INFO SHEET

Planview LeanKit: A Secure Project Collaboration Solution

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

How does Planview LeanKit support your needs? Just ask.

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

LeanKit has an established information security management system (ISMS), which was awarded ISO 27001 certification by Intertek, an independent auditor. Additionally, LeanKit is independently audited against a rigid set of SOC 2 controls annually.

A copy of this documentation can be requested by customers or prospects with an NDA in place.

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. Finally, annual penetration tests are carried out by independent third parties.

2. 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 Planview LeanKit production environment is protected by a robust network infrastructure that provides a secure environment for all customer data. The LeanKit service is on a physically segregated network that requires VPN access and two factor authentication for administrative access. Planview monitors and analyzes system logs to identify unusual traffic patterns, potential intrusion attempts and other security threats. Planview also uses best-of-breed, 3rd party tools and services to provide complete network visibility and protection.

3. How would I be informed were there an incident or breach that could potentially expose sensitive user information?

Planview has 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.

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

The LeanKit solution is constructed on a multi- tier architecture, consisting of web servers, application servers, and 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.

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

LeanKit customer data is logically separated from other customers in a multi-tenant database, ensuring proper client segregation as well as an easy way to retrieve data when a client requests their stored data.

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

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

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

   Data in transit is encrypted with the TLS v1.2 protocol.

   All data stored in the LeanKit solution is automatically encrypted with a unique key, using the AES-256 encryption algorithm. Encryption keys are stored separately, with precautions taken to prevent unauthorized access both to encrypted data and their corresponding encryption keys.

7. What staff has access to the production databases?

   Only a 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 semi-annually, and requires VPN connection with multi-factor authentication.

8. Which of my data stored in the LeanKit solution can be viewed by LeanKit staff?

   Planview grants access on a least-privilege, need-to-know basis to ensure only those employees with a business need to access customer data have it. Access is reviewed regularly and removed promptly upon an employee's departure. Access to production environments is granted using multi-factor authentication and is logged / monitored by a dedicated security team.

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

   LeanKit is hosted in Virginia. The hosting provider is an ISO 27001-certified service organization that provides 24-hour physical security.

   Security measures include comprehensive identification, access control and monitoring systems, automatic fire protection, redundant climate control, and fail-over power supply. No LeanKit staff have access to the hosting provider's physical sites.

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

    Databases are deployed across disparate geographic areas to mirror the primary database in real time, enabling database durability, scalability, and resiliency. Data is then replicated to a disaster recovery site.

    Recovery allows for database restoral during our 7-day retention period to the last 1 hour.

    LeanKit retains user data as long as clients remain members of the service. LeanKit can retain user data indefinitely for active customers. Upon customer request, data can be deleted within 30 days of departure.

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

The LeanKit service is fully redundant with real- time database mirroring. Recovery allows for database restoral during our 7-day retention period to the last 1 hour.

LeanKit performs annual disaster recovery tests to validate the effectiveness of its backup process.

12. What are the RTO and RPO of the disaster recovery solution for the LeanKit service?

For the LeanKit service, the RPO (Recovery Point Objective) is 1 hour, and the RTO (Recovery Time Objective) is 12 hours.

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.

13. How long are backups and operating data retained?

LeanKit retains user data as long as clients remain members of the service. LeanKit can retain user data indefinitely for active customers. Upon customer request, data can be deleted within 30 days of departure.

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

Upon customer request, data is deleted 30 days at the end of the customer's term.

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

All LeanKit 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 LeanKit 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.

16. Does LeanKit support Single Sign On ("SSO") for the login procedure?

Yes, LeanKit 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 LeanKit solution without having to log in separately, with authentication federated from Active Directory. This reflects the industry's standard procedure for SSO that is widely in use. Multi-factor authentication can be integrated with SSO if desired.

17. Is LeanKit a PCI DSS-certified merchant/ service provider?

LeanKit does not process credit card information, and thus does not require PCI (Payment Card Industry) certification.

18. Is LeanKit HIPAA compliant?

Because LeanKit does not store or process any medical related data, the service does not fall under the requirements for HIPAA compliancy.

19. Does LeanKit support two- step verification (aka two factor authentication)?

Yes, LeanKit supports two step verification for added login security.

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

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