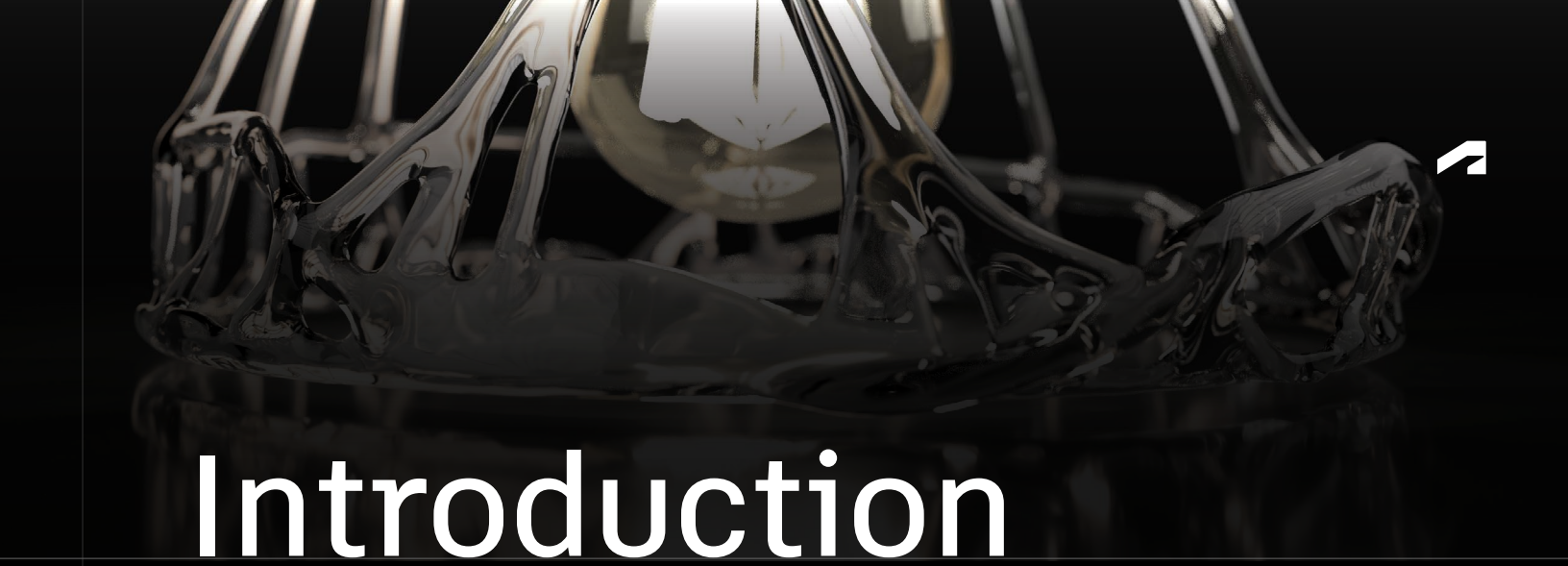
AUTODESK

Fusion Security Whitepaper



Introduction

Autodesk® Fusion™ is a cloud-based 3D CAD, CAM, and CAE platform that connects your product development process in a single environment across desktop (Windows and macOS), web browsers, and mobile devices. The Fusion tools help customers explore design ideas through an integrated concept-to-fabrication toolset, supported by security measures designed to help protect customer data.

Fusion adheres to Autodesk's security framework, based on industry standards and validated by independent third-party SOC 2 and ISO security attestations and certifications. Autodesk's security framework is embedded in Fusion to protect the confidentiality, integrity, and availability of customer information.

Fusion is designed for high availability and scalability, providing our customers with a fast and resilient cloud service. Autodesk's primary cloud hosting provider is Amazon Web Services (AWS), a leader in cloud infrastructure. Autodesk also utilizes cloud services from Microsoft Azure and Google Cloud Platform for targeted capabilities. Autodesk relies on the cloud hosting provider's shared responsibility model, which includes infrastructure composed of the hardware, software, networking, and facilities that run cloud services. For more information, please refer to:

- AWS shared responsibility model
- Microsoft Azure shared responsibility
- Google Cloud shared responsibility guidance

Document Purpose and Scope

This whitepaper describes the security measures, operational practices, and compliance-related resources Autodesk uses to help protect customer data and support customer security reviews. This whitepaper covers all modules and services in:

- Fusion
- Fusion Manage
- Fusion Team

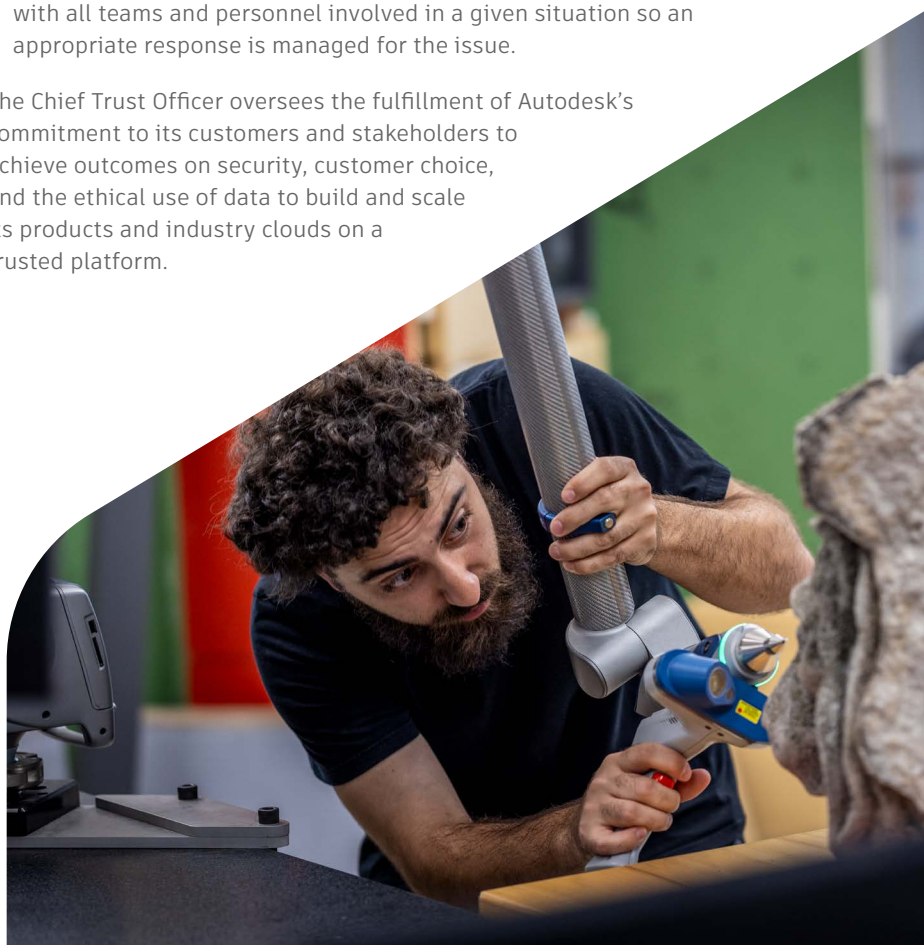
The purpose of this document is to explain Autodesk operations, the software development process, and security measures implemented in the environment to our valued customers, users, and stakeholders. In this document, Autodesk Fusion refers to both the Fusion client software and the Fusion browser access software.

Autodesk Security

The Autodesk security framework is based upon industry standards to meet consistent security practices, enabling us to build secure, run secure, and stay secure.

- **Build secure** - Embedding security into our products is a critical part of securing our customers' investment in Autodesk products and services. We build security into our products and services from the ground up. We integrate security activities into all phases of the development effort to identify and correct early and throughout the build process.
- **Run secure** - Securing our infrastructure is another critical way that we protect the confidentiality, integrity, and availability of our customers' information. We also build security directly into our products and deployment infrastructure. We provide security capabilities, such as endpoint protection, identity and access management, patching and hardening, and offensive security. We integrate these elements as a holistic approach to managing security.
- **Stay secure** - Gaining visibility into our environment offers us valuable insight into persistent suspicious activity, active security incidents, and ongoing exploits impacting Autodesk and our customers. We take proactive steps to defend against these threats with the appropriate incident response. We work closely with all teams and personnel involved in a given situation so an appropriate response is managed for the issue.

The Chief Trust Officer oversees the fulfillment of Autodesk's commitment to its customers and stakeholders to achieve outcomes on security, customer choice, and the ethical use of data to build and scale its products and industry clouds on a trusted platform.



Human Resources Security

Autodesk employees are required to follow the company's Code of Business Conduct, which requires every employee to conduct business lawfully, ethically, with integrity, and with respect for each other and the company's users, partners, and competitors. Per the Acceptable Use Policy, employees must protect the security, confidentiality, integrity, and availability of Autodesk and customer information.

Autodesk security is also supported through an internal information security awareness program, implemented through a variety of training methods (e.g. instructor-led training, e-learning, periodic newsletters). Employees with privileged role(s) and access (e.g. cloud operation teams) are required to take additional role-specific training to better protect customer data through cloud services.

Where permitted by law, background checks are required for employees with access to the computing resources and support systems used by the Autodesk teams.

Access Management

Autodesk has defined access management policies and processes for Autodesk personnel. These policies and processes address the provisioning of accounts, limiting access to Autodesk information and systems only to the extent necessary to perform assigned job responsibilities, and timely termination of access. Autodesk restricts access based upon business and security requirements to help prevent unauthorized access. Privileged access is restricted and requires additional management approvals.

Within Autodesk, multi-factor authentication (MFA) is also required for access to services, network and systems, production environments and access to internal Autodesk network. Access to software source code and production environments is restricted and aligned with business, security, and privacy requirements.

Customer Access Controls

Fusion administrative tools provide a flexible way for administrators to manage users, role-based permissions, and other access controls for end users.

Credentials consisting of an Autodesk ID, user email, and password are required to access Autodesk Fusion. Credentials are secured during network transmission and stored only as a salted hash.

Fusion provides end users with the option to use multi-factor authentication when logging in. Users who opt to enable this feature can use their authorized secure personal device (e.g., cell phone) to receive a code to use in conjunction with their password.

Asset Management

Asset management and protection begins with maintaining an inventory of assets with correlated roles (e.g. owners, custodians) and responsibilities for all assets. Autodesk assets inventory includes the name of the asset owner in an Autodesk managed Asset Management System. Assets are classified based on several criteria, such as asset value and importance, business criticality, implementation environment, and associated security and privacy requirements. Inventory of assets recognizes the context of systems that process, transmit, or store customer information.

Formal rules are defined for acceptable use of information assets and handling of assets throughout the assets' lifecycle.

Cyber Security Risk Management

Autodesk's Trust Risk Management Standard considers information security risks as operational risks, defined by the occurrence of any threat event that could compromise Autodesk assets (i.e., unauthorized use, loss, damage, disclosure, or modification of assets) for the profit, personal interest, or political interest of individuals, groups, or other entities, or because of accidental wrongdoing. Risk assessment in Autodesk is a continuous process of risk evaluation and subsequent implementation of controls or actions to limit and maintain the risk to an acceptable level. Autodesk's Trust Risk Management Standard consists of the following elements: risk assessment, risk treatment and risk monitoring and communication.

Continuous monitoring and reassessments are performed for high and critical risks identified. Risk assessments are performed by Autodesk's security team, and assessment results are presented quarterly to relevant business stakeholders and annually to Autodesk's board of directors. Autodesk's Trust Risk Management Standard methodology follows industry standards and frameworks and includes the following steps: prepare for assessment, conduct assessment, communicate assessment results, and maintain and monitor risk.

Data Classification, Management, and Protection

Autodesk implements controls to manage and protect the end-to-end information lifecycle, from creation/acquisition to retention and deletion. Autodesk considers sensitive information such as customer content as confidential restricted information. Security requirements for confidential-restricted information include:

- **Strong authentication and access restrictions** based on business need-to-know principles to authorized individuals.
- **Encryption of data** in transit and at rest.
- **Storage on secure drives** not directly accessible from the Internet.
- **Defined backup procedures,** retention periods, integrity checks, and destruction procedures.

Customer data stored in the Fusion platform are retained per applicable product terms of use, internal data retention policies defined by Autodesk Fusion Content Storage Standard, and contractual agreements.

Cryptography

Cryptographic controls are implemented for the protection of confidentiality, integrity, and authenticity of information.

Autodesk key management controls define the requirements for the use, protection, and lifetime of cryptographic keys and keying material. Cryptographic key management activities are performed by authorized Autodesk employees who adhere to relevant policies.

Fusion Cryptographic Practices

Fusion implements cryptographic algorithms based on leading best practices and standards. Information is protected with cryptographic controls, taking into consideration the state of the information (i.e., in transit or at rest) and the system or a system component which processes, transmits, or stores information.

Fusion implements cryptographic mechanisms for inbound and outbound data flows. All customer data is encrypted in transit and at rest:

- **Encryption in transit:** TLS v1.2 (min.).
- **Encryption at rest:** AES-256 (Database, Backups, etc.).

Secure Software Development and Change Management

Secure design, coding, testing, and maintenance processes are integrated into Autodesk's secure software development lifecycle methodology. During the design stage, Autodesk creates detailed design documents and threat models, which are reviewed and approved by security architecture experts to assess functionality, scalability, security, and performance. Software engineers and architects perform peer reviews to detect deviations from secure development practices and maximize code quality. An integral part of the secure development process also includes Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and third-party library scanning. Penetration tests are performed at least once a year by an external vendor.

Functional and acceptance testing programs include manual and automated techniques to check that services are developed on predefined and testable criteria.

Performance testing is also integrated into the development lifecycle. Autodesk's quality assurance team conducts load tests throughout the development cycle to identify changes that negatively affect performance as early in the process as possible.

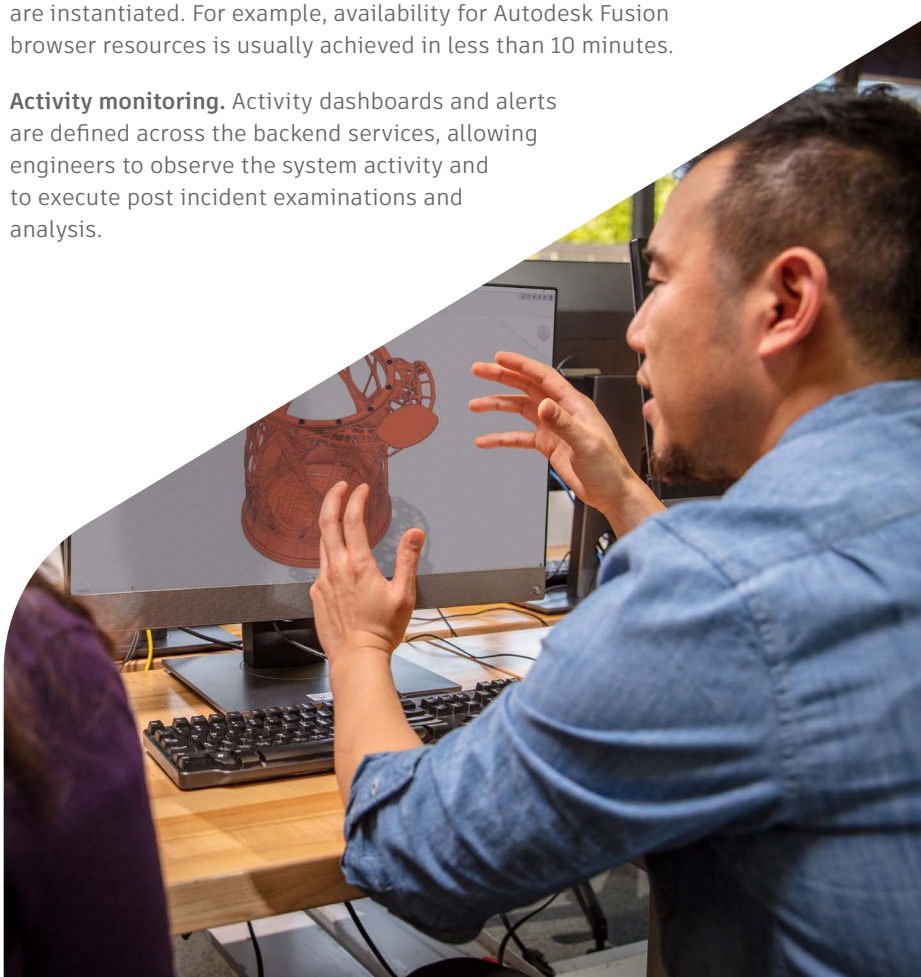
The cloud operations team is responsible for defining and executing procedures for software release management, roll-back plans, system upgrades, system health monitoring, and other activities required for the operational monitoring and maintenance of Autodesk products. Change management policies define release requirements to provide traceability for production software changes. All organizational and operational processes and information-processing changes are controlled, documented, and approved following the change management procedure.

Autodesk practices continuous delivery of code into production through multiple environments: development, staging, and production. These environments are segregated to mitigate the risks of unauthorized access or changes to the production environment.

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 Infrastructure team implements a capacity management policy. These practices include:

- **Frequent recording of resource use**. Autodesk Fusion 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.
- **Resource allocation.** Computational resources are allocated as customers request them. Pre-warmed computation resources are always available. If a spike of activity occurs, new resources are instantiated. For example, availability for Autodesk Fusion browser resources is usually achieved in less than 10 minutes.
- **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.



Operations Security, Vulnerability, and Patch Management

Secure operational procedures and responsibilities are implemented to protect the processing and storage of customer information.

Autodesk security framework requires the implementation of security controls for each system component (e.g., server, database, network device, service, etc.) taking into consideration the classification of information processed, transmitted, or stored. Systems and services are continuously monitored, scanned, and tested to validate the correct operation of security controls. Standard system hardening requirements are enforced through configuration and vulnerability scanning activities.

Information about technical vulnerabilities is continuously monitored and processed in a timely manner. Vulnerability identification methods include automated vulnerability scanners, penetration testing, bug bounty programs, and gathering of threat intelligence. All production systems and system components are in scope of the vulnerability management process.

Identified vulnerabilities are evaluated, and appropriate measures are taken to remediate identified risks. The priority of vulnerability remediation is determined by a combination of the vulnerability severity score corresponding to CVSS (Common Vulnerability Scoring System) v3, exploitability, exposure, and existing compensating controls.

Remediation methods for all in-scope systems and components include patch management, software change, or implementation of compensating controls. Continuous patching is performed.

Fusion Operational Security Controls

In addition to the above-described controls, Fusion has implemented the following operational security controls:

- **Hardening:** All system and application infrastructure components are hardened.
- **Web Application Firewall (WAF):** WAF is configured and enabled to protect against common web application attacks.
- **Anti-malware controls:** Advanced anti-malware and anti-virus technical controls are implemented across Fusion environments and are combined with operational controls such as Security Awareness Training to increase awareness of malware threats across all employees and users.
- **Intrusion detection and prevention:** Alerts from intrusion detection systems are monitored and investigated for any unusual or suspicious behavior; when alert investigation results in a suspect on true positive alert, Autodesk's Incident Response process is triggered.
- **Threat intelligence:** Threat intelligence sources are regularly reviewed and evaluated for applicability in Fusion products; applicable threats are prioritized in accordance with the risk level.

Fusion Availability, Resilience, and Data Protection

Availability and Clustering

Fusion is designed to achieve availability and scalability by employing redundant systems in its supporting infrastructure and distributing loads across auto-scalable instances. Clustering technology keeps Fusion available by limiting single points of failure and directing service requests away from instances that are highly utilized. All services are monitored for resource usage (e.g., CPU, memory, storage), DB operation performance, and liveness probes. Automated compensating behaviors and alerts are triggered in cases where the threshold is reached, and action is needed.

As patches and upgrades are applied to the production environment, a rolling deployment approach is taken for Fusion whenever possible, aiming to limit downtime of the service. Changes that may affect service availability can be announced to customers as scheduled maintenance (2 weeks in advance) or emergency maintenance (as far in advance as possible), each including information on description, impact, and duration.

Backup and Recovery

Backup copies of information, software, and system images are taken and tested regularly in accordance with Autodesk's backup strategy and policies to protect against the loss of data. Backup policies define the frequency of creating backups, appropriate security controls, and retention periods, based on the classification of data. After the expiry of the backup retention period, information is securely disposed.

Backups are encrypted at rest and access is restricted to privileged employees. Recovery testing is periodically conducted to validate the integrity of backup data and to verify the duration of the recovery process.

Data Replication

Replication of customer data is performed between AWS Availability Zones (AZs). Replication limits the possibility of data loss or a delay in service resumption if fail-over to another zone is required.

All customer data submitted to Fusion, up to the last committed transaction, is automatically replicated on a near real-time basis to a secondary availability zone. Data is backed up daily and stored for 30 days into a secondary AWS region, after which it is securely disposed.

Network Security

Network security management processes and controls help protect information in networks and support information processing components. Services and interfaces are grouped taking into consideration their function, sources, and destination of traffic and exposure. Groups are segregated in network segments (e.g., public, DMZ, internal, restricted, etc.) and filtered by appropriate network security devices, permitting only approved network traffic matrices. The deny-all principle is used on all network filtering security devices.

Transfer of information is protected taking into consideration the nature and risks of each channel. Network security is enforced using a combination of physical and logical controls, including encryption, firewalls, and systems-hardening procedures.

Logging and Monitoring

Production systems and applications are configured to log events and activities to support automated event correlation and analysis. Logs are protected against tampering and unauthorized access with special attention to administrator access and operator logs. An audit trail is established for all relevant user-system interactions. The retention period of logging records is kept according to business and regulatory requirements. Security Information and Event Management (SIEM) software is used by the Security Operations Center (SOC) team to monitor, detect, and respond to security or privacy alerts. To provide the shortest possible Mean Time to Remediation, Autodesk uses automated systems to monitor Fusion, validating the health state of the service. Each 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 service health also describes the interrelation between Autodesk services. A service like Autodesk Fusion is highly sensitive to the ACM service (Access Control). Each service must be resilient when a dependent service fails and should gracefully fail when it can no longer operate without any data loss for the customer.

The state of the Fusion service is publicly displayed by Autodesk's Health Dashboard Service.

Incident Response

Autodesk implements a security incident response process to consistently detect, respond, and report incidents, minimize data loss, mitigate risks, and restore information system functionality and service continuity as soon as possible.

Autodesk has a documented Security Incident Response Process (SIRP) to effectively manage security incidents. Roles, responsibilities, and procedures are established to produce a timely and efficient response to potential security or privacy-related incidents. All employees and external parties are required to report any observed or suspected security events in systems or services.

The incident response process includes:

- **Continuous monitoring** of threats and alerts.
- **Establishment** of an information security incident response team.
- **Clear procedures** for identifying, responding, assessing, analyzing, and follow-up of information security incidents.
- **Clear communication** of security incidents with internal and stakeholders.
- **Continuous improvement** from information security incidents to reduce the probability or impact of future incidents.

The SIRP is periodically reviewed and evaluated for effectiveness. The incident response process is tested annually to assess the effectiveness of the process and training of security incident response stakeholders.

Business Continuity and Disaster Recovery

Autodesk's Business Continuity and Disaster Recovery (BCDR) program establishes processes and procedures to recover critical products, including Fusion, following a disruption resulting from a crisis or a disaster situation.

Processes, activities, and resources are defined by performing a Business Impact Analysis (BIA), which identifies critical business processes, services and activities, and key resources necessary for operating that process, service, or activity.

BCDR scenarios, teams, and roles are documented as a Business Continuity Plan (BCP). Events that would initiate this plan include natural disasters, political disturbances, man-made disasters, external human threats, and internal malicious activities.

The BCP is tested annually; BCP test exercises include tabletop and simulation/technical testing.

BCP testing is performed to maximize the effectiveness of contingency operations through an established plan in following phases:

- **Notification phase** to detect and assess damage.
- **Activation phase** to respond to the damage and activate the plan.
- **Recovery phase** to restore temporary operations and recover damage done to the original system.

Third-Party Security and Vendor Risk Management

Autodesk has a third-party risk assessment process to evaluate and identify security, privacy, and compliance risks before engaging third parties that have access to customer information. Compliance with this process is mandatory for all business and product teams across Autodesk.

The Security team conducts assessments, reports identified risk to business owners and tracks third party security risk remediation activities.

Trusted AI

Some Fusion products include AI features that support product design and manufacturing workflows. These features are developed through Autodesk's centralized platform for building customer-facing AI products and features. This platform is certified to ISO 42001, an international standard for AI management systems that establishes a framework for organizations to develop, deploy, and monitor AI technologies responsibly. ISO 42001 certification applies to Autodesk's centralized AI development platform and not to individual Fusion features.

Additional information about the standards and practices Autodesk employs to develop AI within our products is available in the Trusted AI section of the Autodesk Trust Center.

Details about specific AI features in Fusion, including functionality, data sources, and applicable safeguards, are available in the AI transparency cards.

Privacy

Legal requirements related to privacy and protection of personal data are continuously monitored and implemented across Autodesk's operations.

Autodesk discloses how customers' personal data is collected and used. Read the Autodesk Privacy Statement to learn more.

Compliance

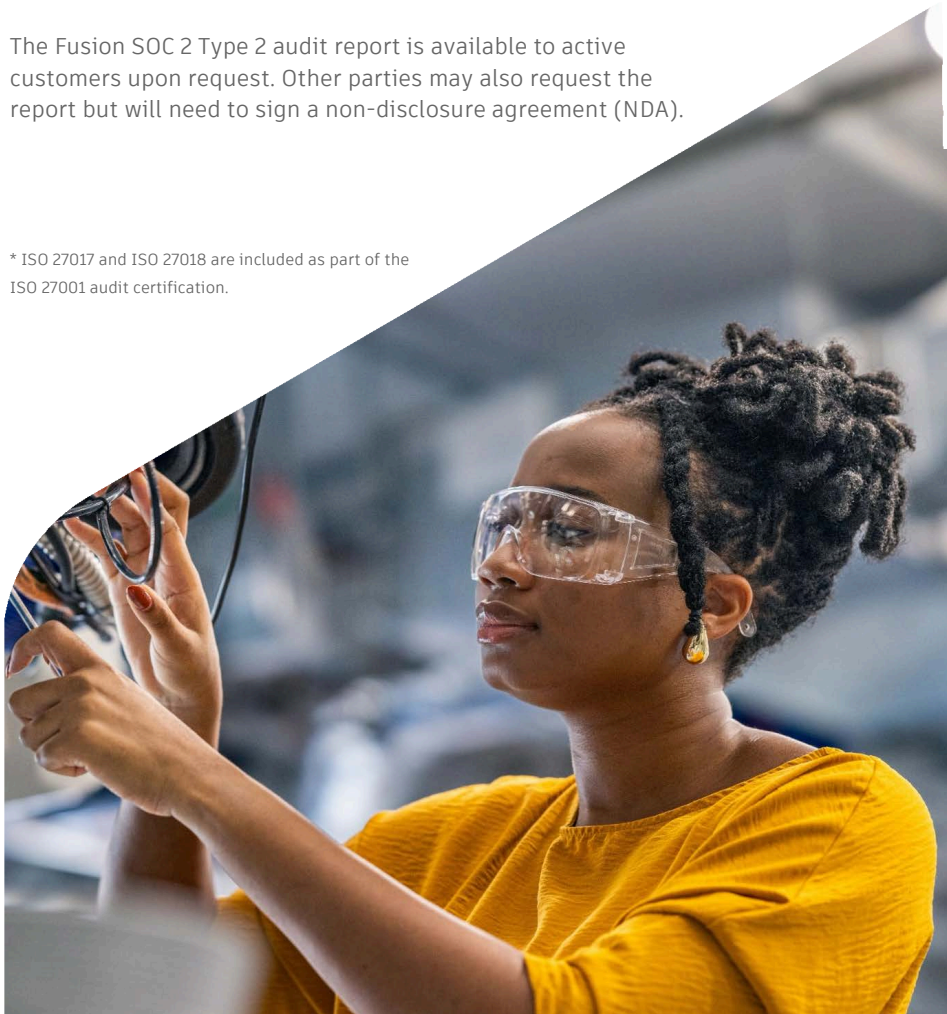
Autodesk assesses its compliance against data protection and information security standards on a regular basis. Autodesk implements security policies based on industry best practices and regularly conducts internal and external audits, attestations, and certifications. Management of information security and the implementation of related processes, policies, and procedures are independently reviewed and audited periodically or when significant changes relevant to security and privacy domains occur. Reviews and audits also include technical inspections to assess the effectiveness of controls to comply with compliance frameworks, regulatory requirements, or contractual requirements.

- **Fusion maintains industry-standard SOC 2 Type 2 attestation.**
- **Fusion is ISO 27001, ISO 27701, ISO 27017 and ISO 27018 certified*.**

The SOC 3 report, which includes Fusion and some other Autodesk products, is available in the Compliance section of the Autodesk Trust Center and the Product Design & Manufacturing Trust Portal. The SOC 3 report provides a high-level summary of the independent SOC 2 assessment without disclosing specific security controls.

The Fusion SOC 2 Type 2 audit report is available to active customers upon request. Other parties may also request the report but will need to sign a non-disclosure agreement (NDA).

* ISO 27017 and ISO 27018 are included as part of the ISO 27001 audit certification.



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

Additional Resources and Relevant Certifications

Autodesk
To learn more about Autodesk, visit http://www.autodesk.com.

Autodesk Trust Center
For more information on our comprehensive security program, visit https://autodesk.com/trust.

Autodesk Trust Portal
For more information on how Autodesk protects your data & content, ensures a high level of security and availability, and mitigates emerging threats, visit https://trustportal.pdm.autodesk.com.