)XVLRQ/LIHFFOHEngineering

The)XVLRQ/LIHFFOHEngineering team is responsible for designing, implementing, and testing the software services provided by)XV LRQ/LIHFFOH.

The design, coding, testing, and maintenance of)XVLRQ/LIHFFOHis 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)XVLRQ/LIHFFOHVsecurity 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)XVLRQ /LIHFFOHCredentials 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 - To view information about Autodesk, visit http://www.autodesk.com.
- Autodesk Trust Center - To view information about Autodesk Trust Center, visit http://trust.autodesk.com.