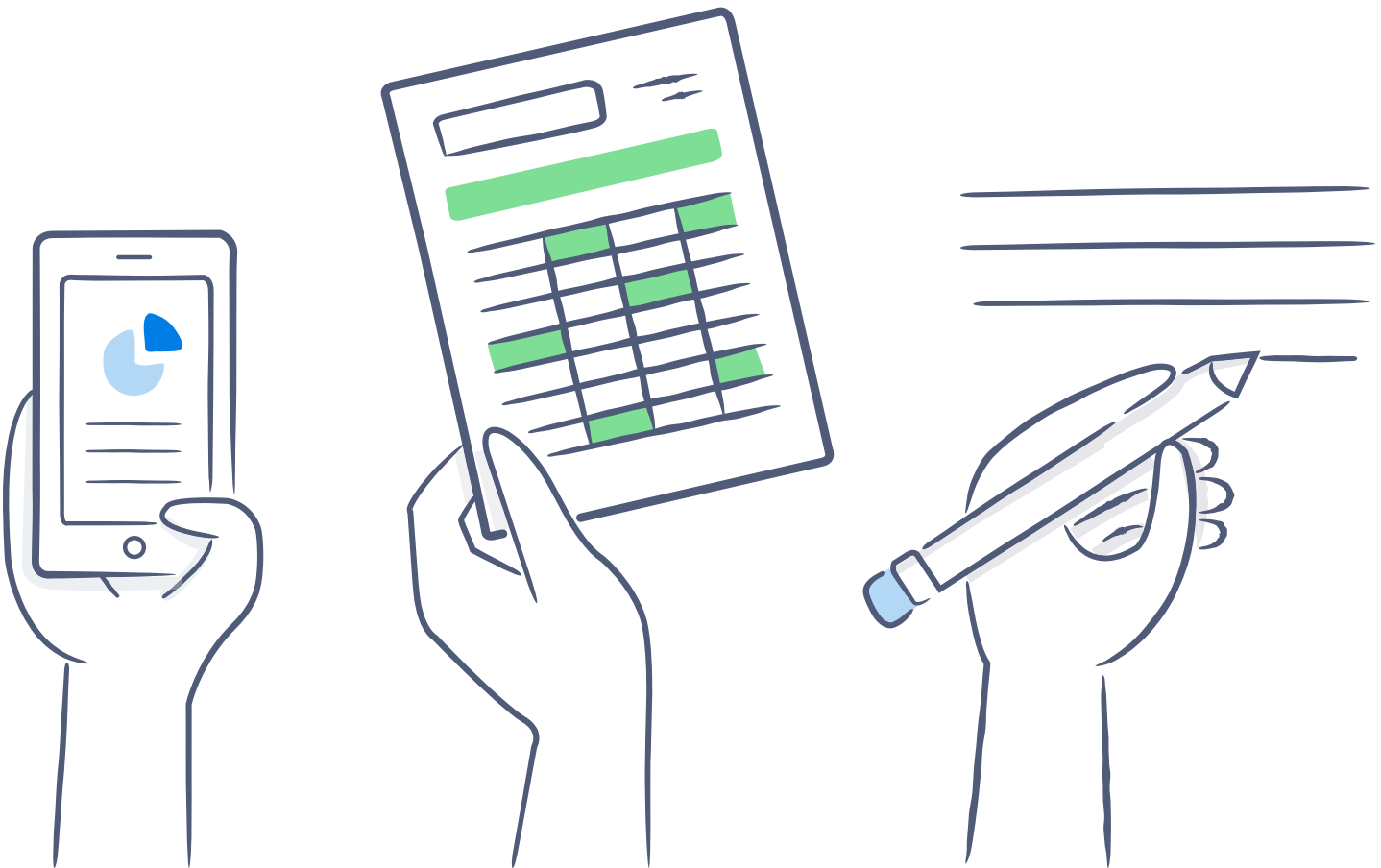
Dropbox Business

Shared responsibility: Working together to keep your data secure



Dropbox Business

Shared responsibility: Working together to keep your data secure

Dropbox works with its Business, Enterprise, and Education customers to keep their data secure. We take comprehensive measures to protect our infrastructure, network, and applications; train employees in security and privacy practices; build a culture where being worthy of trust is the highest priority; and put our systems and practices through rigorous third-party testing and auditing.

While Dropbox is responsible for securing each aspect of the service that's under our control, customers play a key role in ensuring their teams and data are protected and secure. As the admin of a Dropbox Business, Enterprise, or Education team, you have the ability to configure, use, and monitor your account in ways that meet your organization's security, privacy, and compliance needs.

We've put together this guide to help you understand what Dropbox does to keep your account safe, and what you can do to maintain visibility and control over your team's data.

Dropbox's responsibilities

Build security into our architecture

Thousands of businesses around the world trust us to protect their most important files. To earn that trust, we work hard to build secure products that admins like you can rely on. Here are some of the ways that we secure our architecture and networks.

Distributed architecture

Dropbox's architecture distributes different levels of information across multiple services. This 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.

Secure networks

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. Access to the production environment is restricted to only authorized IP addresses and requires multi-factor authentication on all endpoints.

Encrypt user data

Dropbox Business, Enterprise, and Education customers interact with our systems through our mobile, desktop, and web applications, and APIs. Regardless of which app you're using, we protect your files both in transit and at rest.

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 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.

Maintain a reliable service

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 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. For file block storage, Dropbox uses both in-house and third-party systems that are designed to provide annual data durability of at least 99.999999999%.

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.

Limit employee access to backend systems

We know that when you, as a Dropbox Business, Enterprise, or Education customer, store your files with Dropbox, you expect us to be responsible stewards of your data. As part of this responsibility, we make sure that Dropbox employee access to our internal systems is strictly controlled. To start, access between our corporate and production networks is strictly limited. 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. 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.

Maintain employee security and privacy awareness

Part of keeping our service secure is making sure that people who work at Dropbox understand how to be security conscious and recognize suspicious activity. To that end, Dropbox employees are required to acknowledge security policies prior to being granted systems access. Employees also take part in mandatory security and privacy training for new hires and annual follow-up training, and receive regular security awareness training via informational emails, talks, presentations, and resources available on our intranet.

Validate our practices

To help us make sure that our security practices are working as intended, we use third parties to assess their effectiveness. Specialists perform periodic penetration and vulnerability tests on Dropbox's corporate and production environments. Identified issues are prioritized and remediated by our security engineering team. Additionally, third-party auditors evaluate our security practices against international and industry standards. To help you learn more about and evaluate Dropbox's practices, we make our SOC 3 report, and ISO 27001, 27017, 27018, and 22301 certificates available online. You can also request our SOC 2 report, a HIPAA requirements mapping and assessment report, and penetration testing result summaries under a non-disclosure agreement (NDA).

Communicate issues to you

Status of the service

Dropbox makes available a third-party site that communicates the status of our service to Dropbox Business, Enterprise, and Education customers. As a current customer, you can visit status.dropbox.com at any time to view the current site status, as well as past disruptions and maintenance.

Breach notification

Dropbox will notify you in the event of a data breach, as required by applicable law. We maintain incident response policies and procedures, including a breach notification process, which enables us to notify affected customers as needed. If you've entered into a HIPAA Business Associate Agreement or an EU Data Processing Agreement, you will be notified as detailed in those agreements.

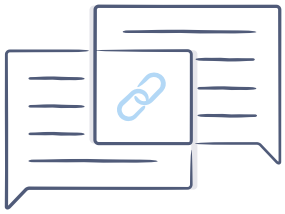
Give you the tools you need to be secure

We want you and other Dropbox Business, Enterprise, and Education admins to have the tools you need to make responsible, informed decisions about your team's security. To help you configure, use, and monitor your account in a way that meets your needs, your Admin Console comes equipped with security features for you to enable on behalf of your team. Through guides like this, our Dropbox Business Security Whitepaper, the Help Center, and our support team, we provide information to help you understand how these settings can help you responsibly configure your account.

Customer responsibilities

Learn about our practices

Determining if Dropbox Business, Enterprise, or Education is the right fit for your company's needs is an important process. We encourage you to take the time to validate our practices, as you would with any other application. To give you the tools you need to verify our security practices, our ISO 27001, 27017, 27018, and 22301 certificates; SOC 3 assurance report; and CSA STAR Level 1 Self-Assessment and Level 2 Certification are available online. We can also provide access to additional documentation under a non-disclosure agreement to help you make an informed decision. This includes our SOC 1 and SOC 2 audit reports, and a mapping of our internal practices and recommendations for customers who are looking to meet the HIPAA/HITECH Security and Privacy Rule requirements, and summaries of our latest application penetration tests. Our Terms of Service, Acceptable Use Policy, and Standard Business Agreement are available online for you to review and make sure that Dropbox Business, Enterprise, or Education is a good fit for your team.



Configure sharing and viewing permissions

Dropbox Business, Enterprise, and Education gives you flexibility to configure your account to support your security, collaboration, and privacy needs. Admins can review and modify these settings through the Admin Console to reflect their sharing or regulatory environment. For example, accounts can be configured so files, folders, and links can't be shared with people outside of your team. When team members create shared folders, they can further customize the folders' settings and choose the appropriate level of access—edit or view-only.

Strengthen authentication

Strong authentication practices help keep your team's data safe. Admins should review available authentication settings and enable those best suited to protecting their accounts. Dropbox Business, Enterprise, and Education accounts include the following options:

Two-step verification

Team admins can require that members use two-step verification to sign in to their accounts. This highly recommended security feature adds an extra layer of protection to users' Dropbox accounts. Once 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.

Single sign-on (SSO)

If your company already manages password policies and authentication with a central identity provider, you may want to set up single sign-on for your Dropbox Business team. By using your existing SSO provider, your team members don't have to remember yet another password. More importantly, authenticating access to Dropbox will be managed using the same password policies as other services at your company.

Conduct regular access reviews

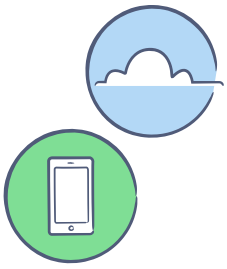
Access to your team's account should evolve as your team membership, internal roles, and devices change. You should frequently check to make sure that only appropriate people, devices, and apps have access to your account to help keep your information in the right hands. Modifying or removing access is simple through the Admin Console.

Team members

Team members can be easily added, removed, and reviewed from the Admin Console. To ensure sensitive data in your Dropbox Business, Enterprise, or Education account can only be accessed by the right people, we recommend frequently reviewing this list. You can then remove access when someone leaves your organization or no longer requires access due to a change in job role. Similarly, you can modify team members' roles in the Admin Console so that each user account has the appropriate level of access.

Devices

You and your team members should frequently review devices linked to your account and remove unused or unauthorized devices. Devices can be unlinked by both team members and team admins. You or your team member also have the option to remotely wipe Dropbox content from you device when unlinking . Unlinking and wiping devices can keep your data secure in the event of loss or theft, or if someone is leaving your team.

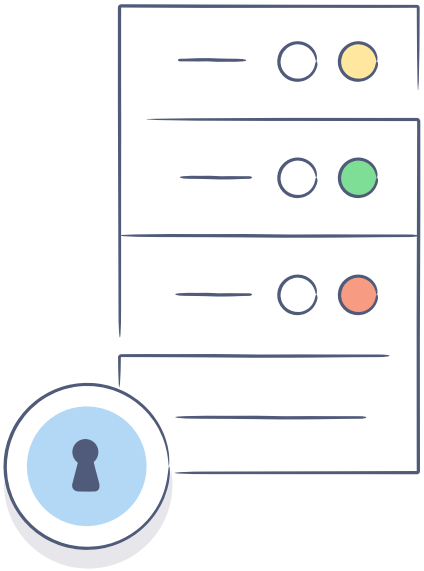


Third-party apps

There is a robust ecosystem of third-party apps that you can link to your Dropbox Business account to gain added functionality. Integrations that provide services such as SIEM, DLP, and identity management can be powerful tools in strengthening your existing security practices. While these third-party apps and integrations can be great complements to your account, it's important to remember that they're not part of our included services. Therefore, they're not covered by the Dropbox Terms of Use or Business Agreement, including a Business Associate Agreement or Data Processing Agreement, which you may have signed with Dropbox. Apps may ask you for various levels of access to your information depending on their service offering. As an admin, you can link or remove team apps—which apply to your entire account—and remove individual apps which team members may have added to their own account. Third-party apps and access can be reviewed and modified through the admin console.

Monitor for unusual activity

As a team admin, you can view and export reports that detail your team's file events, sharing, authentication, and administrator activities. Admins should regularly review these activity reports to keep an eye out for any unusual activity and help keep your team secure. You may also want to consider using a third-party SIEM or other monitoring integration to enhance your capabilities.



Determine encryption needs

Dropbox by default stores a local copy of your files on your computer to make sure you have the files you need right at your fingertips. The local copies of your files are as protected as any other files on your computer. To help keep them secure, we recommend that you enable disk encryption on your devices whenever possible, and require a strong password to access your laptop, phone, tablets, or any device that provides access to your Dropbox account.

Dropbox protects files you upload to your account by automatically splitting those files into discrete blocks and encrypting each block using 256-bit Advanced Encryption Standard (AES). Dropbox manages the encryption keys on behalf of our customers to keep this process simple for users, and to enable certain features.

Dropbox Business, Enterprise, and Education members may choose to also encrypt files before uploading them to Dropbox on their own or through a third-party integration. However, users encrypting data before uploading it to Dropbox are responsible for managing those encryption keys. Encrypting files before uploading them to Dropbox may also reduce the functionality of some features.

Customers interested in learning more about how Dropbox approaches security are encouraged to review the Security Whitepaper, available on our website: dropbox.com/business/articles-videos. To learn more about Dropbox Business, and to request third-party audit reports under a non-disclosure agreement, contact sales@dropbox.com.