Dropbox for Business security
A Dropbox whitepaper

Dropbox

Contents

Millions of users trust Dropbox to easily and reliably store, sync, and share photos, videos, docs, and other files across devices. Dropbox for 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 for 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.

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.

Admin management features

No two organizations are exactly alike, so we've developed a number of tools that empower admins to customize Dropbox for Business to their teams' particular needs. Below are several control and visibility features available via the Dropbox for 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 for 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 manage passwords and basic account security, and create a team-member activity log. Support admins have the tools to address common service requests from team members, like restoring deleted files or helping team members locked out of two-step authentication. Any team member can be set as a support admin.
- User provisioning methods
    - Email invitation. A tool in the Dropbox for Business admin console allows administrators to manually generate an email invitation.
    - Active Directory. Dropbox for Business administrators can automate the creation and removal of accounts from an existing Active Directory system via our Active Directory connector (currently

in beta to select customers) or third-party identity provider. Once integrated, Active Directory can be used to manage membership.

  - Single sign-on (SSO). Dropbox for 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 (SAML), 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.

- Enterprise installer. Admins requiring scaled provisioning can use our enterprise installer for Windows to install Dropbox 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. Admins and users can create and manage lists of members within Dropbox and easily give them access to specific folders. Admins can edit their teams' groups, view and manage specific team members' groups, and choose whether team members can create groups.
- Two Dropboxes. Each user can choose to connect a personal and a work Dropbox across all devices to enable clear separation of business and personal data. Admins can enable or block desktop client access to this feature for team members.
- Sharing permissions. Dropbox for Business account administrators can control whether team members are able to share items with people outside the team, and set different rules for shared folders and shared links. If sharing outside the team is enabled, members will still be able to make individual folders or links "team only" as needed. Admins can also set shared links to be visible to team members only by default.
- 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.

Visibility

- User activity reports. Dropbox for Business admins can generate activity reports at any time for several types of events, filtered by date range. Reports are available for individual users or entire team accounts and can be downloaded in CSV (comma-separated values) format. In addition, admins can integrate their team account activity logs directly into SIEM (security information and event management) or other analysis tools through third-party partner solutions. The following information is available to admins in user activity reports:
  - Passwords. Changes to password or two-step verification settings. Admins do not have visibility

into users' actual passwords.

- **Logins.** Successful and failed sign-ins to the Dropbox website
- **Admin actions.** Changes to settings in the admin console, such as shared folder permissions
- **Apps.** Linking of third-party apps to Dropbox accounts
- **Devices.** Linking of computers or mobile devices to Dropbox accounts
- **Sharing.** Events for both shared folders and shared links, including creating/joining shared folders and sending/opening shared links to documents. In many cases, reports will specify whether actions involve non-team members.
- **Membership.** Additions to and removals from team
- **Groups.** Creation, deletion, and membership information for groups

Summaries of team activity are viewable from the Admin Console. Comprehensive account activity information is available by downloading a report through the Admin Console or integrating with log analysis tools. Additionally, individual file and folder events (edits, deletions, and shared folder membership) can be tracked from each user's Events page.

- **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 for 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 for Business customers have the ability to restore lost files and recover unlimited 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.

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 a user all folders they are currently a member of, as well as any shared folders they have left (with the option to rejoin). A user who owns shared folders can view all members of the folder, revoke folder access for specific users, and transfer folder ownership from this page. Each shared folder's owner can also control whether it can be shared with people outside the team, if others with edit permissions can manage membership, and if files within the folder can be shared with people outside the folder.
- **Links page.** Here, a user can view all active sharing links and the creation dates for each. It also allows

a user to track all links shared from others, and disable currently active links.

- **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

- **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 favorited files.** By default, files are not stored on the internal storage of mobile devices. Dropbox mobile clients feature the ability to mark individual files as favorites, saving them to the device for offline viewing. When a device is unlinked from a Dropbox account, via either the mobile or web interface, favorites are automatically deleted from the device's internal storage.

Shared file and folder permissions

- **View-only permissions for shared folders.** This access allows members of a shared folder to always see the latest versions of the files without having the ability to edit them.
- **Passwords for shared links.** Any shared link can be protected to ensure only collaborators with an owner-defined password can access shared files or folders.
- **Expirations for shared links.** Users can set an expiration for any shared link to provide temporary access to files or folders.

Dropbox for Business API integrations

Through the Dropbox for 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 for 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 for Business account. Apply company policies to your Dropbox for Business deployment and meet regulatory compliance requirements.
- **eDiscovery and legal hold.** Respond to litigation, arbitration, and regulatory investigations with data from your Dropbox for Business account. Search for and collect relevant electronically stored

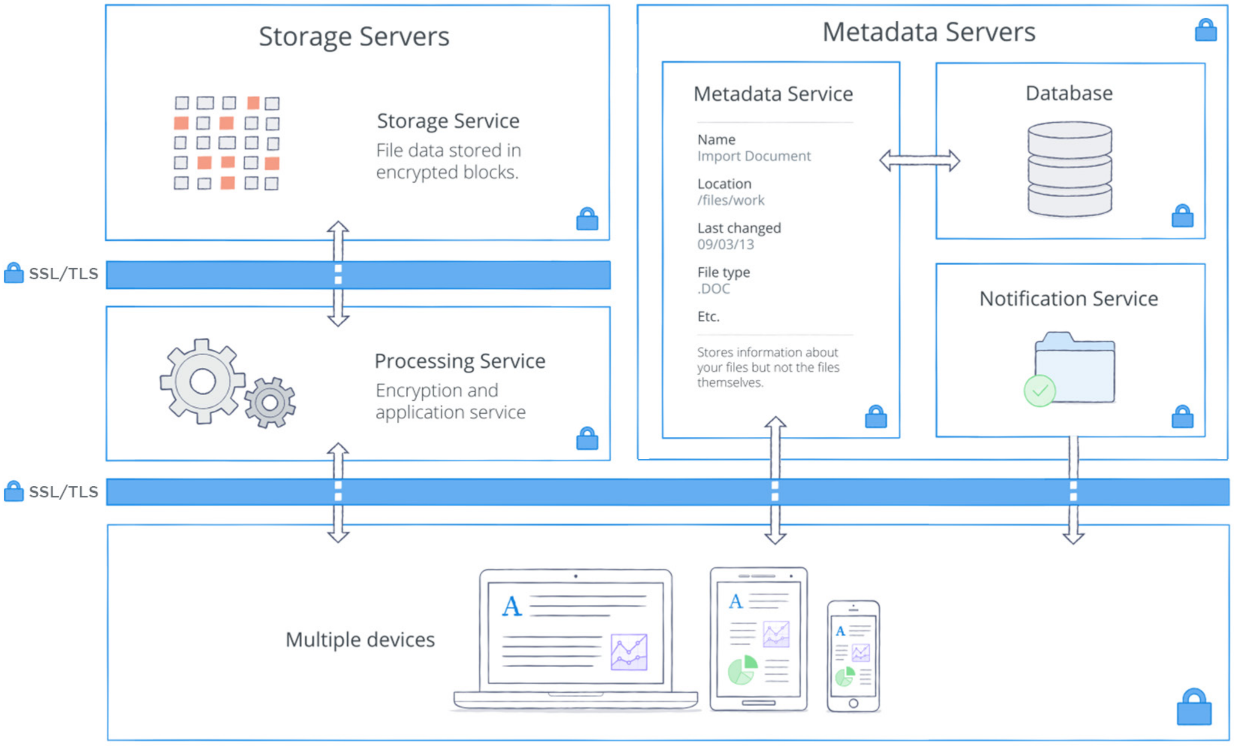
information, and preserve your data through the eDiscovery process, saving your business time and money.

- 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 for 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 for 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 for Business, admins are empowered to deploy and manage business-critical applications for their team. It's especially useful for enterprise customers, as Dropbox for 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 for Business API.

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:

- Encryption and application 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.

Sync

Dropbox sync mechanisms ensure fast, responsive file transfers and enable anywhere access to data across devices.

- **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 by users, this feature looks for new and updated files on the computers of other Dropbox users on the same Local Area Network (LAN). This bypasses the need to download the file from Dropbox servers. A layer of authentication verifies that the user account linked to the computer should have access to the updated files over the LAN.

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. Redundant copies of metadata are distributed across independent devices within a data center in an N+2 availability model. Hourly incremental and daily full backups are performed on all metadata. Dropbox file block storage uses systems including third-party providers that are designed to provide 99.999999999% durability.

This feature, beyond protecting user data, provides high availability of the Dropbox service. In the event of a failed connection to the Dropbox service, a client will gracefully resume operation when a connection is re-established. 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.

In the event of a service availability outage, Dropbox users still have access to the lasted synced copies of their files in the local Dropbox folder on linked devices. Copies of files synced in the Dropbox desktop client/local folder will be accessible from your hard drive during downtime, outages, or when offline.

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

We maintain a business continuity plan (BCP) 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. Our BCP identifies internal and external threats and specifies how people, processes, and infrastructure will be mobilized to prevent and recover from disruptions.

Disaster recovery

To address information security requirements during a major crisis or disaster impacting Dropbox for 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. A durability disaster is defined as a complete or permanent loss of primary metadata data centers, or lost ability to communicate or serve data from metadata data centers. An availability disaster is defined as an outage greater than 10 days, or lost ability to communicate or serve data from storage service/data centers.

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 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 current managed service provider for processing and storage is responsible for the logical and network security of Dropbox services provided through their infrastructure. Connections are protected through the managed service provider’s 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.

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 favoriting of files for offline access.
- **In-product integrations.** We've also created integrations with popular software packages that enable limited access to Dropbox within their interfaces.
  - **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.
  - **Gmail extension.** This Google Chrome browser extension allows users to attach Dropbox files, preview linked Dropbox files, and save attachments to Dropbox directly from the Gmail web interface. Non-public files can only be accessed through Gmail if the user is signed in to Dropbox in the same browser

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.

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 only the 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.

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 Core API and Drop-ins

The Core API and Drop-ins allow developers to offer users in-app access to Dropbox files.

Core API. The Dropbox Core API provides user-level access to Dropbox for developers, and works as a flexible way to read and write to Dropbox. Auth, file, and metadata interaction; shared folder/link interaction; and file operations are all handled through the Core API. Apps using the Core API can be built with one of the three 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 also request file/folder access via Drop-ins (see below).
- File type. The file type permission gives apps access to all files of a specific type (such as text or image files) across a user's entire Dropbox. In addition, the app may also request file/folder access via Drop-ins.
- Full Dropbox. The app receives full access to all the files and folders in a user's Dropbox, as well as request file/folder access via Drop-ins.

Drop-ins. Drop-ins allow easy access to Dropbox with just a few lines of code. Chooser enables selection of files from Dropbox, while 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 for Business API

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

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

Like the Core API and Drop-ins, the Dropbox for Business API uses OAuth 2.0 for authenticating all API requests. Dropbox for 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 for Business account administrator through the standard OAuth 2.0 flow to install their application on a Dropbox for Business account.

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

Dropbox developers

App permission types

There are four different types of Dropbox for 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

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 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 accessed by 100 or fewer users. In order for the app to become accessible to the general public, developers must apply for production status.
    - **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.

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
- VPN front-end 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. All 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.

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.

- Change management
- Penetration testing
- Vulnerability rewards program

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 like iSEC Partners, other industry security teams, and the security research community to keep our applications secure.

The results of tests are assessed by Security personnel, and priorities are assigned to items as assessed by the Security team. As a necessary component of our ISMS, findings and recommendations which 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 personnel.

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 for 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
- 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

Employee policy and access

Upon hire, each Dropbox employee is required to complete a background check and sign a security policy acknowledgement and non-disclosure agreement. 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 take part in mandatory security training for new hires, annual security education certification, and receive regular security awareness training via informational emails, talks/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 between networks is strictly limited to the minimum number of employees and services. 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 is restricted to authorized Dropbox personnel. A badge access system ensures only authorized individuals can have corporate facilities access.
- **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 — like ISO 27001 and SOC 2 — with compliance measures geared to the specific needs of our customers' businesses or industries. Dropbox, our data centers, and our managed service provider undergo regular third-party audits.

ISO 27001. ISO 27001 is recognized as the premier information security standard around the world. Our information security management program was validated by an independent third-party, Netherlands-based Ernst & Young CertifyPoint, which maintains ISO accreditation from the Raad voor Accreditatie (Dutch Accreditation Council) as a member of the International Accreditation Forum (IAF). ISO 27001 certificates issued by Ernst & Young CertifyPoint are recognized as valid in all countries with IAF membership. Our ISO 27001 certificate can be viewed at **www.dropbox.com/static/business/resources/dropbox-certificate-iso-27001.pdf**.

ISO 27018. ISO 27018 is an emerging international standard for privacy and data protection that applies to cloud service providers, like Dropbox, that process personal information on behalf of their customers. This certification demonstrates our commitment to privacy and data protection practices and provides a basis for which our customers can address common regulatory and contractual requirements or questions. Our ISO 27018 certificate is available at **www.dropbox.com/static/business/resources/dropbox-certificate-iso-27018.pdf**.

SOC 1, 2, and 3. We also undergo the following Service Organization Control (SOC) examinations, conducted by Ernst & Young LP. A report is available for each:

- SOC 3. This audit covers the Security, Confidentiality, and Processing Integrity Trust Services Principles, and provides customers with the American Institute of Certified Public Accountants (AICPA) SysTrust Seal of assurance. The report generated as part of this audit is an executive summary of our SOC 2 report and includes our independent third-party auditor's opinion on the effective design and operation of our controls. It can be viewed at **cert.webtrust.org/soc3_dropbox.html**.
- SOC 2 Type II. This audit provides customers with a detailed level of controls-based assurance and covers the Security, Confidentiality, Processing Integrity, and Availability Trust Services Principles. Our SOC 2 report includes a detailed description of our processes and the nearly 100 controls we have in place to protect customer data. This report is available upon request.
- SOC 1 / SSAE 16 / ISAE 3402 (formerly SAS 70). This audit assists customers with internal controls over financial reporting (ICFR) programs, and is primarily used for customers' Sarbanes-Oxley (SOX) compliance. The independent third-party examination for this report is conducted in accordance with Standards for Attestation Engagements No. 16 (SSAE 16) and International Standard on Assurance Engagements No. 3402 (ISAE 3402), which have replaced the previous Statement on Auditing Standards No. 70 (SAS 70) standard. This report is available upon request.

We will continue to participate in regular compliance audits, and current SOC reports will be made available as they are completed.

Dropbox also reviews SOC reports for all subservice organizations. In the event a SOC report is unavailable, we perform security site visits at new facilities to verify applicable physical, environmental, and operational security controls satisfy control criteria and contractual requirements. Procedures for the identification and resolution of security breaches are reviewed as well. We will evaluate additional certifications and compliance standards, and share updates as we receive them.

Dropbox is a Payment Card Industry Data Security Standard (PCI DSS) compliant merchant. However, Dropbox for Business is not meant to process or store credit card transactions. Dropbox provides customers with a PCI Attestation of Compliance (AoC) for our merchant status.

CSA STAR. Dropbox is also a member of the Cloud Security Alliance (CSA), a non-profit organization that promotes and provides education around cloud security best practices. The Dropbox for Business security self-assessment is now available on the CSA's Security, Trust & Assurance Registry (STAR), a publicly available registry that details the security controls, assurance requirements, and maturity levels of various cloud computing services. Our Level 1 Self-Assessment documents how our security practices map to the CSA's best practices and industry-accepted standards.

More information on Dropbox compliance policies is available at **www.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 **www.dropbox.com/privacy**. The Dropbox Privacy Policy, 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 for 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 data 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 at **www.dropbox.com/static/business/resources/dropbox-certificate-iso-27018.pdf**.

U.S.-E.U. and U.S.-Swiss Safe Harbor

Dropbox is certified and complies with the U.S.-EU Safe Harbor framework as set forth by the US Department of Commerce and the European Commission regarding the collection, use, and retention of personal data from EU member states. Dropbox is also certified and complies with the U.S.-Swiss Safe

Harbor framework as set forth by the US Department of Commerce and the Federal Data Protection and Information Commissioner of Switzerland.

Adhering to the seven Safe Harbor Principles ensures an organization provides adequate privacy protection under the EU data protection directive. Complaints and disputes related to our Safe Harbor compliance are investigated and resolved through JAMS, an independent third party.

Both our privacy and Safe Harbor policies can be applied to data protection requirements in most countries worldwide. More information on the Safe Harbor framework can be found at **www.export.gov/safeharbor**, including a searchable list with our current certification status.

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.

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 **www.dropbox.com/business/trust**.

Summary

Dropbox for 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 for Business, contact our sales team at **sales@dropbox.com**.

About Dropbox for 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 for Business also offers administrative tools, phone support, and as much space as you need.