SAFEGUARDING YOUR DATA

LeanKit is committed to keeping your data secure and private. Our multi-tiered approach ensures the highest levels of infrastructure security and defends against physical, network, server, application, and data vulnerabilities.

HOSTED CLOUD PLATFORM

LeanKit runs on Microsoft Azure, a trusted and secure cloud platform that meets the most comprehensive security, privacy and regulatory standards.

✓ **PHYSICAL SECURITY**
Geographically distributed data center facilities run 24x7x365 and employ stringent measures to protect against power failure, physical intrusion, network outages, and more.

✓ **NETWORK SECURITY**
Secure practices and technologies are used to connect virtual machines to each other and to on-premises data centers, while blocking unauthorized traffic.

✓ **THREAT MITIGATION**
Anti-malware, intrusion detection, denial-of-service (DDoS) attack prevention, and regular penetration testing protect you against online threats.

CONTROLS AND CERTIFICATIONS

To help you comply with national, regional, and industry-specific requirements governing the collection and use of data, LeanKit's data centers adhere to rigorous standards of compliance. Certifications include:

- ✓ ISO 27001, 27002, 27018, HIPAA, and CSA CCM
- ✓ Payment Card Industry (PCI) DSS Service Provider, Level 1 Certification
- ✓ SSAE16 SOC 1, SOC 2 and SOC 3
- ✓ Content Protection and Security Standard (CPS)

Please refer to the Microsoft Trust Center for more security and compliance information.

APPLICATION SECURITY

At LeanKit, security is built into all phases of our software development lifecycle. From secure design and coding guidelines to post deployment monitoring and alerts, we are continuously implementing new measures to safeguard your data.

- 24x7x365 application infrastructure monitoring.
- Access to customer data by LeanKit personnel is heavily restricted.
- Operating systems are hardened to remove all unnecessary software.
- LeanKit application data is encrypted in transit and at rest.
- Transport Layer Security (TLS) protocol ensures secure browser access.
- LeanKit does not provide any third party with direct or unfettered access to customer data.

ACCESS MANAGEMENT

Limit unauthorized access to LeanKit and keep your data secure with the following account-based security options.

- Default board level user settings to all new users for consistency.
- Customize user access for each LeanKit board with role based permissions.
- Limit board creation and deletion access to specific users.
- Strong password control and account lockout policies.
- Granular settings to control file attachments, and RSS and Calendar feeds.

HIGH AVAILABILITY AND DISASTER RECOVERY

LeanKit builds resiliency and continuity into our underlying infrastructure to reduce the risk of failures and ensure rapid recovery in the event of an outage.

- **HIGH AVAILABILITY**
  Our system is engineered with fault tolerance in mind, leveraging redundancy and replication mechanisms to provide the highest levels of application responsiveness.
- **DISASTER RECOVERY**
  Comprehensive DR planning, processes and practices ensure that LeanKit can be quickly and fully recovered in the event of a disaster. Our two tier, geo-dispersed backup approach enables data sources to be rapidly restored without inconsistencies.

LeanKit takes a holistic approach to safeguarding your data that encompasses every aspect of physical, network, server, and application security.