Planview LeanKit™

DATA SHEET

# Security, Trust, and Assurance

## A closer look at Planview LeanKit safeguards

### Security, trust and assurance

**Security: Planview® protects all of your data**

- ✓ Confidentiality
- ✓ Integrity
- ✓ Availability

**Trust: Your data is yours**

- ✓ Applicable legislation
- ✓ Data ownership and Data Retention
- ✓ Escrow and exit strategies
- ✓ Privacy statement
- ✓ Cookie information

**Assurance: Tested and approved**

- ✓ ISO-certified service
- ✓ Cloud Security Alliance- STAR
- ✓ Enterprise-ready service
- ✓ Independent audits

## Security: Planview Protects All of Your Data

### Confidentiality

#### Locked-up network perimeter

The Planview LeanKit™ ("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 also monitors and analyzes system logs to identify unusual traffic patterns, potential intrusion attempts and other security threats. Planview also uses other 3rd party tools and services to provide end-to-end network visibility and protection.

#### Permissions management

Permission management controls all access to LeanKit boards. Users can be assigned permissions to perform actions on a board based on the user role that they are assigned for that board. Available board permissions are; No Access, Reader, User, Manager, and Administrator. This model allows for tight, granular control within the system to ensure data integrity and confidentiality.

#### World-class Security

Planview uses TLS protocol with 256-bit AES encryption to protect data in transit in LeanKit. No user data (including login information) is ever sent through unencrypted public channels. Furthermore, all data is encrypted at rest within the primary, secondary and tertiary databases. The encryption keys are stored separately, and managed by Planview.

### Strong passwords and unique user names

Each LeanKit user is identified with a unique user name and authenticated with a personal password in the system. With strong passwords enabled, the required minimum length of a password is eight characters; one upper case letter, one lower case letter, and one numeric or special character are requirements. Password also can not match previous passwords.

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.

### Integration with Single Sign-On (SSO)

No need to remember multiple passwords. LeanKit supports single sign-on (SSO) and utilizes SAML and active directory federation service for its enterprise clients. Multi-factor authentication can be enabled for additional security.

## Integrity

### Physical and environmental measures

The LeanKit production environments are currently hosted in Virginia, USA for our U.S./Latin America customers, Germany or The Netherlands for customers located elsewhere. LeanKit uses ISO-27001 certified and SOC2/SSAE16 audited co-location facilities, which provide around-the-clock physical security and top-notch environmental protection. It includes comprehensive identification systems, automatic fire protection, redundant climate control and fail-over power supply.

### Protection against malware

Planview provides anti-virus software for all its critical systems commonly affected by malware.

### Audit logging and monitoring

LeanKit has comprehensive traceability through object history, with all changes logged and visible. LeanKit stores all data in a secure manner, with information intact from any changes in any manner.

## Availability

### System status

System availability is monitored by multiple 3rd party applications and / or services. This information is published on the publicly facing, LeanKit status website. Why publish information about system availability? Because Planview believes system availability transparency provides customers with operational visibility and helps foster a trusting relationship with all of our customers.

### Multi-layer redundancy

The LeanKit network infrastructure is designed with redundancy and maximum availability. In the event of failure, all operation-critical components, including network, web, application and database servers, as well as storage, has been deployed and configured for near-seamless transition.

### Robust Networking Environment

LeanKit capitalizes on the reliability, flexibility, security, scalable and high-performant network infrastructure that hosts our service.

The global footprint of our network allows us to deliver our services safely and quickly to all customers regardless of their location.

### Disaster recovery and business contingency

The LeanKit 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, an emergency response team of selected Planview staff is summoned to activate the disaster recovery plan.

### Backup and restoration

Planview has put into effect redundancy and backup routines for its production databases. In the unlikely event of multiple server failure, the backups serve the sole purpose of restoring the whole production system. All data stored on the primary database servers is mirrored on standby servers in near-real time. The standby servers are located in physically separate datacenters and are configured to automatically take over production tasks if a primary database server fails.

# Trust: Your Data is Yours

## Data ownership

All customer data stored in LeanKit is owned solely by the customer. Customers can download their files at any time, provided appropriate permissions are in place. Upon termination of service, customers can request their data be archived and will be provided access for retrieval.

## Data retention

Data can be restored to a point-in-time up to the last 1 hour for the past 7 days.

## Privacy statement

The sole personal information viewable by Planview support and sales staff is the user contact information – i.e. name, e- mail address, address, phone number(s), and membership in projects.

LeanKit administrators are able to view the names of all boards or lanes and its members created within the service. Planview does not share this information with anyone, nor does it ever sell or market this information to any third party. Planview employees are prohibited access to any user data or uploaded documentation.

Planview has formulated a privacy statement which explains how the company gathers and disseminates user-related information. The statement is available on the Planview website: : https://www.planview.com/legal/privacy-statement/.

## Cookie information

LeanKit and Planview.com use cookies to optimize the user experience. Cookies help make LeanKit work according to user expectations. LeanKit issues a session "cookie" only to record encrypted authentication information for the duration of a specific session. The session "cookie" does not include either the username or password of the user - it contains only an authentication ticket ID and the sub-domain portion of the hostname.

LeanKit does not use "cookies" to store other confidential user and session information, but instead implements more advanced security methods based on dynamic data and encoded session IDs. No other data related to authentication or sessions is stored on the client. Planview does not collect any personally identifiable or sensitive information without written consent and permission.

# Assurance: Tested and Approved

## ISO-certified service

Planview has been awarded ISO-27001 certification – an international standard for information security. This includes proactive management of information security risks and controls. ISO-27001, a high-end certificate, guarantees that LeanKit has well-established structures for information security that run throughout the organization – from top to bottom.

## Independent audits

Planview commits considerable resources to continually assessing security threats, as well as developing its infrastructure and system's security functions. The LeanKit infrastructure and application is subject to regular vulnerability scans (on a quarterly basis) with annual penetration tests carried out by independent third parties. Additionally, Planview entrusts external auditors to evaluate its information security practices and general IT controls.

## About Planview

As the global leader in work and resource management, Planview makes it easier for all organizations to achieve their business goals. We provide the industry's most comprehensive solutions designed for strategic planning, portfolio and resource management, product innovation, capability and technology management, Lean and Agile delivery, and collaborative work management. Our solutions span every class of work, resource, and organization to address the varying needs of diverse and distributed teams, departments, and enterprises. Headquartered in Austin, Texas, Planview's more than 700 employees serve 5,000 customers worldwide through a culture of innovative technology leadership, deep market expertise, and highly engaged communities. For more information, visit www.planview.com.