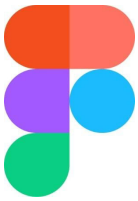


Figma, Inc.

System and Organization Controls (SOC) 3

Report on Figma, Inc.'s Assertion Related to Its Figma System Relevant to Security, Availability, and Confidentiality

Throughout the Period
November 1, 2022 to October 31, 2023

Contents

I. Independent Service Auditor's Report on a SOC 3 Examination

Tel: 415-397-7900
Fax: 415-397-2161
www.bdo.com

One Bush Street, Suite 1800
San Francisco, CA 94104

Independent Service Auditor's Report on a SOC 3 Examination

To the Management of
Figma, Inc.
San Francisco, CA

Scope

We have examined Figma, Inc.'s (Figma or service organization) accompanying assertion titled *Assertion of Figma, Inc. Management* (assertion) that the controls within Figma's Figma System (the System) were effective throughout the period November 1, 2022 to October 31, 2023 to provide reasonable assurance that Figma's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) *s*et forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Figma uses subservice organizations to perform certain activities. A list of these subservice organizations and the activities performed is provided in Attachment A. The assertion indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Figma, to achieve Figma's service commitments and system requirements based on the applicable trust services criteria. Figma's description of the boundaries of the system in Attachment A presents the types of complementary subservice organization controls assumed in the design of Figma's controls but does not disclose the actual controls at the subservice organizations. 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

Figma 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 Figma's service commitments and system requirements were achieved. Figma has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Figma 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 controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period November 1, 2022 to October 31, 2023 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 AICPA. 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.

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 the service organization'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 Figma'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.

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

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the operating effectiveness of controls is subject to the risks 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 Figma's system were effective throughout the period November 1, 2022 to October 31, 2023 to provide reasonable assurance that Figma's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Restricted Use

This report is intended solely for the information and use of Figma, user entities of Figma's system during some or all of the period November 1, 2022 to October 31, 2023, business partners of Figma subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.

- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

BDO USA, P.C.

February 2, 2024

II. Assertion of Figma, Inc. Management

Assertion of Figma, Inc. Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Figma, Inc.'s (Figma or the service organization) Figma System (the System) throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that Figma's service commitments and system requirements relevant to security, availability, and confidentiality (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented in Attachment A, *Figma, Inc.'s Description of the Boundaries of Its Figma System* and identified the aspects of the system covered by our assertion.

Figma uses subservice organizations to perform certain activities. A list of these subservice organizations and the activities performed is provided in Attachment A. The description of the boundaries of the system in Attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Figma, to achieve Figma'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 Figma's controls. The description of the boundaries of the system does not extend to the actual controls at the subservice organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2022 to October 31, 2023 to provide reasonable assurance that Figma's service commitments and system requirements were achieved based on the trust services criteria relevant to the applicable trust services criteria set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*. Figma'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 were achieved.

We assert that the controls within the system were effective throughout the period November 1, 2022 to October 31, 2023 to provide reasonable assurance that Figma's service commitments and system requirements were achieved based on the applicable trust services criteria.

Figma, Inc.

February 2, 2024

Attachment A — Figma, Inc.'s Description of the Boundaries of Its Figma System

Attachment A — Figma, Inc.'s Description of the Boundaries of Its Figma System

Scope and Description of the Boundaries of the System

This is a System and Organization Controls (SOC) 3 report and includes a description of the boundaries of Figma, Inc.'s (Figma, service organization, or Company) Figma System (the System) and the controls in place to meet the criteria for 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*, in AICPA *Trust Services Criteria*, throughout the period November 1, 2022 to October 31, 2023 (the period) which may be relevant to the users of the System. It does not encompass all aspects of the services provided or procedures followed for other activities performed by Figma.

Figma uses subservice organizations to perform certain services. A list of these subservice organizations and the services performed is provided in the following table. The description of the boundaries of the system does not extend to the actual controls at the subservice organizations.

Subservice Organization	Services Performed
Amazon Web Services, Inc. (AWS)	Provides the infrastructure-as-a-service and platform-as-a-service environment that provides the physical and environmental safeguards, infrastructure support and management, and storage services for Figma.
Okta, Inc. (Okta)	Identity and Access Management Tool that provides single sign on (SSO) and multifactor authentication (MFA) services.
Perma Security Inc. (Opal)	Identity and access management platform used by Figma to perform user access reviews and provision user access.

The scope of this report includes the Systems and services operated by Figma, including Figma (for design + dev) and FigJam (for whiteboard). These systems and services are hosted on AWS in the following regions:

- US West
- US East
- EU Central
- EU West

The scope of this report does not include the following:

- Figma Community (https://www.figma.com/community)
- Any plug-ins or widgets added to your Figma Design and FigJam files to improve your workflows and enhance your usage of the Figma Platform. Learn more about plug-ins and widgets at https://help.figma.com/hc/en-us/sections/4404285845015-Plugins-Widgets

Company Background

Figma was founded in 2012 and provides a web-based software as a service (SaaS) interface design tool that allows users to easily brainstorm, create, collaborate, and securely share interface and application designs. Figma's mission is to make design accessible to everyone. Figma is compatible with your web browser and offers mobile, iOS, Android, and desktop applications so users can design and brainstorm on their preferred device. Figma has been adopted by many organizations ranging from startups to large multinational organizations. Figma is headquartered in San Francisco and operates offices worldwide. Learn more at www.figma.com.

Services Provided

Figma for design + dev

Figma is where teams come together to design, test, and ship better products. The first design tool built for the web, Figma combines powerful features with multiplayer functionality to make it faster, easier, and more fun for teams to design products together — from start to finish.

FigJam for Whiteboarding

FigJam is an online whiteboard for teams to ideate and brainstorm together. Purpose-built for the earliest stages of design, FigJam makes everything from discovery to design sprints easier and more fun — whether you're working alone or collaborating with your extended team.

The systems in scope for this report are Figma and FigJam (collectively referred as Figma Platform or the System), which are hosted in AWS, and the supporting IT infrastructure and business process.

System Incidents

A system incident is an incident that leads to the loss of, or disruption to, operations, services, or functions and results in Figma's failure to achieve its service commitments or system requirements. Such an occurrence may arise from a security event, security incident, failure to comply with applicable laws and regulations, error, or other means. In determining whether a system incident occurred resulting in Figma's failure to achieve one or more of its service commitments or system requirements, considerations may include, but are not limited to, the following:

- Whether the occurrence resulted from one or more controls that were not suitably designed or operating effectively.
- Whether public disclosure of the occurrence was required (or is likely to be required) by cybersecurity laws or regulations.
- Whether the occurrence had a material effect on the service organization's financial position or results of operations and required disclosure in a financial statement filing.
- Whether the occurrence resulted in sanctions by any legal or regulatory agency.
- Whether the occurrence resulted in the service organization's withdrawal from material markets or cancellation of material contracts.

Incidents and events relevant to Figma's service commitments and system requirements based on the applicable trust services criteria are important in monitoring, identifying, and evaluating if a

system incident has occurred; however, incidents and events relevant to Figma's service commitments and system requirements based on the applicable trust services criteria do not always rise to the level of a system incident. The evaluation of an incident or event relevant to Figma's service commitments and system requirements based on the applicable trust services criteria will make that determination.

Figma did not identify any system incidents that occurred during the period November 1, 2022 to October 31, 2023 resulting in Figma's failure to achieve one or more of its service commitments or system requirements based on these considerations.

Significant Changes to the System During the Period

There were no significant changes to the Figma System that are likely to affect users' understanding of how the Figma System services were provided during the examination period.

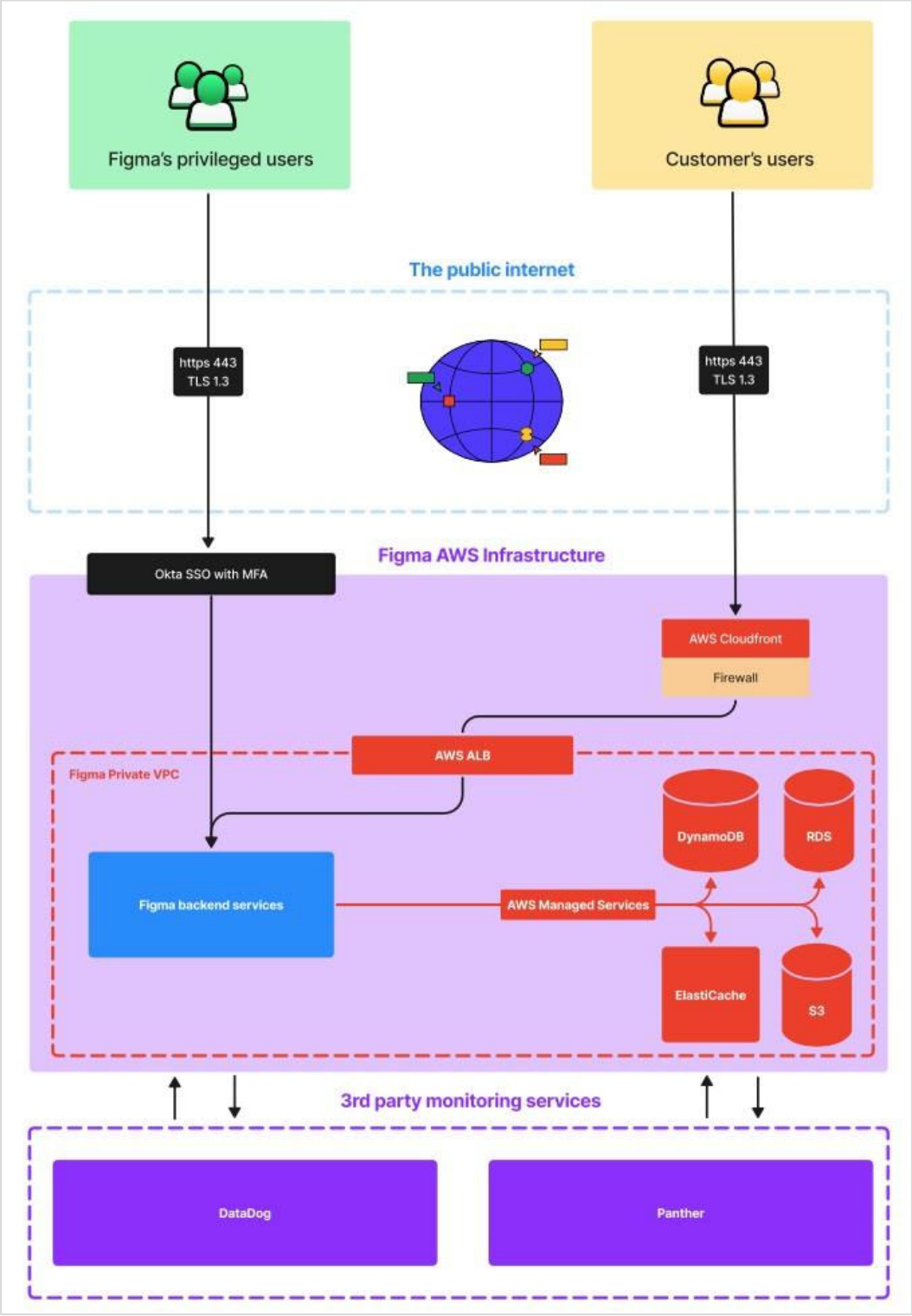
Components of the System Used to Provide the Services

Infrastructure

The System is hosted on AWS in the United States and European Union (EU) across multiple regions and availability zones to support fault tolerance, high availability, and disaster recovery. The infrastructure is managed and configured using configuration management software. AWS operates under a shared responsibility model. Under this model, Figma uses AWS for services related to server hosting, physical and environmental protection, network management, and disk storage supporting the System. Furthermore, Figma is responsible for configuring and maintaining the System architecture in AWS to help ensure availability, security, and resiliency requirements. At Figma, customer data is defined as any application(s) and/or material(s) that are developed by a customer on the Figma Platform or uploaded to the Figma Platform by a Customer, as well as any personal data pertaining to Customers' authorized users of the Figma Platform processed by Figma on behalf of the customer under the SSA agreement. In other words, customer data is any data submitted to the Figma Platform. customer data is subject to technical safeguards, as described in Exhibit C of Figma's SSA (https://www.figma.com/ssa/).

The System is based on a multi-tenant architecture that applies common and consistent management processes and controls to all customers. The System is also designed with logical security controls in place where each customer's data is segregated from other customers' data. The infrastructure has been designed to provide high availability, and all critical infrastructure components are redundant across multiple AWS availability zones. Web servers and databases are deployed in multiple availability zones, each consisting of one or more discrete data centers with fully redundant power, networking, and connectivity housed in separate secured facilities. The System is built on Linux servers and runs on Amazon Relational Database Service (RDS) databases.

The following diagram shows major components of the System:



Production Infrastructure

Data Storage: AWS Simple Storage Service (S3) and RDS are managed services provided by AWS. Figma maintains RDS databases to store customer user data and metadata associated with Figma design and FigJam files. Figma's usage and maintenance of RDS only apply to Figma's U.S. AWS environment. AWS S3 is the primary data store for images, components, and other contents of Figma design and FigJam files. Figma's usage and maintenance of S3 apply to both Figma's U.S. and EU AWS environments. Figma customers who are on the Enterprise plan can choose to localize key parts of their Figma design and FigJam file data in the EU (https://help.figma.com/hc/en-us/articles/15643274574871-Enable-localized-file-hosting-in-the-EU). All customer data in RDS and S3, regardless of where it's stored, is encrypted at rest, backed up, and replicated across availability zones and regions.

Network Connections: Content Delivery Networks (CDNs), Load Balancers, and Envoy proxies are used to connect to the service within AWS. All customer traffic is routed through AWS CloudFront, with features such as AWS Shield and AWS Web Application Firewall (WAF) to protect against distributed denial-of-service (DDoS) attacks and other types of malicious traffic. Figma's production environment is hosted on a virtual private cloud (VPC), which is shared by all customers, and isolates Figma's production environment from other development and administrative environments. Customer traffic into and out of the production environment uses Transport Layer Security (TLS) connections to secure data in transit.

Application Servers: The Figma Platform application servers run on AWS Elastic Cloud Compute (EC2), AWS Lambda, Amazon Elastic Kubernetes Service (EKS), and AWS Fargate, and use encrypted Elastic Block Store (EBS) volumes. AWS Security Groups are used to restrict communication between servers and databases within the VPC.

Corporate Infrastructure

Figma's corporate infrastructure is located in its San Francisco, California headquarters and has satellite offices in New York City, New York; Seattle, Washington; London, England; Umeå, Sweden; Paris, France; Berlin, Germany; Tokyo, Japan; and Singapore, Republic of Singapore. At a minimum, Figma employees connect remotely to the Figma production network through a Figma-managed laptop, unique username and password, multifactor authentication, and via an acceptable geolocation.

Software

Figma utilizes the following third-party tools and services to build, support, secure, maintain, and monitor the Figma Platform and processes:

Tools/Services	Description
Amazon CloudFront	Content Delivery Network
Amazon EC2	Hosting Service
Amazon EKS	Managed Kubernetes Service
Amazon RDS	Database Solution
Amazon S3	File Storage Service

Tools/Services	Description
Asana	Project and Task Management Service
Aviator	Merge Queue Platform
AWS Shield	DDoS Protection Service
AWS WAF	Web Application Firewall
Buildkite	Continuous Integration and Testing
Checkr	U.S. Background Check Service
Datadog	Infrastructure Monitoring Service
Detectify	Application Vulnerability Scanner
FileVault	Laptop Hard-Disk Encryption
Freshservice	Helpdesk Ticketing Tool
GitHub	Source Code Repository
Greenhouse	Recruiting Software
HackerOne	Bug Bounty Program
Ironclad	Contract Management
Jamf Protect	Mobile Device Management Software
Lattice	Feedback and Performance Review Software
Navex	Ethical Reporting Tool
Notion	Internal Documentation Repository
Okta	Identity and Access Management Tool
Opal	Identity and Access Management Tool
Osquery	Endpoint Logging and Host-Based Intrusion Detection
PagerDuty	Incident Response Alerting and Escalation Tool
Panther	Security Monitoring and Alerting
Rootly	Incident Management and Tracking Tool
Santa	Anti-Malware Software
Semgrep	Static Code Analysis Tool
Sterling	International Background Check Service
Workday	Human Resources Information System
Zendesk	Product Support Ticketing Tool
Zip	Vendor Procurement Tool

People

Figma has a well-defined organizational structure in place that defines organizational structures, lines of reporting, and areas of authority. The people listed in the table below consist of the personnel involved in the governance, operation, and use of the Figma Platform:

Team/Department	Responsibility
Engineering and Product	Design, test, deployment, and maintenance of the Figma Platform: • Provide scalability and reliability of the Figma Platform. • Perform research and development activities. • Optimize data capabilities and workflows.
Security and Security Compliance	• Security of the Figma Platform and the corporate/ production infrastructure. • Management of threats, vulnerabilities, and incidents. • Provide anti-abuse against malicious actors. • Perform risk mitigation and risk treatment. • Perform third-party vendor risk management. • Security governance and policy management. • Deliver new-hire and annual security awareness and privacy training.
Legal	• Ensure Figma and the Figma Platform maintain compliance with applicable statutory, regulatory, and contractual obligations. • Negotiate contractual obligations with third parties and partner ecosystem. • Manage relationships with the Board of Directors.
Information Technology (IT)	Provision, maintain, and properly dispose of corporate laptops: • Manage business applications and employee/contingent workers identities. • Manage physical technology in global offices.
People Operations (HR)	• Ensure employees/contingent workers are properly onboarded. • Facilitate the employee/contingent workers termination process. • Assist in the recruiting of employees. • Perform background checks in accordance with local laws. • Manage and oversee global offices.
Product Support	• Directly support customers and their use of the Figma Platform. • Create public and internal documentation related to the use of the Figma Platform.

To drive clarity and transparency in the hiring process, Figma has documented detailed job descriptions highlighting the roles, responsibilities, and skill requirements posted on its website for current open positions. The recruiting process includes formal in-depth candidate assessments (i.e., interviews) to determine if candidates have relevant qualifications to fulfill the required roles and responsibilities.

Upon hire, each candidate must pass a background check in accordance with local laws. Checks may include criminal history, education verification, employment verification, and reference checks. Employees must also sign an Employee Invention Assignment and Confidentiality Agreement, which outlines the confidentiality commitments employees must abide by during and after their employment with Figma. Confidentiality agreements are also in place for all contingent workers with access to sensitive information.

Processes and Procedures

Processes include the automated and manual procedures involved in the operation and maintenance of the Figma Platform. Procedures are developed, documented, and socialized for a variety of processes, including those related to Engineering, Security, IT, People Operations, etc., as detailed later in this System Description. These processes are drafted in alignment with Figma's Information Security Policies and are reviewed and updated as necessary to continue aligning with Figma's structure and business.

Data

Data, as defined for the System, includes all electronic data or information submitted by the customer to Figma. The customer defines and controls the data they load and store in the Figma Platform. This type of data is also referred to as customer data. Access to customer data is restricted to authorized Figma personnel based on role, or access is granted after receiving proper approval from management and/or the System owner.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations, with specific requirements established in customer organization contracts.

Figma has deployed secure methods and protocols for the transmission of confidential or sensitive information over public networks. Databases and data stores housing sensitive customer data are encrypted at rest.

Data Classification and Confidentiality of Information

All Figma employees and contingent workers share the responsibility of safeguarding information with an appropriate level of protection by observing the Data Classification and Handling Policy. Data and information are classified in terms of legal requirements, value, sensitivity, and criticality to Figma, and are labeled to manage appropriate handling based on the guidelines listed below.

The following guidelines are used to classify data at Figma:

Classification Level	Description	Examples
Sensitive	Data is Sensitive when the unauthorized disclosure, alteration, or destruction of that data could have a significant adverse effect on Figma or its personnel, customers, or vendors. This category includes information that Figma has a regulatory and legal obligation to safeguard in the most stringent manner.	• Customer data and meta\data hosted on the Figma Platform (i.e., design file data) • System access credentials (i.e., username, password) • Cryptographic keys • Source code • Trade secrets • Audit logs
Internal	Internal data is information that is created and used in the normal course of business but is not generally publicly available. Internal data should not be disclosed to third parties outside of Figma without a business need and should be protected with reasonable and appropriate controls.	• Financial information and investment plans • Company All-hands Presentation Decks • Internal product road maps • Project plans • Policies and procedures • Design and work specifications • Non-public employee and contingent worker information
Public	Public information, as the name implies, is data that is already publicly available or becomes publicly available without the act or omission of Figma. Public data does not require any additional controls when used.	The following information, once made public by Figma: • Press releases • Marketing materials • Information in the public domain

Complementary Subservice Organization Controls

In some instances, a service organization's controls cannot provide reasonable assurance that its service commitments and system requirements were achieved without the subservice organizations performing certain activities in a defined manner. Such activities are referred to as complementary subservice organization controls (CSOCs). The following CSOCs are those controls that Figma's management assumed, in the design of the System, would be implemented by a subservice organization and are necessary, in combination with controls at Figma, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved.

Number	CSOC	Applicable Criteria
Amazon Web Services, Inc., Okta, Inc., and Perma Security Inc.		
1.	Controls should be in place and operating effectively to ensure that logical access to systems and infrastructure utilized by Figma and data stored within those systems are properly restricted to authorized personnel and monitored.	CC6.1 — CC6.3
2.	Controls should be in place and operating effectively to ensure that physical access to the subservice organizations facilities, which house Figma production systems or data, is restricted to authorized personnel and monitored.	CC6.4
3.	Controls should be in place and operating effectively to ensure that documented procedures exist for the identification, escalation, and resolution of significant security, availability, and operational incidents.	CC7.1 — CC7.5, A1.1 — A1.3
4.	Controls should be in place and operating effectively to ensure that changes to systems utilized by Figma are authorized, tested, approved, and documented.	CC8.1
5.	Controls should be in place and operating effectively to ensure that appropriate system redundancy and environmental controls are maintained.	CC7.5, A1.1 — A1.3

User Entity Responsibilities

User entities must perform specific activities in order to benefit from Figma's services. These activities may affect the user entity's ability to effectively use Figma's services but do not affect the ability of Figma to achieve its service commitments and system requirements. These activities may be specified in agreements between user entities and Figma, user manuals, and/or other communications. These activities are referred to as user entity responsibilities (UERs).

UERs are listed in the following table. They are the responsibility of the user entities of the System and are expected to be in operation at user entities to complement Figma's controls. The list of UERs does not represent a comprehensive set of all the controls that should be employed by user entities. Other controls may be required at user entities.

Number	UER
1.	User entity is responsible for understanding and complying with their contractual obligations to Figma.
2.	User entity is responsible for creating a username and password and ensuring the strength, complexity, and confidentiality of the passwords assigned to their user accounts.
3.	User entity is responsible for setting up, inviting, and managing their individual accounts and team and organization members, as well as authorizing new users and managing any terminations or transfers.

Number	UER
4.	User entity is responsible for requesting, approving, and provisioning Figma's product support access to their account.
5.	User entity is responsible for monitoring and removing Figma support access timely upon provisioning.
6.	User entity is responsible for requesting their account to Figma to be removed or deleted.
7.	User entity is responsible for performing periodic review of access and configurations for appropriateness.
8.	User entity is responsible for monitoring their activity log in their individual accounts.
9.	User entity is responsible for ensuring access to data and sensitive content is appropriately restricted to authorized users only.
10.	User entity that uses SAML or SSO is responsible for deploying appropriate auditing controls for logging their employees when accessing the SAML/SSO Identity Provider.
11.	User entity is responsible for running virus scans on all media attachments and their contents.
12.	User entity is responsible for endpoint protection of systems used to access the System.
13.	User entity is responsible for having data classification policies relating to uploading of information in the System.
14.	User entity is responsible for reporting issues, failures, incidents, etc., to Figma in the event of a security, availability, and/or confidentiality issue.
15.	User entity is responsible for notifying Figma of changes made to its authorized technical or administrative contact information in a timely manner.
16.	User entity is responsible for installing and managing the actions that a plug-in or widget will have on their instance.

Attachment B — Principal Service Commitments and System Requirements

Attachment B — Principal Service Commitments and System Requirements

Figma designs its processes and procedures to meet its objectives related to the System. Those objectives are based on the service commitments that Figma makes to user entities, the laws and regulations that govern the provision of the System, and the financial, operational, and compliance requirements that Figma has established for the System.

Security, availability, and confidentiality commitments to user entities are documented and communicated in the terms and conditions within the sign-up page in Figma and through the Software Services Agreement (SSA) with customers. The description of the service offering relevant components, boundaries, and customer responsibilities are documented on Figma's website https://www.figma.com/security/.

Figma's security, availability, and confidentiality commitments, and related operational requirements, include, but are not limited to, the following:

Service Commitments	Description
Security	The System and customer data is protected against unauthorized access, use, or modification through a range of security processes and controls to identify issues and minimize impact.
Availability	The System is available for operation and use as committed or agreed.
Confidentiality	The Company will not disclose information to any person or entity, except the Company's employees, agents, contingent workers, and service providers bound by non-disclosure obligations and who have a need to know.

Figma establishes operational requirements that support the achievement of security, availability, and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Figma's policies and procedures, system operation and boundaries, and terms and conditions with its customers. Information Security Policies are defined, posted, and available, delineating how systems and data are protected. These include policies around how the System is operated, how employees are hired and trained, the use of encryption technologies to protect customer data at rest and in transit, and a formal process to grant and revoke access to customer data.