced security experts for security audits and penetration tests.

### Personnel training

Projectplace staff working with system development and maintenance is required to undergo regular security training in order to keep up-to-date with current developments. The company devotes significant resources for training from vendors and security experts to ensure that Projectplace.com represents cutting-edge security to our customers.

### Security Policy

Projectplace has made an external security policy available to demonstrate the company's strong commitment to security. It discloses Projectplace's accessibility and security routines and is available on the Projectplace web site, at: [www.projectplace.com/terms/securitypolicy/](http://www.projectplace.com/terms/securitypolicy/).

### Privacy Statement

Projectplace has created a privacy statement to explain how the company gathers and disseminates user-related information. The statement is available on the Projectplace web site, at [www.projectplace.com/terms/privacystatement/](http://www.projectplace.com/terms/privacystatement/).

## CONTACT

### SWEDEN (HEAD OFFICE)

PROJECTPLACE INTERNATIONAL AB  
KLARABERGSGATAN 60, 1 TR  
111 21 STOCKHOLM  
TEL: +46 (0)8 586 302 00  
FAX: +46 (0)8 586 302 01  
E-MAIL: [info@projectplace.se](mailto:info@projectplace.se)  
[www.projectplace.se](http://www.projectplace.se)

### DENMARK

PROJECTPLACE DENMARK APS  
LINDEVANGS ALLE 3, 2  
2000 FREDERIKSBERG  
TEL: +45 7020 8490  
E-MAIL: [info@projectplace.dk](mailto:info@projectplace.dk)  
[www.projectplace.dk](http://www.projectplace.dk)

### NETHERLANDS

PROJECTPLACE NEDERLAND BV  
SCHIPHOL BOULEVARD 359  
1118 BJ LUCHTHAVEN SCHIPHOL, AMSTERDAM  
TEL: +31-20-201 11 11  
FAX: +31-20-206 52 21  
E-MAIL: [info@projectplace.nl](mailto:info@projectplace.nl)  
[www.projectplace.nl](http://www.projectplace.nl)

### NORWAY

PROJECTPLACE NORGE AS  
ST OLAVS PLASS 2  
0165 OSLO  
TEL: +47 21 42 41 40  
FAX: +47 48 31 71 70  
E-MAIL: [info@projectplace.no](mailto:info@projectplace.no)  
[www.projectplace.no](http://www.projectplace.no)

### GERMANY

PROJECTPLACE GMBH  
WERFTHAUS  
SPEICHERSTRASSE 55  
WESTHAFEN  
60327 FRANKFURT AM MAIN  
TEL: +49 (0)69 380 7000 00  
E-MAIL: [info@projectplace.de](mailto:info@projectplace.de)  
[www.projectplace.de](http://www.projectplace.de)

Projectplace International is the European leader in project collaboration on the Web. Since 1998, Projectplace has been driving the development of online project tools, inspired by Social Project Management. Today, the service is available in seven languages and has helped over 600.000 users to improve communication and collaboration in their projects. The company has 120 employees based at the headquarters in Stockholm and in local offices in Oslo, Copenhagen, Frankfurt and Amsterdam. Visit us at [www.projectplace.com](http://www.projectplace.com)