Autodesk® Fusion Lifecycle
Security Whitepaper

February 2020
## Contents

**Introduction** .............................................................................................................................................................................. 4

**Document Purpose** ........................................................................................................................................................................ 4

**Cloud Infrastructure** ....................................................................................................................................................................... 4

- High Availability ........................................................................................................................................................................ 4
- Clustering ...................................................................................................................................................................................... 4
- Disaster Recovery ........................................................................................................................................................................... 5
- Data Replication ............................................................................................................................................................................ 5
- Geographic Redundancy .............................................................................................................................................................. 5
- Backup .......................................................................................................................................................................................... 5
- Power System Redundancy ........................................................................................................................................................... 5
- Internet Connectivity Redundancy ................................................................................................................................................ 6
- Fail-over Testing ............................................................................................................................................................................. 6
- Physical Infrastructure Security .................................................................................................................................................... 6
- Operations Incident Management ................................................................................................................................................ 6
- Patch Management ........................................................................................................................................................................ 6
- Change Management ...................................................................................................................................................................... 7
- Capacity Management ................................................................................................................................................................... 7
- Alerts and Monitoring .................................................................................................................................................................... 8
- Zero Downtime During Deployments ....................................................................................................................................... 8
- Performance and Scalability ........................................................................................................................................................ 8
- Fusion Lifecycle Operational Controls ....................................................................................................................................... 8

**Fusion Lifecycle Engineering** .................................................................................................................................................. 9

**Fusion Lifecycle Application Controls** ....................................................................................................................................... 9

- Authentication ............................................................................................................................................................................... 9
- Administrative Controls ............................................................................................................................................................... 9
- Provisioning Users .......................................................................................................................................................................... 9
- User Group and Role-Based Security ....................................................................................................................................... 10
- Accessing Security Information ................................................................................................................................................ 10
- Monitoring and Auditing User Activity .................................................................................................................................. 10
- Restricting Access .......................................................................................................................................................................... 10
- User Controls ................................................................................................................................................................................ 10
- Setting Access Controls on Data ............................................................................................................................................... 10
- Versioning File Attachments ..................................................................................................................................................... 10
Autodesk Security .................................................................................................................................................. 11
Vulnerability Scans and Penetration Testing ........................................................................................................ 11
Network Security .................................................................................................................................................. 11
Encryption ............................................................................................................................................................ 12
Privacy ................................................................................................................................................................. 12
Security Standards and Attestations ..................................................................................................................... 12

Resources .............................................................................................................................................................. 12
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.

As a secure, cloud-based product, Fusion Lifecycle offers the benefits of collaboration across a product’s lifecycle while safeguarding customer data. The Fusion Lifecycle application is designed and built using best-in-class cloud software practices and powered by Amazon Web Services (AWS), the world’s leader in cloud infrastructure. We have designed our services to be scalable and secure, thus providing our customers with a resilient and safe application. We know our customers’ business is relying on us and we take that responsibility seriously.

Document Purpose

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

Cloud Infrastructure

The Cloud Infrastructure 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 Infrastructure team tests the effectiveness of the disaster recovery plan by verifying that access to Fusion Lifecycle can be maintained after a simulated infrastructure failure at least once per year.

In the event of Autodesk's declaration of a disaster, Fusion Lifecycle's disaster recovery process aims to, within one working day, restore Fusion Lifecycle and minimize customer data loss to that same timeframe. However, the inherent uncertainty of disasters may mean that these recovery objectives are not achieved in every case, and these recovery objectives do not apply to a disaster or multiple disasters causing the compromise of both data centers at the same time or development and test bed environments, such as the Sandbox services.

Data Replication

Replication of customer data is performed between Amazon Web Services (AWS) Availability Zones (AZs) and AWS Regions. 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.

Backup

All customer data submitted to Fusion Lifecycle, up to the last committed transaction, is automatically replicated on a near real-time basis to the secondary site and is backed up on a regular basis and stored on backup media for an additional 90 days in production environments after which it is securely overwritten or deleted from Fusion Lifecycle. Any backups are verified for integrity and stored in Autodesk data centers.

Power System Redundancy

AWS data centers contain redundant electrical power systems to maintain operations 24 hours a day, 7 days a week. Uninterruptible Power Supplies (UPSs) automatically provide backup 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 to each of the data centers.

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 on AWS secure data centers that are protected from unauthorized physical access and environmental hazards by a range of security controls. Some physical and environmental controls are summarized below. A full overview of AWS Security Processes is available at https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf.

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

The Cloud Infrastructure team has a patch management policy that helps ensure effective patch deployment. Where possible, automation is in place to check for new patches and prepare deployment lists that can be approved by authorized Cloud Infrastructure personnel. The 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 Infrastructure team has a change management policy which includes the following activities:

- **Request for Change (RFC) process.** An RFC form must be submitted for all changes. The form includes the name of the change initiator, the change priority, the business justification for the change, and a requested change implementation date.

- **Backout plans.** The Cloud Infrastructure team creates detailed back out plans prior to deployment so that system state can be restored if a change causes a service disruption. Backout plans include executable instructions defined in scripts that restore system state with minimal manual steps.

- **Defined maintenance windows.** The Cloud Infrastructure team specifies scheduled, emergency, and extended maintenance windows. They schedule planned maintenance during off-peak hours.

- **Test plan.** The Cloud Infrastructure team defines a set of tests to verify that functionality is accessible after the deployment of a change.

- **Test execution.** Once deployment is complete, the Cloud Infrastructure and Autodesk Fusion Lifecycle QA team execute the tests to check that functionality identified as at-risk remains available.

Capacity Management

Customer access to cloud services is provisioned on-demand through a self-service model; therefore, 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 Infrastructure 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.

- **Capacity planning.** The Cloud Infrastructure team uses capacity management 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.

- **Activity monitoring.** Activity dashboards and alerts are defined across the backend services, allowing engineers to observe the system activity and to execute post-incident examinations and analysis.
Alerts and Monitoring

In order to provide the shortest possible Mean Time to Remediation (MTR), Autodesk uses automated systems to monitor Fusion Lifecycle, validating the health state of the service. Every single component, from the database to the services, is individually monitored. In the case of an event impacting the service, alerts are generated, and the Cloud Infrastructure team is notified through an escalation process.

The state of the Fusion Lifecycle service is publicly displayed by Autodesk’s Health Dashboard Service: https://health.autodesk.com.

Zero Downtime During Deployments

As patches are applied to the production environment, a rolling deployment approach is taken for Fusion Lifecycle. This helps ensure that customers do not experience any downtime of the service.

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.

Fusion Lifecycle Operational Controls

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

- **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.

Fusion Lifecycle 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 encrypted in transit via HTTPS and SSL. Passwords are stored as a one-way salted hash using the SHA-256 algorithm.

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 add and deactivate users and delegate administrative authority to other users.
User 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, to 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.

Autodesk Security

The Autodesk Security team is a dedicated group of product security engineers focused on identifying and enforcing security within the Autodesk cloud environment. The Autodesk Security team’s responsibilities include:

- **Infrastructure review.** Reviewing the security posture of Autodesk’s cloud infrastructure design and implementation.
- **Security policy.** Defining, ensuring implementation, and conducting annual reviews of security policies, including identity and access management, password management and vulnerability management.
- **Compliance.** Driving compliance with established security procedures by conducting internal reviews and security audits.
- **Data security.** Identifying and implementing technologies that secure customer information.
- **Security assessment.** Engaging third-party security experts to conduct information security assessments.
- **Incident response.** Monitoring cloud services for security issues and responding to incidents as needed.

Vulnerability Scans and Penetration Testing

Fusion Lifecycle services undergo an annual penetration test and regular scans for security threats and vulnerabilities defined by the Open Web Application Security Project (OWASP) and SANS Top 25. The application also undergoes static analysis and third-party library scans.

Network Security

Network security is enforced using a combination of physical and logical controls, including encryption, firewalls, and systems-hardening procedures. Additionally, AWS provides network security controls that protect their physical data centers. For more information, see the security whitepaper: [https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf](https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf).
Encryption

All network traffic is encrypted when transmitted over the Internet to the perimeter of the Autodesk cloud environment. Sensitive information, such as credentials, application session information, access tokens, files, and user profiles, is encrypted at rest.

Privacy

Autodesk is transparent on how customers’ personal data is collected and used. Read the Autodesk Privacy Statement to learn more.

Security Standards and Attestations

Autodesk has selected industry standard attestations and certifications for Fusion Lifecycle – ISO 27001, ISO 27017, and ISO 27018 certifications.

Resources

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

- To learn more about Autodesk, visit http://www.autodesk.com.
- For more information on our comprehensive security program, visit http://trust.autodesk.com.

Autodesk and Fusion Lifecycle are registered trademarks or trademarks of Autodesk, Inc., and/or its subsidiaries and/or affiliates in the USA and/or other countries. All other brand names, product names, or trademarks belong to their respective holders. Autodesk reserves the right to alter product and services offerings, and specifications and pricing at any time without notice, and is not responsible for typographical or graphical errors that may appear in this document.

© 2020 Autodesk, Inc. All rights reserved.