Dropbox

Security Measures

Dropbox has implemented and will maintain appropriate administrative, technical and physical safeguards to protect Stored Data as set forth below. Dropbox may update these Security Measures from time to time, provided however that Dropbox will notify Customer if Dropbox updates the Security Measures in a manner that materially diminishes the administrative, technical or physical security features described herein.

1. Services Security.

   1.1. Dropbox Architecture. Dropbox's Services are designed with multiple layers of protection, covering data transfer, encryption, network configuration and application-level controls that are distributed across a scalable, secure infrastructure. For example, End Users of Dropbox Business, Business Plus, Standard, Advanced, Enterprise, and Education ("Core FSS") can access files and folders at any time from the desktop, web and mobile clients. Such clients connect to secure services to provide access to files, allow file sharing with others, and update linked devices when files are added, changed or deleted. The Services can be utilized and accessed through a number of interfaces. Each has security settings and features that process and protect user data while ensuring ease of access.

   1.2. Encryption. To protect Stored Data in transit between Dropbox and Customer, 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, or other cipher with at least equivalent key strength. File data at rest is encrypted using 256-bit AES encryption, or cipher with at least equivalent key strength. Dropbox's 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 are distributed for decentralized processing.

   1.3. Reliability. The Services are developed with multiple layers of redundancy to guard against data loss and ensure availability.

   1.4. User Management Features. End Users of Core FSS as of the Effective Date of the Agreement have the ability to restore lost files and recover previous versions of files, ensuring changes to files can be tracked and retrieved, with the exception of files that have been permanently deleted by an End User which cannot be restored or recovered as a result of the design of Core FSS. The Services offers a two-step authentication procedure which adds an extra layer of protection.

2. Information Security.

   2.1. Policies. Dropbox has established a thorough set of security policies covering 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. Dropbox personnel are notified of updates to these policies and are provided security training.

   2.2. Personnel Policy and Access. Dropbox's internal policies require onboarding procedures that include background checks (to the extent allowed by local laws), security policy acknowledgement, communicating updates to security policy, and non-disclosure agreements. All personnel access is promptly removed when an employee or contractor leaves the company. Dropbox employs technical access controls and internal policies to prohibit employees and contractors from arbitrarily accessing user files and to restrict access to metadata and other information about end users' accounts. In order to protect end user privacy and security, only a small number of employees and contractors have access to the environment where end user files are stored. A record of access request, justification and approval are recorded by management and access is granted by appropriate individuals.

2.3. Network Security. Dropbox maintains network security and monitoring techniques that are designed to provide multiple layers of protection and defense. Dropbox employs industry-standard protection techniques, including firewalls, network security monitoring, and intrusion detection systems to ensure only eligible traffic is able to reach Dropbox's infrastructure.

2.4. Change Management. Dropbox ensures that security-related 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 systems that directly support the Services. Changes to Dropbox's infrastructure are restricted to authorized personnel only. Changes to the application level of the Services 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.

2.5. Compliance. Dropbox, its data center providers, and its managed service provider undergo regular third party security audits. Dropbox will continue to participate in regular Service Organization Controls 2 (SOC 2) audits. Dropbox also reviews SOC 1 and/or SOC 2 reports for all subservice organizations. In the event a SOC 1 and/or SOC 2 report is unavailable, Dropbox performs security site visits to verify applicable physical, environmental, and operational security controls satisfy control criteria and contractual requirements. Dropbox evaluates additional certifications and compliance attestations, as made available to Dropbox by the subservice providers, on an ongoing basis. Excluded Features are not included in the scope of the SOC reports.

3. Physical Security

3.1. 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.

3.2. Office. Dropbox maintains a physical security team that is responsible for enforcing physical security policy and overseeing the security of our corporate offices. Access to areas containing corporate services is restricted to authorized personnel via elevated roles granted through the badge access system.

4. Continued Evaluation. Dropbox will conduct periodic reviews of its information security policies and procedures as measured against industry security standards and will continually evaluate whether additional or different security measure are required to respond to new security risks or findings generated by periodic reviews.