Project Management Cloud **SECURITY** made easy

LOADSPRING™ is the market leader in Project Management Cloud solutions and is known for empowering client innovation through its easy to use LOADSPRING CLOUD PLATFORM. But did you know that we also make security easier and more effective? That's because our security measures are automatic and run seamlessly in the background at all times. But it's more than just technology. It's part of our DNA, including personnel background screenings throughout their employment with us.

Your critical project management data is protected 24/7/365, yet still allows effortless access from anywhere in the world. Our secure systems and Customer Experience Teams make sure of that—monitoring and countering security threats every minute of the day.

Our rigorous procedures and advanced technology alleviate external threats through industry-leading security standards such as:

- Application & Data Architecture
- Network & Hardware Security
- Security & Performance Monitoring
- Data-Center Security & Overview
- User-Session & Password Security
- Redundancy & Disaster Recovery

Simple information security is spelled C-I-A

Our powerful security infrastructure requires no effort from you or your IT staff, and keeps your data continually sheltered. In fact, LOADSPRING exceeds the requirements of most Fortune 500 corporations and government organizations. We adhere to ISO/IEC 27002:2005 standards and are SOC 2 Type II certified, which provide best-practice recommendations for information security management used by those who are responsible for initiating, implementing or maintaining information Security Management Systems. Our information security is defined by these standards in three areas that make up CIA:

1. Confidentiality: Ensures that information is accessible only by those you authorize. We've spent years developing our multi-layered security system that not only defends our network from hackers, but also keeps them from gaining information about your projects, networks and systems.

2. Integrity: We safeguard the accuracy and completeness of information and processing methods. We protect your data's integrity against user corruption and disasters by maintaining a complex system of data backup, backup testing and recovery.

3. Availability: We make certain that authorized users can easily access data and assets whenever needed. We guarantee 24/7/365 access by housing our server and networking equipment exclusively in 5 worldwide Class-A data center facilities. Each has significant redundant bandwidth, networking equipment, fire suppression and auxiliary power.

The ultimate security wrapper

Our LOADSPRING CLOUD PLATFORM is not only effortless and intuitive, it provides an airtight security wrapper around your entire Project Management software enterprise. It controls authentication protocols for all your applications. In addition, we custom-configure the portal to meet any other standards required by your security management team.

- **Business continuity planning**
- **Disaster recovery planning**
- **System access control**
- **System development & maintenance**
- **Physical & environmental security**
- **Compliance**
- **Personnel security**

Application and Data Architecture

System separation—Independent VLANs and dedicated databases keep data separate in our private clouds.
Server location—Servers are in the nearest geographic location to your business. Facilities are located in: Boston, MA; San Diego, CA; Toronto, Canada; London, England; Tokyo, Japan.
Firewall infrastructure—A multi-tiered, High Availability(HA), top notch firewall infrastructure.
Customer connections—All connections from LOADSPRING to the customer are secured using 2048-bit SSL.

Network and Hardware Security

Firewall hardening—Enterprise-level front- and back-end firewalls are hardened to industry standards.
Switching & routing—Enterprise-level switching.*
Network protocols—Only HTTPS, SFTP, & SMTP network protocols (inbound).
Network topology—Consists of an entry point into a physically and logically-controlled DMZ and 3 separate private networks.
Server equipment—Enterprise-level hardware built by leading U.S. server manufacturers.*
Intrusion detection—Network-based intrusion detection for the networks.*

Security and Performance Monitoring

System monitoring—A sophisticated internal and external monitoring system logs all server activity and availability and proactively corrects or escalates to the LOADSPRING Customer Support Team 24/7/365.*
Alert limits—Performance-monitoring systems with 80% alert limits deliver virtually limitless scalability.

Data Center Security and Overview

Physical access— Requires 24 hour advance notice, a valid federally-issued ID and listing on LOADSPRING's authorization list.
Facility security—Onsite personnel 24/7/365. Electronic and physical security. Mantrap entry. Biometric and Badge-only access.
Power protection—Two 2MW Caterpillar diesel generators. 2N Power Ware UPS, PDUs and static transfer switches. 72+ hour fuel supply. Regular systems testing.
Connectivity and bandwidth—We leverage a multicarrier blend of up to 7 distinct internet providers ensurring maximum up time and the fastest possible service.
Air conditioning—Tightly-controlled temperature and humidity. Redundant Stultz CRAC units. Water leak detection.
Fire suppression—VESDA™ smoke detection and FM-200 fire suppression system.

User-Session and Password Security

User-sessions security—Username/password authentication required with at least 8 characters, including a number and symbol, expire every 45 days. Enforcement of 5 password history and disabled after 5 invalid attempts.
Password reset-management—Requests submitted to local System Manager with authorization to reset passwords. Once reset, user must change own secret password upon first login. If local System Manager is unavailable, LOADSPRING will reset after following user verification procedure.

Redundancy and Disaster Recovery

Disaster-recovery procedures—Even in the event of a full data center outage, your data is fully recoverable. Procedures are based on severity level and response time required to mitigate and prioritize system failures.
Infrastructure redundancy—
    Micro DR—Critical component redundancy consisting of firewalls, switches, servers, and storage (standard).
    Macro DR—Critical server redundancy comprised of domain controllers, webservers and security servers (standard).
Data redundancy—
    Standard RTO/RPO—Daily offsite data duplication.
    Advanced RTO/RPO—Asynchronous high availability data services to alternate data center facility with customized RTO/RPO (optional).

*Detailed equipment and system specifications can only be provided under NDA for security reasons.

We're ready to make your job simpler and easier.
Call, write or click to learn more about the benefits we can deliver to your project management and IT teams.

LOADSPRING

+1.978.685.9715   www.loadspring.com