Dropbox Business

# Felles ansvar: Samarbeid for å holde dataen sikker

Dropbox samarbeider med sine Business- og Education-kunder om å holde dataene sikre. Vi iverksetter omfattende tiltak for å beskytte vår infrastruktur, vårt nettverk og våre apper, vi lærer opp ansatte i sikkerhets- og personvernpraksis, vi bygger en kultur hvor det å være verdig tillit er den høyeste prioritet, og vi utsetter våre systemer og rutiner for grundig testing og revisjon via tredjeparter.

Selv om Dropbox er ansvarlig for å sikre hvert aspekt av tjenesten som er under vår kontroll, spiller kundene en viktig rolle i å forsikre at teamene og dataene deres er beskyttet og sikkert. Som administrator av et Dropbox Business- eller Education-team har du muligheten til å konfigurere, bruke og overvåke kontoen din på måter som oppfyller organisasjonens krav til sikkerhet, personvern og overholdelse.

Vi har lagd denne veiledningen for å hjelpe deg forstå hva Dropbox gjør for å holde kontoen din trygg, og hva du kan gjøre for å opprettholde synlighet og kontroll over teamets data.

# Dropbox sitt ansvar

## Bygg sikkerhet inn i arkitekturen

Tusenvis av bedrifter over hele verden setter sin lit til oss for å beskytte det viktigste arbeidet deres. For å gjøre oss fortjent til denne tilliten jobber vi hardt med å lage sikre produkter som administratorer som deg kan stole på. Her er noen av metodene vi bruker for å sikre vår arkitektur og våre nettverk.

### Distribuert arkitektur

Dropbox' arkitektur distribuerer ulike informasjonsnivåer på tvers av flere tjenester. Dette gjør ikke bare synkronisering raskere og mer pålitelig, det øker også sikkerheten. Programarkitekturen til Dropbox forhindrer at tilgang til tjenester brukes til å gjenskape filer eller Paper-dokumenter.

### Sikre nettverk

Det opprettholdes en streng atskillelse mellom det interne Dropbox-nettverket og det offentlige nettet. Trafikk som skal via nettet, og som kommer til og fra produksjonsnettverket, kontrolleres nøye gjennom en egen proxy-tjeneste som igjen er beskyttet av restriktive brannmurregler. Tilgang til produksjonsmiljøet er utelukkende begrenset til autoriserte IP-adresser og krever autentisering med flere faktorer på alle endepunkter.

## Kryptert brukerdata

Dropbox Business- og Education-kunder samhandler med våre systemer via våre mobilapper, skrivebordsprogrammer, webapper og API-er. Uavhengig av hvilken app du bruker, beskytter vi filene dine og dataen i Paper-dokumentene dine både når de brukes og ikke.

### Data under overføring

For å beskytte data under overføring mellom Dropbox-apper og serverne, bruker Dropbox Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for dataoverføring, som oppretter en sikker tunnel som beskyttes av 128-bits AES-kryptering eller høyere. Fildata i transitt mellom en Dropbox-klient (for tiden skrivebord, mobil, API eller nett) og den vertsbaserte tjenesten, blir kryptert med SSL/TLS. På liknende vis vil Paper-dokumentdata i transitt mellom en Paper-klient

(for tiden mobil, API eller nett) og de vertsbaserte tjenestene krypteres via SSL/TLS. For sluttpunkt som vi kontrollerer (skrivebord og mobil) og moderne nettlesere, bruker vi avanserte kodenøkler og støtter fullkomment hemmelighold av videresending og sertifikatlås. I tillegg flagger vi alle informasjonskapsler for autentisering på nettet som sikre og aktiverer HTTP Strict Transport Security (HSTS) med includeSubDomains aktivert.

For å forhindre mellomleddsangrep blir autentisering av Dropbox-frontservere utført via offentlige sertifikater hos klienten. En kryptert tilkobling forhandles før overføringen av filer eller Paper-dokumenter, noe som sørger for sikker levering av filer til Dropbox sine frontservere.

**Inaktive data**

Dropbox-filer i hvile krypteres med 256-bit Advanced Encryption Standard (AES). Filene lagres i flere datasentre i separate filblokker. Hver blokk blir fragmentert og kryptert ved hjelp av en kraftig chiffer. Bare blokker som har blitt endret mellom revisjoner, blir synkronisert. Paper-dokumenter i stillstand krypteres også med bruk av 256-bit Advanced Encryption Standard (AES). Paper-dokumenter lagres i flere tilgjengelighetssoner med bruk av tredjepartssystemer.

# Opprettholde en pålitelig tjeneste

Et lagringssystem er bare så godt som det er pålitelig, og på grunn av dette utviklet vi Dropbox med flere lag av redundans for å beskytte mot tap av data og for å sikre tilgjengelighet. Overflødige kopier av metadata er fordelt over selvstendige enheter innenfor et datasenter i minst en N+2-tilgjengelighetsmodell. Trinnvise sikkerhetskopier av metadata tas hver time og komplette sikkerhetskopier utføres hver tredje dag. Metadata lagres på servere som Dropbox administrerer og er vert for. For filblokklagring bruker Dropbox egne og tredjeparts lagringssystemer som er designet for å levere en årlig dataholdbarhet på minst 99,999999999 %.

Dersom det mot formodning skulle forekomme tjenesteavbrudd, har Dropbox-brukere fremdeles tilgang til den siste synkroniserte kopien av filene sine i den lokale Dropbox-mappen på tilkoblede datamaskiner. Kopier av filer som synkroniseres i skrivebordsklienten / den lokale mappen for Dropbox, vil være tilgjengelige fra brukernes harddisk under nedetider, avbrudd eller når de er frakoblet Internett.

På samme måte fordeles overflødige kopier av Paper-dokumentdata over selvstendige enheter innenfor et datasenter i en N+1-tilgjengelighetsmodell, og vi har konfigurert for daglige fullstendige sikkerhetskopier av Paper-dokumentdata. For lagring av Paper-dokumenter bruker Dropbox tredjepartssystemer som er designet for å levere en årlig dataholdbarhet på minst 99,999999999%. Dersom det mot formodning skulle forekomme tjenesteavbrudd, har brukere fremdeles tilgang til de siste synkroniserte kopiene av sine Paper-dokumenter i «offline»-tilstand i mobilapplikasjonen.

# Begrensert tilgang for ansatte til backend-systemer

Vi vet at når du, som Dropbox Business- eller Education-kunde, lagrer filene og Paper-dokumentene dine i Dropbox, forventer du at vi skal være ansvarlige forvaltere av dine data. Som en del av dette ansvaret sørger vi for at Dropbox-ansattes tilgang til våre interne systemer er strengt kontrollert. Tilgangen mellom våre bedrifts- og produksjonsnettverk er strengt begrenset. For eksempel er produksjonsnettverkstilgang SSH-nøkkelbasert og begrenset til ingeniørteam som trenger tilgang for å utføre oppgavene sine. Brannmurkonfigurasjonen er strengt kontrollert og begrenset til et lite antall administratorer. Tilgang til andre ressurser, inkludert datasentre, konfigureringsverktøy for servere, produksjonsservere og verktøy for utvikling av kildekode gis ved eksplisitt godkjenning av aktuell ledelse. En oppføring av tilgangsforespørselen, rettferdiggjørelsen og godkjenningen blir registrert av ledelsen, og tilgang blir gitt av egnede personer.

# Opprettholde bevissthet blant ansatte om sikkerhet og personvern

Et aspekt ved å opprettholde sikkerheten til tjenesten vår er å sørge for at folk som jobber i Dropbox, forstår hvordan man skal være sikkerhetsbevisst og gjenkjenne mistenkelig aktivitet. For å nå dette målet er Dropbox-ansatte pålagt å godta sikkerhetsretningslinjer før de får tilgang til systemene. Alle som ansettes, deltar også på obligatorisk sikkerhets- og personvernsopplæring for nyansatte, årlig oppfølgingsopplæring og får jevnlig sikkerhetsbevissthetstrening via informerende e-poster, foredrag, presentasjoner og ressurser tilgjengelige på intranettet.

# Valider praksisen vår

For å sikre at våre sikkerhetsrutiner fungerer etter hensikten, bruker vi tredjeparter til å vurdere hvor effektive rutinene er. Spesialister utfører periodiske inntrengnings- og sårbarhetstester i Dropbox' bedrifts- og produksjonsmiljøer. Identifiserte problemer prioriteres og utbedres av vårt sikkerhetsteam. I tillegg evaluerer tredjepartskontrollører våre sikkerhetsrutiner mot internasjonale standarder og bransjestandarder. Hvis du vil lære mer om og evaluere Dropbox' praksiser, er vår SOC 3-rapport og våre ISO 27001-, 27017-, 27018- og 22301- sertifikater tilgjengelig på nettet. Du kan også be om vår SOC 2-rapport, en vurderings- og testrapport om HIPAA-krav, en vurdering og rapport for BSI C5 (tilgjengelig på engelsk og tysk), og sammendrag av inntrengningstestresultatene under en avtale om taushetsplikt (NDA).

# Kommunisering av spørsmål til deg

### Status for tjenesten

Dropbox gjør en tredjeparts nettsted tilgjengelig som kommuniserer statusen for tjenesten vår til Dropbox Business- og Education-kunder. Som eksisterende kunde kan du gå til status.dropbox.com når som helst for å se gjeldende anleggsstatus, samt tidligere forstyrrelser og vedlikehold.

### Bruddvarsling

Dropbox varsler deg om eventuelle datainnbrudd, i henhold til gjeldende lover. Vi følger retningslinjer og prosedyrer for hendelsesrespons, inkludert en bruddvarslingsprosess som gjør oss i stand til å varsle berørte kunder etter behov. Hvis du har inngått en HIPAA-avtale for forretningsforbindelser eller en EU-databehandlingsavtale, vil du bli varslet som beskrevet i disse avtalene.

# Vi gir deg verktøyene du trenger for å være sikker

Vi ønsker at du og andre Dropbox Business- og Education-administratorer har de verktøyene dere trenger for å ta ansvarlige og informerte beslutninger om teamets sikkerhet. For å hjelpe deg med å konfigurere, bruke og overvåke kontoen din på en måte som innfrir dine krav, er Administratorverktøy utstyrt med sikkerhetsfunksjoner som du kan aktivere på vegne av teamet ditt. Gjennom veiledninger som denne, vår sikkerhetshvitebok for Dropbox Business, vårt hjelpesenteret og vårt kundestøtteteam gir vi informasjon for å hjelpe deg med å forstå hvordan disse innstillingene kan hjelpe deg konfigurere kontoen din på en ansvarlig måte.

# Kundens ansvar

## Lær om våre praksiser

Det å avgjøre om Dropbox Business eller Education innfrir din bedrifts behov er en viktig prosess. Vi anbefaler deg å bruke tid på å validere praksisen vår, slik du ville gjort med andre programmer. For å gi deg de verktøyene du trenger for å bekrefte våre sikkerhetsrutiner, er ISO 27001-, 27017-, 27018- og 22301- sertifikatene, SOC 3 -rapporten og CSA STAR-vurderingen på nivå 1 og sertifiseringen på nivå 2 tilgjengelige på nettet. Vi kan også gi tilgang til ytterligere dokumentasjon under en taushetsavtale for å hjelpe deg i å ta en informert avgjørelse. Dette inkluderer SOC 1- og SOC 2-revisjonsrapportene våre, C5-vurderingsrapporten vår (tilgjengelig på engelsk og tysk), og en kartlegging av våre interne rutiner og anbefalinger for kunder som ønsker å overholde kravene i HIPAA-/HITECH-reglene for sikkerhet, personvern, og bruddvarsling, samt sammendrag av våre nyeste programinntrengningtester. Våre vilkår for bruk, retningslinjer for akseptabel bruk og standard forretningsavtale er tilgjengelig på nettet slik at du kan lese gjennom og evaluere om Dropbox Business eller Education er en god løsning for ditt team.

## Konfiguring av deling og visning av tillatelser

Dropbox Business og Education gir deg fleksibiliteten til å konfigurere kontoen din for å oppfylle kravene dine til sikkerhet, samarbeid og personvern. Administratorer kan se gjennom og endre disse innstillingene via Administratorverktøy, slik at de tilpasses med hensyn til deling og tilsyn. For eksempel kan man konfigurere kontoer slik at mapper, koblinger og Paper-dokumenter kan deles med personer utenfor teamet. Når teammedlemmene oppretter delte mapper for Dropbox-filer kan de tilpasse innstillingene for mapper ytterligere og velge passende tilgangsnivå, dvs. redigering eller skrivebeskyttet.

# Styrket godkjenning

Grundige godkjenningspraksiser bidrar til å holde teamets data trygge. Administratorer bør gjennomgå tilgjengelige godkjenningsinnstillinger og aktiver de som passer best til å beskytte kontoene. Dropbox Business- og Education-kontoer inkluderer følgende alternativer:

### Totrinns verifisering

Teamadministratorer kan kreve at medlemmene bruker to-trinns verifisering for å logge på kontoen sin. Denne høyt anbefalte sikkerhetsfunksjonen gir et ekstra lag med beskyttelse på en brukers Dropbox-konto. Når to-trinns verifisering er aktivert, krever Dropbox en sekssifret sikkerhetskode eller sikkerhetsnøkkel i tillegg til passord når du logger på eller tilknytter en ny datamaskin, mobiltelefon eller nettbrett.

### Single Sign-On (SSO)

Hvis bedriften din allerede administrere passordrutiner og godkjenning med en sentral identitetsleverandør, kan det være lurt å konfigurere Single Sign-On for ditt Dropbox Business- eller Education-team. Hvis du bruker din eksisterende SSO-leverandør, trenger ikke teammedlemmene å huske enda et passord. I tillegg vil godkjenningstilgang til Dropbox administreres ved hjelp av de samme passordretningslinjene som andre tjenester i bedriften.

# Gjennomfør regelmessig tilgangsgjennomgang

Tilgangen til teamets konto bør utvikles etter hvert som teamets medlemskap, interne roller og enheter endrer seg. Du bør jevnlig kontrollere at kun de riktige personene, enhetene og appene har tilgang til kontoen din, slik at informasjonen alltid er i rette hender. Det er enkelt å endre eller fjerne tilgang via Administratorverktøy.

### Teammedlemmer

Teammedlemmer kan enkelt legges til, fjernes og gjennomgått fra Administratorverktøy. For å være sikker på at sensitive data i Dropbox Business- eller Education-kontoen kun kan åpnes av riktige personer, anbefaler vi jevnlig gjennomgang av denne listen. Deretter kan du fjerne tilgangen når noen forlater organisasjonen eller ikke lenger trenger tilgang på grunn av en endring i jobbrollen. På samme måte kan du endre teammedlemmenes rolle i Administratorverktøy, slik at hver brukerkonto har korrekt tilgangsnivå.

### Enheter

Du og dine teammedlemmer bør ofte gjennomgå hvilke enheter som er knyttet til kontoen, og fjerne ubrukte eller uautoriserte enheter. Både teammedlemmer og teamadministratorer kan fjerne forbindelser for enheter. Du og teammedlemmene dine har også muligheten til å eksternt slette Dropbox-innhold fra enheten når koblingen fjernes. Ved å fjerne forbindelse for og slette innhold på enheter kan du sikre dataene dine i tilfelle tap eller tyveri, eller hvis noen forlater teamet ditt.

### Tredjepartsapper

Det finnes et robust økosystem av tredjepartsapper som du kan koble til Dropbox Business- eller Education-kontoen din for å legge til flere funksjoner. Integrasjoner som tilbyr tjenester som SIEM, DLP og identitetshåndtering kan være kraftige verktøy som vil forbedre dine eksisterende sikkerhetsrutiner. Selv om disse tredjepartsappene og -integrasjonene kan være gode supplement til kontoen din, er det viktig å huske på at de ikke er en del av våre inkluderte tjenester. De dekkes derfor ikke av Dropbox' vilkår for bruk eller forretningsavtale, inkludert eventuell avtale for forretningsforbindelser eller databehandlingsavtale som du har inngått med Dropbox. Appene kan be deg om ulike tilgangsnivåer til informasjonen din avhengig av appens tjenestetilbud. Som administrator kan du forbinde eller fjerne teamapper, som gjelder for hele kontoen, og fjerne enkeltapper som teammedlemmer kan ha lagt til sin egen konto. Tredjepartsapper og -tilgang kan gjennomgås og endres gjennom Administratorverktøy.

# Overvåk for å oppdage uvanlig aktivitet

Som teamadministrator kan du vise og eksportere rapporter som viser teamets filhendelser, delingsaktiviteter, godkjenningsaktiviteter og administratoraktiviteter i detalj. Administratorer bør jevnlig gjennomgå disse aktivitetsrapportene for å holde et øye med eventuell uvanlig aktivitet, og således bidra til sikkerheten i teamet. Det kan også være lurt å bruke en tredjeparts SIEM eller annen overvåkingsintegrasjon for bedre sikkerhet.

# Avgjør krypteringsbehovet

Dropbox lagrer som standard en lokal kopi av filene på datamaskinen din for å være sikker på at du har de filene du trenger lett tilgjengelig. De lokale kopiene av filene dine er like beskyttet som alle andre filene på datamaskinen din. For å bidra til sikkerheten anbefaler vi at du aktiverer diskkryptering på enhetene når det er mulig, og bruker et sterkt og unikt tilgangspassord på din bærbare PC, telefon, nettbrett eller hvilken som helst enhet som gir tilgang til din Dropbox-konto. Ved å bruke sterke og unike passord på enhetene dine vil du også beskytte tilgangen til Paper-dokumentene dine.

Dropbox beskytter filene du laster opp til kontoen din ved å automatisk dele disse filene inn i atskilte blokker og kryptere hver blokk med 256-biter Advanced Encryption Standard (AES). På samme måte beskytter Dropbox Paper-dokumentene ved å kryptere dem når de ikke brukes i fast lager med 256-bit AES (Advanced Encryption Standard). Dropbox administrerer krypteringsnøklene på vegne av våre kunder for å gjøre prosessen enkel for brukerne og for å aktivere visse funksjoner.

Dropbox Business- og Education-medlemmer kan velge å kryptere filene selv eller via en tredjeparts integrering før filene lastes opp til Dropbox. Men brukerne som krypterer dataene før opplasting til Dropbox, er ansvarlig for å administrere disse krypteringsnøklene. Hvis du krypterer filene før du laster dem opp til Dropbox, kan det også føre til redusert funksjonalitet av noen funksjoner.

Kunder som er interessert i å lære mer om Dropbox' tilnærming til sikkerhet, oppfordres til å lese gjennom sikkerhetshviteboken som er tilgjengelig på nettstedet vårt: dropbox.com/business/trust. Hvis du vil vite mer om Dropbox Business eller Education, eller vil be om tredjeparts revisjonsrapporter under en avtale om taushetsplikt, kan du kontakte sales@dropbox.com.