Dropbox Business security
A Dropbox whitepaper

Contents

Introduction

Millions of users trust Dropbox to easily and reliably store, sync, and share photos, videos, docs, and other files across devices. Dropbox Business brings that same simplicity to the workplace, with advanced features that help teams share instantly across their organizations and give admins the visibility and control they need. But more than just an easy-to-use tool for storage and sharing, Dropbox Business is designed to keep important work files secure. To do this, we've created a sophisticated infrastructure onto which account administrators can layer and customize policies of their own. In this paper, we'll detail the back-end policies, as well as options available to admins, that make Dropbox the secure tool for getting work done.

Except where noted, the information in this whitepaper applies to all of the following products:

- Dropbox Business (Standard, Advanced, and Enterprise)
- Dropbox Education

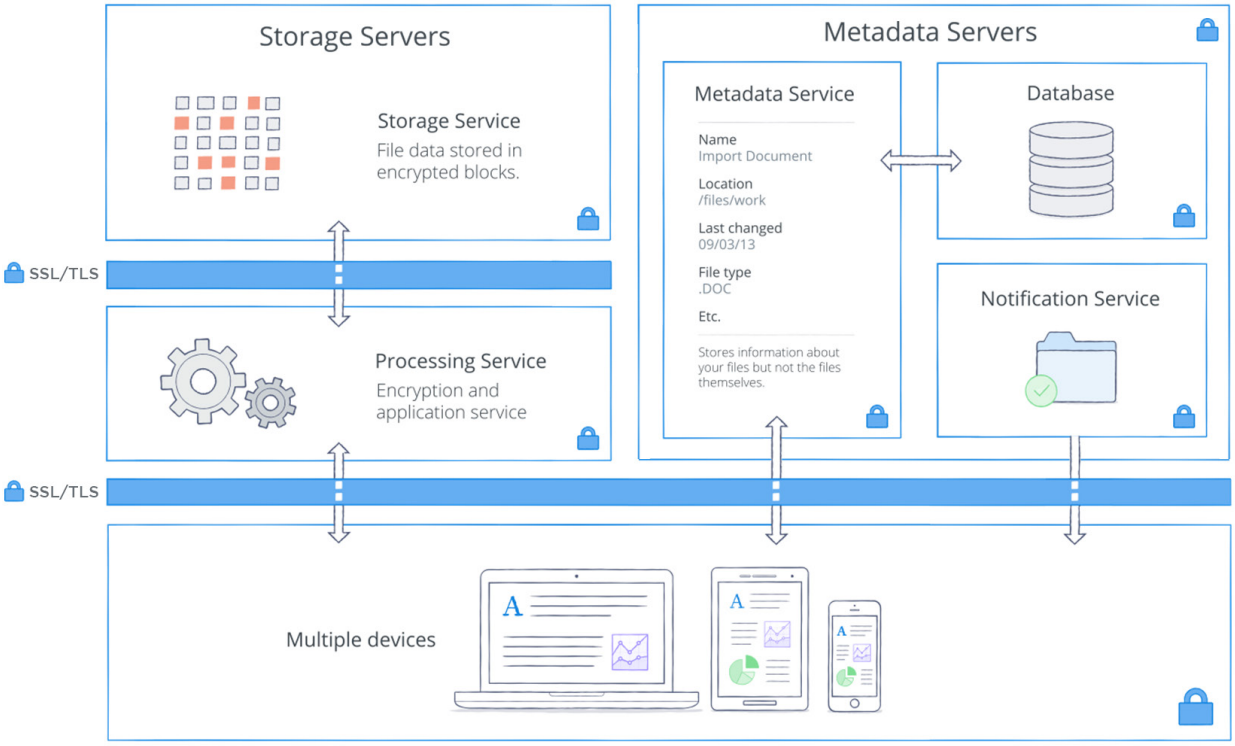
Under the hood

Our easy-to-use interfaces are backed by an infrastructure working behind the scenes to ensure fast, reliable uploads, downloads, sync, and sharing. To make this happen, we're continually evolving our product and architecture to speed data transfer, improve reliability, and adjust to changes in the environment. In this section, we'll explain how data is transferred, stored, and processed securely.

Architecture

Dropbox is designed with multiple layers of protection, covering data transfer, encryption, network configuration, and application-level controls, all distributed across a scalable, secure infrastructure.

Dropbox users can access files and folders at any time from the desktop, web, and mobile clients, or through third-party applications connected to Dropbox. All of these clients connect to secure servers to provide access to files, allow file sharing with others, and update linked devices when files are added, changed, or deleted.



Our architecture is comprised of the following services:

- **Processing service.** By design, Dropbox provides a unique security mechanism that goes beyond traditional encryption to protect user data. The Encryption and Application Services process files from the Dropbox applications by splitting each into blocks, encrypting each file block using a strong cipher, and synchronizing only blocks that have been modified between revisions. When a Dropbox application detects a new file or changes to an existing file, the application notifies the encryption and application services of the change, and new or modified file blocks are processed and transferred to the storage service. For detailed information on the encryption used by these services both in transit and at rest, please see the **Encryption** section below.
- **Storage service.** The actual contents of users' files are stored in encrypted blocks with this service. Prior to transmission, the Dropbox client splits files into file blocks in preparation for the block storage service. The storage service acts as a Content-Addressable Storage (CAS) system, with each individual encrypted file block retrieved based on its hash value.
- **Metadata service.** Certain basic information about user data (including file names and types), called metadata, is kept in its own discrete storage service and acts as an index for the data in users' accounts. Dropbox metadata is stored in a MySQL-backed database service, and is sharded and replicated as needed to meet performance and high availability requirements. Metadata includes basic account and user information, like email address, name, and device names. Metadata also includes basic information about files, including file names and types, that helps support features like version history, recovery, and sync.
- **Notification service.** This separate service is dedicated to monitoring whether or not any changes have been made to Dropbox accounts. No files or metadata are stored here or transferred. Each client establishes a long poll connection to the notification service and waits. When a change to any file in Dropbox takes place, the notification service signals a change to the relevant client(s) by closing the long poll connection. Closing the connection signals that the client must connect to the metadata service securely to synchronize any changes.

With the help of third-party security specialists, our dedicated internal security teams identify and address vulnerabilities, allowing us to mitigate risks and protect these services. These groups conduct regular application, network, and other security testing and auditing to ensure the security of our back-end network.

Distributing different levels of information across these services not only makes syncing faster and more reliable, it also enhances security. The nature of the Dropbox architecture means access to any individual service cannot be used to re-create files. For information on the types of encryption used on the various services, please see the **Encryption** section below.

File data storage

Dropbox stores metadata about files (such as the date and time a file was last changed) and the actual contents of files (file blocks). File metadata is stored on Dropbox servers. File content is stored in one of two systems: Amazon Web Services (AWS) or Magic Pocket, Dropbox's in-house storage system. Magic Pocket consists of both proprietary software and hardware and has been designed from the ground up to be reliable and secure. In both Magic Pocket and AWS, file blocks are encrypted at rest, and both systems meet high standards for reliability. For more details, please see the **Reliability** section below.

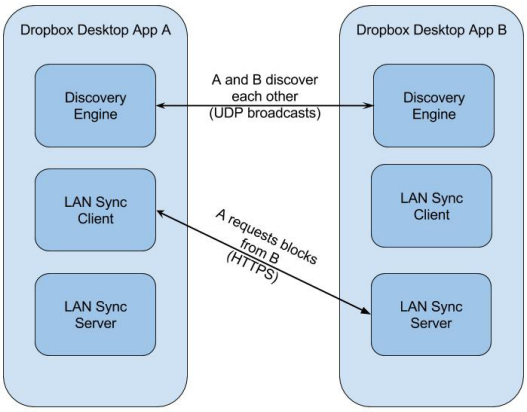
Sync

Dropbox offers industry-recognized best-in-class file sync. Our sync mechanisms ensure fast, responsive file transfers and enable anywhere access to data across devices. Dropbox is also resilient. In the event of a failed connection to the Dropbox service, a client will gracefully resume operation when a connection is reestablished. Files will only be updated on the local client if they have synchronized completely and successfully validated with the Dropbox service. Load balancing across multiple servers ensures redundancy and a consistent synchronization experience for the end user.

- Delta sync. Using this sync method, only modified portions of files are downloaded/uploaded. Dropbox stores each file in discrete, encrypted blocks and only updates the blocks that have changed.
- Streaming sync. Instead of waiting for a file upload to complete, streaming sync will begin downloading to a second device before files have finished uploading from the first device. This is automatically employed when separate computers are linked to the same Dropbox account or when different Dropbox accounts share a folder.
- LAN sync. When enabled, this feature downloads new and updated files from other computers on the same Local Area Network (LAN), saving time and bandwidth compared to downloading the files from Dropbox servers.

  Architecture

  There are three main components of the LAN sync system that run on the desktop app: the discovery engine, the server, and the client. The discovery engine is responsible for finding machines on the network to sync with. This is limited to machines that have authorized access to the same personal or shared Dropbox folder(s). The server handles requests from other machines on the network, serving the requested file blocks. The client is responsible for trying to request file blocks from the network.



Discovery engine

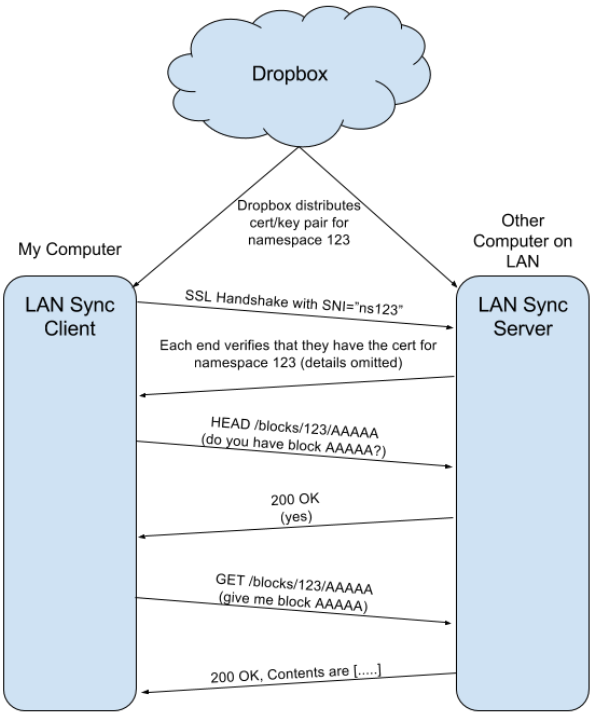
Each machine on the LAN periodically sends and listens for UDP broadcast packets over port 17500 (which is reserved by IANA for LAN sync). These packets contain the version of the protocol used by that computer; the personal and shared Dropbox folders supported; the TCP port that's being used to run the server (which may be different from 17500 if that port is unavailable); and a random identifier for the machine. When a packet is seen, the IP address of the machine is added to a list for each personal or shared folder, indicating a potential target.

Protocol

The actual file block transfer is done over HTTPS. Each computer runs an HTTPS server with endpoints. A client will poll multiple peers to see if they have the blocks, but only download blocks from one server.

To keep all of your data safe, we make sure that only clients authenticated for a given folder can request file blocks. We also make sure that computers cannot pretend to be servers for folders that they do not control. To solve for this, we generate SSL key/certificate pairs for every personal Dropbox or shared folder. These are distributed from Dropbox servers to the user's computers that are authenticated for the folder. The key/certificate pairs are rotated any time membership changes (for example, when someone is removed from a shared folder). We require both ends of the HTTPS connection to authenticate with the same certificate (the certificate for the Dropbox or shared folder). This proves that both ends of the connection are authenticated.

When making a connection, we tell the server which personal Dropbox or folder we are trying to connect for by using Server Name Indication (SNI) so that the server knows which certificate to use.



Server/client

With the protocol described above, the server just needs to know which blocks are present and where to find them.

Based on the results of the discovery engine, the client maintains a list of peers for each personal Dropbox folder and shared folder. When the LAN sync system gets a request to download a file block, it sends a request to a random sample of the peers that it has discovered for the personal Dropbox or shared folder, and then requests the block from the first one that responds that it has the block.

To avoid latencies, we use connection pools to allow us to reuse already-started connections. We don't open a connection until it is needed, and once it is open we keep it alive in case we need it again. We also limit the number of connections to any single peer.

If a file block is not found or downloaded successfully, or if the connection turns out to be too slow, the system falls back to getting the block from Dropbox servers.

Reliability

A storage system is only as good as it is reliable, and to that end, we've developed Dropbox with multiple layers of redundancy to guard against data loss and ensure availability.

Metadata

Redundant copies of metadata are distributed across independent devices within a data center in at least an N+2 availability model. Incremental backups are performed hourly, and full backups are performed daily. Metadata is stored on servers hosted and managed by Dropbox.

File content

Redundant copies of file blocks are stored independently in at least two separate geographic regions and replicated reliably within each region. (Note: For customers who choose to have their files stored in our European infrastructure, file blocks are replicated within Europe only. See the **Data centers** section below.) Both Magic Pocket and AWS are designed to provide annual data durability of at least 99.999999999%.

Dropbox's architecture, applications, and sync mechanisms work together to protect user data and make it highly available. In the rare event of a service availability outage, Dropbox users still have access to the latest synced copies of their files in the local Dropbox folder on linked computers. Copies of files synced in the Dropbox desktop client/local folder will be accessible from a user's hard drive during downtime, outages, or when offline. Changes to files and folders will be synced to Dropbox once service or connectivity is restored.

Incident response

We have incident response policies and procedures to address service availability, integrity, security, privacy, and confidentiality issues.

- Promptly respond to alerts of potential incidents
- Determine the severity of the incident
- If necessary, execute mitigation and containment measures
- Communicate with relevant internal and external stakeholders, including notification to affected customers to meet breach or incident notification contractual obligations and to comply with relevant laws and regulations.
- Gather and preserve evidence for investigative efforts
- Document a postmortem and develop a permanent triage plan

The incident response policies and processes are audited as part of our SOC 2, ISO 27001, and other compliance audits.

Business continuity

Dropbox has established a business continuity management system (BCMS) to address how to resume or continue providing services to users—as well as how to function as a company—if business-critical processes and activities are disrupted. We conduct a cyclic process consisting of the following phases:

- Business impact and risk assessments. We conduct a business impact assessment (BIA) at least annually to identify processes critical to Dropbox, assess the potential impact of disruptions, set prioritized timeframes for recovery, and identify our critical dependencies and suppliers. We also conduct a company-wide risk assessment at least annually. The risk assessment helps us systematically identify, analyze, and evaluate the risk of disruptive incidents to Dropbox. Together, the risk assessment and BIA inform continuity priorities, and mitigation and recovery strategies for business continuity plans (BCPs).
- Business continuity plans. Teams identified by the BIA as critical to Dropbox's continuity use this information to develop BCPs for their critical processes. These plans help the teams know who is responsible for resuming processes if there's an emergency, who in another Dropbox office or location can take over their processes during a disruption, and which methods for communications should be used during a continuity event. These plans also help prepare us for a disruptive incident by centralizing our recovery plans and other important information, such as when and how the plan should be used, contact and meeting information, important apps, and recovery strategies. Dropbox's continuity plans are tied into our company-wide crisis management plan (CMP), which establishes Dropbox's crisis management and incident response teams.
- Plan testing/exercising. Dropbox tests selected elements of its business continuity plans at least annually. These tests are consistent with the BCMS' scope and objectives, are based on appropriate scenarios, and are well-designed with clearly defined aims. The tests may range in scope from tabletop exercises to full-scale simulations of real-life incidents. Based on the results of the testing, as well as experience from actual incidents, teams update and improve their plans to address issues and strengthen their response capabilities.
- Review and approval of BCMS. At least annually, our executive staff reviews the BCMS as part of reviewing Dropbox's Trust Program.

Disaster recovery

To address information security requirements during a major crisis or disaster impacting Dropbox Business operations, we maintain a disaster recovery plan. The Dropbox Infrastructure Team reviews this plan annually and tests selected elements at least annually. Relevant findings are documented and tracked until resolution.

Our Disaster Recovery Plan (DRP) addresses both durability and availability disasters, which are defined as follows.

- A durability disaster consists of one or more of the following:
  - A complete or permanent loss of a primary data center that stores metadata, or of multiple data centers that store file content
  - Lost ability to communicate or serve data from a data center that stores metadata, or from multiple data centers that store file content
- An availability disaster consists of one or more of the following:
  - An outage greater than 10 days
  - Lost ability to communicate or serve data from a storage service/data center that stores metadata, or from multiple storage services/data centers that store file content

We define a Recovery Time Objective (RTO), which is the duration of time and a service level in which business process or service must be restored after a disaster, and a Recovery Point Objective (RPO), which is the maximum tolerable period in which data might be lost from a service disruption. We also measure the Recovery Time Actual (RTA) during Disaster Recovery testing, performed at least annually.

Dropbox incident response, business continuity, and disaster recovery plans are subject to being tested at planned intervals and upon significant organizational or environmental changes.

Data centers

Dropbox corporate and production systems are housed at third-party subservice organization data centers and managed service providers located in different regions of the United States. Subservice organization data center SOC reports are reviewed

at a minimum annually for sufficient security controls. These third-party service providers are responsible for the physical, environmental, and operational security controls at the boundaries of Dropbox infrastructure. Dropbox is responsible for the logical, network, and application security of our infrastructure housed at third-party data centers.

Our managed service provider for processing and storage of some file content, Amazon Web Services (AWS), is responsible for the logical and network security of Dropbox services provided through their infrastructure. Connections are protected through their firewall, which is configured in a default deny-all mode. Dropbox restricts access to the environment to a limited number of IP addresses and employees.

Infrastructure in Europe

Dropbox offers Europe-based storage of file content for European customers. Our infrastructure is hosted by Amazon Web Services in Frankfurt, Germany and replicated within the Frankfurt region to ensure redundancy and protect against data loss.

Product features (security, control, and visibility)

Dropbox provides the administrative control and visibility features that empower both IT and end users to effectively manage their businesses and data. Below is a sampling of features available to team admins and users, as well as third-party integrations for managing core IT processes.

Note: Availability of features varies by subscription plan. See **dropbox.com/business/plans** for details.

Admin management features

No two organizations are exactly alike, so we've developed a number of tools that empower admins to customize Dropbox Business to their teams' particular needs. Below are several control and visibility features available via the Dropbox Business Admin Console.

Controls

- Tiered admin roles. The following three access levels can be assigned to each account admin to enable more effective team management.
  - Team admin. Can set team-wide security and sharing permissions, create admins, and manage members. The team admin has all available admin permissions. Only team admins can set other team members as admins or change admin roles, and there must always be at least one team admin on a Dropbox Business account.
  - User management admin. Can address most team management tasks, including adding and removing team members, managing Groups, and viewing a team's activity feed. Any team member can be set as a user management admin.
  - Support admin. Can address common service requests from team members, like restoring deleted files or helping team members locked out of two-step verification. Support admins can also reset non-admin passwords and export an activity log for a specified team member.
- User provisioning methods
  - Email invitation. A tool in the Dropbox Business Admin Console allows administrators to manually generate an email invitation.
  - Active Directory. Dropbox Business administrators can automate the creation and removal of accounts from an existing Active Directory system via our Active Directory connector or a third-party identity provider. Once integrated, Active Directory can be used to manage membership.
  - Single sign-on (SSO). Dropbox Business can be configured to allow team members access by signing into a central identity provider. Our SSO implementation, which uses the industry-standard Security Assertion Markup Language 2.0

(SAML 2.0), makes life easier and more secure by placing a trusted identity provider in charge of authentication and giving team members access to Dropbox without an additional password to manage. Dropbox has also partnered with leading identity management providers so that users can be provisioned and deprovisioned automatically. Please see the Dropbox Business API integrations section below.

  - API. The Dropbox Business API can be used by customers to build custom user provisioning and identity management solutions. Please see the **Dropbox Business API integrations** section below.

- Domain management. Dropbox provides a set of tools for companies to simplify and speed up the process of onboarding users and controlling Dropbox usage.
  - Domain verification. Companies can claim ownership of their domains and unlock the other domain management tools.
  - Invite enforcement. Admins can require individual Dropbox users who have been invited to the company's Dropbox team to migrate to the team or change the email address on their personal account.
  - Domain insights. Admins are able to see key information, such as how many individual Dropbox accounts are using company email addresses.
  - Account capture. Admins can force all Dropbox users using a company email address to join the company's team or change the email address on their personal account.
- Enterprise installer. Admins requiring scaled provisioning can use our enterprise installer for Windows to install the Dropbox desktop client silently and remotely via managed-software solutions and deployment mechanisms.
- Two-step verification requirement. Admins can choose to require two-step verification for all team members or just specific members. Other multi-factor authentication requirements can be enforced through your SSO implementation.
- Password reset. As a proactive security measure, admins can reset passwords for the entire team or on a per-user basis.
- Groups. Teams can create and manage lists of members within Dropbox and easily give them access to specific folders. Dropbox can also sync Active Directory groups using the Active Directory Connector.
  - Company-managed groups. Only admins can create, delete, and manage the membership for this type of group. Users cannot request to join or leave a company-managed group.
  - User-managed groups. Admins can choose whether users can create and manage their own groups. Admins can also change a user-managed group to a company-managed group at any time to take control of it.
- Restricting multiple accounts on computers. Admins can block team members from linking a second Dropbox account to computers that are linked to their work Dropbox account.
- Sharing permissions. Team admins have comprehensive control of their team's sharing abilities using Dropbox, including:
  - whether team members can share files and folders with people outside the team
  - whether team members can edit folders owned by people outside the team
  - whether shared links created by team members will work for people outside the team
  - whether team members can create file requests and collect files from team members and/or people outside the team
  - whether people can view and make comments on files owned by the team
- Team folders. Admins can create team folders that automatically give groups and other collaborators the correct access level (view or edit) to the content they need.
  - Granular access and sharing controls. Sharing controls let admins manage membership and permissions at the top level or sub-folder level so that people and groups inside and outside the company have access to specific folders only.
  - Team folder manager. Admins can view all their team folders and customize sharing policies from a central place to help prevent mis-sharing of confidential materials.
- Permanent delete permissions. The team admin of a Dropbox Business account can limit the ability to permanently delete files to team admins only.
- Web sessions. Active browser sessions can be tracked and terminated from both the Admin Console and individual users' account settings.

- App access. Admins have the ability to view and revoke third-party app access to user accounts.
- Unlink devices. Computers and mobile devices connected to user accounts can be unlinked by the admin through the Admin Console or the user through individual account security settings. On computers, unlinking removes authentication data and provides the option to delete local copies of files the next time the computer comes online (see **Remote wipe**). On mobile devices, unlinking removes files marked as favorites, cached data, and login information. If two-step verification is enabled, users must re-authenticate any device upon relinking. Additionally, users' account settings provide the option to send a notification email automatically when any devices are linked.
- Remote wipe. When employees leave the team or in the event of device loss, admins can remotely delete Dropbox data and local copies of files. Files will be removed from both computers and mobile devices when they come online and the Dropbox application is running.
- Account transfer. After deprovisioning a user (either manually or via directory services), admins can transfer files from that user's account to another user on the team.
- Suspended user state. Admins have the ability to disable a user's access to their account while preserving their data and sharing relationships to keep company information safe. Admins can later reactivate or delete the account.
- Sign in as user. Team admins can sign in as members of their teams. This gives admins direct access to the files and folders in team member accounts so that they can make changes, share on behalf of team members, or conduct audits of file-level events. "Sign in as user" events are recorded in the team's activity log, and admins can determine whether members are notified of these events.
- Network control. Admins can restrict Dropbox usage on the company network to only the Enterprise team account. This feature integrates with the company's network security provider, enabling it to inspect the Dropbox traffic on the company network and block any traffic that exists outside of the sanctioned account.
- Enterprise mobility management (EMM). Dropbox integrates with third-party EMM providers to give Dropbox Enterprise admins more control over how team members use Dropbox on mobile devices. Admins can restrict mobile app usage for Dropbox Enterprise accounts to just managed devices (whether company-provided or personal), gain visibility into app usage (including available storage and access locations), and remote wipe a lost or stolen device.
- Device approvals. Dropbox enables admins to set limits on the number of devices that a user can sync with Dropbox, and to choose whether approvals are user-managed or admin-managed. Admins can also create an exception list of users that are not restricted to a certain number of devices.

Visibility

- Activity feed. Dropbox Business records user and admin actions in the team's activity feed, which can be accessed from the Admin Console. The activity feed offers flexible filtering options that enable admins to conduct targeted investigations of account and file activity. For example, they can view the full history of a file and how users have interacted with it, or view all activity for the team over a specified time period. The activity feed can be exported as a downloadable report in CSV format and also integrated directly into a SIEM (security information and event management) product or other analysis tool through third-party partner solutions. The following events are recorded in the activity feed:
  - Logins. Successful and failed sign-ins to the Dropbox website
    - Successful or failed login attempt
    - Failed login attempt via single sign-on (SSO)
    - Failed login attempt or error via EMM
    - Logged out
    - Change of IP address for web session
  - Passwords. Changes to password or two-step verification settings. Admins do not have visibility into users' actual passwords.
    - Changed or reset password
    - Enabled, reset, or disabled two-step verification
    - Set up or changed two-step verification to use SMS or a mobile app

  - Added, edited, or removed a backup phone for two-step verification
  - Added or removed a security key for two-step verification
- Membership. Additions to and removals from the team
  - Invited a team member
  - Joined the team
  - Removed a team member
  - Suspended or unsuspended a team member
  - Recovered a removed team member
  - Requested to join the team based on account domain
  - Approved or declined a request to join the team based on account domain
  - Sent domain invites to existing domain accounts
  - User joined the team in response to account capture
  - User left domain in response to account capture
  - Blocked or unblocked team members from suggesting new team members
  - Suggested a new team member
- Apps. Linking of third-party apps to Dropbox accounts
  - Authorized or removed an application
  - Authorized or removed a team application
- Devices. Linking of computers or mobile devices to Dropbox accounts
  - Linked or unlinked a device
  - Used remote wipe and successfully deleted all files or failed to delete some files
  - Change of IP address for desktop computer or mobile device
- Admin actions. Changes to settings in the Admin Console, such as shared folder permissions

  Authentication and single sign-on (SSO)
  - Reset team member's password
  - Reset all team members' passwords
  - Blocked or unblocked team members from disabling two-step verification
  - Enabled or disabled SSO
  - Made sign-in via SSO required
  - Changed or removed the SSO URL
  - Updated the SSO certificate
  - Changed the SSO identity mode

  Membership
  - Blocked or unblocked users from requesting to join the team based on account domain
  - Set team membership requests to be automatically approved or require manual admin approval

  Member account management
  - Changed a team member's name
  - Changed a team member's email address
  - Gave or removed admin status, or changed the admin role

- Signed in or signed out as a team member
- Transferred or deleted the contents of a removed member's account
- Permanently deleted the contents of a removed member's account

Global sharing settings

- Blocked or unblocked team members from adding shared folders owned by non-team members
- Blocked or unblocked team members from sharing folders with non-team members
- Turned on warnings that are shown to users before they share folders with non-team members
- Blocked or unblocked non-team members from viewing shared links
- Set shared links to be team-only by default
- Blocked or unblocked people from making comments on files
- Blocked or unblocked team members from creating file requests
- Added, changed, or removed a logo for shared link pages

Team folder management

- Created a team folder
- Renamed a team folder
- Archived or unarchived a team folder
- Permanently deleted a team folder
- Downgraded a team folder to a shared folder

Domain management

- Attempted to verify or successfully verified a domain, or removed a domain
- Dropbox Support verified or removed a domain
- Enabled or disabled sending domain invites
- Turned on or off "Automatically invite new users"
- Changed account capture mode
- Dropbox Support granted or revoked account capture

Enterprise mobility management

- Enabled EMM for test (optional) mode or deploy (required) mode
- Refreshed EMM token
- Added or removed team members from EMM excluded users list
- Disabled EMM
- Created an EMM exception list report
- Created an EMM mobile app usage report

Changes to other team settings

- Merged teams
- Upgraded the team to Dropbox Business or downgraded to a free team
- Changed the team name
- Created a team activity report
- Blocked or unblocked team members from having more than one account linked to a computer

- Allowed all team members or only admins to create groups
- Blocked or unblocked team members from permanently deleting files
- Started or ended a Dropbox Support session for a reseller

- **Sharing.** Events related to sharing files, folders, and links. Where applicable, reports specify whether actions involved people outside the team.

  Shared files

  - Added or removed a team member or non-team member
  - Changed the permissions for a team member or non-team member
  - Added or removed a group
  - Added a shared file to the user's Dropbox
  - Viewed the content of a file that was shared via a file or folder invitation
  - Copied shared content to the user's Dropbox
  - Downloaded shared content
  - Commented on a file
  - Resolved or unresolved a comment
  - Deleted a comment
  - Subscribed or unsubscribed to comment notifications
  - Claimed an invitation to a file owned by the team
  - Requested access to a file owned by the team
  - Changed the parent of a shared folder
  - Unshared a file

  Shared folders

  - Created a new shared folder
  - Added or removed a team member, non-team member, or group
  - Added a shared folder to the user's Dropbox, or user removed their own access to a shared folder
  - Added a shared folder from a link
  - Changed the permissions of a team member or non-team member
  - Transferred folder ownership to another user
  - Unshared a folder
  - Claimed membership to a shared folder
  - Requested access to a shared folder
  - Added requesting user to a shared folder
  - Blocked or unblocked non-team members from being added to a folder
  - Allowed any team member to add people to a folder or only the owner
  - Changed group access to a shared folder

  Shared links

  - Created or removed a link
  - Made the contents of a link visible to anyone with the link or team members only
  - Made the contents of a link password protected

    - Set or removed the expiration date of a link
    - Opened a link
    - Downloaded the contents of a link
    - Copied the contents of a link to the user's Dropbox
    - Created a link to a file via an API app
    - Shared a link with a team member, non-team member or group
    - Blocked or unblocked non-team members from viewing links to files in a shared folder
    - Shared an album

    File requests

    - Created, changed, or closed a file request
    - Added users to a file request
    - Added or removed a file request deadline
    - Changed a file request folder
    - Received files via a file request
- Groups. Creation, deletion, and membership information for groups
    - Created, renamed, moved, or deleted a group
    - Added or removed a member
    - Changed a group member's access type
    - Changed group to team-managed or admin-managed
    - Changed the external ID of a group
- File events. Individual file and folder events
    - Added a file to Dropbox
    - Created a folder
    - Viewed a file
    - Edited a file
    - Downloaded a file
    - Copied a file or folder
    - Moved a file or folder
    - Renamed a file or folder
    - Reverted a file to a previous version
    - Rolled back changes in files
    - Restored a deleted file
    - Deleted a file or folder
    - Permanently deleted a file or folder

- Technical support identity verification. Before any troubleshooting or account information is provided by Dropbox Support, the account admin must provide a one-time use, randomly-generated security code to validate his or her identity. This PIN is only available through the Admin Console.

User management features

Dropbox Business also includes tools for end users to further protect their accounts and data. The authentication, recovery, logging, and other security features below are available through the various Dropbox user interfaces.

Recovery and version control. All Dropbox Business customers have the ability to restore lost files and recover previous versions of files, ensuring changes to important data can be tracked and retrieved.

Two-step verification. This highly recommended security feature adds an extra layer of protection to a user's Dropbox account. Once two-step verification is enabled, Dropbox will require a six-digit security code in addition to a password upon sign-in or when linking a new computer, phone, or tablet.

- Admins can choose to require two-step verification for all team members or just specific members.
- Account administrators can track which team members have two-step verification enabled.
- Dropbox two-step authentication codes can be received via text message or apps which conform to the Time-based One-Time Password (TOTP) algorithm standard.
- In the event a user cannot receive security codes via these methods, they may opt to use a 16-digit, one-time-use emergency backup code. Alternately, they may use a secondary phone number to receive a backup code via text message.
- Dropbox also supports the open standard FIDO Universal 2nd Factor (U2F), which enables users to authenticate with a USB security key they've set up rather than a six-digit code. A U2F security key uses cryptographic communication and provides additional protection against credential theft attacks like phishing.

User account activity. Each user can view the following pages from their account settings to obtain up-to-date information regarding their own account activity:

- Sharing page. This page shows the shared folders that are currently in the user's Dropbox, as well as shared folders the user can add. It also shows individual files that have been shared with the user by others. A user can unshare folders and files and set sharing permissions (described below).
- Links page. This page shows all active shared links that the user has created and the creation date for each. It also shows all links shared with the user by others. The user can disable links or change permissions (described below).
- Events page. A running log of all individual file and folder edits, additions, and deletions is available on this page. Shared folder activity including membership and changes from other members of the folder can be tracked here as well.
- Email notifications. A user can opt in to receive an email notification immediately when a new device or app is linked to their Dropbox account.

User account permissions

- Linked devices. The Devices section of a user's account security settings displays all computers and mobile devices linked to the user's account. For each computer, the IP address, country, and approximate time of most recent activity is displayed. A user can unlink any device, with the option to have files on linked computers deleted the next time it comes online.
- Active web sessions. The Sessions section shows all web browsers currently logged into a user's account. For each, the IP address, country, and login time of the most recent session, as well as the approximate time of most recent activity, is displayed. A user can terminate any session remotely from the user's account security settings.
- Linked apps. The Apps linked section provides a list of all third-party apps with access to a user's account, and the type of access each app holds. A user can revoke any app's permission to access the user's Dropbox.

Mobile security

- Fingerprint scanning. Users can enable Touch ID on iOS devices and Fingerprint lock (where supported) on Android devices as a method to unlock the Dropbox mobile app.
- Erase data. For additional security, a user can enable the option to erase all Dropbox data from the device after 10 failed passcode attempts.

- Internal storage and saved files. By default, files are not stored on the internal storage of mobile devices. Dropbox mobile clients feature the ability to save files to the device for offline viewing. When a device is unlinked from a Dropbox account, via either the mobile or web interface, saved files are automatically deleted from the device's internal storage.

Shared file and folder permissions

- Permissions for shared folders. A team member who owns a shared folder can remove folder access for specific users, change view/edit permissions for specific users, and transfer folder ownership. Depending on the team's global sharing permissions, each shared folder's owner may also be able to control whether it can be shared with people outside the team, whether others with edit permissions can manage membership, and whether links can be shared with people outside the folder.
- Permissions for shared files. A team member who owns a shared file can remove access for specific users and disable commenting for the file.
- Passwords for shared links. Any shared link can be protected with an owner-defined password. Before any file or folder data is transmitted, an access control layer verifies that the correct password has been submitted and all other requirements (such as team, group, or folder ACL) have been met. If so, a secure cookie is stored in the user's browser to remember that the password was verified previously.
- Expirations for shared links. Users can set an expiration for any shared link to provide temporary access to files or folders.

Dropbox Business API integrations

Through the Dropbox Business API and our partners, you can add additional security tools to manage your data and accounts:

- Security information and event management (SIEM) and analytics. Connect your Dropbox Business account to SIEM and analytics tools to monitor and evaluate user sharing, sign-in attempts, admin actions, and more. Access and manage employee activity logs and security-relevant data through your central log management tool.
- Data loss prevention (DLP). Automatically scan file metadata and content to trigger alerts, reporting, and actions when important changes are made in your Dropbox Business account. Apply company policies to your Dropbox Business deployment and help meet regulatory compliance requirements.
- eDiscovery and legal hold. Respond to litigation, arbitration, and regulatory investigations with data from your Dropbox Business account. Search for and collect relevant electronically stored information, and preserve your data through the eDiscovery process, saving your business time and money.
- Digital rights management (DRM). Add third-party content protection for sensitive or copyrighted data stored in employee accounts. Gain access to powerful DRM features including client-side encryption, watermarking, audit trails, access revocation, and user/device blocking.
- Data migration and on-premises backup. Migrate data to Dropbox from existing servers or other cloud-based solutions, saving time, money, and effort. Automate backups from your Dropbox Business account to on-prem servers.
- Identity management and single sign-on (SSO). Automate the provisioning and deprovisioning process and speed up onboarding for new employees. Streamline management and bolster security by integrating Dropbox Business with an existing identity system.
- Custom workflows. Build in-house apps that integrate Dropbox into existing business processes to enhance their internal workflows.

By giving developers access to the team-level functionality of Dropbox Business, admins are empowered to deploy and manage business-critical applications for their team. It's especially useful for enterprise customers, as Dropbox Business now fits even more seamlessly into their existing third-party solutions. See the **Apps for Dropbox** section below for more information on the Dropbox Business API.

Application security

Dropbox user interfaces

The Dropbox service 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. It allows users to upload, download, view, and share their files. The web interface also allows users to open existing local versions of files through their computer's default application.
- Desktop. The Dropbox desktop application is a powerful sync client that stores files locally for offline access. It gives users full access to their Dropbox accounts, and runs on Windows, Mac, and Linux operating systems. Files are viewed and can be shared directly within the operating systems' respective file browsers.
- Mobile. The Dropbox app is available for iOS, Android, Windows, and BlackBerry smartphones and tablets, allowing users to access all their files on the go. The mobile app also supports local storage of files for offline access.
- API. Dropbox APIs provide a flexible way to read and write to Dropbox user accounts as well as access to advanced functionality like search, revisions, and restoring files. The APIs can be used to manage the user lifecycle for a Dropbox Business account, perform actions on all members of a team, and enable access to Dropbox Business admin functionality.

Encryption

Data in transit

To protect data in transit between Dropbox apps and our servers, Dropbox uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for data transfer, creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. File data in transit between a Dropbox client (currently desktop, mobile, API, or web) and the hosted service is always encrypted via SSL/TLS. For end points we control (desktop and mobile) and modern browsers, we use strong ciphers and support perfect forward secrecy and certificate pinning. Additionally, on the web we flag all authentication cookies as secure and enable HTTP Strict Transport Security (HSTS) with includeSubDomains enabled.

Note: Dropbox uses TLS exclusively and has deprecated the use of SSLv3 due to known vulnerabilities. However, TLS is frequently referred to as "SSL/TLS," so we use that designation here.

To prevent man-in-the-middle attacks, authentication of Dropbox front-end servers is performed through public certificates held by the client. An encrypted connection is negotiated before the transfer of any files and ensures secure delivery of files to Dropbox front-end servers.

Data at rest

Dropbox files at rest are encrypted using 256-bit Advanced Encryption Standard (AES). Files are primarily stored in multiple data centers in discrete file blocks. Each block is fragmented and encrypted using a strong cipher. Only blocks that have been modified between revisions are synchronized.

Key management

The Dropbox key management infrastructure is designed with operational, technical, and procedural security controls with very limited direct access to keys. Encryption key generation, exchange, and storage is distributed for decentralized processing.

- File encryption keys. By design, Dropbox manages file encryption keys on users' behalf to remove complexity, enable advanced product features and strong cryptographic control. File encryption keys are created, stored and protected by production system infrastructure security controls and security policies.
- Internal SSH keys. Access to production systems is restricted with unique SSH key pairs. Security policies and procedures

require protection of SSH keys. An internal system manages the secure public key exchange process, and private keys are stored securely.

- Key distribution. Dropbox automates the management and distribution of sensitive keys to systems that are required for operations.

Certificate pinning

Dropbox does certificate pinning in modern browsers that support the HTTP Public Key Pinning specification, and on our desktop and mobile clients in most scenarios and implementations. Certificate pinning is an extra check to make sure that the service you're connecting to is really who they say they are, and not an imposter. We use it to guard against other ways that skilled hackers may try to spy on your activity.

Protecting authentication data

Dropbox goes beyond regular hashing to protect the login credentials of users. In keeping with industry best practices, each password is salted with a randomly generated, unique per-user salt, and we use iterative hashing to slow down computation. These practices help protect against brute force, dictionary, and rainbow attacks. As an added precaution, we encrypt the hashes with a key stored separately from the database, which helps to keep passwords secure in the event of a database-only compromise.

Malware scanning

We've developed an automated scanning system that's designed to stop malware from being spread through Dropbox's shared link feature. The system leverages both proprietary technology and industry-standard detection engines.

Apps for Dropbox

The Dropbox Platform is composed of a robust ecosystem of developers who build on top of our flexible Application Programming Interfaces (APIs). Over 300,000 apps for productivity, collaboration, security, administration, and more have been built on the Dropbox Platform.

Dropbox API

The Dropbox API allows developers to offer users in-app access to Dropbox files and works as a flexible way to read and write to Dropbox. Auth, file, and metadata interaction; shared file, folder, and link interaction; and file operations are all handled through the Dropbox API.

Apps using the Dropbox API can be built with one of the following permissions levels:

- App folder. A dedicated folder named after the app is created within the Apps folder of a user's Dropbox. The app receives read and write access to this folder only and users can provide content to the app by moving files into this folder. In addition, the app may request file/folder access via the Chooser or Saver (see below).
- Full Dropbox. The app receives full access to all the files and folders in a user's Dropbox, and may also request file/folder access via the Chooser or Saver (see below).

Chooser and Saver. The Chooser and the Saver allow easy access to Dropbox with just a few lines of code. The Chooser enables selection of files from Dropbox, while the Saver allows users to save files directly to Dropbox. In essence, they take the place of traditional Open and Save dialog boxes, and restrict an app's access to only the files and/or folders the user specifically selects on a one-off basis.

Dropbox uses OAuth, an industry-standard protocol for authorization, to allow users to grant apps account access without

exposing their account credentials. We support OAuth 2.0 for authenticating all API requests; requests are authenticated through the Dropbox website or mobile app.

Dropbox Business API

The Dropbox Business API allows apps to manage entire Dropbox Business accounts and perform Core API actions on all members of a team. It gives apps programmatic access to Dropbox Business admin functionality, specifically the Dropbox Business audit log and team usage statistics, as well as group and shared folder management.

In addition to Core API calls, the Dropbox Business API features additional endpoints designed specifically for businesses. These include endpoints for user and group information and management, auditing, and webhook notifications.

App permission types

There are four different types of Dropbox Business API permissions, with varying level of access to team and user data. Developers should only request access to the minimum set of permissions that their apps require:

- Team information. Information about the team and aggregate usage data
- Team auditing. Team information, plus the team's detailed activity log
- Team member file access. Team information and auditing, plus the ability to perform any action as any team member
- Team member management. Team information, plus the ability to add, edit, and delete team members

Like the Dropbox API, the Dropbox Business API uses OAuth 2.0 for authenticating API requests. Dropbox Business API OAuth tokens can enable extensive access to account data. The OAuth response will include an additional team_id field. It's the developer's responsibility to properly secure the OAuth tokens server-side, and ensure they are not cached in insecure environments or downloaded to client devices. Developers will need to direct a Dropbox Business account administrator through the standard OAuth 2.0 flow to install their application on a Dropbox Business account.

For more information on Dropbox APIs, visit dropbox.com/developers.

Dropbox developer guidelines

We provide a number of guidelines and practices to help developers create API apps that respect and protect user privacy while enhancing users' Dropbox experience.

- App keys. For each distinct app a developer writes, a unique Dropbox app key must be used. In addition, if an app provides services or software that wrap the Dropbox Platform for other developers to use, each developer must also sign up for their own Dropbox app key.
- App permissions. Developers are instructed that an app should use the least privileged permission it can. When a developer submits an app for production status approval, we review that the app doesn't request an unnecessarily broad permission based on the functionality provided by the app.
- App review process
  - Development status. When a Dropbox API app is first created, it is given development status. The app functions the same as any production status app, except that it can only be linked with up to 500 total Dropbox users. Once an app links 50 Dropbox users, the developer has two weeks to apply for and receive production status approval before the app's ability to link additional Dropbox users will be frozen.
  - Production status and approval. In order to receive production status approval, all API apps must adhere to our developer branding guidelines and Terms & Conditions, which include prohibited uses of the Dropbox Platform. These uses include: promoting IP or copyright infringement, creating file sharing networks, and downloading content illegally.

Developers are first prompted for additional information regarding their app's functionality, and how it uses the Dropbox API before submitting for review. Once the app is approved for production status, any number of Dropbox users can link to the app.

API partnerships

Dropbox has worked closely with our partners to develop integrations with popular software packages. These integrations enable access to data in Dropbox within their interfaces, creating a seamless and secure experience for end users of both services.

- **Microsoft Office for mobile and web.** Our Microsoft Office integrations allow users to open Word, Excel, and PowerPoint files stored in their Dropbox; make changes in the Office mobile or web apps; and save those changes directly back to Dropbox. Users are prompted to grant access on the first attempt to open a Dropbox file in each Office mobile app or any Office web app. Subsequent launches will retain these links.
- **Adobe Acrobat and Acrobat Reader.** Our integrations with the desktop and mobile (Android and iOS) versions of these apps enable users to view, edit, and share PDFs stored in their Dropbox. Users are prompted to grant access on the first attempt to open a Dropbox file in each app. Changes to PDFs are saved back to Dropbox automatically.

Network security

Dropbox diligently maintains the security of our back-end network. Our network security and monitoring techniques are designed to provide multiple layers of protection and defense. We employ industry-standard protection techniques, including firewalls, network vulnerability scanning, network security monitoring, and intrusion detection systems to ensure only eligible and non-malicious traffic is able to reach our infrastructure.

Our internal private network is segmented according to use and risk level. The primary networks are:

- Internet-facing DMZ
- Priority infrastructure DMZ
- Production network
- Corporate network

Access to the production environment is restricted to only authorized IP addresses and requires multi-factor authentication on all endpoints. IP addresses with access are associated with the corporate network or approved Dropbox personnel. Authorized IP addresses are reviewed on a quarterly basis to ensure a secure production environment. Access to modify the IP address list is restricted to authorized individuals.

Traffic from the internet destined to our production network is protected using multiple layers of firewalls and proxies.

Strict limitation is maintained between the internal Dropbox network and the public internet. Internet-bound traffic to and from the production network is carefully controlled through a dedicated proxy service and those, in turn, are protected by restrictive firewall rules.

Dropbox instruments sophisticated tool sets to monitor laptops and desktops with Mac and Windows operating systems and production systems for malicious events. All security logs are collected in a centralized location for forensic and incident response following the industry standard retention policy.

Dropbox identifies and mitigates risks via regular network security testing and auditing by both dedicated internal security teams and third-party security specialists.

Points of presence (PoPs)

To optimize website performance for users, Dropbox leverages third-party content delivery networks (CDNs) and Dropbox-hosted points of presence (PoPs) in California, Texas, Virginia, New York, Washington, the UK, the Netherlands, Germany, Japan, Singapore, and Hong Kong. No user data is cached at these locations, and all data being transferred is encrypted with SSL/TLS. Physical and logical access to Dropbox-hosted PoPs are restricted to authorized Dropbox personnel only. Dropbox performs optimizations at both the transport (TCP) layer and the application (HTTP) layer.

Peering

Dropbox operates using the autonomous system AS19679 and has network peering arrangements with internet service providers. Dropbox has an open peering policy, and all customers are welcome to peer with us.

Peering with Dropbox requires a minimum of 50 Mbps of in-continent traffic destined to or through the customer's network. We also require an up-to-date PeeringDB entry for all public peering requests, including exchange information with properly formatted public fabric addresses, ASNs, and NOC/peering contact information.

We ask that peers also maintain their private peering facility details, as we use this information for private peering (PNI) targeting.

Vulnerability management

Our security team performs automated and manual application security testing and works with third-party specialists on a regular basis to identify and patch potential security vulnerabilities and bugs.

The input from these activities are assessed by Security personnel, and priorities are assigned to items as assessed by the Security team. As a necessary component of our information security management system, findings and recommendations that result from all of these assessment activities are reported to Dropbox management, evaluated, and appropriate action is taken, as determined to be necessary. High-severity items are documented, tracked, and resolved by assigned security engineers.

Change management

A formal Change Management Policy has been defined by the Dropbox Engineering team to ensure that all application changes have been authorized prior to implementation into the production environments. Source code changes are initiated by developers that would like to make an enhancement to the Dropbox application or service. All changes are stored in a version control system and are required to go through automated Quality Assurance (QA) testing procedures to verify that security requirements are met. Successful completion of QA procedures leads to implementation of the change. All QA-approved changes are automatically implemented in the production environment. Our software development lifecycle (SDLC) requires adherence to secure coding guidelines, as well as screening of code changes for potential security issues via our QA and manual review processes.

All changes released into production are logged and archived, and alerts are sent to Dropbox Engineering team management automatically.

Changes to Dropbox infrastructure are restricted to authorized personnel only. The Dropbox Security team is responsible for maintaining infrastructure security and ensuring that server, firewall, and other security-related configurations are kept up-to-date with industry standards. Firewall rule sets and individuals with access to production servers are reviewed on a periodic basis.

Scanning and security penetration testing (internal and external)

Our security team performs automated and manual application security testing on a regular basis to identify and patch potential security vulnerabilities and bugs on our desktop, web, and mobile applications.

Additionally, Dropbox contracts with third-party vendors to perform periodic penetration and vulnerability tests on the corporate and production environments. We work with third-party specialists, other industry security teams, and the security research community to keep our applications secure.

We also look for vulnerabilities through automatic analysis systems. This includes systems we develop internally, open source systems we modify for our needs, or external vendors we hire for continuous automated analysis.

Bug bounties

While we work with professional firms for pentesting engagements and do our own testing in-house, bug bounties (or vulnerability rewards programs) tap into the expertise of the broader security community. Our bug bounty program provides an incentive for researchers to responsibly disclose software bugs and centralize reporting streams. This involvement of the external community provides our security team with independent scrutiny of our applications to help keep users safe.

We've established a scope for eligible submissions and Dropbox applications, as well as a responsible disclosure policy that promotes the discovery and reporting of security vulnerabilities and increase user safety. This policy sets forth the following guidelines:

- Share the security issue with us in detail
- Give us reasonable time to respond before making any information about the security issue public.
- Do not access or modify user data without permission of the account owner.
- Act in good faith not to degrade the performance of our services (including denial of service).

Issues can be reported by submitting a report to HackerOne at **hackerone.com/dropbox**.

Dropbox information security

Dropbox has established an information security management framework describing the purpose, direction, principles, and basic rules for how we maintain trust. This is accomplished by assessing risks and continually improving the security, confidentiality, integrity, and availability of the Dropbox Business systems. We regularly review and update security policies, provide security training, perform application and network security testing (including penetration testing), monitor compliance with security policies, and conduct internal and external risk assessments.

Our policies

We've established a thorough set of security policies covering the areas of Information security, Physical security, Incident response, Logical access, Physical production access, Change management, and Support. These policies are reviewed and approved at least annually, and are enforced by the Dropbox security team. Employees, interns, and contractors participate in mandatory security training when joining the company and ongoing security awareness education.

- Information security. Policies pertaining to user and Dropbox information, with key areas including device security; authentication requirements; data and systems security; user data privacy; restrictions on and guidelines for employee use of resources; and handling of potential issues

- User data privacy. Our requirements for protecting and handling user information and user data at Dropbox in order to adhere to our Privacy Policy
- Physical security. How we maintain a safe and secure environment for people and property at Dropbox (see **Physical security** section below)
- Incident response. Our requirements for responding to potential security incidents, including assessment, communication, and investigation procedures
- Logical access. Policies for securing Dropbox systems, user information, and Dropbox information, covering access control to corporate and production environments
- Physical production access. Our procedures for restricting access to the physical production network, including management review of personnel and de-authorization of terminated personnel
- Change management. Policies for code review and managing changes that impact security by authorized developers to application source code, system configuration, and production releases
- Support. User metadata access policies for our support team regarding viewing, providing support for, or taking action on accounts
- Business continuity. Policies and procedures for maintaining or restoring critical business functions in the event of a disruption, from planning and documentation to execution
- Crisis management. Policies and procedures on how Dropbox would handle an extraordinary widespread event that could disrupt our most important operations or threaten our strategic objectives

Employee policy and access

Upon hire, each Dropbox employee is required to complete a background check, sign a security policy acknowledgement and non-disclosure agreement, and receive security training. Only individuals that have completed these procedures are granted physical and logical access to the corporate and production environments, as required by their job responsibilities. In addition, all employees are required to complete annual security training, and they receive regular security awareness training via informational emails, talks and presentations, and resources available on our intranet.

Employee access to the Dropbox environment is maintained by a central directory and authenticated using a combination of strong passwords, passphrase-protected SSH keys, two-factor authentication, and OTP tokens. Remote access requires the use of VPN protected with two-factor authentication, and any special access is reviewed and vetted by the security team.

Access to corporate and production networks is strictly limited based on defined policies. For example, production network access is SSH key-based and restricted to engineering teams requiring access as part of their duties. Firewall configuration is tightly controlled and limited to a small number of administrators.

In addition, our internal policies require employees accessing production and corporate environments to adhere to best practices for the creation and storage of SSH private keys.

Access to other resources, including data centers, server configuration utilities, production servers, and source code development utilities are granted through explicit approval by appropriate management. A record of the access request, justification, and approval are recorded by management, and access is granted by appropriate individuals.

Dropbox employs technical access controls and internal policies to prohibit employees from arbitrarily accessing user files and to restrict access to metadata and other information about users' accounts. In order to protect end user privacy and security, only a small number of engineers responsible for developing core Dropbox services have access to the environment where user files are stored. All employee access is promptly removed when an employee leaves the company.

As Dropbox becomes an extension of our customers' infrastructure, they can rest assured that we are responsible custodians of their data. See the **Privacy** section below for more details.

Physical security

Infrastructure

Physical access to subservice organization facilities where production systems reside are restricted to personnel authorized by Dropbox, as required to perform their job function. Any individuals requiring additional access to production environment facilities are granted that access through explicit approval by appropriate management.

A record of the access request, justification, and approval are recorded by management, and access is granted by appropriate individuals. Once approval is received, a responsible member of the infrastructure team will contact the appropriate subservice organization to request access for the approved individual. The subservice organization enters the user's information into their own system and grants the approved Dropbox personnel badge access and, if possible, biometric scan access. Once access is granted to approved individuals, it is the data center's responsibility to ensure that access is restricted to only those authorized individuals.

Corporate offices

- Physical security. The Dropbox Physical Security Team is responsible for enforcing physical security policy and overseeing the security of our offices.
- Visitor and access policy. Physical access to corporate facilities, other than public entrances and lobbies, is restricted to authorized Dropbox personnel and registered visitors who are accompanied by Dropbox personnel. A badge access system ensures only authorized individuals have access to restricted areas within the corporate facilities.
- Server access. Access to areas containing corporate servers such as server rooms is restricted to authorized personnel via elevated roles granted through the badge access system. The lists of authorized individuals approved for physical access to corporate and production environments are reviewed at least quarterly.

Compliance

There are many different compliance standards and regulations that may apply to your organization. Our approach is to combine the most accepted standards with compliance measures geared to the specific needs of our customers' businesses or industries.

ISO

The International Organization for Standardization (ISO) has developed a series of world-class standards for information and societal security to help organizations develop reliable and innovative products and services. At Dropbox, we have ISO-certified our data centers, technology, systems, applications, people, and processes by an independent third-party, Netherlands-based EY CertifyPoint, which maintains its ISO accreditations from the Raad voor Accreditatie (Dutch Accreditation Council).

ISO 27001 (Information Security)

ISO 27001 is recognized as the premier information security management system (ISMS) standard around the world that leverages the best practices detailed in ISO 27002. To be worthy of your trust, we're continually and comprehensively managing our physical, technical, and legal controls at Dropbox.

View the Dropbox Business, Enterprise, and Education ISO 27001 certificate

ISO 27017 (Cloud Security)

ISO 27017 is a new international standard for cloud security that provides guidelines for security controls applicable to the

provision and use of cloud services. The security, privacy, and compliance requirements that Dropbox and its customers can solve together are explained in our **Shared Responsibility Guide**.

View the Dropbox Business, Enterprise, and Education ISO 27017 certificate

ISO 27018 (Cloud Privacy and Data Protection)

ISO 27018 is an emerging international standard for privacy and data protection that applies to cloud service providers like Dropbox who process personal information on behalf of their customers and provides a basis for which customers can address common regulatory and contractual requirements or questions.

View the Dropbox Business, Enterprise, and Education ISO 27018 certificate

ISO 22301 (Business Continuity)

ISO 22301 is an international standard for business continuity that guides organizations on how to decrease the probability of disruptive events and respond to them appropriately if they occur by minimizing potential damage. The Dropbox business continuity management system (BCMS) is part of our overall risk management strategy to protect people and operations during times of crises.

View the Dropbox Business, Enterprise, and Education ISO 22301 certificate

SOC

The Service Organization Controls (SOC) Reports, known as either the SOC 1, SOC 2, or SOC 3, are frameworks established by the American Institute of Certified Public Accountants (AICPA) for reporting on internal controls implemented within an organization. Dropbox has certified its operations, processes, and technology by an independent third-party auditor, Ernst & Young LLP.

SOC 3 for Security, Confidentiality, Integrity, Availability, and Privacy

The SOC 3 assurance report covers the five Trust Service Principles of Security, Confidentiality, Integrity, Availability, and Privacy (TSP Section 100). The Dropbox general-use report is an executive summary of the SOC 2 report and includes the independent third-party auditor's opinion on the effective design and operation of our controls.

View the Dropbox Business, Enterprise, and Education SOC 3 examination

SOC 2 for Security, Confidentiality, Integrity, Availability, and Privacy

The SOC 2 report provides customers with a detailed level of controls-based assurance, covering the five Trust Service Principles of Security, Confidentiality, Processing Integrity, Availability, and Privacy (TSP Section 100). The SOC 2 report includes a detailed description of Dropbox's processes and more than 100 controls that we have in place to protect your stuff. In addition to our independent third-party auditor's opinion on the effective design and operation of our controls, the report includes the auditor's test procedures and results for each control. The SOC 2 examination for Dropbox Business, Enterprise, and Education is available **upon request**.

SOC 1 / SSAE 16 / ISAE 3402 (formerly SAS 70)

The SOC 1 report provides specific assurances for customers who determine that Dropbox Business, Enterprise, or Education is a key element of their internal controls over financial reporting (ICFR) program. These specific assurances are primarily used for our customers' Sarbanes-Oxley (SOX) compliance. The independent third-party audit is conducted in accordance with the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and the International Standard on Assurance

Engagements No. 3402 (ISAE 3402). These standards have replaced the deprecated Statement on Auditing Standards No. 70 (SAS 70). The SOC 1 examination for Dropbox Business, Enterprise, and Education is available **upon request**.

Cloud Security Alliance: Security, Trust, and Assurance Registry (CSA STAR)

The CSA Security, Trust & Assurance Registry (STAR) is a free, publicly-accessible registry that offers a security assurance program for cloud services, thereby helping users assess the security posture of cloud providers they currently use or are considering contracting with.

Dropbox Business, Enterprise, and Education have received the CSA STAR Level 2 Certification, a third-party independent assessment of our security controls by EY CertifyPoint based on the requirements of ISO 27001 and the CSA Cloud Controls Matrix (CCM) v.3.0.1, a set of criteria that measures the capability levels of cloud services. Dropbox Business has also completed the CSA STAR Level 1 Self-Assessment, a rigorous survey based on CSA's Consensus Assessments Initiative Questionnaire (CAIQ), which aligns with the CCM, and provides answers to almost 300 questions a cloud customer or a cloud security auditor may wish to ask.

View our CSA STAR Level 1 Self-Assessment and Level 2 Certification on the CSA website

HIPAA/HITECH

Dropbox signs Business Associate Agreements (BAAs) with US-based 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 makes available a mapping of our internal practices and recommendations for customers who are looking to meet the HIPAA/HITECH Security and Privacy Rule requirements with Dropbox Business, Enterprise, or Education.

Customers interested in requesting these documents can contact our sales team at **sales@dropbox.com**. If you're a current Dropbox Business team admin, you can sign a BAA electronically from the Account page in the **Admin Console**.

For more details, see our **Getting Started with HIPAA** guide.

Students and Children (FERPA and COPPA)

Dropbox Business, Enterprise, and Education allows customers to use the services in compliance with the vendor obligations imposed by the US Family Education Rights and Privacy Act (FERPA). Educational institutions with students under the age of 13 can also use Dropbox Business, Enterprise, or Education consistent with the Children's Online Privacy Protection Act (COPPA), provided that they agree to specific contractual provisions requiring the institution to obtain parental consent regarding the use of our services.

PCI DSS

Dropbox is a Payment Card Industry Data Security Standard (PCI DSS) compliant merchant. However, Dropbox Business, Enterprise, and Education are not meant to process or store credit card transactions. The PCI Attestation of Compliance (AoC) for our merchant status is available upon request through the sales team (**sales@dropbox.com**) or the Account page in the **Admin Console**.

For more information about Dropbox Business, Enterprise, and Education compliance

Visit **dropbox.com/business/trust/compliance**

Privacy

People and organizations trust Dropbox with their most important work files every day, and it's our responsibility to protect those files and keep them private.

Privacy policy

Our privacy policy is available at **dropbox.com/privacy**. The Dropbox Privacy Policy, Business Agreement, Terms of Service, and Acceptable Use Policy provide notice of the following terms:

- What kind of data we collect and why
- With whom we may share information
- How we protect this data and how long we retain it
- Where we keep and transmit your data
- What happens if the policy changes or if you have questions

ISO 27018

Dropbox Business is one of the first major cloud service providers to achieve certification with ISO 27018—an emerging global standard for privacy and data protection in the cloud. ISO 27018 was published in August 2014 and was designed specifically to address user privacy. The standard lays out many requirements regarding how Dropbox will and won't use your organization's information:

- **Your organization is in control of your data.** We only use the personal information you give us to provide you the services you signed up for. You can add, modify, or delete files from Dropbox when you need to.
- **We'll be transparent about your data.** We'll be transparent about where your data resides on our servers. We'll also let you know who our trusted partners are. We'll tell you what happens when you close an account or delete a file. Lastly, we'll tell you if any of these things change.
- **Your data is safe and secure.** ISO 27018 is designed as an enhancement to ISO 27001, one of the most accepted information security standards in the world. We received ISO 27001 certification in October 2014, and the requirements for security and privacy under ISO 27018—such as those around encryption and strict employee access controls—go hand in hand.
- **You can verify our practices.** As part of our adherence to ISO 27018 and ISO 27001, we will undergo annual audits by an independent third party to maintain these certifications. You can **view our ISO 27018 certificate**.

Transparency

Dropbox is committed to transparency in handling law enforcement requests for user information, as well as the number and types of those requests. We scrutinize all data requests to make sure they comply with the law and are committed to giving users notice, as permitted by law, when their accounts are identified in a law enforcement request.

These efforts underscore our commitment to guarding the privacy of our users and their data. To this end, we maintain a **transparency report** and have established a set of Government Request Principles. The following principles govern our actions when receiving, scrutinizing, and responding to government requests for our users' data:

- **Be transparent.** Online services should be allowed to report the exact number of government data requests received, the number of accounts affected by those requests, and the laws used to justify the requests. We'll continue to advocate for the right to provide this important information.
- **Fight blanket requests.** Government data requests should be limited to specific people and investigations. We'll resist requests directed to large groups of people or that seek information unrelated to a specific investigation.

- **Protect all users.** Laws authorizing governments to request user data from online services shouldn't treat people differently based on their citizenship or where they live. We'll work hard to reform these laws.
- **Provide trusted services.** Governments should never install backdoors into online services or compromise infrastructure to obtain user data. We'll continue to work to protect our systems and to change laws to make it clear that this type of activity is illegal.

Our transparency reports can be viewed at **dropbox.com/transparency**

EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield

When transferring data from the European Union, the European Economic Area, and Switzerland, Dropbox relies upon a variety of legal mechanisms, including contracts with our users. Dropbox is certified and complies with the EU-U.S. and Swiss-U.S. Privacy Shield frameworks as set forth by the U.S. Department of Commerce and the European Commission regarding the collection, use, and retention of personal information transferred from the European Union, the European Economic Area, and Switzerland to the United States. You can find Dropbox's Privacy Shield certification at **www.privacyshield.gov/list**. You can also learn more about Privacy Shield at **www.privacyshield.gov**.

Adhering to the Privacy Shield Principles ensures that an organization provides adequate privacy protection under the EU data protection directive. Complaints and disputes related to our Privacy Shield compliance are investigated and resolved through JAMS, an independent third party. To learn more, please see our Privacy Policy at **dropbox.com/privacy.**

EU General Data Protection Regulation (GDPR)

The General Data Protection Regulation 2016/679, or GDPR, is a European Union regulation that marks a significant change to the existing framework for processing personal data of individuals in the EU. The GDPR introduces a series of new or enhanced requirements that will apply to companies like Dropbox which handle personal data. It takes effect on 25 May 2018 and will replace the current EU Directive 95/46 EC, better known as the Data Protection Directive. Like all responsible companies, Dropbox is continuing to build and execute on our detailed GDPR compliance plans and are on the way to full compliance in advance of 25 May 2018. For more information, please see **dropbox.com/help/9314**.

Dropbox Trust Program

Trust is the foundation of our relationship with millions of people and businesses around the world. We value the confidence you've put in us and take the responsibility of protecting your information seriously. To be worthy of your trust, we built and will continue to grow Dropbox with an emphasis on security, compliance, and privacy.

The Dropbox Trust Program policy establishes a risk assessment process, which is designed to address environmental, physical, user, third party, applicable laws and regulations, contractual requirements and various other risks that may affect system security, confidentiality, integrity, availability, or privacy. Performance reviews occur at least annually. More information about the Dropbox Trust Program is available at **dropbox.com/business/trust**.

Summary

Dropbox Business offers easy-to-use tools to help teams collaborate effectively, while providing the security measures and compliance certifications organizations require. With a multi-layered approach that combines a robust back-end infrastructure with a customizable set of policies, we provide businesses a powerful solution that can be tailored to their unique needs. To learn more about Dropbox Business, contact our sales team at **sales@dropbox.com**.

About Dropbox Business

Dropbox lets you bring your docs, photos, and videos anywhere and share them easily. Keep files up to date across multiple devices and stay in sync with your team—effortlessly. Dropbox Business also offers administrative tools, phone support, and as much space as you need.