# Keeping your Autodesk Collaborative Project Management On-Demand Solution Secure

Autodesk emphasizes strict personnel security measures, and has developed a rigorous set of engineering and infrastructure support processes for Autodesk Collaborative Project Management on-demand solutions.

Keeping your data secure is crucial to your company's success. Here are the measures Autodesk implements in four areas—people, processes, technology, and facilities—to help ensure the safety of your information.

## People

Companies know that most of their business software security breaches are caused by insiders—whether inadvertently, through negligence, or on purpose. That means it's crucial for the employees who develop, maintain, and support Autodesk Collaborative Project Management applications to play a key role in keeping these applications secure. Therefore, Autodesk emphasizes strict personnel security measures, including:

- **Least-privilege access.** Only users with a clear need to access production environments are granted access. When employees leave the company or change roles, access is immediately revoked.
- **Support staff access.** Autodesk support staff will only access your company's data after obtaining explicit permission from your company.
- **Anti-phishing training.** Autodesk personnel with access to customer data or the application infrastructure are trained to recognize phishing attacks and other forms of social engineering designed to compromise trust.
- **Background checks.** Autodesk performs background checks for all new employees who may handle customer data.

## Processes

Autodesk has developed a rigorous set of engineering and infrastructure support processes for Autodesk Collaborative Project Management on-demand solutions. Autodesk reliably maintains and audits security with each new release, using proven, repeatable controls, including:

- **SAS70 auditing.** Autodesk engages an outside auditor to prove the capability and maturity of existing security processes, and to verify the integrity of documented, established security controls.
- **Change control.** To maintain maximum availability of Autodesk Collaborative Project Management on-demand solutions, Autodesk enforces a strict change control process for the production environment. Autodesk always performs significant changes and routine maintenance during predetermined service windows, which are communicated to customers in advance.

Autodesk®

- **Independent security reviews.** Autodesk engages third-party security experts to conduct application and network penetration testing.

## Technology

To provide the highest level of service, Autodesk uses leading-edge security, performance, and availability technologies, including:

- **Data segregation.** Although all customers share the same application environment, their data stores are completely segregated to prevent unauthorized access.
- **Encryption.** To secure every transaction that involves customer data, Autodesk supports the highest level of commercial-grade encryption available. All data transmissions over public networks are secured using SSL/TLS.
- **Access control.** Autodesk Collaborative Project Management on-demand applications provide flexible configuration options to meet existing customer standards, including IP-based restrictions, password complexity, and session time-out rules.
- **Application acceleration.** To deliver optimal performance and availability, Autodesk employs protocol optimization, distributed load balancing, and application acceleration techniques.

## Facilities

To ensure the security and availability of Autodesk Collaborative Project Management on-demand solutions, Autodesk strategically chooses locations and providers of hosting services that offer the following features:

- **Global availability.** Autodesk Collaborative Project Management on-demand applications are hosted in state-of-the-art facilities on three continents. Should a major disaster occur on one continent, the application service delivery load would be shifted to other facilities unaffected by the event.
- **Replication.** To minimize the impact of any catastrophic event, Autodesk replicates all customer information to data centers around the globe. Within each data center, redundant storage eliminates the impact of localized hardware failures.
- **Connectivity.** To ensure network connectivity during a major telecommunications failure, Autodesk provisions independent Internet connections via global Tier 1 providers.
- **Physical security.** Autodesk maintains strict access control at each hosting facility. Even Autodesk employees must be escorted by the hosting provider while on-site.
- **Power/HVAC.** To ensure uptime even if a support system fails, Autodesk employs redundant power and cooling systems.
- **Hardware redundancy.** Autodesk maintains at least N+1 redundancy on all critical hardware and infrastructure.

To provide the highest level of service, Autodesk uses leading-edge security, performance, and availability technologies.

To ensure the security and availability of Autodesk Collaborative Project Management on-demand solutions, Autodesk strategically chooses locations and providers of hosting services.

Autodesk®