PROJECTMANAGER

Security White Paper

Security Framework

Table of Contents

Introduction 3

Application Security 3

Cloud Authentication 4

Session Timeout 4

Forms Authentication 4

Password Policy 4

Secure Password Policy 4

Account Lockout 5

Password and Storage Encryption 5

Security and Testing Processes 5

Encryption 5

Email Security 5

Perfect Forward Secrecy 6

Web Security 6

PCI Compliance 6

Network and Infrastructure Security 6

Data Centers 6

Data Center Certificates 6

Physical Security 7

Cooling Systems 7

Network Hardware 7

Server Power and Backup 7

Note on Privacy Shield Commitments 7

DDoS prevention 8

Disaster Recovery and Continuity 8

Redundancy 8

Vulnerability Management and Penetration Testing 9

Business Continuity Testing 9

Firewalls 9

Organizational Security 9

Vendor and Third-party supplier management 9

Breach Notification 10

NIST Cybersecurity Framework 10

Personnel 10

Privacy 10

Conclusion 11

Contact Us 11

Introduction

ProjectManager is a leading project management and work collaboration SaaS platform. Teams like yours from all over the world use ProjectManager's powerful work management features to plan, track, monitor, report and drive business growth and success.

Thousands of customers, including Fortune 500 companies and government agencies like NASA and the United Nations, have trusted ProjectManager with their data so that they can spend more time doing the work that drives their business forward. Keeping our customer's data secure is core to our product development, testing processes, customer service practices and vetting of technology partners.

ProjectManager's Security Framework was developed to provide a best-in-class level of security for our customers. It consists of standards and best practices that form a multi-tiered approach to safeguarding data integrity, confidentiality, infrastructure and network stability.

The ProjectManager Security Framework includes:

1. Application Security
2. Network and Infrastructure Security
3. Data Security
4. Organizational Security
5. Cloud Security
6. Industry Compliance

The framework also includes best practices for industry compliance by conducting regular internal reviews and audits to maintain the most up-to-date security practices and protocols.

In this white paper, we will outline the considerations and precautions that ProjectManager takes to ensure that your data remains safe and secure.

Application Security

Cloud Authentication

Customers can login with Google Authenticator or Microsoft Login (SSO), which can be enabled on the login page. The Google or Microsoft IDs used must match the user's email address used to login.

SSO simplifies the login process. It ensures compliance, provides effective access control and reporting, and reduces risk of password fatigue, and hence weak passwords.

Session Timeout

To secure user accounts, ProjectManager enables an application sign-out after four hours of inactivity. Once a session has timed out, users must login to their account again.

Forms Authentication

All ProjectManager users are required to have a unique ID and password. Within ProjectManager, users with administrative access can manage and control individual user security and permissions, including adding or removing user licenses.

Login credentials are submitted through a secured SSL connection with a minimum of TLS 1.2 encryption. Users are not required to download or install software to access their data.

Password Policy

Secure Password Policy

The secure password policy governs the creation and protection of the user's account data. Every ProjectManager user must have a unique account ID and password to access the software. Passwords are passed from the web server and browser to the user account through a hypertext protocol secured connection (HTTPS), an industry-standard encryption protocol.

Account Lockout

As an additional layer of protection against brute force attacks, ProjectManager initiates an account lockout policy. After ten consecutive unsuccessful login attempts, the account is locked and must be unlocked with a password reset, which is sent to the user's email address.

Password and Storage Encryption

All passwords stored on ProjectManager's cloud servers are encrypted using an industry-standard cryptographic safeguard.

Security and Testing Processes

Defined application security processes are embedded into every phase of our software development life cycle (SDLC). ProjectManager regularly conducts the following measures:

- Research and adoption of SaaS & Cloud Infrastructure security best practices
- Regular security reviews of architecture, new features, integrations and cross-platform solutions
- Manual and automated source code reviews for vulnerabilities and code quality
- Regular inspections and assessment of pre-production environments

Encryption

All customer data transmitted to our servers from public networks is protected using strong encryption protocols. We mandate that all connections to our servers—including web access, API access, mobile apps and IMAP/POP/SMTP email client access—employ Transport Layer Security (TLS 1.2/1.3) encryption with strong ciphers. This ensures a secure connection through authentication at both ends of the connection, and encryption of the transferred data.

Email Security

For email, our services leverage opportunistic TLS by default. TLS encrypts and delivers email securely, mitigating eavesdropping between mail servers whose peer services support this protocol.

Perfect Forward Secrecy

ProjectManager has full support for Perfect Forward Secrecy (PFS) for all encrypted connections. This ensures that, even if security is compromised, no previous communication can be decrypted.

Web Security

We have HTTP Strict Transport Security header (HSTS) enabled for all of our web connections. This directs all modern browsers to only allow access to ProjectManager over an encrypted connection, even if you navigate to an insecure page at our site. Additionally, we flag all our web authentication cookies as secure.

PCI Compliance

ProjectManager utilizes a PCI Level 1 compliant third-party processor, and thus, payments made through our billing processor are PCI compliant.

Network and Infrastructure Security

Data Centers

The ProjectManager cloud application is hosted by LiquidWeb. ProjectManager's dedicated servers have a global uptime average of >99.999% with Tier 1 Premium Bandwidth.

Data Center Certificates

ProjectManager's servers meet the following standards for certification, capability and/or compliance:

- SOC 2 SSAE-16 Audit Compliance
- SOC 3 Report
- HIPAA Capability
- GDPR Compliance
- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework

Physical Security

ProjectManager’s servers are located at Liquid Web's highly secure Michigan Data Center with the following security protocols in place:

- 24/7/365 monitored facilities
- CCTV security cameras covering inside, outside and all entrances
- Site entrances use an electronic perimeter access card system
- Sites are remotely monitored by a 3rd party security company
- Entrances are secured by mantraps with interlocking doors

Cooling Systems

- Multiple Liebert 20, 22, 30 and 45-ton upflow and downflow AC Units
- Stand alone HVAC systems that don't allow wide-scale outage
- Designed for addition of air-side economization

Network Hardware

- Redundant fiber entrance expandable to 1,840 gigabits per second
- Multiple redundant gigabit ethernet links to Data Center 1 and Data Center 2
- Fully redundant Cisco 6509 Sup720 and Nexus 7000 distribution switches
- Redundant gigabit ethernet links for each rack switch
- Cisco 4948 48-Port 10/100/1000 rack switches

Server Power and Backup

- Expandable 13,500 kVA utility power feeds
- Multiple ASCO closed transition bypass isolation transfer switches
- Multiple N+1 generac diesel generators
- Multiple N+1 Powerware 9395 550 kVA UPS systems
- Liebert and Eaton power distribution units
- Multiple service entrance feeds

Note on Privacy Shield Commitments

Please note the following regarding the independent recourse mechanism available to investigate unresolved complaints if your organization wishes its Privacy Shield commitments to cover personal data other than human resources data on an annual basis.

If that is the case, you must designate a private sector-developed independent recourse mechanism, or you may choose to cooperate with the EU Data Protection Authorities (DPA) and have a DPA panel serve as your independent recourse mechanism. Your annual selection will apply to all information received by your organization under the Privacy Shield other than human resources data.

DDoS prevention

We use technologies from well-established and trustworthy service providers to prevent denial-of-service (DDoS) attacks on our servers. These providers offer multiple DDoS mitigation capabilities aimed at preventing disruptions caused by bad traffic while allowing good traffic through. This keeps our websites, applications and APIs available and performing.

Disaster Recovery and Continuity

ProjectManager's dedicated servers in LiquidWeb's Michigan and Arizona Data Centers offer continuous backup and business continuity.

Application data is stored on resilient storage that is replicated across data centers. Data in the primary data center is replicated in the secondary in near-real-time. In case of failure of the primary data center, the secondary data center takes over, and operations are carried on smoothly with minimal-to-no loss of time.

Both data centers are equipped with multiple ISPs. In addition to 24/7/365 onsite security, the servers are monitored 24/7 to assess system health, maintain optimal performance and detect problems early. Both data centers have a dedicated immediate response team.

Redundancy

ProjectManager has processes that require full redundancy with our network infrastructure, including:

- Tier 1 Premium Bandwidth
- Uninterruptible power supplies with redundant battery cabinets
- State-of-the-art environmental conditions

LiquidWeb's Data Centers support all of those redundancy requirements and feature several zones for added redundancy within the regions, as well as geographic redundancy for disaster recovery.

Vulnerability Management and Penetration Testing

Using a combination of manual and automated processes, ProjectManager continuously monitors for security threats and has protocols in place to investigate and remediate any vulnerabilities. ProjectManager also engages with external 3rd party specialist penetration testers to validate this process.

Business Continuity Testing

In addition to our disaster recovery plan, ProjectManager and its data centers operate with a Business Continuity Plan that calls for regular testing to ensure network infrastructure and security processes are working appropriately. Our Business Continuity Plan is a comprehensive approach to restoring all systems as quickly as possible in any service interruption.

Firewalls

ProjectManager has implemented and regularly manages system firewalls. Engineers periodically apply tests to the firewall to ensure operability and compliance with the latest cybersecurity threats. In addition, our servers are built with full redundancy to secure data in the event of any impacts.

Organizational Security

ProjectManager has developed internal policies that are best-in-class for managing data and security risks. Our infrastructure and development team defined and implemented escalation, management, risk assessment, disaster recovery, business continuity and ongoing operational management.

We continually strive to improve our processes over time with a continuous assessment and monitoring model, along with regular assessments of procedures and protocols.

Vendor and Third-Party Supplier Management

We evaluate and qualify our vendors based on our vendor management policy. We onboard new vendors only after thorough reviews of their processes and their ability to deliver service and perform risk assessments.

We take appropriate steps to ensure our security stance is maintained by establishing agreements that require the vendors to adhere to confidentiality, availability and integrity commitments we have made to our customers. We monitor the effective operation of the organization’s processes and security measures by conducting periodic reviews of their controls.

Breach Notification

As data controllers, we notify the concerned Data Protection Authority of a breach within 72 hours after we become aware of it, according to the General Data Protection Regulation (GDPR). Depending on specific requirements, we notify customers when necessary. As data processors, we inform the concerned data controllers without undue delay.

NIST Cybersecurity Framework

ProjectManager follows the guidelines set out by the NIST Cyber Security Framework, a collaboration between the U.S. government and industry in response to Executive Order 13636 "Improving Critical Infrastructure Cyber Security."

Five key policies categorize the framework—Identify, Protect, Detect, Respond and Recover—to follow comprehensive planning, monitoring and action response plans to bolster cloud security. For more information about how ProjectManager aligns to the NIST Cyber Security Framework, refer to the NIST Cloud Security Checklist document.

Personnel

ProjectManager has strict security policies for employee access to customer data. All data access events are monitored and logged, and we restrict access to customer data to those with appropriate internal clearance.

Access to data centers requires authentication along with personal certificates and is tightly restricted. Our confidentiality agreement and acceptable use agreement binds all employees.

Privacy

Internal processes are designed to safeguard customer privacy and confidentiality of sensitive information. The ProjectManager Privacy Policy discloses the type of information we can collect and how we may use this information.

We do not collect personally identifiable information unless voluntarily submitted by the visitor to our sites or service. Access to customer data is strictly limited to select personnel and only on an as-needed basis.

Conclusion

ProjectManager strives to not only be the best work management software on the market, but also the most secure. The data governance measures outlined in this white paper are a reflection of the deep commitment that ProjectManager has to keeping our customer’s data safe.

If you would like to learn more about how ProjectManager’s security offerings can work for your organization, reach out to our sales team at sales@projectmanager.com.

Contact Us

Our Support Team is available by phone or email Monday through Friday, 8am–5pm CST.

☎ (800) 765-2495

✉ support@projectmanager.com

⌂ 3420 Executive Center Drive
Suite 200
Austin, TX 78731