Contents

Introduction ............................................................................................................................... 1
Document Purpose ................................................................................................................... 1
Cloud Operations...................................................................................................................... 1

High Availability..................................................................................................................... 1
Physical Infrastructure Security............................................................................................... 3
Operations Incident Management ............................................................................................ 4
Patch Management .................................................................................................................. 4
Change Management ............................................................................................................... 5
Capacity Management ............................................................................................................ 5
Performance and Scalability .................................................................................................... 6

PLM Operational Security Controls ....................................................................................... 6
Fusion Lifecycle Engineering ................................................................................................. 7
PLM Application Controls ....................................................................................................... 7

Authentication ......................................................................................................................... 7
Administrative Controls .......................................................................................................... 8
User Controls ........................................................................................................................... 9

Cloud Security......................................................................................................................... 9
Vulnerability Scans and Penetration Testing .......................................................................... 10
Network Security .................................................................................................................... 10
Encryption .............................................................................................................................. 10
Security Standards and Attestations ....................................................................................... 10

Resources ............................................................................................................................... 11
Introduction

Autodesk® Fusion Lifecycle brings powerful product lifecycle management tools to web browsers and mobile devices through Autodesk’s cloud computing platform. Autodesk Fusion Lifecycle provides customers with an integrated and intuitive set of tools for building custom security policies that match the needs of their organization. To keep customer information highly available, Autodesk Fusion Lifecycle runs on a scalable infrastructure that enables Fusion Lifecycle to remain responsive as demand increases. To maintain business continuity in the event of a disaster, a high-speed private network over which data are replicated links regionally isolated data centers.

Document Purpose

The purpose of this document is to explain Autodesk Fusion Lifecycle operations, software development process and security measures implemented in the environment.

Cloud Operations

The Cloud Operations team is responsible for defining and executing procedures for application release management, hardware and operating system upgrades, system's health monitoring, and other activities required for the maintenance of Fusion Lifecycle.

High Availability

Fusion Lifecycle is designed to achieve a high level of availability by employing redundant systems in its supporting infrastructure and distributing load across a scalable fleet of instances.
Clustering

Clustering technology keeps Fusion Lifecycle highly available by limiting single points of failure and directing service requests away from instances that are highly utilized. Infrastructure components, including HTTP servers and application servers, are deployed in clusters and accessed through load balancers.

Disaster Recovery

The Fusion Lifecycle disaster recovery plan covers contingencies, including power failures, ISP outages, and natural disasters. In addition to developing and implementing disaster recovery technology and procedures, the Cloud Operations team tests the effectiveness of the disaster recovery plan by verifying that access to Fusion Lifecycle can be maintained after a simulated infrastructure failure.

Data Replication

Replication of customer data is performed between data centers in different regions over a private communication link. Replication limits the possibility of data loss or a delay in service resumption if fail-over to a backup data center is required.

Geographic Redundancy

Similar physical infrastructure is maintained in regionally isolated data centers to provide protection against events such as natural disasters.

Power System Redundancy

Redundant electrical power systems are installed in data centers to maintain operations 24 hours a day, seven days a week. Uninterruptible Power Supplies (UPSs) automatically providebackup to primary electrical systems in the event of a failure. Generators at each data center provide long-term backup power if an outage occurs.

Internet Connectivity Redundancy

A redundant multi-vendor system is used to maintain Internet connectivity.
Fail-Over Testing

Fail-over testing simulates the effects of different types of hardware and software failures to confirm that fault tolerant systems work as expected. Fail-over testing gives confidence that customers can continue to access functionality and data even if parts of the Fusion Lifecycle infrastructure are unavailable. The ability of Fusion Lifecycle to switch between redundant components, including databases, virtual instances, and data centers, is vetted by these tests. Fail-over tests are executed as needed.

Physical Infrastructure Security

Fusion Lifecycle runs in secure data centers that are protected from unauthorized access and environmental hazards by a range of security controls.

Facilities Access Control

Data centers are guarded 24 hours a day, seven days a week by professional security staff. The perimeter of each data center as well as rooms that contain computing and support equipment are protected by video surveillance. Video surveillance is preserved on digital media that allows recent activity to be viewed on demand. Data center entrances are guarded by mantraps that restrict access to a single person at a time. All visitors and contractors must present identification to be admitted and are escorted by authorized personnel at all times. Only employees with a legitimate business need are provided with data center access and all visits are logged electronically.

Fire Prevention

Fire detection and suppression systems, such as smoke alarms and heat-activated wet pipes, are installed throughout each data center to guard rooms containing computing equipment and support systems. Fire detection sensors are installed in the ceiling and underneath a raised floor.
Climate Controls

Data center climate controls protect servers, routers, and other equipment subject to failure if strict environmental ranges are violated. Monitoring by both systems and personnel is in place to prevent dangerous conditions, such as overheating, from occurring. Adjustments that keep temperature and other environmental measurements within acceptable ranges are made automatically by control systems.

Operations Incident Management

The Fusion Lifecycle incident management policy is guided by the ITIL V3 framework, which defines best practices for driving incident resolution. The Fusion Lifecycle incident management policy emphasizes logging of remediation steps and the use of root cause analysis to build a knowledge base of actionable procedures. The goal of the Fusion Lifecycle incident management policy is not only to quickly and effectively close incidents, but also to collect and distribute incident information so that processes are continuously improved and future responses are driven by accumulated knowledge.

Patch Management

Where possible, automation is in place to check for new patches and prepare deployment lists that can be approved by authorized Cloud Operations personnel. Patching policy also defines criteria for determining the impact of a patch on systems stability. If a patch is identified as having a possibly high impact, thorough regression testing is completed before the patch is deployed. Change Management tracks deployment of patches to production systems.
Change Management

The Cloud Operations team has a change management policy. Following activities are performed by the operations team:

- Requiring the submission of a Request For Change (RFC) form, which includes the name of the change initiator, the change priority, the business justification for the change, and a requested change implementation date.
- Cloud Operations team creates detailed back out plans prior to deployment so that system state can be restored if a change causes a service disruption. Back out plans include executable instructions defined in scripts that restore system state with a minimum of manual steps.
- Defining maintenance windows. Scheduled, emergency, and extended maintenance windows are specified by the Cloud Operations team and regularly planned maintenance is scheduled during off-peak hours.
- Defining tests to verify that functionality is accessible after the deployment of a change.
- Once deployment is complete, the Cloud Operations and Product QA team execute the tests to check that functionality identified as at-risk remains available.

Capacity Management

Because customer access to cloud services is provisioned on-demand through a self-service model, traffic patterns are highly variable and subject to usage spikes. When a spike occurs, the availability of a service can be negatively impacted if the pool of computing resources powering the service is exhausted. To maintain a high level of availability, the Cloud Operations team implements a capacity management policy. These practices include:

- Frequent recording of resource use - Fusion Lifecycle resource use is collected at frequent intervals across a range of infrastructure components, including virtual instances, virtual storage volumes, and virtual network devices. Usage statistics are stored in a capacity management repository.
• Building a capacity plan documenting current resource use and forecasting future requirements - the capacity management repository is used by the Cloud Operations team to generate a detailed capacity plan that documents current levels of use and models future levels based on statistical analysis and the impact of upcoming enhancements to business functionality. The capacity plan is updated as needed or if significant changes to usage patterns are detected.

**Performance and Scalability**

To provide a high level of availability, performance and load tests are executed throughout the software development lifecycle. Key members of the Fusion Lifecycle leadership team must sign-off on test results before a release can be deployed.

**PLM Operational Security Controls**

Fusion Lifecycle provides a high level of protection of sensitive customer data from unauthorized access.

• **Administrative functionality** – Fusion Lifecycle's administrative tools provide a flexible way for administrators to manage users, role-based permissions, password policy, and other access controls for end users.

• **Physical restrictions to data centers** – Physical restrictions to data centers prevent unauthorized parties from accessing the hardware and support systems used by Fusion Lifecycle.

• **Background checks** – Background checks are required for employees with physical access to the computing resources and support systems used by Fusion Lifecycle.

• **Geographically isolated data centers** – Geographically isolated data centers are used to prevent service interruptions due to regional events such as natural disasters.

• **Data replication** – Data replication copies customer data across redundant data centers so that business continuity can be maintained if a fail-over between facilities occurs.

• **Redundant technologies** - Redundant technologies such as load balancers and clustered databases limit single points of failure.
Fusion Lifecycle Engineering

The Fusion Lifecycle Engineering team is responsible for designing, implementing, and testing the software services provided by Fusion Lifecycle.

The design, coding, testing, and maintenance of Fusion Lifecycle is based on a software development process. During the design stage, detailed design documents are produced and are reviewed by architects to assess functionality and scalability of the design. During implementation, peer code reviews by software engineers and architects are conducted to detect deviations from Fusion Lifecycle application development practices. The design phase uses a joint application design process including architects and software engineers to assess the functionality, scalability, and performance characteristics of the user stories. During the implementation sprints, code reviews by architects and software engineers are conducted to maximize code quality. All code produced during the process includes functional unit testing and no user story is complete until quality assurance personnel verify the acceptance criteria. Performance testing of Fusion Lifecycle is also integrated into the development lifecycle. Fusion Lifecycle’s performance team conducts load tests throughout the development sprints to catch changes that negatively affect performance as early in the process as possible.

PLM Application Controls

Fusion Lifecycle provides administrators with security tools that allow detailed identity and access management policies to be created. Non-administrative users can use Fusion Lifecycle’s security tools to manage ownership of their workspace items and set sharing permissions on their reports.

Authentication

Credentials, consisting of a user ID and password, are required to access Fusion Lifecycle. Credentials are secured during network transmission and stored only as a salted hash generated by the SHA-2 cryptographic hash function.
Administrative Controls

Administrators can create custom identity and access management policies that align with those already in use by their organization.

Provisioning Users

Administrators can create and deactivate users and delegate administrative authority to other users.

Using Group and Role-based Security

Fusion Lifecycle roles allow administrators to customize access control levels to match the job responsibilities defined within their organizations. Roles are collections of permissions to data and functionality that are related to a job function. Once a role is created, it can be associated with a user group so that users within the group are granted the role’s permissions. For example, a “Customer Details” role can contain permissions allowing customer information to be viewed, added, and deleted. To grant these permissions to users who are responsible for registering customers, a group named “Customer Registration” can be created and populated with employees belonging to the department that processes new customers. The “Customer Details” role can then be associated with the “Customer Registration” group, allowing members of the group to create and delete customer information. By providing a flexible way of assigning permissions using groups and roles, Fusion Lifecycle enforces the principle of least privilege, which requires that each user’s access to data and functionality be limited to what is needed for the completion of assigned tasks.

Accessing Security Information

Administrators can view a wide range of security information, including group membership, workspace permissions assigned to users, and revision control settings.

Monitoring and Auditing User Activity

Fusion Lifecycle helps enforce accountability by making detailed activity logs available to administrators. Activity logs provide information about the actions performed by users, including workspace item modifications, workflow actions, and logins.
Restricting Access
Fusion Lifecycle allows administrators to create network access restrictions based on IP address white lists.

User Controls
Users can control access to workspace items, reports, and files they own subject to administrative restrictions. Users can also use file versioning to restore old versions of files they have attached to workspace items.

Setting Access Controls on Data
Users can grant access to their workspace items by modifying an item’s ownership list. Adding an owner to a workspace item allows the additional owners to view and edit the item. Access to reports can be granted to other users or groups by the report owner.

Versioning File Attachments
Fusion Lifecycle maintains a version history for files that have been attached to workspace items. When an attachment is checked out, modified, and checked in, a new version of the attachment is created and a change record is added to the version history. Versioning protects the integrity of data by allowing invalid changes to be rolled back and provides an auditable list containing information about each file modification.

Cloud Security
The Cloud Security team is a dedicated group of information security specialists focused on identifying and enforcing security within the Autodesk Fusion Lifecycle cloud environment. The Cloud Security team’s responsibilities include:

• Reviewing the security of cloud infrastructure design and implementation.
• Defining and ensuring implementation of security policies including identity and access management, password management and vulnerability management.
• Driving compliance with established security procedures by conducting internal reviews and audits.
• Identifying and implementing technologies that secure customer information
• Engaging third-party security experts to conduct information security assessments
• Monitoring cloud services for possible security issues and responding to incidents as needed
• Conducting annual reviews of security policy.

**Vulnerability Scans and Penetration Testing**

The Cloud Security team conducts security scans and penetration testing of Fusion Lifecycle services. Security scans and penetration-testing cover a wide range of vulnerabilities defined by the Open Web Application Security Project (OWASP) and SANS top 25.

**Network Security**

Network security is enforced using a combination of physical and logical controls, including encryption, firewalls, and systems hardening procedures. Stand-alone hardware firewalls are deployed at the perimeter of the cloud. All ports except those required to serve customer requests are blocked.

**Encryption**

Network traffic containing sensitive information, such as credentials, application session information, access tokens and user profiles, is transmitted securely over the Internet to the perimeter of our environment. Customer data is stored in drives secured with disk encryption. Customer file attachments are stored on Amazon encrypted S3 buckets.

**Security Standards and Attestations**

Fusion Lifecycle security controls are reviewed by an independent auditor and listed in AT Section 101 SOC 2 audit report. Autodesk Fusion Lifecycle’s cloud environment is ISO 27001 certified.
Resources

The following resources provide general information about Autodesk and other topics referenced in the main section of this document.

- Autodesk Trust Center - To view information about Autodesk Trust Center, visit http://trust.autodesk.com.