Dropbox Service Organization Controls (SOC) 3 Report

Management's Report of its Assertions on the Effectiveness of Its Controls over the Dropbox Standard, Dropbox Advanced, Dropbox Enterprise, and Dropbox Education System Based on the Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

Period: October 1, 2022 to September 30, 2023

Ernst & Young LLP
Suite 1600
560 Mission Street
San Francisco, CA 94105-2907

Tel: +1 415 894 8000
Fax: +1 415 894 8099
ey.com

Report of Independent Accountants

Management of Dropbox, Inc.

Scope:

We have examined management's assertion, contained within the accompanying Management's Report of its Assertions on the Effectiveness of Its Controls over the Dropbox Standard, Dropbox Advanced, Dropbox Enterprise, and Dropbox Education System (Assertion), that Dropbox, Inc.'s controls over the Dropbox Standard, Dropbox Advanced, Dropbox Enterprise and Dropbox Education System (System) were effective throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that Dropbox, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (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)*.

Dropbox, Inc. uses Amazon Web Services (AWS) (Subservice Organization) to provide physical safeguards, environmental safeguards, infrastructure support and management, and storage services. The description of the boundaries of the system presented in the Dropbox Standard, Dropbox Advanced, Dropbox Enterprise, and Dropbox Education System Description Overview indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with related controls at Dropbox, Inc., to provide reasonable assurance that Dropbox, Inc.'s service commitments and system requirements are achieved based on the applicable trust service criteria. The description of the boundaries of the system presents the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS. Our procedures did not extend to the services provided by AWS and we have not evaluated whether the controls management assumes have been implemented at AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period October 1, 2022 to September 30, 2023.

Management's responsibilities

Dropbox, Inc.'s management is responsible for its service commitments and system requirements, and for designing, implementing, operating, and monitoring effective controls within the system to provide reasonable assurance that Dropbox, Inc.'s service commitments and system requirements were achieved. Dropbox, Inc. management is also responsible for providing the accompanying assertion about the effectiveness of controls within the system, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the System and describing the boundaries of the System
- Identifying the service commitments and system requirements and the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of the System.

Building a better working world

Our responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. 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. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Dropbox, Inc.'s relevant security, availability, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we consider necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Dropbox, Inc.'s cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

We are required to be independent of Dropbox, Inc. and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

Inherent limitations:

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Dropbox, Inc.'s service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the System or controls, or the failure to make needed changes to the System or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion:

In our opinion, Dropbox, Inc.'s controls over the System were effective throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst & Young LLP

December 1, 2023

Management's Report of its Assertion on the Effectiveness of Its Controls Over the Dropbox Standard, Dropbox Advanced, Dropbox Enterprise, and Dropbox Education System Based on the Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

We, as management of Dropbox, Inc., are responsible for:

- Identifying the Dropbox Standard, Dropbox Advanced, Dropbox Enterprise, and Dropbox Education System (System) and describing the boundaries of the System, which are presented in the Dropbox Standard, Dropbox Advanced, Dropbox Enterprise, and Dropbox Education System Description Overview
- Identifying our principal service commitments and system requirements which are presented in the Dropbox Standard, Dropbox Advanced, Dropbox Enterprise, and Dropbox Education System Description Overview
- Identifying the risks that would threaten the achievement of our principal service commitments and service requirements that are the objectives of our System
- Identifying, designing, implementing, operating, and monitoring effective controls over the Dropbox Standard, Dropbox Advanced, Dropbox Enterprise, and Dropbox Education System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories and associated criteria that are the basis of our assertion

Dropbox, Inc. uses Amazon Web Services (AWS) to provide physical safeguards, environmental safeguards, infrastructure support and management, and storage services. The description of the boundaries of the system presented in the Dropbox Standard, Dropbox Advanced, Dropbox Enterprise, and Dropbox Education System Description Overview indicates that complementary controls at AWS that are suitably designed and operating effectively are necessary, along with controls at Dropbox, Inc. to achieve the service commitments and system requirements. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Dropbox, Inc.'s controls. It does not disclose the actual controls at AWS.

We confirm to the best of our knowledge and belief that the controls over the System were effective throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus – 2022*).

Dropbox Standard, Dropbox Advanced, Dropbox Enterprise, and Dropbox Education System Description Overview

Company Background

Since 2008, Dropbox, Inc. ("Dropbox" or "the Company") has helped users store their files (such as documents, photos, and videos), access them from anywhere, and share them easily. Since 2011, the Company has continued to launch products serving additional customer markets, such as Dropbox Business and Dropbox Education. In 2023, the Company reorganized these products into four service plans: Dropbox Standard, Advanced, Enterprise, and Education (collectively, "the Dropbox Service Plans").

Description of Services

The in-scope products are included within the Standard, Advanced, Enterprise, and Education plans, which offer specific feature packages tailored to different organizational needs. Dropbox Education is designed specifically for the needs of higher education institutions.

Dropbox FSS provides cloud storage, file synchronization, and collaboration capabilities to organizations around the world. Users can collaborate in, store, and share files seamlessly, as well as access important information from any supported operating system or device. The service is designed to keep users' data safe, confidential, and available. In addition, administrators for in-scope products have a central console that provides visibility and control over user activity.

Dropbox Paper provides a collaborative and flexible document-editing workspace which adds collaborative functionality, administrator control, and enterprise visibility. A common set of control processes applies across all Dropbox products. However, Dropbox Paper uses a mostly distinct set of systems within the Dropbox infrastructure environment.

Dropbox Backup is a secure cloud backup and recovery solution for files and folders. Dropbox Backup automatically backs up computers and connected external drives directly to the cloud and quickly recovers users' content. A common set of control processes applies across this product similar to the Dropbox product.

Dropbox Transfer provides a way to send large files-up to 100 GB-that do not require collaboration with another party even if the recipient is not a Dropbox customer. A common set of control processes applies across this product similar to the Dropbox product.

Dropbox Capture provides a way to record your screen, camera, and microphone. Allowing you to create video messages, audio recordings, screenshots, and GIFs to share with others. A common set of control processes applies across all Dropbox products, however Dropbox Capture uses some distinct control processes.

Dropbox Managed Encryption Keys Service is a key management system used by Dropbox customers that encrypts data, using unique team keys and a multi-layered key encryption approach as extra security measures. This product is offered under the Dropbox Enterprise plan only.

Dropbox Replay is a media review and approval tool that allows collaborators to mark up, comment, and finalize video, image, and audio projects. A common set of control processes applies across this product similar to the Dropbox product.

System and Network Summary

All in-scope products are designed with multiple layers of protection, including secure data transfer, encryption, network architecture, and application-level controls that are distributed across a scalable, secure infrastructure

User Interfaces

For in-scope products, the services can be utilized and accessed through a number of interfaces. Each has security settings and features that process and protect user data while ensuring ease of access.

Web*:* This interface can be accessed through any modern web browser. In-scope products with a web interface include: Dropbox FSS, Paper, Backup, Transfer, Capture, Dropbox Managed Encryption Keys Service, and Replay.

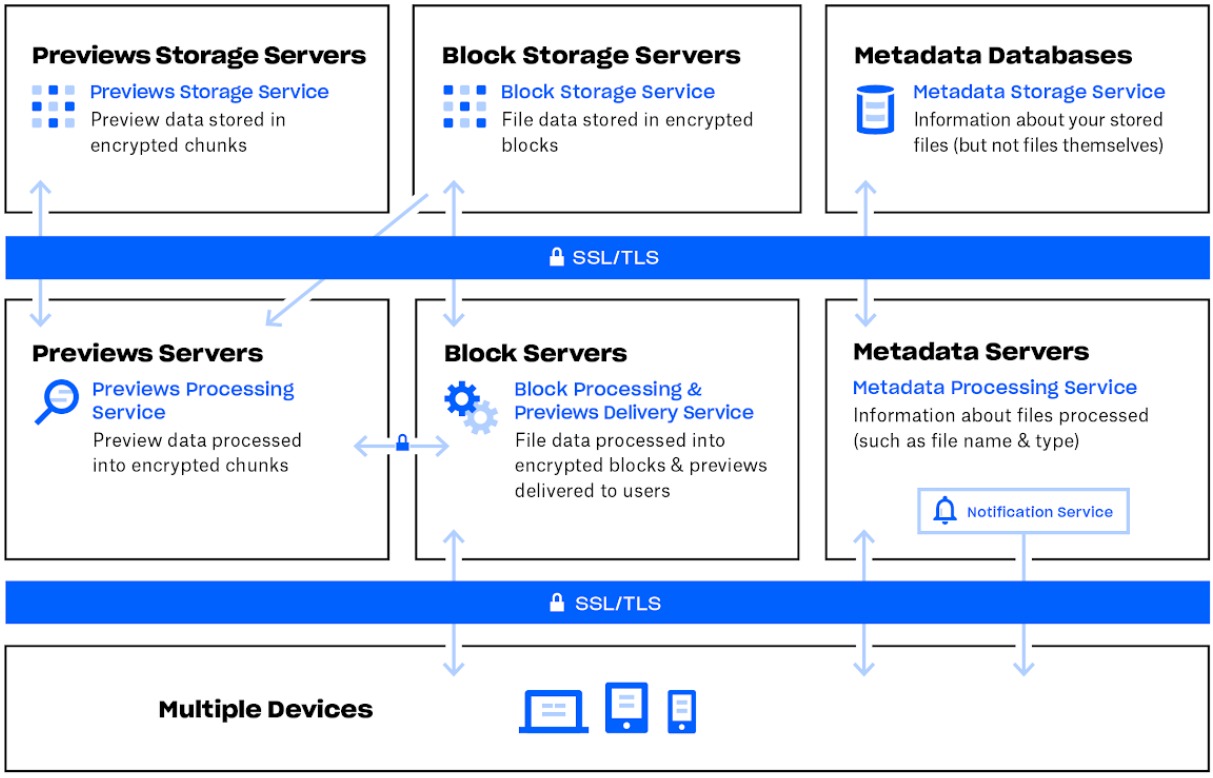
Desktop: The Dropbox FSS desktop application is a synchronization client that stores files locally for offline access. It gives users full access to their Dropbox accounts. The Dropbox Capture desktop application creates video messages, audio recordings, screenshots, and GIFs. Both desktop applications run on Windows and Mac operating systems. Files are viewed and can be shared directly within the operating systems' respective file browsers.

Mobile: The Dropbox FSS mobile and paper mobile applications are available for iOS and Android mobile devices and tablets, allowing users to access all their documents on the go.

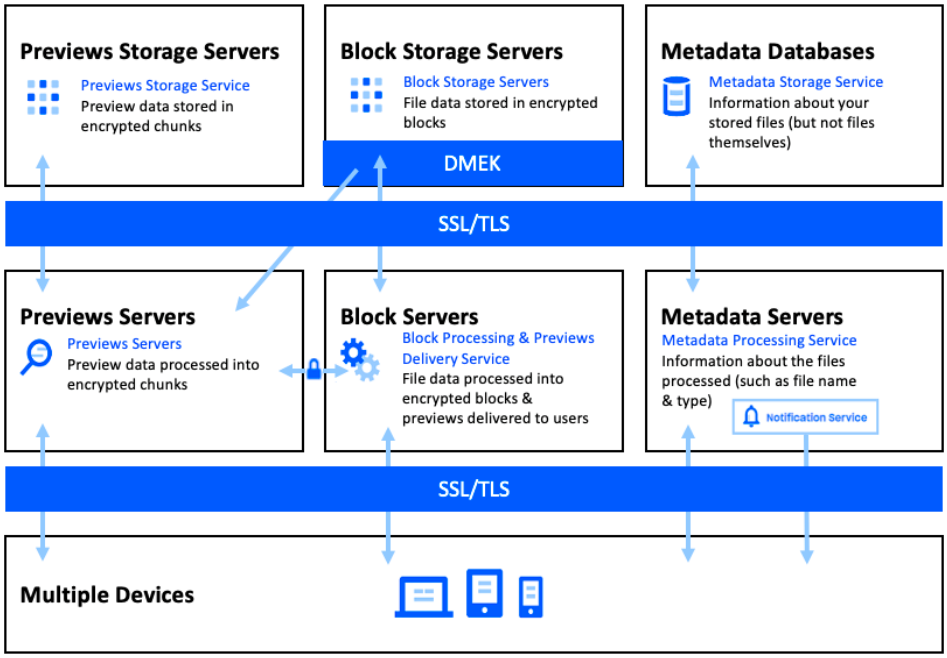
Application Programming Interface (API): The Dropbox FSS API is available for administrators and their developers to create applications that can read and write to Dropbox. It contains endpoints and data types for managing documents and folders in Dropbox Paper, in addition to offering support for advanced functionality like managing team members, search, revisions, and file restoration. Users grant applications that implement the APIs different levels of account access. Additional information about the Dropbox FSS API, including guidance on data portability and security authentication protocols that may be invoked while using the API, is published on the company website at https://www.dropbox.com/developers.

Infrastructure

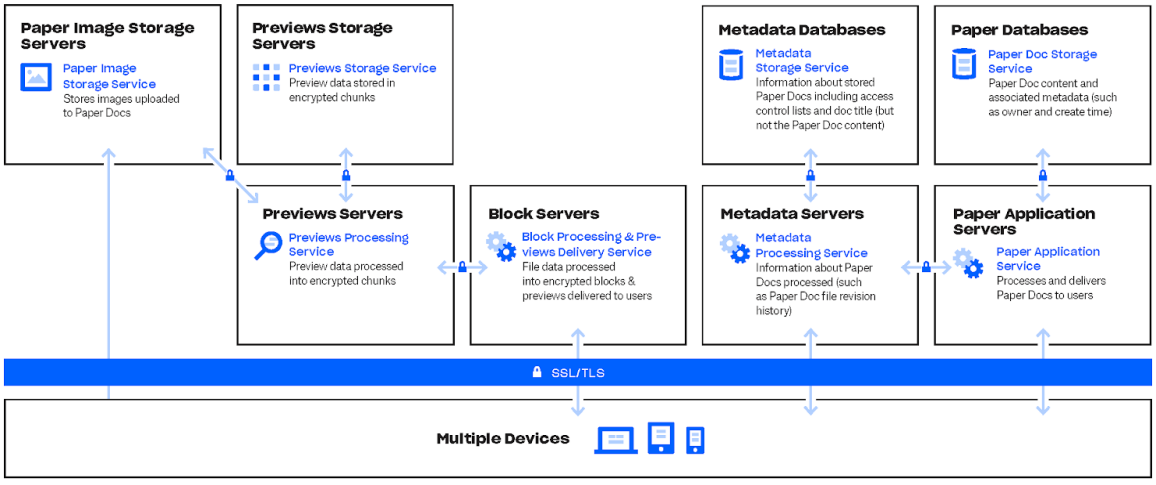
Dropbox's FSS, Backup, Transfer, Capture and Replay infrastructure consists of the components depicted in Diagram 1 below:



The Dropbox Managed Encryption Keys infrastructure consists of the components depicted in Diagram 2 below:



The Paper infrastructure consists of the components depicted in Diagram 3 below:



Metadata Servers

The Metadata Servers are responsible for processing information about files and Paper docs stored in Dropbox, including location of files and docs within each user's account, file and doc revision history, and shared folder membership. Dropbox directly manages the Metadata Servers, which are located in third party co-located data centers.

The Notification Service establishes a long poll connection and heartbeat between the Dropbox application(s) on each user device. When a change to any file occurs, the Notification Service signals a change to the relevant application(s) by closing the long poll connection. Dropbox directly manages servers that run the Notification Service. These servers are located in third party co-located data centers.

Closing the connection signals that the application(s) must communicate with the Metadata Service to synchronize any changes. Communications between the Dropbox application(s) and the Notification service are encrypted; no file data or file metadata is transferred.

Metadata Databases

File metadata is stored in a MySQL database service on the Metadata Servers. File metadata is replicated to at least two (2) additional instances for performance and availability. Dropbox directly manages the Metadata Databases, which are located in third party co-located data centers.

Block Servers

For all in-scope products, Block Servers process data from the Dropbox clients by splitting each file into blocks, anonymizing each block with a hash value, encrypting each file block using a 256-bit key, and only synchronizing blocks that have been modified between revisions. When a Dropbox client detects a new file or changes to existing files, the application notifies the Block Servers of the change and new or modified file blocks are processed and transferred to the Block Storage Servers. Additionally, Block Servers are used to deliver files and previews to users. Block Servers are either in Dropbox-managed third-party co-located data centers or are virtualized on AWS EC2 and are managed by Amazon. Regardless of whether the servers are virtual or physical, their configurations and the processes which are run on them to facilitate the services are not differentiated. Additional controls may be applied to the AWS environment in order to manage administrator access.

Block Storage Servers

The Block Storage Servers are responsible for storing and serving individual file blocks. The servers act as a Content Addressable Storage (CAS) system: individual file blocks are retrieved based on their hash value and each file block is encrypted at rest using a 256-bit cipher. Block Storage Servers are either in Dropbox-managed third-party co-located data centers or are on AWS S3 and are managed by Amazon.

Dropbox Managed Encryption Keys service (DMEK)

DMEK is a tool that allows for encryption for individual teams' files and folders. The files and folders of a team using DMEK will be encrypted at the block level, folder level, and team level. The team level encryption key (or keys) are stored in an AWS Hardware Security Module (HSM). DMEK also allows for revocation and rotation of the team level encryption key.

Previews Servers

The Previews Servers produce previews for images uploaded to Paper docs, as well as hyperlinks embedded within Paper docs. Paper uses the same Previews Servers described in the Dropbox infrastructure diagram above.

For images uploaded to Paper docs, the Previews Servers fetch image data stored in the Paper Image Storage Servers from the AWS Cloudfront Portal. Communication sessions between the Previews Servers and AWS Cloudfront are secured with TLS 1.2. For hyperlinks embedded within Paper docs, the Previews Servers fetch image data from the source link and render a preview of the image using either HTTP or HTTPS as specified by the source link. As described above, previews are ultimately served to users by Block Servers. Dropbox uses a combination of AWS EC2 and directly-managed third party co-located data centers to host Previews Servers.

Previews Storage Servers

The Previews Storage Servers are responsible for storing cached preview chunks. Each preview chunk is encrypted at rest using a 256-bit cipher. Previews Storage Servers are deployed on AWS S3 within multiple AWS availability zones to provide for fail-over redundancy.

Paper Application Servers

The Paper Application Servers serve the application to the users, including processing user requests, performing notification services, executing integrity scanning on Paper docs, and logging performance of the application. Paper Application Servers write inbound user edits to the Paper Databases, and render the output of edited Paper docs back to the user. Communication sessions for the transmission of data from the Paper Application to the Paper Databases are secured with TLS 1.2. Dropbox deploys Paper Application Service servers on AWS EC2 infrastructure in multiple availability zones to provide for failover redundancy.

Paper Databases

The Paper Databases are responsible for storing all Paper doc data. This includes information about a Paper doc (such as the title, owner, create time, and other information), as well as content within the Paper doc itself, including comments and tasks. Paper doc data is stored in AWS RDS MySQL databases, and is replicated to at least one (1) additional instance for performance and availability. Dropbox configures Paper doc data to be encrypted at rest using a 256-bit key on AWS RDS.

Paper Image Storage Servers

The Paper Image Storage Servers are responsible for storing images uploaded to Paper documents . Communication sessions for the transmission of image data from the Paper Application to the Paper Image Storage Servers are secured with TLS 1.2. Paper Image Storage Servers are deployed on AWS S3 within multiple AWS availability zones to provide for fail-over redundancy.

Previews Servers

The Previews Servers produce previews for images uploaded to Paper docs, as well as hyperlinks embedded within Paper docs. Paper uses the same Previews Servers described in the Dropbox infrastructure diagram above.

For images uploaded to Paper docs, the Previews Servers fetch image data stored in the Paper Image Storage Servers from the AWS Cloudfront Portal. Communication sessions between the Previews Servers and AWS Cloudfront are secured with TLS 1.2. For hyperlinks embedded within Paper docs, the Previews Servers fetch image data from the source link and render a preview of the image using either HTTP or HTTPS as specified by the source link. As described above, previews are ultimately served to users by Block Servers. Dropbox uses a combination of AWS EC2 and directly-managed third party co-located data centers to host Previews Servers.

Previews Storage Servers

Paper uses the same Previews Storage Servers described in the Dropbox infrastructure diagram to store cached image previews. As described above, Previews Storage Servers are deployed on AWS S3 within multiple AWS availability zones to provide for fail-over redundancy.

Networks

The Dropbox internal private network is segmented according to use and risk level. The primary segments are the Production network and the Corporate network. The Production network is where the systems that compose the in-scope products reside. The Corporate network is where supporting IT systems and the corporate intranet reside.

The Dropbox service allows only authorized users to access files and Paper docs through authorized interfaces to the production network from the internet-facing production edge network. An encrypted connection is negotiated before the transfer of information to ensure secure delivery of data between the Dropbox application and back-end infrastructure (Metadata Servers, Metadata Databases, Block Servers, Block Storage Servers, Previews Servers, and Previews Storage Servers). An encrypted connection is also utilized to ensure secure delivery of data between the Paper application and back-end infrastructure (Paper Application Servers, Paper Databases, Paper Image Storage Servers, Previews Servers, and Previews Storage Servers). Access to the Dropbox corporate network, where supporting IT systems reside, is limited to appropriate individuals and authorized devices through a variety of mechanisms. Remote access to the corporate network must route through the secure VPN system.

Containers

Dropbox services utilize container technologies to allow for application/service isolation, runtime consistency, and rapid deployment, providing an immutable infrastructure and multi-tenancy. Containerization technologies in use leverage standard Dropbox controls related to change management, access control, vulnerability management, and monitoring. Additionally, containers are required to leverage the kernel and OS image of the related operating system. Configuration settings for containers are managed using dedicated images, which are developed, tested, and validated through annual scans performed against CIS benchmarks prior to deployment. Monitoring of container infrastructure is in place to detect and respond to anomalous activity as well as key availability metrics.

Containers rely on the production OS host-layer security monitoring. Metrics are available to facilitate tracking and remediation of identified issues. Containers utilize standard Dropbox authentication tools and pathways for authentication of authorized standard and administrative users. These tools and pathways are the same as the related hosts. Controls related to user lifecycle management, inclusive of provisioning, modification, deprovisioning and review of access and in place to ensure access is restricted to authorized Dropbox users and services. Controls related to encryption of data in transit/ at rest rely on application-level encryption configurations. Dropbox-approved security tools are in place to facilitate remote access connections to containers by authorized Dropbox users. While permissions mirror OS-level access, discrete tools are utilized to remotely access containers.

Data Center Co-location (Third Party) Organizations

Dropbox outsources data center co-location services to third party organizations. Dropbox performs specific control activities to monitor and validate the physical, environmental, and operational security of its third party data center co-location facilities. Dropbox is responsible for the logical, network, and application security of Dropbox's infrastructure housed at the third party organizations.

The data center co-location services are utilized for Metadata Servers, Block Servers, Block Storage Servers, and Previews Servers, and are provided by Digital Realty, Vantage Data Centers, CoreSite Realty Corporation, and Flexential. All co-location facilities are located in the United States, and are dispersed between Northern California, Northern Texas, Northern Virginia, and Oregon.

Managed Services (Third Party) Organizations

Amazon Web Services (AWS)

Amazon Web Services (AWS) is a component of the production environment and is utilized for processing (AWS EC2) and storing (AWS S3) Dropbox files. AWS is also utilized for serving the Paper application (AWS EC2), storing Paper docs (AWS RDS), and storing Paper image data (AWS S3). Lastly, AWS is utilized for processing (AWS EC2) and storing (AWS S3) cached previews.

AWS EC2, S3, and RDS provide multiple location fail-over redundancy to support service availability. AWS, as a third party service organization, also provides IT infrastructure managed services and is responsible for the logical and network security of Dropbox services provided through the AWS infrastructure (EC2, S3, and RDS).

Connections to AWS EC2 and AWS RDS instances are protected through the AWS EC2 Firewall, which is configured in a default "deny-all" mode. Dropbox has listed authorized IP addresses which may connect to the AWS environment. The authorized IP addresses are managed via the AWS API by a service maintained by Dropbox Security, and Dropbox relies on AWS services to enforce the defined configurations.

Access to AWS S3 buckets is restricted to AWS IAM users and roles with appropriate AWS IAM permissions. AWS IAM permissions for AWS S3 buckets are granted by AWS IAM policies and are not given by default. AWS IAM Users, Roles, and policies are managed via the AWS API and AWS Management Console by Dropbox Security, and Dropbox relies on AWS services to enforce the defined configurations.

Dropbox encrypts Dropbox file data, Paper image data, Paper doc data, and previews at rest on AWS infrastructure. However, AWS is responsible for the physical, environmental, and operational security controls at its facilities. Dropbox personnel do not have physical access to AWS facilities.

The Dropbox Governance, Risk, and Compliance Team reviews AWS's independent third party assurance assessments (e.g., SOC 1, SOC 2, ISO 27001) to verify applicable physical, environmental, and operational security controls operate effectively and satisfy Dropbox's internal requirements and contractual agreements.

Dropbox uses systems provided by Amazon Web Services (AWS) that are located in Amazon's data centers specifically the US West, US East, EU Frankfurt, EU London, Asia Pacific (Tokyo), and Asia Pacific (Sydney) regions).

Control Environment

The Dropbox control environment and the security, availability, processing integrity, confidentiality, and privacy controls implemented within the applications provide for a secure and reliable cloud-based storage and collaboration environment. Dropbox's executive leadership has established the Dropbox Trust Program, an internal control structure and standardized model that consists of key processes such as change management, access control, security management, and human resource management. Executive leadership supports the program by reviewing and approving its objectives and performance annually. The Dropbox Trust Program serves as an Information Security Management System (ISMS), as prescribed by the ISO/IEC 27001:2022 international information security standard, the ISO/IEC 27017:2015 international information security standard for cloud services, the ISO/IEC 27018:2019 international privacy and data protection standard for cloud service providers which act as data processors, and a Privacy Information Management System (PIMS), as prescribed by ISO/IEC 27701: 2019. The Dropbox Trust Program also functions as a Business Continuity Management System (BCMS), as prescribed by the ISO 22301:2019 international business continuity standard. The Dropbox Trust Program provides the framework for addressing the security principles outlined in the Cloud Security Alliance Cloud Controls Matrix (CSA CCM). The Dropbox Trust Program provides the framework for addressing the security controls outlined in the NIST Special Publication (SP) 800-171 Revision 2 and the Health Insurance Portability and Accountability Act (HIPAA) Security, Breach Notification, and Privacy Rules.

The Dropbox Trust Program Policy defines the organizational structures, roles, and responsibilities critical to the success of the Program. The policy provides the overall framework for planning, directing, controlling, and implementing the control environment. This structure assigns roles and responsibilities for efficient operations, appropriate staffing, and segregation of duties where applicable. Reporting lines and organizational structures are available to Dropbox personnel on the corporate intranet.

The Board of Directors maintains the necessary experience, stature, independence, and financial expertise to provide oversight of the company. The Dropbox Trust Management Team presents the Trust Program's top risks and roadmap on an annual basis to members of the Board of Directors. These members approve the Dropbox Trust Program and provide feedback on the results of the Trust Program's top risks.

The Dropbox Trust Management Team plays a key role in the Dropbox Trust Program and regularly reviews and updates security policies, provides security training, performs application and network security testing, monitors compliance with security policies, and conducts internal and external assessments of the control environment. Such reviews occur at least annually and on an as-needed basis.

The Trust Management Team also performs an annual review of the overall effectiveness of the Dropbox Trust Program to ensure continual improvement of the security, availability, processing integrity, confidentiality, and privacy controls.

Furthermore, Dropbox employees undergo a formal performance review at least annually. The performance review evaluates employee qualifications to support the achievement of the company's objectives, including, but not limited to, compliance with the Worldwide Code of Conduct and company policies, level of competence and compensation changes, and internal control responsibilities. The employee's manager or delegate delivers actionable feedback to foster development and growth.

Policies

Dropbox develops and maintains formal policies and procedures concerning various security, availability, processing integrity, confidentiality, and privacy matters. The policies and procedures allow employees to perform their job responsibilities in accordance with established goals and objectives and to sustain an effective control environment

The information security policies are developed in relation to the organization's security, availability, processing integrity, confidentiality, and privacy commitments. The policies are reviewed at least annually, or as needed, by the Dropbox Trust Management Team, which consists of representative individuals from Teams within the organization, including the Security, Engineering, Operations, and Legal Teams.

Dropbox has established the following policies intended for employees and contractors:

- Dropbox Trust Program
- Information Security
- Physical Security
- User Data Privacy
- Data Classification
- Incident Response
- Mobile Device Security
- Unauthorized Copyright Materials
- Vulnerability Management
- Baseline Security Configuration
- Travel Security
- Privacy Program
- Payments Environment Security

Dropbox has established the following policies intended for employees and contractors with responsibilities for organizational resilience and safety:

- Business Continuity

Dropbox has established the following policies intended for employees and contractors with access to Dropbox systems:

- Logical Access Control
- Change Management
- Production Physical Access
- Sales and Customer Experience Security

Dropbox Engineering Teams maintain a series of operating procedures which provide guidance to its members on the day-to-day performance of their roles. The operating procedures are updated on an annual basis (e.g. for significant changes related to engineering operations).

The policies and supporting operating procedures are made available within the corporate network and provide employees with direction for corporate and production environment security, physical and environmental safety, logical access management, change management, incident management, compliance, monitoring, and risk management. New employees must acknowledge the Information Security Policy as a component of the onboarding process. The Trust Management Team reviews and updates the policies based on technological, regulatory, contractual, and environmental changes to the Dropbox systems, and communicates significant changes to Dropbox personnel via email and the corporate intranet. As deemed necessary by the Trust Management Team, communications are sent to internal users via email to notify them of changes to their security obligations or to provide recommendations on how to best protect themselves from current security threats.

Additionally, the Dropbox Legal Team maintains a Worldwide Code of Conduct which is reviewed at least annually. The Code of Conduct is designed to deter wrongdoing and promote employee integrity, honesty and ethics, compliance with local laws and regulations, and fiscal responsibility. Dropbox requires employees and contractors with access to systems to read and acknowledge the Code of Conduct as part of the onboarding process and at least annually thereafter.

Internal Communications

Effective communication and exchange of information is an integral component of Dropbox's internal control system. Dropbox ensures that information is identified, processed, and reported by various systems in a form and time frame necessary to manage operations.

Dropbox has developed various methods of internal communication to ensure employees understand their individual roles and responsibilities. These methods include:

- Employee onboarding orientation and required ongoing security awareness and role based training programs.

- Technical learning events hosted by members of engineering, product, and design.
- Meetings with respective Teams and management.
- Periodic communication regarding changes to information security policies and current security threats.
- The existence and communication of a security intranet page available to all Dropbox personnel, and includes information security policies, the design and operation of the system, how to report suspected security, availability, processing integrity, confidentiality, or privacy incidents or breaches, best practices, industry news updates, etc.

The Dropbox Security Team is responsible for maintaining knowledge of current security news, issues, and threat intelligence. The Team is also responsible for communicating security practices to employees and communicating specialized information on threat intelligence to teams on a need-to-know basis.

External Communications

Dropbox communicates with its customers to provide information and support by maintaining blogs, a help center, and forums, and through the Dropbox website and applications.

A description of the Dropbox in-scope systems and its boundaries is available to users via the Dropbox Help Center and the Dropbox Security Whitepaper on the Dropbox website. Details made available through the Dropbox website include features, usage guidelines, and additional information.

The security and confidentiality obligations of customers are communicated via the Shared Responsibility Guide on the Dropbox website and through a combination of online documents which include installation, setup, and configuration guidelines. In addition, Dropbox communicates its security, availability, processing integrity, confidentiality, and privacy commitments to customers through the Dropbox Terms of Service, Privacy Policy, and Business Agreements for Dropbox in-scope products , and/or custom service agreements. The standard or custom version of the Business Agreements provide notice of the following terms for in-scope products: the obligations of Dropbox customers and Dropbox commitments to those customers, any dispute brought by the customer related to the terms may be reported through an established dispute resolution process, the notice and use of Subcontractors and Sub-processors in the offer and provision of the services, the countries to where customer data can be transferred, the effect of termination on customer data accessibility and/or transportability, and a general description of the security measures used to transfer, store, and process customer data.

Any material changes to the standard Business Agreements are communicated to customers of the Dropbox Services Plans. Customers have up to 30 days to terminate their contract if they object to terms in the updated Business Agreement.

Additionally, the Dropbox Privacy Policy and Business Agreements contain terms that address third party (including governmental or law enforcement) requests for user data. These documents describe the process and procedures that Dropbox and the customer will follow in the event such a request is received. The documents include Dropbox's commitment to providing the customer with prompt notification upon receipt of a request, unless such a notification is prohibited by law.

Dropbox will sign business associate agreements (BAAs) with Dropbox Standard, Advanced, Enterprise, and Education customers who require them in order to comply with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH).

Dropbox services are only provisioned after a standard or custom Business Agreement has been signed by an authorized user who has the authority to bind the company to one of the Business Agreements.

As necessary, Dropbox may contact customers via email or in-product notifications to inform them of specific security, availability, processing integrity, confidentiality, and privacy issues, material changes to the Terms of Service and Privacy Policy, or changes to their obligations. Users are able to opt-out of specific types of marketing email communications at any time using their account settings.

Dropbox provides forums and contact information on its website and customer support channels where customers can report potential security, availability, processing integrity, confidentiality, or privacy incidents, concerns, or other complaints.

Dropbox users have the ability to request access to or request the deletion of personal information Dropbox has collected about them that is not part of their file data or user account profile information by sending such requests to privacy@dropbox.com. Dropbox reviews the requests and, if the request is determined to be legitimate and authentic, makes reasonable efforts to honor the request within 30 days. The Dropbox Customer Experience Team denies requests deemed not to be legitimate and authentic and informs the requestor in writing as to the reason their request was denied.

Risk Management

Dropbox maintains a risk management framework to regularly analyze and manage risks to an acceptable level for the system environment and effectiveness of controls. The risk management framework is part of the Dropbox Trust Program and is in conformity with the ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 27701:2019 international information security, privacy, and data protection standards and the ISO 22301:2019 international business continuity standard.

The Dropbox Governance, Risk, and Compliance Team assesses risks that may affect the control environment or the systems at least annually. This includes evaluating dynamic technical and environmental risks, threats from users and third parties, potential impacts to business continuity, and assessing relevant laws, regulations, and contractual requirements. The Governance, Risk and Compliance Team then analyzes those risks in consideration of their associated existing controls, likelihood of occurrence, and impact to the security, availability, processing integrity, confidentiality, and privacy of the system.

The Dropbox Insurance Team transfers risk by obtaining and maintaining cybersecurity insurance as a way to mitigate financial impact risk and renews the insurance on an annual basis. If the risks are still at an unacceptable level, the Team documents additional mitigation tasks, and then predicts the likelihood and impact of the risks after the implementation of the mitigation plan.

The risk and business impact analyses and resulting conclusions are documented and retained for future reference. Dropbox has developed a risk and business impact analysis process to ensure all applicable risks are identified, addressed, and monitored to ensure protection of information assets.

The Dropbox Security Team identifies individuals who are accountable and responsible for monitoring the effectiveness of controls during the risk and business impact analysis procedures.

Monitoring and System Operations

An Intrusion Detection System (IDS) and a Security Incident Event Management (SIEM) system have been configured to notify the Dropbox Security Team of any potential security events. The Security Team reviews alerts prioritized by the system as high and responds to those alerts in a timely manner, within five (5) business days. The response time is commensurate with the severity of the identified issue.

The Dropbox IT Team uses malware protection software to protect Dropbox laptops and desktops with Mac and Windows operating systems from malware. The team configures the malware protection software to automatically receive updates to identify and stop malicious software. The malware protection software is installed on machines assigned to Dropbox personnel during the initial machine configuration process. Those machines are configured with a baseline image, which includes malware protection software. As defined in Dropbox's documented information security policies, the removal or bypass of system security features (which applies to malware) is not allowed. All machines are configured to either block uninstallation of the malware protection software (PC) or automatically reinstall the malware protection software if an uninstallation is detected (Mac).

The Dropbox Security Team uses signature-based and heuristics-based malware detection software on the edge fleet within the production environment to detect and analyze malicious activities on a weekly basis. The team configures the software to automatically run malware database updates on a daily basis. The software runs in real time to detect threats, report malicious activities to system administrators, and quarantine malware for analysis.

Dropbox logs internal infrastructure user and administrator activities, such as successful and failed log-ons and privilege escalations, within the Production environment. The set of logged events are reviewed annually. Logs are stored in a logically separate system and write-access to the logs is restricted to appropriate personnel. Alerts are sent to the Security Team when specific criteria are found by the system within the logs or when there is an audit logging process failure. The Security Team responds to alerts in a timely manner, within five (5) business days. The response time is commensurate with the severity of the identified issue.

Incident Management

Dropbox provides a mechanism for reporting suspected or observed security, availability, processing integrity, confidentiality, or privacy incidents or weaknesses for its employees and contractors. Employees and contractors are required to report security and confidentiality incidents per their acceptance of the Information Security Policy. Dropbox has established incident response procedures. These procedures are followed when a security, availability, processing integrity, confidentiality, or privacy incident is reported and determined to be valid. The Dropbox Engineering Team receives alerts about large scale events, such as service outages or data integrity issues, from its managed services provider. The team acknowledges these alerts in a timely manner and responds to them as necessary. The Dropbox Engineering Team or Security Team (depending on the type of incident) assigns a severity level to the incident based on pre- defined criteria and initiates the procedures with an email announcement and ticket assigned to the impacted Team. An on-call Incident Manager and Technical Lead coordinate the response procedures. Escalation procedures are in-place in the event such an escalation is required.

Dropbox Security Team performs an exercise to test the effectiveness of the incident response process on an annual basis. A ticket is filed to the Offensive Security Team to conduct a penetration exercise without the knowledge of the Detection and Response Team. The Detection and Response Team responds to the intrusion accordingly and documents and tracks relevant findings identified until resolution.

A post-mortem review of each significant severity incident is completed to review the root cause and other contributing factors, and to determine steps (including system changes, as necessary) to prevent, detect, and minimize the risk of future incidents.

The Dropbox Legal Team maintains appropriate contacts with relevant authorities (e.g., regulators, law enforcement, government officials) and evaluates that list on a regular basis. Dropbox may contact the relevant authorities in the event of certain types of incidents, as deemed necessary by the Legal Team and the Trust Management Team.

Additionally, Dropbox maintains a whistleblower hotline for employees and contractors with access to systems to communicate concerns and violations of the Dropbox Worldwide Code of Conduct or any other ethical concerns. Any violations to the Dropbox Worldwide Code of Conduct are appropriately handled, which may include disciplinary action, up to and including termination of employment or any other working relationship with Dropbox.

Confidentiality and Privacy

All in-scope products are designed to maintain confidentiality of the files and Paper docs stored and shared using the services. Files or folders are only accessible to individuals to whom the owner (end-user) designates and the team's administrator. Access to Paper docs can be restricted by limiting access to members of the team the user belongs to or by limiting access to users who have been explicitly invited to the Paper doc or Paper folder containing the doc, as well as their administrators.

Dropbox has established a User Data Privacy Policy specifically addressing the limited conditions and access procedures internal personnel must follow prior to accessing end- user files and Paper docs.

Dropbox requires employees and contractors with access to systems to sign a confidentiality agreement and acknowledge Dropbox security policies as part of the onboarding process. Security policies (and changes therein) are available within the corporate network.

Dropbox security, confidentiality, and privacy requirements and commitments are communicated to third parties through the initial contractual agreement, amendments, and renewals, when appropriate. Dropbox also requires a confidentiality agreement be put in-place before it shares confidential information with third parties which receive customer data.

Processing Integrity

Processing integrity is at the core of the Dropbox services. Dropbox has implemented several processes and controls to validate that each file and Paper doc maintains its integrity and is not corrupted during each step of the process: creation, upload, processing, storage, download, and deletion.

Procedures are in place ensuring that Dropbox deletes files from the Storage Servers within 90 days when a user or the administrator marks the files for permanent deletion. The 90 day periods apply only during the normal course of operations.

Similarly, Dropbox has implemented several processes and controls for Paper docs, including the application of pre-defined integrity checks on user edits, automated processing checks, and database restorations. These processes ensure that data is not corrupted during each of the following processes: edits, processing, storage, and deletion.

Procedures are in place ensuring that Dropbox deletes Paper docs and Paper image data from the Paper Databases, and Paper Image Servers within 60 days of a user marking the Paper docs for permanent deletion. The 60 day periods apply only during the normal course of operations.

Additionally, procedures are in place ensuring that Dropbox deletes previews from the Previews Storage Servers within 90 days after the user or the administrator marks the files or Paper docs for permanent deletion. The 90 day periods apply only during the normal course of operations.

Capture desktop client continually attempts to complete an upload in order to maintain sync. If the upload continues to fail after the final attempt, a failed sync notification will be displayed to the user. Failed files will remain in a temporary local folder until an upload completes successfully.

Availability

As enterprise services, the in-scope products employ many different mechanisms to maintain and preserve the availability of its systems.

An external website maintained by Dropbox communicates the current status of the in-scope services to users and provides a record of past service disruptions and maintenance at https://status.dropbox.com/.

Dropbox Files

Dropbox in-scope products process and store two types of data: metadata and file block data.

File block data is stored using a combination of AWS S3 and Dropbox-managed servers. Both AWS S3 and Dropbox-managed environments provide for multiple-location fail-over redundancy.

Metadata is replicated in near-real time to at least two (2) additional instances of the metadata database to provide for fail-over redundancy. The replication uses replication techniques that come with the database's standard software. A primary database has at least two replicas which continuously receive updates as part of this process.

Full backups of metadata are taken every three (3) days on Dropbox infrastructure. Code is configured to perform backups in cycles, with the maximum cycle length being set to three (3) days. Full backups are also stored on AWS S3 for additional redundancy. A process is configured to periodically send a copy of the most recent full backup on the Dropbox infrastructure to AWS S3 every five (5) days.

Paper Docs

Dropbox configures full backups of Paper doc data every day and stores them on AWS infrastructure. Dropbox also replicates Paper doc data in near-real time to at least one (1) additional instance to provide for fail-over redundancy.

Additionally, Dropbox also replicates Paper image data stored on AWS infrastructure within multiple AWS availability zones to provide for fail-over redundancy.

Storage Location

Qualified customers can choose to store their Dropbox files (blocks) in Germany within the EU (Frankfurt) region. Additionally, storage servers are available in Australia and Japan for qualified customers. File metadata is stored in the US on Dropbox's proprietary servers. Paper docs and previews are currently stored in the US within the AWS US West, US East, EU Frankfurt, EU London, Asia Pacific (Tokyo), and Asia Pacific (Sydney) regions.

Disaster Recovery

Dropbox maintains a disaster recovery plan that addresses information security requirements during a major crisis or disaster that impacts the in-scope products system operations. The plan specifies actions to be taken in the event of a major incident or emergency at Dropbox's data center co-location facilities. The plan also includes a Recovery Time Objective (RTO) and Recovery Point Objective (RPO) that should be met in the event of a disaster.

The Dropbox Engineering Team reviews this plan annually and updates it as needed. The Engineering Team tests selected elements of the disaster recovery plan at least annually. Elements of the plan are selected for testing based on the Team's determination of availability risk or in order to test elements that have been recently introduced or have not been previously tested. Relevant findings are documented within the Plan document itself and resulting tasks are linked from those results to a task management system, which tracks progress on the issue until resolution.

Business Continuity

As part of the Dropbox Trust Program, Dropbox maintains a Business Continuity Program and Business Continuity & Emergency Management Policy based on the ISO 22301:2019 international business continuity standard. The Business Continuity Program and Business Continuity & Emergency Management Policy define the purpose, scope, commitment to satisfy applicable requirements, and commitment to continual improvement. The program and policies assign ownership, roles and responsibilities, and lines of communication, detail the recovery procedures and work-arounds, and describe the method for business continuity plan invocation. The Business Continuity & Emergency Management Policy also outlines processes for handling extraordinary events that may disrupt operations or threaten strategic objectives.

Dropbox conducts a business impact analysis (BIA) for business processes at least once a year or if there are any major changes, such as the addition of a new significant business process or new critical location, to the business environment. The BIA analyzes processes that are critical to Dropbox and the effect a business disruption might have upon them, sets time frames for recovery, and finds key dependencies, partners, and suppliers.

Dropbox maintains Business Continuity Plans for each team associated with business-critical functions. Business Continuity Teams review these plans at least annually. The business continuity plans establish an incident command structure, orders of succession, response and recovery of critical processes, workaround procedures, devolution, and reconstitution planning. Teams with critical processes test their BCPs at least annually and the relevant findings are documented in a post mortem with an associated improvement plan that is tracked until resolution. In addition, Dropbox conducts evaluations of the business continuity capabilities of its business-critical suppliers at least once a year.

Capacity and Network Management

Dropbox Engineering Management prepares a monthly capacity forecast model based on current usage data and projected future demands on the system. The forecast includes several different metrics, including server demands, power demands, and network bandwidth usage. Future use is forecasted and used by Dropbox management to evaluate the potential need for additional capacity each month.

Dropbox establishes service level agreements or minimum services levels with network infrastructure service providers. These agreements specify contractual requirements for the availability and service conditions of the network connections used for the in-scope products.

Complementary Subservice Organization Control (CSOC) Considerations

Components of the production system are hosted in a third party managed service provider (Amazon Web Services (AWS)).

AWS owns and operates Logical Security, Change Management, and Physical Security controls required to maintain the environments hosting the Dropbox services. Controls at AWS are not included in the scope of this report.

The affected criteria are included below along with the expected minimum controls in place.

Criteria	Controls expected to be in place at third party (AWS)
CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	IT access above least privileged, including administrator access, is approved by appropriate personnel prior to access provisioning. IT access privileges are reviewed on a quarterly basis by appropriate personnel. User access to systems is revoked in a timely manner upon termination.

Criteria	Controls expected to be in place at third party (AWS)
CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware such as firewalls and routers, is restricted to authorized individuals through a badge access system or equivalent, and is monitored by video surveillance. Requests for physical access privileges to the entity's computer facilities require management approval. Documented procedures exist for the identification and escalation of potential physical security breaches. Visitors must be signed in by an authorized workforce member before gaining entry and must be escorted at all times.
CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Changes are authorized, tested, and approved prior to implementation.
A1.1**:** The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Processing capacity is monitoring and maintained on an ongoing basis.
A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Environmental protections have been installed including the following: • Cooling systems • Battery and generator backups • Fire detection and suppression mechanisms • Environmental protection equipment receive maintenance on at least an annual basis.