Autodesk® **PLM 360**

# Secure, Cloud-Based PLM

## Autodesk PLM 360 is the next-generation cloud-based alternative from Autodesk—a name you can trust.

With over ten years experience providing cloud-based solutions, Autodesk knows keeping customer data secure in the Cloud is critical to your success.


The Autodesk® PLM 360 cloud-based platform is a next-generation alternative to traditional product lifecycle management that's delivered by Autodesk—a trusted provider of secure cloud technology for over a decade. Autodesk upholds that trust every day by employing a range of safeguards designed to put user experience and security at the forefront of all Autodesk PLM 360 endeavors.

**Operational Excellence**
Autodesk safeguards Autodesk PLM 360 data according to applicable computing industry certifications, rigorous international compliance measures, and a customer-centric approach to data storage.

**Auditing**
Autodesk requires the data centers that host Autodesk PLM 360 to maintain SSAE16 certification as set forth by the Auditing Standards Board of the American Institute of Certified Public Accountants. Autodesk relies on SSAE16 reports to hire service providers entrusted with the Autodesk PLM 360 computing environment.

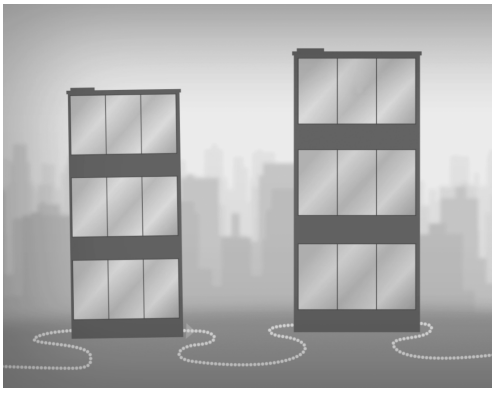
**Quality Procedures**
The Autodesk PLM 360 host data center protects data by adhering to strict internal policies in accordance with internationally accepted data protection legislation, including PIPEDA, European Data Protection Directives, and the US-EU Safe Harbor Framework.

**Facilities**
Autodesk PLM 360 protects sensitive client data using a multi-faceted strategy to prevent tampering or theft of computing assets.

**Physical Security**
The Autodesk PLM 360 host data center runs computing hardware stored inside buildings staffed by security agents 24 hours a day, 7 days a week, 365 days a year. All security personnel pass a rigorous background security check as a condition of employment. Cameras monitor employee ingress and egress through all entrances and record activity inside hallways and rooms where computing hardware resides. Security teams preserve all video recordings on secure digital media and may recall all recent activities on demand.

For more information about Autodesk PLM 360, visit **www.autodeskplm360.com.**

Autodesk®



### Restricted Access
The Autodesk PLM 360 host data center maintains high-level, three-factor authentication—key card, pin pad, and biometric fingerprint scans—to ensure only authorized individuals gain entry to the data center. Upon termination of any Autodesk PLM 360 client contracts, Autodesk follows industry best practices for proper data destruction as part of all decommissioning procedures.

### Software Protections
Autodesk PLM 360 employs several layers of software application security to ensure that only authorized users may perform the actions granted by each client's administrators.

### Encrypted Communications
Autodesk PLM 360 uses 256-bit SSL encryption to strengthen data privacy and network communication security over the internet. Data centers deploy firewall products in high-availability pairs to offer protection through system redundancy. Firewalls configured this way continuously monitor the flow of traffic through the Autodesk PLM 360 network and servers.

### Device Segregation
The Autodesk PLM 360 host data center segregates server hardware on a private VLAN (virtual local area network) to ensure all communications remain private and confidential and removed from other servers. Autodesk PLM 360 further segregates customers' data by leveraging an isolated multi-tenancy model to provide an additional layer of separation at the application level.

### Activity Logs
Security systems within the Autodesk PLM 360 host data center record the logins, user actions, and data additions and deletions that occur within the Autodesk PLM 360 host environment. Security personnel preserve all activity logs in a protected location for later reference. Autodesk PLM 360 also logs user and administrator transactions. Logs exist at the system level, administrative level, and record levels.

### Fail-Safe Measures
Autodesk uses fail-safe strategies to mitigate the undesirable consequences of operational failures.

### Redundant Protections
The Autodesk PLM 360 host data center runs Autodesk PLM 360 in a clustered database environment to prevent system disruption caused by a single point of failure.

### Access Control
To help protect unattended devices from unauthorized access, Autodesk PLM 360 offers an adjustable system timeout (logout) setting, configurable password retention policies to align with existing customer policies, and immediate user lockout after a configurable number of failed login attempts.

### Regular Backups
The Autodesk PLM 360 host data center actively replicates data into a second data center located in the same geographical region. Data replication allows for near continuous operation in the event of a data center level outage.

Learn more at **www.autodeskplm360.com**.

### About Autodesk
Autodesk, Inc., is a leader in 3D design, engineering, and entertainment software. Customers across the manufacturing, architecture, building, construction, and media and entertainment industries—including the last 17 Academy Award winners for Best Visual Effects—use Autodesk® software to design, visualize and simulate their ideas. Since its introduction of AutoCAD® software in 1982, Autodesk continues to develop the broadest portfolio of innovative software for global markets.

For additional information about Autodesk, visit **www.autodesk.com**.

Autodesk®


plm_360_2013_security_brochure_en_v2