Report on Autodesk, Inc.’s Cloud Products and Infrastructure System Relevant to Security, Availability, and Confidentiality Throughout the Period May 1, 2025 to October 31, 2025

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Autodesk, Inc. ("Autodesk")

Scope

We have examined Autodesk's accompanying assertion titled "Assertion of Autodesk, Inc. Management" (assertion) that the controls within Autodesk's Cloud Products and Infrastructure System (system) were effective throughout the period May 1, 2025 to October 31, 2025, to provide reasonable assurance that Autodesk's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*.

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Autodesk, to achieve Autodesk's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of Autodesk's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Autodesk uses subservice organizations to provide supporting infrastructure, security, and authentication services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Autodesk, to achieve Autodesk's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Autodesk's controls. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Autodesk is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Autodesk's service commitments and system requirements were achieved. Autodesk has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Autodesk is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Autodesk's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Autodesk's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Autodesk's Cloud Products and Infrastructure System were effective throughout the period May 1, 2025 to October 31, 2025, to provide reasonable assurance that Autodesk's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Autodesk's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Louisville, Colorado
December 12, 2025

Section 2

Assertion of Autodesk, Inc. Management

AUTODESK
Make Anything

Assertion of Autodesk, Inc. ("Autodesk") Management

We are responsible for designing, implementing, operating and maintaining effective controls within Autodesk's Cloud Products and Infrastructure System (system) throughout the period May 1, 2025 to October 31, 2025, to provide reasonable assurance that Autodesk's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Autodesk, to achieve Autodesk's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of Autodesk's controls.

Autodesk uses subservice organizations for supporting infrastructure, security, and authentication services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Autodesk, to achieve Autodesk's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Autodesk's controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period May 1, 2025 to October 31, 2025, to provide reasonable assurance that Autodesk's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Autodesk's controls operated effectively throughout that period. Autodesk's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period May 1, 2025 to October 31, 2025, to provide reasonable assurance that Autodesk's service commitments and system requirements were achieved based on the applicable trust services criteria.

Autodesk, Inc.

Attachment A

Autodesk, Inc.’s Description of the Boundaries of Its Cloud Products and Infrastructure System

Type of Services Provided

Autodesk, Inc. (“Autodesk” or the “Company”), develops three dimensional (3D) design, engineering, and entertainment software. Autodesk’s broad portfolio allows companies across different sectors to use integrated tools for design, simulation, collaboration, production, and more.

The boundaries of the system in this section details Autodesk’s Cloud Products and Infrastructure System. Any other Company services are not within the scope of this report.

Autodesk’s Cloud Products and Infrastructure System includes the following:

Product Family	Product Feature and Supporting Services	Description
Fusion	Fusion Manage • Classification Service • Fusion Manage • Gluon • Fusion Manage Extension • Numbering Scheme Service	Cloud-based Product Data Management (PDM) system where teams can collaborate across the value chain.
	Fusion Operations	Manufacturing execution system (MES), providing real-time data for production management.
	Fusion Team • FusionDM • A360 Mobile Nova • Fusion Supportal • Fusion Team Forge API • Fusion Team GDPR • Fusion DM Jobs • Fusion HQ • Fusion Symphony Profile • SymphonyDM	A cloud-based collaboration and data management workspace for Fusion users that lets teams securely store, share, version, and review design files in one place.
	Fusion • BOM Eventual Consistency Service • BOM Export • Fusion Receipt Validator • Fusion Machine Connect Service • Fusion Automation Service • Autodesk Libraries Platform Favorites GDPR (FLIBGDPR) • Autodesk Libraries Platform Domain Services (LDS) • Manufacturing Artificial Intelligence (AI) solutions • Fusion Electronics (EAGLEWEB) • Fusion360 Session Concurrency • FUSCOPY • Fusion Synthetic Monitors • Fusion Health Service • Fusion JS Service	A cloud-connected 3D CAD, CAM, CAE, and PCB platform that combines design, engineering, simulation, and manufacturing tools in a single integrated environment.

Product Family	Product Feature and Supporting Services	Description
	• Fusion360 Workflow Service • Fusion Guide (FGUIDE) • Fusion360 Abus Adapter • Fusion360 Notification Service • AnyCAD	
	Fusion Generative Design • Fusion 360 Automated Modeling • Fusion Generative Design Previewer • Fusion Generative Design • Autodesk Generative Design Explore (AGDEX)	An AI-driven design tool in Autodesk Fusion that automatically generates optimized 3D design options based on user-defined goals, constraints, and materials—helping engineers explore stronger, lighter, and more efficient solutions.
	Manufacturing Data Management (MFGDM) • APS Manufacturing Data Model • Fusion Atlas Service • Manufacturing Design GraphQL • MFG Design Rest API Service • Fusion PIM Migration Service • PIM Configuration • PIM Data Management • Product Information Model • PIM PP Extraction	A set of data-management capabilities within Autodesk Fusion that helps manufacturing teams securely store, control, version, and track CNC, CAM, and production-related files—keeping tooling, machine setups, and process data organized and consistent across the shop floor.
	Simulation • Fusion E-Cooling (SIMECOOL) • Fusion Electronics Cooling Micro FrontEnd (FECMFE) • Fusion Sim GCP Nastran (SIMNAS) • Fusion Sim GCP Explicit (SIMEXP) • Fusion 360 ECAD • Fusion Simulation Post Processor Container service (SIMWEB) • Fusion Simulation Post Processor Services (HWKSVC) • Fusion Injection Molding • Fusion Structural Simulation Post Processor service (NASEXP)	Advanced simulation functionality, including structural simulation, manufacturability, and generative design to optimize part design and performance for FEA, electronic cooling, injection molding, and more.
EMS Product	Flow Production Tracking (formerly ShotGrid)	Flow Production Tracking (formerly ShotGrid) is a powerful production management and review platform that streamlines scheduling, budgeting, and collaboration with customizable workflows and robust media review tools.

Product Family	Product Feature and Supporting Services	Description
ADSK Common Services	FDA (Front End Design Automation) • ACADIO-P-UE1	A design automation that exposes web service API that provides clients the ability to run scripts on their design files, it leverages the APS Platform to automate repetitive tasks.
	Rendering 360	Autodesk Rendering uses cloud power to create high-resolution renderings without costly hardware, allowing users to render from Autodesk apps and view previews as they design.
	Autodesk Platform Services • Autodesk Compute Platform (ACP) (FCSL2-P-UE1) • Platform Content Service	A collection of cloud APIs and services that let developers build apps, integrations, and automations on top of Autodesk's data and products.
AECO Services	Autodesk Docs • Content Catalog	Autodesk Docs provides a central, cloud-hosted location where project teams can store, manage, review, and share 2D/3D design files and construction documents.
	Autodesk Construction Cloud (ACC) • Integrated Insight Service (IIS)	A unified, cloud-based platform that connects project teams, workflows, and data across the entire construction lifecycle—from design through planning, building, and operations—to improve collaboration, reduce risk, and deliver projects more efficiently.
	BCF Import (BCF-P-UE1)	BCF (BIM Collaboration Format) is a standard AEC file format used to exchange BIM issues, comments, and changes across different software, improving communication and coordination among project teams.
	UDA Global Configuration	The UDA Global Configuration is a static service that provides configuration JSON to Autodesk products using UDA components. It defines settings like trusted Autodesk domains, subscription expiration, and error tracking. For example, Fusion uses it to verify that thumbnail URLs come from approved Autodesk domains.

The Boundaries of the System Used to Provide the Services

The boundaries of Autodesk's Cloud Products and Infrastructure System are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of Autodesk's Cloud Products and Infrastructure System.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

The Company utilizes Amazon Web Services (AWS), Snowflake, and MongoDB to provide the resources to host Autodesk's Cloud Products and Infrastructure System. The Company leverages the experience and resources of AWS and MongoDB to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring Autodesk's Cloud Products and Infrastructure System architecture within AWS and MongoDB to ensure the availability, security, and resiliency requirements are met.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

Infrastructure
Amazon Elastic Compute Cloud (Amazon EC2)
Amazon Elastic Container Service (Amazon ECS)
AWS Identity and Access Management (IAM)
Amazon Simple Storage Service (Amazon S3)
Amazon Relational Database Service (Amazon RDS)
Amazon Virtual Private Cloud (Amazon VPC)
Amazon Dynamo DB (DDB)
MongoDB

Software

Software consists of the programs and software that support Autodesk's Cloud Products and Infrastructure System operating systems and databases. The list of software and ancillary software used to build, support, secure, maintain, and monitor Autodesk's Cloud Products and Infrastructure System include the following business functions:

- Operating System
- Database
- Security monitoring
- Security monitoring and endpoint protection
- Availability monitoring

- Asset Management
- Anti-virus/anti-malware solution
- Multi-factor authentication (MFA)
- Centralized source code control system
- Ticketing system
- Human Resources (HR) Management System
- File Management
- Domain Driven Design (DDD)
- Key management
- Cloud security
- IAM service
- Security management

People

The Company develops, manages, and secures Autodesk's Cloud Products and Infrastructure System via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Leadership Team	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
Sales, Marketing, Customer Success, and Digital Platform and Experience	Responsible for customer experience including customer support, sales management, brand experience, and user experience, and builds and maintains key Company platforms.
Architecture, Engineer, and Construction Solutions	Responsible for supporting AEC customers by delivering end to end CAD and BIM solutions, inclusive of early-stage planning, design, and construction.
Platform Services and Emerging Technologies	Responsible for platform services including emerging technology, platform customer support, and platform access management.
Product Development and Manufacturing Solutions (PDMS)	Responsible for driving aggressive growth by delivering exceptional experiences that help customers in the design and manufacturing industry achieve the new possible with converged design and make processes that include: • Build, test, and deploy code • Manage access
Entertainment and Media Solutions	Responsible for entertainment and media solutions products including customer support and managing access to that suite of products and services.
People and Places (PPL)	Responsible for attracting, developing, supporting, and retaining the workforce needed to achieve Autodesk objectives. PPL partners with leaders across the business to ensure the organization is staffed with skilled talent; employees are supported through every stage of the employment lifecycle; and policies and processes align with legal, ethical, and cultural expectations.

People	
Group/Role Name	**Function**
Legal and Government Affairs	Responsible for protecting the Company's legal interests, ensuring compliance with applicable laws and regulations, and shaping the Company's external operating environment through strategic public policy engagement. This organization acts as a trusted advisor to leadership, guiding decision-making, mitigating risk, supporting ethical business practices, and influencing governmental and regulatory outcomes that impact the Company and its customers.
Finance	Responsible for ensuring the Company's financial health by planning, managing, analyzing, and reporting financial performance. Finance partners with business leaders to drive strategic decision-making, ensure efficient use of resources, safeguard company assets, and maintain compliance with accounting standards and regulatory requirements.

Procedures

Procedures include the automated and manual procedures involved in the operation of Autodesk's Cloud Products and Infrastructure System. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, information technology (IT), and HR. These procedures are drafted as a part of the security policies and are updated and approved as necessary for changes in the business, but at least annually.

- Security Policy
- Access Control Policy
- Business Continuity and Disaster Recovery Standard
- Network Configuration and System Hardening Standard
- Data Classification Standard
- Data Loss Prevention Standard
- IT Asset Management Standard
- Security Incident Management Standard
- Security Logging and Monitoring Standard
- Security Risk Management Standard
- Security Software Development Lifecycle (SSDLC) and Change Management Standard
- Security Training and Awareness Standard
- Third Party Security Risk Management Standard
- Vulnerability Management Standard
- Cloud Services Data Destruction Guidelines

Data

Data includes electronic data or information uploaded to Autodesk's in-scope products by customers (also referred to as user entities). This data is considered confidential information for the purposes of this report. Confidential data is protected based on risk throughout its full lifecycle from unauthorized use, loss, or acquisition from an unauthorized party. Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts. Autodesk Trust has an established framework and policies based on legal, statutory, and regulatory requirements to govern its data.

Cryptographic controls are implemented, as deemed necessary by the data classification. Trust has established framework and policies based on PCI DSS requirements.

Content, a subset of Data, includes files, designs, models, data sets, images, documents, or similar material submitted or uploaded to the in-scope products by user entities; and user entity specific output generated from the in-scope products, if any, based on the user entities' own raw data or information. Content is considered confidential information for the purposes of this report.

Customers maintain ownership of and responsibility for their Content and responsibility for their conduct while using Autodesk's in-scope products. Autodesk's in-scope products provide the ability to create, submit, post, or otherwise make Customer Content available to Autodesk and/or others. Autodesk personnel will not access Customer Content except (a) as part of providing, maintaining, securing, or modifying in-scope products; (b) at the Customer's request or with Customer consent as part of addressing or preventing a service, support, or technical issue; or (c) in connection with legal obligations or proceedings.

Autodesk also maintains internally generated information and configuration data (referred to as Operational Data) from the normal operations of the systems.

The Company has deployed secure methods and protocols to protect the transmission of confidential and sensitive information over public networks. Encryption is enabled for databases housing sensitive customer data.

Autodesk has procedures in place to securely delete customer data when customers leave the service in accordance with its data deletion commitments to its customers.

Complementary User Entity Controls (CUECs)

The Company's controls related to Autodesk's Cloud Products and Infrastructure System cover only a portion of overall internal control for each user entity of Autodesk's Cloud Products and Infrastructure System It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls, taking into account the related CUECs identified for the specific criterion. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls
CC2.2 CC2.3	• User entities are responsible for understanding and complying with their security and confidentiality contractual obligations to Autodesk.
CC6.1 CC6.2 CC6.3	• User entities are responsible for the establishment and termination of user accounts within Autodesk.
CC6.1	• User entities are responsible for keeping their user account credentials secure in Autodesk. • User entities are responsible for restricting access and distribution of reports generated from Autodesk. • Customers are responsible for setting password requirements for their internal users.
CC6.1 C1.1 C1.2	• Customers are responsible for the management of files and permissions within their projects.
CC6.2 CC6.3	• Customers are responsible for provisioning, deprovisioning, and reviewing the list of users within their projects.
CC2.2 CC2.3 CC7.3 CC7.4 CC7.5	• User entities are responsible for communicating relevant security, availability, and confidentiality issues and incidents to Autodesk through identified channels.
CC6.1 C1.2	• User entities are responsible for the management of their data uploaded to Autodesk's Cloud Products and Infrastructure System, including the movement and deletion of that data.
CC9.1 A1.2 A1.3	• User entities are responsible for developing their own business continuity plans that address their inability to access or utilize Autodesk's Cloud Products and Infrastructure System.

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

Autodesk has contracted with subservice organizations in support of its in-scope products' system to provide supporting infrastructure, security, and authentication services. The controls relating to the physical security, infrastructure maintenance, and network availability of the subservice organizations have been carved out of the scope of Autodesk's SOC 2 Type II report.

Company management receives and reviews the AWS, MongoDB, Snowflake, SentinelOne, CrowdStrike, and Microsoft Entra ID/MS Authenticator SOC 2 reports annually. In addition, through its operational activities, Company management monitors the services performed by AWS, MongoDB, Snowflake, SentinelOne, CrowdStrike, and Microsoft Entra ID/MS Authenticator to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreements, stay informed of changes planned at the hosting facilities, and relay any issues or concerns to AWS, MongoDB, Snowflake, SentinelOne, CrowdStrike, and Microsoft Entra ID/MS Authenticator management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to Autodesk's Cloud Products and Infrastructure System to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls, taking into account the related CSOCs expected to be implemented at AWS, MongoDB, Snowflake, SentinelOne, CrowdStrike, and Microsoft Entra ID/MS Authenticator as described below.

Criteria	Complementary Subservice Organization Controls
CC6.1 C1.1	• AWS, MongoDB, and Snowflake should encrypt databases in their control.
CC6.4	• AWS, MongoDB, and Snowflake should restrict data center access to authorized personnel. • AWS, MongoDB, and Snowflake should monitor data centers 24/7 by closed circuit cameras and security personnel.
CC6.5 C1.2	• AWS, MongoDB, and Snowflake should securely decommission and physically destroy production assets in its control.
CC6.8	• CrowdStrike and SentinelOne should have updated intelligence and protection mechanisms in place to prevent or detect unauthorized or malicious software installed on the in-scope systems.
CC7.2 A1.2	• AWS, MongoDB, and Snowflake should install fire suppression and detection and environmental monitoring systems at the data centers. • AWS, MongoDB, and Snowflake should protect data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • AWS, MongoDB, and Snowflake should oversee the regular maintenance of environmental protections at its data centers.
CC9.1 A1.2	• AWS, MongoDB, and Snowflake, should notify the Company in the event of database replication failure. • AWS, MongoDB, and Snowflake, should notify the Company in the event of database backup failure.
A1.1 A1.2 A1.3	• Microsoft Entra ID/MS Authenticator is responsible for notifying the Company of availability disruption.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Autodesk designs its processes and procedures related to in-scope products and platform services to meet security, availability, and confidentiality objectives. Those objectives are based on the service commitments that Autodesk makes to user entities; the laws and regulations that govern the provision of Autodesk's services; and the financial, operational, and compliance requirements that Autodesk has established for their services.

Commitments to user entities are documented and communicated in the Privacy Statement, Data Processing Addendum, and Terms of Use, as well as in the description of the service offering provided online. Security, availability, and confidentiality commitments are standardized and include, but are not limited to, the following:

Trust Services Category	Service Commitments	System Requirements
Security	• Autodesk will maintain administrative, technical, and physical safeguards designed to protect to the security, confidentiality, and availability of customer data. • Upon becoming aware of a security incident, Autodesk will notify the customer promptly.	• Employee provisioning and deprovisioning standards • Logical access controls • Risk assessment standards • Change management controls • Monitoring controls • Employee security training • Intrusion detection standards • Encryption standards
Availability	• Autodesk will maintain the availability of the services.	• Backup standards • Business continuity standards • Disaster recovery testing standards
Confidentiality	• Autodesk will use the same degree of reasonable care over customer confidential information that it uses to protect its own confidential information. • Autodesk will not use or disclose the customer's confidential information for any purpose other than those listed in the Terms of Use. • Upon termination or expiration of the agreement, Autodesk will either delete or return all customer data unless required by law.	• Data classification standards • Customer data deletion and retention standards • Employee confidentiality agreements • Vendor confidentiality agreements