Adobe Acrobat DC:n ja Document Cloud -palveluiden tietoturvan yleiskuvaus

Sisältö

Vaikka Adobe Sign on osa Document Cloud PDF -palveluita, sen tietoturvatoiminnot ovat erilliset.

Lyhyt yhteenveto

Adobe pitää digitaalisten kokemusten tietoturvaa erittäin tärkeänä. Tietoturvakäytännöt ovat juurtuneet syvälle sisäiseen ohjelmistokehitykseemme, toimintaprosesseihimme ja työkaluihimme. Eri toimintoja edustavat ryhmät pystyvät estämään, tunnistamaan ja käsittelemään ongelmia nopeasti, kun ne noudattavat näitä käytäntöjä. Pysymme ajan tasalla viimeisimpien uhkien ja haavoittuvuuksien suhteen tekemällä yhteistyötä yhteistyökumppanien, johtavien tutkijoiden, tietoturvatutkimuslaitosten ja muiden teollisuuden organisaatioiden kanssa. Sovellamme säännöllisesti edistyneitä suojaustekniikoita tarjoamiimme tuotteisiin.

Adoben palvelut, jotka koskettavat asiakkaan sisältöä, ovat suorittaneet useita alan hyväksyntiä. Katso yksityiskohtainen luettelo kaikista Adoben tuotteiden ja ratkaisujen tukemista vaatimustenmukaisuuden hyväksynnistä ja standardeista sekä viranomaissäädöksistä täältä: Hyväksynnät, standardit ja säädökset. Lue lisätietoja EU:n tietosuoja-asetuksesta sivulta GDPR-valmius.

Tämä White Paper kuvaa Adoben toteuttamaa syvällisen puolustuksen lähestymistapaa ja suojausmenettelyjä Adobe Acrobat DC:n, Acrobat Reader DC:n, Document Cloudin, Document Cloud -palveluiden ja niihin liittyvien tietojen suojauksen parantamiseksi.

Acrobat DC:n ja Document Cloud -palveluiden esittely

Adobe Acrobat DC auttaa organisaatioita vastaamaan asiakkaiden jatkuvien yhteyksien ja tuottavuuden tarpeisiin millä tahansa laitteella yhdistämällä viimeisimmän Acrobat-tietokoneohjelmiston Acrobat Reader -mobiilisovelluksen premium-ominaisuuksiin ja Adobe Document Cloudin verkkopalveluihin. Acrobat DC:n ja Document Cloud -palveluiden avulla asiakkaat voivat muuntaa sisällön digitaaliseksi dokumentiksi, joka voidaan jakaa muiden kanssa, ja luoda kätevästi, käsitellä ja muuntaa PDF-tiedostoja mistä tahansa Adoben pilvipalvelusta, tietokonesovelluksesta tai mobiilisovelluksesta.

Acrobat-dokumenttien tietoturvaominaisuudet

Hävitys

Adobe Acrobat DC:ssä on hävitystyökalujen sarja, jonka avulla asiakkaat voivat suojata arkaluonteisia tai luottamuksellisia tietoja, kuten poistaa pysyvästi sekä tekstin että kuvat dokumentista ennen sen jakelua. Lisäksi käyttäjät voivat hakea ja hävittää kaavojen mukaan tietoja, kuten puhelinnumerot, luottokorttien numerot ja sähköpostiosoitteet. Hävitetyt tiedot poistetaan kokonaan tiedostosta eikä niitä vain peitetä, kuten muilla työkaluilla tai menetelmillä tehdään. Dokumentin puhdistustoiminnolla asiakkaat voivat poistaa myös piilotietoja ja muita kuin kuvaobjekteja, kuten metatietoja, joita voi olla PDF-tiedostossa.

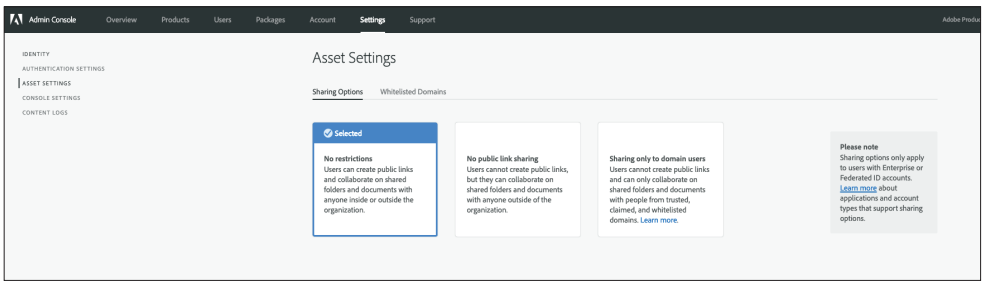
Tiedostojen jako

Kaikki pilveen tallennetut Document Cloud -tiedostot merkitään automaattisesti ”yksityisiksi”, mikä tarkoittaa, että ne näkyvät vain ne sinne ladanneelle käyttäjälle. Käyttäjän on tehtävä nimenomaisia toimia sisällön jakamiseksi, tai se jää yksityiseksi. Document Cloudin kaikki sisältö jaetaan lähettämällä linkki Document Cloudin sisältöön vastaanottajalle sähköpostitse, tekstiviestinä tai millä tahansa yhteistyöohjelmistolla.

Document Cloud -palveluiden käyttäjät voivat jakaa tiedostoja kahdella tavalla: Vain luku tai Tarkistus. Jos käyttäjä lähettää linkin Vain luku -rajoituksella, vastaanottaja saa tarkastella sisältöä vain luku -dokumenttina. Jos käyttäjä valitsee kuitenkin dokumentin lähetyksen tarkistukseen, vastaanottaja voi kommentoida dokumenttia, mutta ei pysty muokkaamaan tai muuttamaan sitä millään tavalla.

Resurssiasetukset ja jakamisrajoitukset

Resurssiasetusten avulla organisaatio voi hallita sitä, miten työntekijät jakavat resursseja organisaation ulkopuolelle. IT-järjestelmänvalvoja voi valita rajoittavan asetuksen, joka rajoittaa työntekijöitä käyttämästä tiettyjä jakamistoimintoja Document Cloudissa, kuten rajoittaa kutsupohjaisen jakamisen vastaanottajiin, jotka ovat väitetyillä, luotetuilla ja sallituilla toimialueilla. Kun tämä käytäntö on asetettu, käyttäjät eivät voi jakaa organisaation omistamia resursseja ulkoisille käyttäjille, jotka eivät ole sallittujen toimialueiden luettelossa.



Resurssiasetukset hallintakonsolissa

Microsoft Information Protection (MIP)

Jos olet asiakas, joka käyttää Acrobat DC:tä tai Acrobat Reader DC:tä Microsoft Information Protection (MIP) -ratkaisuilla, kuten Azure Information Protection (AIP), suojattujen tiedostojen avaamiseen ja tietojen suojaukseen Microsoft Office 365:n avulla, katso tämä dokumentti.

Acrobat Reader DC:n suojattu tila

Adobe toimittaa hiekkalaatikkoteknologian uusimman toteutuksen, jota kutsutaan suojatuksi tilaksi ja joka esiteltiin Adobe Reader X:ssä. Sen tarkoituksena on suojata asiakkaita haittakoodilta, joka yrittää kirjoittaa tietokoneen tiedostojärjestelmään tai lukea siitä PDF-tiedostojen välityksellä.

Hiekkalaatikko on suojausmenetelmä, joka luo toimiville ohjelmille rajoitetun ohjelmistojen suoritusympäristön vähäisillä oikeuksilla. Hiekkalaatikot suojaavat käyttäjien järjestelmiä, jotta suoritettavaa koodia sisältävät epäluotettavat dokumentit eivät vahingoita niitä. Acrobat Reader DC:n yhteydessä epäluotettava sisältö on mikä tahansa PDF-tiedosto ja sen käynnistämät prosessit. Acrobat Reader DC käsittelee kaikkia PDF-tiedostoja potentiaalisesti vioittuneina ja rajoittaa kaiken PDF-tiedoston käsittelyn hiekkalaatikkoon.

Acrobat Reader DC:n suojattu tila auttaa puolustautumaan sellaisia hyökkääjiä vastaan, jotka yrittävät asentaa tietokonejärjestelmään haittaohjelmia. Tämä tukee organisaation toimia, joilla halutaan estää ei-toivottuja henkilöitä käyttämästä ja poimimasta arkaluonteisia tietoja ja immateriaaliomaisuutta tietokoneesta tai yrityksen tietoverkosta. Suojattu tila otetaan käyttöön oletusarvoisesti, kun käyttäjä käynnistää Acrobat Reader DC:n. Se rajoittaa ohjelmalle annettavaa pääsytasoa. Tämä suojaa Microsoft Windows -laitteita haitallisilta PDF-tiedostoilta, jotka saattavat yrittää kirjoittaa tietokoneen tiedostojärjestelmään tai lukea siitä, poistaa tiedostoja tai muuttaa järjestelmän tietoja muulla tavalla.

Suojattu tila Windows 8:ssa ja uudemmissa voi toimia myös Windows AppContainerissa, mikä antaa vielä vahvemman lukitun ympäristön asiakkaille, jotka ottavat suojatun tilan käyttöön.

Acrobat Reader DC:n suojattu näkymä

Suojattu näkymä vastaa Acrobat Reader DC:n suojattua tilaa. Se on hiekkalaatikkoteknologian toteutus monipuolisia Acrobat DC -ominaisuuksia varten. Acrobat DC -ohjelmistossa Adobe laajentaa suojatun tilan toimintaa niin, että se tekee enemmän kuin kirjoituspohjaisten hyökkäysten eston. Nyt sisällytetään myös lukupohjaiset hyökkäykset, joissa yritetään varastaa arkaluonteisia tietoja tai immateriaaliomaisuutta PDF-tiedostojen avulla.

Suojatun tilan tavoin suojattu näkymä sulkee epäluotettavien ohjelmien (esim. mikä tahansa PDF-tiedosto ja sen käynnistämät prosessit) suorituksen rajoitettuun hiekkalaatikkoon, minkä ansiosta vältetään se, että haitallinen koodi voisi kirjoittaa tietokoneen tiedostojärjestelmään tai lukea siitä PDF-muodon avulla. Suojattu näkymä olettaa, että kaikki PDF-tiedostot ovat mahdollisesti haitallisia, ja rajoittaa käsittelyn hiekkalaatikkoon, ellei nimenomaisesti määritetä, että tiedosto on luotettava.

Suojattua näkymää tuetaan molemmissa skenaarioissa, joissa käyttäjät avaavat PDF-dokumentteja — yksittäisessä Acrobat DC -sovelluksessa ja selaimessa. Suojattu näkymä Windows 8- ja uudemmissa versioissa toimii aina AppContainerissa. Tämä mahdollistaa vielä tehokkaamman lukitun ympäristön asiakkaille, jotka ottavat käyttöön suojatun tilan.

Kun käyttäjä avaa mahdollisesti ei-luotetun tiedoston suojatussa näkymässä, Acrobat DC näyttää viestin katseluikkunan yläreunassa. Viestirivi osoittaa, että tiedostoon ei voi luottaa ja muistuttaa käyttäjää, että hän on suojatussa näkymässä, missä useat Acrobat DC -ominaisuudet eivät ole käytössä, ja käyttäjän vuorovaikutusta tiedoston kanssa on rajoitettu. Oleellista on, että tiedosto on vain-luku -muodossa ja suojattu näkymä puolustaa järjestelmää upotettua tai liittyvää haitallista sisältöä vastaan.

Jos käyttäjä luottaa tiedostoon ja haluaa ottaa kaikki Acrobat DC -toiminnot käyttöön, hän voi napsauttaa kaikkien toimintojen käyttöönottoa osoittavaa painiketta keltaisella viestirivillä. Tämä toiminto poistaa suojatun näkymän käytöstä ja suo tiedostolle pysyvän luotetun aseman lisäämällä sen Acrobatin etuoikeutettujen sijaintien luetteloon. Kaikki luotettavan PDF-tiedoston avaukset tämän jälkeen poistavat käytöstä suojatun näkymän rajoitukset.

Document Cloudin palveluiden arkkitehtuuri

Adobe Document Cloud -palveluihin sisältyy:

- **Organisoi PDF** — PDF-dokumentin sivujen lisäys, poisto, kierto ja järjestely
- **Luo PDF** — Word-, Excel- ja PowerPoint-dokumenttien ja kuvien muunnos PDF-tiedostoiksi
- **Vie PDF** — PDF-tiedostojen kätevä muunnos muokattaviksi Microsoft Word-, Excel-, PowerPoint- tai RTF-tiedostoiksi
- **Muokkaa PDF** — Olemassa olevien PDF-tiedoston muokkaus mobiililaitteella tai kannettavalla tietokoneella
- **Yhdistä PDF** — Useiden tiedostojen yhdistäminen yhdeksi PDF:ksi ja dokumenttipakettien kokoaminen mistä tahansa
- **Send & Track**— Dokumenttien lähetys, seuranta ja toimituksen vahvistus
- **Adobe Scan** — Minkä tahansa sieppaus ja muunnos hakukelpoiseksi, laadukkaaksi PDF-dokumentiksi
- **Adobe Sign** — Dokumenttien valmistelu ja lähetys suojattuun ja luotettuun, juridisesti sitovaan sähköiseen allekirjoitukseen millä tahansa laitteella

Document Cloudin palveluiden tietoturva

Käyttöoikeuksien ja tunnistetietojen hallinta

IT-järjestelmänvalvojat myöntävät loppukäyttäjille käyttöoikeudet Adobe Document Cloudin palveluihin hyödyntämällä nimetyn käyttäjän lisensointia Adoben hallintakonsolissa. Acrobat Document Cloud tukee kolmea (3) erityyppistä nimetyn käyttäjän lisensointia:

- **Adobe ID** — Adoben isännöimille, käyttäjän hallitsemille tileille, joita yksittäiset käyttäjät luovat, omistavat ja valvovat. Adobe ID -tileistä pääsee Acrobat Document Cloudin palveluihin vain, jos IT-järjestelmänvalvoja ottaa käyttöön niihin pääsyn.
- **Enterprise ID** — Adoben isännöimä, yrityksen hallitsema vaihtoehto tileille, jotka asiakkaan yrityksen organisaation IT-järjestelmänvalvojat ovat luoneet ja joita he hallitsevat. Organisaatio omistaa ja hallitsee käyttäjätilejä ja kaikkia liittyviä resursseja.
- **Federated ID** — Yrityksen hallitsema tili, jossa kaikki tunnistetietoprofiilit saadaan organisaation kertasisäänkirjauksen (SSO) käyttäjätietojen hallintajärjestelmästä. Profiilit luo, omistaa ja hallitsee IT-infrastruktuuri. Adobe integroituu useimpien SAML 2.0 -yhteensopivien tunnistetietojen toimittajien kanssa.

Useimmat yritysorganisaatiot käyttävät Enterprise ID:tä tai Federated ID -tunnuksia työntekijöilleen, urakoitsijoilleen ja freelancer-työntekijöille, jos sähköpostiosoite on yrityksen toimialueella, koska näin ne voivat säilyttää sekä käyttöoikeuksien että kyseisen ID:n avulla tallennetun käyttäjän luoman sisällön (UGC) hallinnan. Katso lisätietoja kustakin käyttöoikeustyypistä Adoben asiakastuen sivustolta.

Sekä Adobe ID:n että Enterprise ID:n salasanan tallennuksessa hyödynnetään SHA-256-hajautusalgoritmia yhdessä salasanan salt-arvojen ja useiden hajautusiteraatioiden kanssa. Adobe seuraa jatkuvasti Adoben isännöimiä tilejä epätavallisten tai poikkeavien tilitoimintojen varalta ja arvioi näitä tietoja suojausuhkien vähentämiseksi nopeasti. Adobe ei vastaa käyttäjien salasanojen hallinasta Federated ID -tilien tapauksessa. Lisätietoja on Adoben tunnistetietojen hallintapalveluiden suojauksen yleiskuvauksessa.

Sähköiset ja digitaaliset allekirjoitukset

Document Cloudin palveluiden käyttäjillä on valittavana kaksi työkalua suojattuun työskentelyyn allekirjoituksilla:

- **Fill & Sign -työkalun** avulla, joka perustuu Adobe Signiin, käyttäjät voivat hallita koko allekirjoitusprosessia, joka on Euroopan unionin, Yhdysvaltojen ja useimpien teollisuusmaiden sähköisen allekirjoituksen lakien mukainen. Sen avulla he voivat pyytää allekirjoitusta muilta, seurata allekirjoitusprosessia ja arkistoida allekirjoitettuja dokumentteja ja kirjausketjuja automaattisesti. Suojausta sovelletaan koko prosessiin, ja Adobe sertifioi dokumentit ja kirjausketjut koskemattomuuden osoittavalla sinetillä.

Seuranta ei ole saatavana mobiilikäyttöön.

Lisätietoja Adobe Signista ja sen tietoturvatoiminnoista on Adobe Signin teknisessä yleiskuvauksessa.

- **Certificates-työkalulla** voit allekirjoittaa dokumentteja varmennepohjaisilla digitaalisilla allekirjoituksilla, jotka on saatu Adoben hyväksymän luotettavan luettelon (AATL) tai Euroopan unionin luottamusluettelon (EUTL) luottamuspalvelujen tarjoajilta. Allekirjoitusta kolmannen osapuolen varmenteiden myöntäjän varmennetunnuksella pidetään yleisesti suojattuna dokumenttien sähköisen allekirjoituksen menetelmänä. Tunnus on erityisesti linkitetty allekirjoittajaan ja tunnus pystyy tunnistamaan allekirjoittajan. Allekirjoittajan varmenne on kryptografisesti sidottu dokumenttiin allekirjoitusvaiheen aikana käyttämällä yksityistä avainta, joka on ainoastaan kyseisellä allekirjoittajalla.

  Acrobat DC vahvistaa allekirjoittajan allekirjoituksen — ja allekirjoitetun dokumentin alkuperäisyyden — luomalla automaattisesti yhteyden varmenteiden myöntäjään tarkistusta varten. Tämäntyyppinen allekirjoitus noudattaa PDF:n sähköisten allekirjoitusten standardeja, kuten PDF Advanced Electronic Signature (PAdES) osat 2, 3 ja 4 sekä Yhdysvaltain puolustusministeriön Joint Interoperability Test Command (JITC) -organisaation kryptografian ja julkisen avaimen infrastruktuurin (PKI) käyttöä AES-256:n, RSA-4096:n, SHA- 512:n ja RSA-PSS:n kanssa. Certificates-työkalun avulla käyttäjät voivat myös lisätä aikaleimoja dokumentteihin ja varmentaa ne koskemattomuuden osoittavalla sinetillä.

Document Cloudin palveluiden sisällön tallennus

Vaikka järjestelmänvalvojat jakavat yksittäistä pilvitallennustilaa Enterprise ID- ja Federated ID -tileille Adobe-hallintakonsolin avulla, heillä ei ole suoraa pääsyä mihinkään käyttäjän Document Cloud -palveluiden tallennustilan tiedostoihin. Enterprise ID:n tai Federated ID:n poistaminen tekee mistä tahansa pilvitallennustilassa olevista tiedoista käyttökelvottomia loppukäyttäjälle ja kyseisen käyttäjän tiedot poistetaan 90 päivän jälkeen.

Järjestelmänvalvojat voivat myös allokoida tallennustilaa hallintakonsolilla Adobe ID -tileille. Vaikka järjestelmänvalvojat eivät voi poistaa Adobe ID -tilejä, he voivat peruuttaa sekä myönnetyn tallennustilakiintiön että pääsyn sovelluksiin ja palveluihin. Näihin tileihin liittyvät tiedot poistetaan 90 päivän jälkeen.

Adobe Document Cloud -palvelut hyödyntävät multitenant-tallennusta. Asiakkaan sisältö on käsitelty Amazon Elastic Compute Cloud (Amazon EC2) -esiintymällä ja tallennettu Amazon Simple Storage Services (Amazon S3) -säiliöiden yhdistelmille ja MongoDB-esiintymällä Amazon Elastic Block Store (Amazon EBS) -tallennustilassa. Itse sisältö on tallennettu Amazon S3 -säiliöihin ja sisältöä koskevat metatiedot on tallennettu Amazon EBS -tilaan MongoDB:n avulla — kaikki on suojattu tunnistetietojen ja käyttöoikeuksien hallinnan (IAM) rooleilla kyseisen Amazon Web Services (AWS) -alueen sisällä.

Metatiedot ja tukiresurssit, jotka on tallennettu Amazon EBS -tilaan, on salattu AES 256-bittistä salausta käyttämällä Federal Information Processing Standard (FIPS) 140-2 -standardia, joka on hyväksytty kryptografisille algoritmeille. Ne ovat yhtenäisiä National Institute of Standards and Technology (NIST) 800-57 -suositusten kanssa.

Tiedot on tallennettu vikasietoisesti useisiin datakeskuksiin ja useille laitteille kussakin datakeskuksessa. Kaikki verkkoliikenne käy läpi systemaattisen tietojen todennuksen ja

tarkistussummalaskelmat vioittumisen estämiseksi ja eheyden varmistamiseksi. Lopuksi tallennettu sisältö replikoidaan synkronisesti ja automaattisesti toisiin datakeskuksiin asiakkaan alueella, jotta datan eheys voidaan säilyttää siinäkin tapauksessa, että data katoaisi kahdesta eri paikasta.

Lisätietoja taustalla olevista Amazon-palveluista:

- MongoDB
- Amazon S3
- AWS Key Management Service (KMS)
- Amazon EC2 -palvelu

Erityinen salausavain

Oletusarvoisesti Amazon S3:n tallennettu sisältö ja resurssit on salattu AES 256-bittisillä symmetrisillä suojausavaimilla, jotka ovat uniikkeja kullekin asiakkaalle ja kunkin asiakkaan väitetyille toimialueille. Jos järjestelmänvalvojat haluavat lisätä lisäkerroksen valvontaa ja suojausta organisaationsa joillekin tai kaikille toimialueille, he voivat käyttää erityistä salausavainta, jota AWS KMS hallitsee ja jota kierrätetään automaattisesti vuositasolla.

Järjestelmänvalvojat voivat myös peruuttaa tämän erityisen salausavaimen hallintakonsolilla, mikä tekee kaikista tällä avaimella salatuista tiedoista käyttökelvottomia loppukäyttäjille ja estää sekä sisällön latauksen palvelimeen ja lastauksen, kunnes salausavain on aktivoitu uudelleen.

Huomaa: Vaikka Adobe Document Cloud -tiedostot voidaan salata käyttämällä erityistä salausavainta, metatietoja ei voi salata kyseisellä avaimella.

Lisätietoja salauksen hallinnasta erityisellä avaimella saa näiltä Adoben ohjesivuilta:

- Salauksen hallinta
- Erityisten salausavainten usein kysytyt kysymykset

Amazon Web -palvelut

Kuten aikaisemmin on todettu, kaikki Adobe Document Cloud -palveluiden komponentit isännöidään Yhdysvalloissa AWS:llä, kuten Amazon EC2 ja Amazon S3. Amazon EC2 on web-palvelu, joka antaa automaattisesti skaalattavaa laskentakapasiteettia pilvipalvelusta, mikä tekee laskennasta helpompaa. Amazon S3 on yleisesti tunnustettu erittäin luotettavaksi tietojen tallennuksen infrastruktuuriksi minkä tahansa tietomäärän tallentamiseksi ja noutamiseksi.

AWS-alusta toimittaa palveluita alan käytäntöjen mukaisesti, ja se joutuu läpikäymään alan yleiset hyväksynnät ja auditoinnit (aws.amazon.com/security/). Saat lisätietoja AWS-alustasta ja Amazonin tietoturvan valvonnasta AWS Cloud Security -verkkosivustolta.

AWS:n ja Adoben toimintavastuut

AWS käyttää, hallitsee ja valvoo komponentteja hypervisor-virtualisointikerroksesta alaspäin niiden tilojen fyysiseen suojaukseen, joissa Adobe Document Cloud -palvelut toimivat. Adobe ottaa vastuun ja hallinnan vieraskäyttöjärjestelmästä (myös päivityksistä ja suojauspäivityksistä) ja sovellusohjelmistosta sekä AWS:n järjestämän tietoturvaryhmän palomuurin konfiguroinnista.

AWS toimittaa myös erilaisia peruslaskentaresursseja, kuten tiedonkäsittelyä ja tallennusta ohjaamalla Adoben käyttämää pilvi-infrastruktuuria. AWS-infrastruktuuriin kuuluvat tilat, verkko ja laitteisto sekä suorittava ohjelmisto (esimerkiksi isäntäkäyttöjärjestelmä, virtualisointiohjelmisto jne.), joka tukee näiden resurssien toimitusta. Amazon suunnittelee ja hallitsee AWS-alustaa alan vakiokäytäntöjen ja erilaisten suojauksen vaatimustenmukaisuuden standardien mukaisesti.

Suojattu hallinta

Adobe käyttää Secure Shell (SSH)- ja Secure Sockets Layer (SSL) -protokollia AWS-infrastruktuurin hallintaan.

Asiakkaan tietojen maantieteellinen sijainti AWS-verkossa

Kaikki Document Cloudiin ladattu käyttäjän luoma sisältö on tallennettuna AWS:n Yhdysvaltojen itäosan (Virginia) alueellisissa datakeskuksissa. Sisältö varmuuskopioidaan kussakin datakeskuksessa ja muissa alueen datakeskuksissa alueen sisällä kuormituksen tasapainottamisen ja vikasietoisuuden saavuttamiseksi.

Asiakkaan tunnistetietojen maantieteellinen sijainti AWS-verkossa

Tunnistetiedot on tallennettu usean alueen datakeskuksiin, joiden kuormitus on tasapainotettu. Ne sijaitsevat Virginiassa (US-itä), Oregonissa (US-länsi), Irlannissa (EU-länsi) ja Singaporessa (AP-kaakko). Tunnistetiedot replikoidaan kaikkiin datakeskuksiin. Adobe noudattaa maanrajojen ylittävän tiedonsiirtoa koskevia voimassa olevia lakeja, kuten seuraavassa dokumentissa on tarkemmin selvitetty: https://www.adobe.com/fi/privacy/eudatatransfers.html.

Asiakastietojen eristys / asiakkaiden erottelu

AWS käyttää vahvoja vuokraajan eristyksen suojauksen ja hallinnan toimintoja. Virtualisoituna multitenant-ympäristönä AWS toteuttaa suojauksen hallintaprosesseja ja muuta suojausvalvontaa, mikä on suunniteltu eristämään kukin asiakas muista AWS-asiakkaista. Adobe käyttää AWS:n käyttäjätietojen ja käyttöoikeuksien hallintaa (IAM) rajoittaakseen edelleen pääsyä laskenta- ja tallennusesiintymiin.

Suojattu verkkoarkkitehtuuri

AWS seuraa ja valvoo tiedonsiirtoa verkon ulkorajalla ja tärkeimmillä sisärajoilla käyttämällä verkkolaitteita, kuten palomuuria ja muita rajapintaan liittyviä laitteita. Nämä rajapintalaitteet käyttävät sääntösarjoja, käyttöoikeusluetteloja (ACL) ja konfiguraatioita vahvistaakseen tietojen virtausta tiettyihin informaatiojärjestelmän palveluihin. Käyttöoikeusluettelot tai liikenteen kulkukäytännöt ovat olemassa kussakin hallitussa liitännässä liikenteen kulun hallintaan ja vahvistukseen.

Amazon Information Security hyväksyy kaikki ACL-käytännöt ja työntää ne kuhunkin hallittuun liitäntään käyttämällä AWS ACL-Manage-työkalua, mikä auttaa varmistamaan, että nämä hallitut liitännät vahvistavat kaikkein ajantasaisimpia ACL-luetteloja.

Verkon valvonta ja suojaus

AWS toimittaa korkeatasoisen palvelun suorituskyvyn ja käytettävyyden käyttämällä erilaisia automatisoituja monitorointijärjestelmiä. Valvontatyökalut auttavat havaitsemaan epätavallisia tai hyväksymättömiä toimintoja ja tiloja sisääntulon ja lähdön kommunikaatiopisteissä. AWS-verkko antaa merkittävän suojauksen perinteisissä verkkosuojausasioissa:

- Jaetut palvelunestohyökkäykset (DDoS-hyökkäykset)
- Välistävetohyökkäykset (MITM-hyökkäykset)
- IP-osoitehuijaus
- Portin tutkiminen
- Muiden vuokraajien tekemä pakettien tutkinta

Katso lisätietoja verkon valvonnasta ja suojauksesta AWS-pilvisuojauksen verkkosivustolta.

Tietomurtojen tunnistus

Adobe valvoo Adobe Document Cloud -palveluita aktiivisesti käyttämällä alan vakiojärjestelmiä tietomurtojen tunnistukseen (IDS) ja tietomurtojen estojärjestelmiä (IPS).

Tallennus lokitiedostoon

Adobe suorittaa palvelinpuolen kirjausta lokitiedostoon Adobe Document Cloud -palveluiden asiakastoiminnasta, jotta se voi diagnosoida palvelukatkoja, tietyn asiakkaan ongelmia ja raportoituja vikoja. Lokit tallentavat vain Adobe ID:t, jotta voidaan diagnosoida tietyn asiakkaan asioita eikä tieto sisällä käyttäjänimi/salasana-yhdistelmää. Vain valtuutettu Adoben teknisen tuen henkilökunta, oleellisimmat insinöörit ja tietyt kehittäjät voivat päästä lokeihin tietyn esiin tulleen ongelman diagnosoimiseksi.

Palvelun valvonta

AWS valvoo sähköisiä, mekaanisia ja perustoimintojen tukijärjestelmiä ja laitteistoja palveluongelmien välittömän tunnistuksen avuksi. Jotta laitteisto pidetään jatkuvassa käyttökunnossa, AWS suorittaa jatkuvaa ennakoivaa kunnossapitoa.

Tietojen tallennus ja varmuuskopiointi

Adobe tallentaa kaikki Adobe Document Cloud -palvelut Amazon S3:ssa, joka antaa vahvan ja kestävän tallennusinfrastruktuurin. Kestävyyden tuottamiseksi Amazon S3:n PUT and COPY -toiminnot tallentavat synkronisesti asiakkaan tietoja useisiin tiloihin ja varastoivat objekteja vikasietoisen hajautetusti useisiin laitteisiin eri tiloissa Amazon S3 -alueella.

Amazon S3 laskee tarkistussummat kaikessa verkkoliikenteessä tunnistaakseen datapakettien vioittumisen tallentaessaan tai noutaessaan dataa. Datan replikointi Amazon S3 -datan objekteille tapahtuu alueellisessa klusterissa, jossa tiedot on tallennettu, eikä niitä replikoida muiden alueiden datakeskusklustereissa.

Metatiedot replikoidaan ottamalla pikakuvia Amazon EBS -volyymeista ja tallennus on samanlainen kuin Amazon S3:ssa. Katso lisätietoja AWS:n suojauksesta AWS-pilvisuojauksen verkkosivustolta.

Muutosten hallinta

AWS valtuuttaa, kirjaa lokiin, testaa, hyväksyy ja dokumentoi muutoksen nykyiseen AWS-infrastruktuuriin toimialan vastaavien järjestelmien standardien mukaisesti. Amazon aikatauluttaa AWS:n päivitykset minimoimalla niiden vaikutukset asiakkaisiin. AWS kommunikoi asiakkaiden kanssa joko sähköpostitse tai AWS Service Health Dashboardin kautta, kun palvelun käyttöön on kohdistumassa todennäköisesti negatiivisia vaikutuksia. Adobe ylläpitää myös Adoben järjestelmien tilaa Adobe Document Cloudille.

Korjauspäivitysten hallinta

AWS säilyttää vastuun korjausjärjestelmistä, jotka tukevat AWS-palveluiden, kuten hypervisor- ja verkkopalveluiden, toimitusta. Adobe on vastuussa AWS:ssä toimivien vieraskäyttöjärjestelmien (OS), ohjelmistojen ja sovellusten korjauksesta. Kun korjauksia tarvitaan, Adobe toimittaa uuden esirajoitetun käyttöjärjestelmän ja sovelluksen esiintymän todellisen korjaustiedoston sijasta.

AWS:n fyysiset ja ympäristöön liittyvät ohjaukset

AWS:n fyysiset ja ympäristöön liittyvät ohjaukset on erityisesti kuvattu SOC Type 1- ja SOC Type 2 -raporteissa. Seuraavassa osassa kuvataan joitakin AWS-datakeskuksissa eri puolilla maailmaa käytettyjä suojaustoimenpiteitä ja ohjauksia. Katso lisätietoja AWS:n suojauksesta AWS-pilvisuojauksen verkkosivustolta.

Fyysinen tilan suojaus

AWS-datakeskuksissa käytetään toimialan arkkitehtuurin ja teknisen suunnittelun vakiolähestymistapoja. AWS-datakeskukset sijaitsevat nimettömissä tiloissa, ja Amazon valvoo fyysistä pääsyä sekä rakennuksen ympärillä että rakennuksen sisääntulopisteissä käyttämällä ammattimaista tietoturvahenkilökuntaa, videovalvontaa, tietomurtojen tunnistusjärjestelmiä ja muita sähköisiä menetelmiä. Valtuutetun henkilökunnan on läpäistävä kahden tekijän todennus vähintään kaksi kertaa, ennen kuin he pääsevät datakeskuksen kerroksiin. Kaikkien vierailijoiden ja urakoitsijoiden on esitettävä henkilöllisyys, ja heidät kirjaa sisään ja heitä saattaa koko ajan valtuutettu henkilökunta.

AWS myöntää pääsyn datakeskukseen ja tietoja siitä vain niille työntekijöille ja urakoitsijoille, joilla on oikeutettu tarve näihin etuoikeuksiin. Kun työntekijällä ei ole enää liiketoiminnan asettamaa tarvetta näihin etuoikeuksiin, hänen pääsynsä peruutetaan välittömästi, vaikka hän jatkaisi työskentelyä Amazonilla tai AWS:ssä. Kaikki AWS:n työntekijöiden fyysinen pääsy datakeskuksiin kirjataan lokiin ja sitä valvotaan tavanomaisesti.

Palontorjunta

AWS asentaa automaattisen tulipalon tunnistus- ja estolaitteistot kaikkiin AWS-datakeskuksiin. Tulipalon havaintojärjestelmässä käytetään savuntunnistusantureita kaikissa datakeskusympäristöissä, mekaanisen ja sähköisen infrastruktuurin tiloissa, jäähdytinhuoneissa ja generaattorilaitteistohuoneissa. Nämä alueet on suojattu joko märkäputki-, double- interlocked pre-action- tai kaasutoimisilla sprinklerijärjestelmillä.

Valvottu ympäristö

AWS käyttää ilmaston valvontajärjestelmää, jotta säilytetään vakiokäyttölämpötila palvelimille ja muulle laitteistolle, mikä estää ylikuumenemisen ja pienentää käyttökatkojen mahdollisuutta. AW- datakeskukset säilyttävät ilmasto-olosuhteet optimaalisilla tasoilla. AWS-henkilökunta ja järjestelmänvalvovat ja ohjaavat sekä lämpötilaa että kosteutta asianmukaisilla tasoilla.

Varmuusvirransaanti

AWS:n datakeskusten sähköjärjestelmät on suunniteltu täysin vikasietoisiksi ja ylläpidettäviksi vaikutuksetta toimintaan — 24 tuntia päivässä seitsemänä päivänä viikossa. Katkottoman tehonsyötön (UPS) yksiköt syöttävät varavirtaa tilan kriittisille ja oleellisille laitteille sähkökatkoksen tapahtuessa. Datakeskukset käyttävät generaattoreita varavirran tuottamiseen koko laitokselle.

Järjestelmäpalautus

AWS:n datakeskuksilla on korkeatasoinen käytettävyys, koska järjestelmä- tai laitteistovioilla on niihin minimaalinen vaikutus. Kaikki datakeskukset on rakennettu klustereihin eri globaaleille alueille, ja ne pysyvät online 24x7x365 asiakkaiden palvelemiseksi — mikään datakeskus ei ole "kylmä". Vikatapauksessa automaattiset prosessit siirtävät asiakkaan tietoliikenteen pois vaikutukselle altistuneelta alueelta.

Ydinsovellukset otetaan käyttöön N+1-konfiguraatiossa, joten jos datakeskukseen tulee vika, on olemassa riittävästi kapasiteettia ottaa käyttöön liikenteen kuormituksen tasapainotus jäljellä oleville keskuksille. Katso lisätietoja AWS:n järjestelmäpalautuksen protokollista AWS-pilvisuojauksen verkkosivustolta.

Adoben riskin ja haavoittuvuuden hallinta

Adobe pyrkii varmistamaan, että riskin ja haavoittuvuuden hallinnan, tapauksiin vastaamisen, lievennyksen ja ratkaisuprosessi on joustava ja tarkka. Valvomme jatkuvasti uhkia, jaamme tietoja tietoturva-asiantuntijoiden kanssa eri puolilla maailmaa, ratkaisemme tapaukset, kun ne tapahtuvat, ja syötämme nämä tiedot takaisin kehitystyöryhmillemme, jotta voimme saavuttaa korkeimmat suojaustasot kaikille Adoben tuotteille ja palveluille.

Penetraatiotestaus

Adobe hyväksyy ja toimii johtavien kolmannen osapuolen tietoturvayritysten kanssa suorittaakseen penetraatiotestausta, joka voi paljastaa mahdollisia suojaushaavoittuvuuksia ja parantaa Adoben tuotteiden ja palveluiden yleistä suojausta. Kun Adobe on saanut kolmannen osapuolen toimittaman raportin, se dokumentoi nämä haavoittuvuudet, arvioi niiden vakavuuden ja prioriteetin ja luo sitten lieventämisstrategian tai korjaussuunnitelman. Adobe suorittaa täyden penetraatiotestin vuosittain ja tekee haavoittuvuusskannauksia kuukausittain.

Adobe Document Cloudin suojaustyöryhmä suorittaa sisäisesti kaikkien Document Cloudin osien ja palveluiden riskien arvioinnin vuosineljänneksittäin ja ennen jokaista uutta versiota. Document Cloudin suojaustyöryhmä tekee yhteistyötä teknisten toimintojen ja kehityksen johdon kanssa, jotta varmistetaan, että kaikki suuren riskin haavoittuvuudet lievennetään ennen jokaista versiota. Katso lisätietoja Adoben penetraation testausmenettelyistä Adobe Secure Engineering -yleiskuvauksesta.

Tapausvastaus ja -ilmoitus

Uusia haavoittuvuuksia ja uhkia kehittyy koko ajan, ja Adobe pyrkii vastaamaan ja lieventämään vasta tunnistettuja uhkia. Sen lisäksi, että Adobe on tilannut koko alaa kattavat haavoittuvuuksien ilmoitusluettelot, kuten Yhdysvaltain Computer Emergency Readiness Team (US-CERT), Bugtraq, ja SANS, se on tilaa myös suurimpien suojausmyyjien toimittamia viimeisimpien suojaushälytysten luetteloja.

Lisätietoja Adoben tapauksiin vastaamisen ja ilmoitusten prosessista on Adoben tapauksiin vastaamisen yleiskuvauksessa.

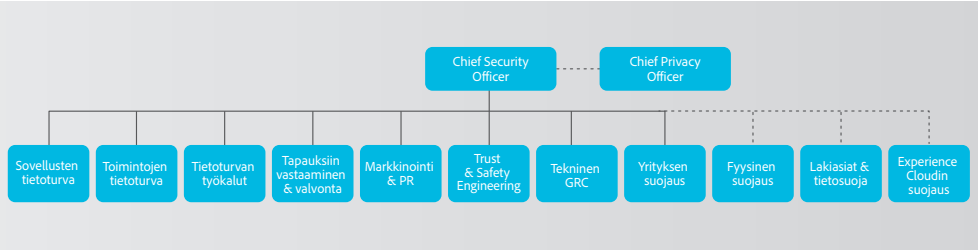
Tekninen rikosanalyysi

Tapaustutkimuksissa Document Cloudin työryhmä noudattaa Adoben teknisen rikosanalyysin prosessia, joka sisältää altistuneiden laitteiden täydellisen kuvasieppauksen tai muistivedoksen, todisteiden turvaamisen ja alkuperäisketjutallenteet.

Adoben tietoturvaorganisaatio

Osana sitoutumistamme tuotteittemme ja palveluidemme tietoturvaan Adobe koordinoi kaikki tietoturvatoiminnot chief security officerin (CSO) tasolla. Adoben Chief Security Officerin (CSO) toimisto koordinoi kaikkia tuote- ja tietoturva-aloitteita ja Adobe Secure Product Lifecycle (SPLC) -prosessin toteutusta.

CSO johtaa myös Adobe Secure Software Engineering Team (ASSET) -työryhmää, joka on tietoturva-asiantuntijoiden erityinen keskitetty ryhmä ja joka konsultoi Adoben tärkeimpiä tuote- ja toimintaryhmiä, kuten Adobe Document Cloud -työryhmää. ASSET-tutkijat työskentelevät yhdessä yksittäisten Adoben tuote- ja toimintaryhmien kanssa ja auttavat niitä tuotteiden ja palvelujen sopivien suojaustasojen kehityksessä. He neuvovat näitä työryhmiä suojauskäytännöissä, jotta nämä soveltaisivat selkeitä ja toistettavia kehitys-, käyttöönotto-, toiminto- ja ongelmienkäsittelyprosesseja.



Adoben tietoturvaorganisaatio

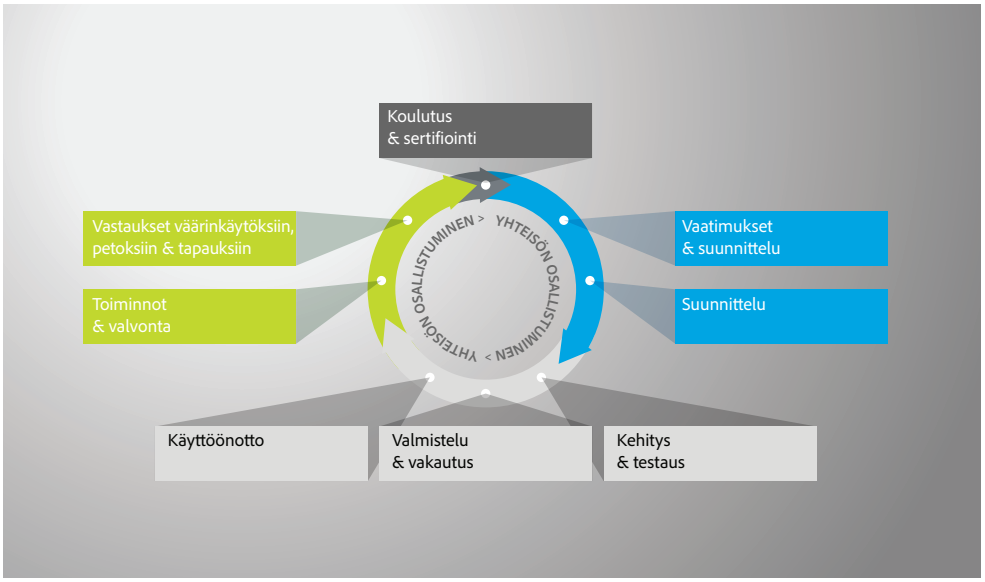
Adoben suojattu tuotekehitys

Kuten muutkin Adoben tärkeät tuote- ja palveluorganisaatiot Adobe Document Cloudin organisaatio käyttää Adoben SPLC-prosessia. Adobe SPLC on monipuolinen useiden satojen erityisten suojatoimintojen sarja, joihin kuuluvat ohjelmiston kehityskäytännöt, -prosessit ja -työkalut. Se on integroitu tuotteen elinkaaren useisiin vaiheisiin suunnittelusta ja kehityksestä laadunvarmistukseen, testaukseen ja käyttöönottoon. ASSET:n suojaustutkijat antavat erityistä SPLC-opastusta kullekin avaintuotteelle tai -palvelulle mahdollisten suojausongelmien arvioinnin perusteella. Adobe SPLC:tä täydennetään jatkuvasti yhteisön osallistumisen avulla, ja se säilyy ajantasaisena, kun teknologiassa, suojauskäytännöissä ja uhkaympäristöissä tapahtuu muutoksia.

Adoben suojattu tuotteen elinkaari

Adobe SPLC -toimintoihin kuuluvat, tietyn Adobe Document Cloudin osan mukaan, joitakin tai kaikki seuraavista suositelluista parhaista käytännöistä, prosesseista ja työkaluista:

- Suojauskoulutus ja -hyväksyntä tuoteryhmille
- Tuotteen terveyden, riskin ja uhkaympäristön analyysi
- Suojatut koodausohjeet, säännöt ja analyysi
- Palvelun toteutussuunnitelmat, suojaustyökalut ja testausmenetelmät, jotka ohjaavat Adobe Document Cloudin suojausryhmää käsittelemään Open Web Application Security Project (OWASP) -projektin 10:tä kriittisintä web-sovelluksen suojausriskiä ja CWE/SANS-luettelon 25:tä vaarallisinta ohjelmistovirhettä
- Suojausarkkitehtuurin tarkistus ja penetraatiotestaus
- Lähdekoodin tarkistukset haavoittuvuuksiin mahdollisesti johtavien tunnettujen vikojen poistamiseen
- Käyttäjän luoman sisällön (UGC) arviointi
- Sovelluksen ja verkon skannaus
- Täyden valmiuden tarkistus, vastaussuunnitelmat ja kehittäjän koulutusmateriaalien julkaisu



Adoben suojattu tuotteen elinkaari

Adoben ohjelmiston suojaussertifioinnin ohjelma

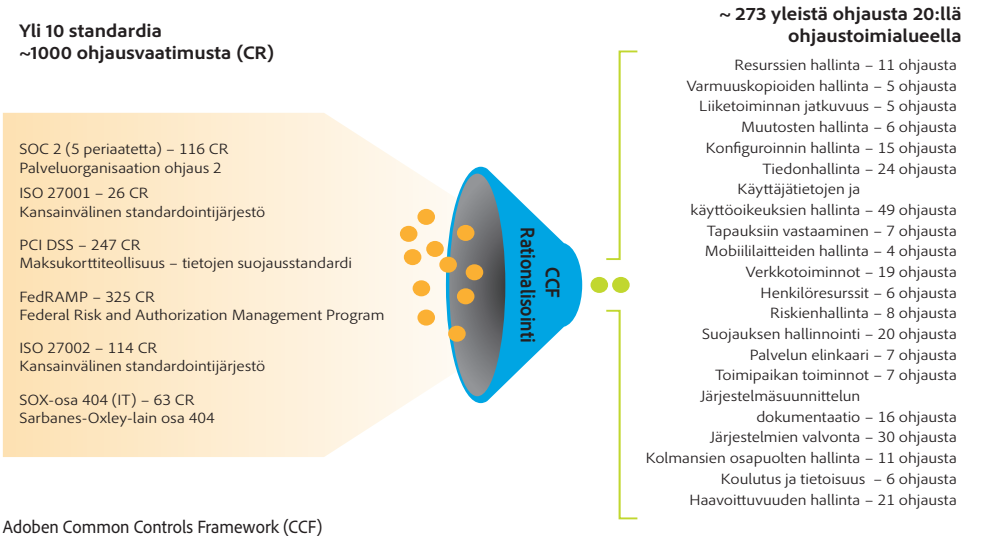
Adobe suorittaa jatkuvaa tietoturvakoulutusta osana Adobe SPLC:tä kehitysryhmille parantaakseen tietoturvatietämystä koko yrityksessä ja parantaakseen tuotteidemme ja palveluidemme yleistä suojausta. Työntekijät, jotka osallistuvat Adoben ohjelmiston suojaussertifioinnin ohjelmaan, saavat eri sertifiointitasoja suorittamalla suojausprojekteja. Katso lisätietoja tuotteidemme suojauskäytännöistä Adobe Secure Engineering -yleiskuvauksesta.

Katso lisätietoja Adoben ohjelmiston suojaussertifioinnin ohjelmasta Adoben suojauskulttuurin white paper -julkaisusta.

Document Cloudin palveluiden vaatimustenmukaisuus

Adobe Common Controls Framework (CCF) on sarja suojaustoimintoja ja vaatimustenmukaisuusohjauksia, jotka on toteutettu tuoteoperaatioiden työryhmissä sekä eri osissa infrastruktuuri- ja sovellustyöryhmiä.

Kun Adobe luo CCF:n, se analysoi yleisimpien pilvipohjaisten liiketoimintojen suojaussertifiointikriteerejä ja järkeisti yli 1000 vaatimusta Adoben erityisiksi ohjauksiksi, jotka liittyvät noin tusinaan alan standardiin.



Adoben Common Controls Framework (CCF)

Nykyiset säädökset ja Adobe Document Cloud -palveluiden vaatimuksenmukaisuus

SOC 2 on suojausperiaatteiden sarja, joka määrittää johtavan käytännön suojaukselle, luottamuksellisuudelle ja tietoturvalle oleelliset ohjaukset. Adobe Document Cloud -palvelut ovat SOC 2 Type 2 (suojaus ja käytettävyys) -yhteensopivia.

ISO 27001 on globaalisti käytettyjen standardien sarja, joka kuvaa tiukat suojausvaatimukset ja muodostaa systemaattisen lähestymistavan asiakastietojen luottamuksellisuuden, eheyden ja käytettävyyden hallintaan. Adobe Document Cloud -palvelut ovat standardin ISO 27001:2013 mukaisia.

Maksukorttiteollisuuden tietoturvastandardi (PCI DSS) on sovelluskohtainen tietojen suojausstandardi organisaatioille, jotka käsittelevät maksukorttitietoja, kuten luottokorttinumeroita. Koska Adobe on PCI DSS -yhteensopiva toimittaja, se voi auttaa asiakkaita PCI-vaatimusten noudattamisessa kortinhaltijaan liittyvien henkilökohtaisesti tunnistettavien tietojen turvalliseen käsittelyyn.

Gramm-Leach-Bliley Act (GLBA) edellyttää, että rahoituslaitokset turvaavat asiakkaiden henkilötiedot. Adobe Document Cloud -palvelut ovat GLBA-valmiita, mikä tarkoittaa, että ne antavat rahoitusalan asiakkaillemme mahdollisuuden GLBA-vaatimusten noudattamiseen palveluntoimittajien käytössä.

Federal Risk and Authorization Management Program (FedRAMP) on hallinnonlaajuinen ohjelma, joka tarjoaa selkeän lähestymistavan suojauksen arviointiin, valtuutukseen ja jatkuvaan pilvipohjaisten tuotteiden ja palveluiden valvontaan. Adobe Document Cloud -palvelut ovat FedRAMP-räätälöityjä, mikä tarkoittaa, että ne mahdollistavat asiakkaillemme FedRAMP-vaatimusten täyttämisen.

U.S. Family Educational Rights and Privacy Act (FERPA) on suunniteltu säilyttämään Yhdysvaltalaisten opiskelijoiden koulutustietojen ja hakemistotietojen luottamuksellisuuden. FERPA-ohjeiden mukaan Adobe voi sopimuksellisesti sopia ', että se toimii "koulun virkamiehenä", kun on kyse säädellyistä opiskelijatiedoista, mikä mahdollistaa oppilaitosasiakkaillemme FERPA-vaatimusten noudattamisen.

SAFE-BioPharma-standardi kuvaa vaatimuksia standardoidulle käyttäjätietojen luottamukselle joko käyttäjätietojen todennukseen tai digitaaliseen allekirjoitukseen. Adobe Document Cloud on sertifioitu noudattavat SAFE-BioPharma- digitaalisen tunnistuksen standardia. Adobe Acrobat DC:n käyttö on turvallista ja se on yhteensopiva SAFE-BioPharma-työnkulkujen kanssa. Lisäksi Adobe Document Cloud -palvelut ja Adobe Sign ovat SOC 2 Type 2 -yhteensopivia.

Lisätietoja Adobe Signin nykyisestä vaatimustenmukaisuuden tilanteesta Adobe Signin teknisessä yleiskuvauksessa.

Lopulta asiakkaat ovat vastuussa siitä, että ne varmistavat juridisten velvoitteiden noudattamiseen ja varmentavat, että ratkaisumme täyttävät heidän vaatimustenmukaisuuden tarpeensa ja että ne on suojattu asianmukaisesti.

Adoben työntekijät

Adobella on työntekijöitä ja toimistoja eri puolilla maailmaa, ja se toteuttaa seuraavia prosesseja ja menettelyjä yrityksen laajuisesti yrityksen suojaamiseksi tietoturvauhkia vastaan.

Työntekijöiden pääsy asiakastietoihin

Adobe ylläpitää segmentoituja kehitys- ja tuotantoympäristöjä Adobe Document Cloudille. Se käyttää teknisiä ohjauksia rajoittaakseen verkko- ja sovellustason pääsyn live-tuotantojärjestelmiin. Työntekijöillä on tietyt valtuutukset käyttää kehitys- ja tuotantojärjestelmiä, ja sellaisten työntekijöiden, joilla ei ole oikeutettua liiketoiminnan syytä, pääsyä näihin järjestelmiin on rajoitettu.

Taustatarkistukset

Adobe vastaanottaa taustatarkistusraportteja rekrytointitarkoituksiin. Adoben tyypillisesti hakeman raportin luonne ja laajuus sisältää koulutustaustaan, työhistoriaan ja tuomioistuimen tietoihin, kuten rikosrekisteriin, liittyvät kyselyt ja viitteet, jotka on saatu työtovereilta ja tuttavilta, sovellettavan lain mukaan. Nämä taustatarkistusvaatimukset soveltuvat tavallisiin Yhdysvalloissa palkattaviin uusiin työntekijöihin, kuten niihin, jotka tulevat hallitsemaan järjestelmiä tai joilla on pääsy asiakastietoihin. Yhdysvaltojen uusien toimistojen kautta tulevien väliaikaisten työntekijöiden on täytettävä taustatarkistusvaatimukset kyseisen toimiston kautta Adoben taustatarkistusohjeiden mukaisesti. Yhdysvaltojen ulkopuolella Adobe suorittaa taustatarkistuksia tietyille uusille työntekijöille Adoben taustatarkistuskäytännön ja sovellettavien paikallisten lakien mukaisesti.

Työntekijän työsuhteen päättäminen

Kun työntekijä poistuu Adoben palveluksesta, työntekijän esimies toimittaa lähtevän työntekijän lomakkeen. Kun lomake on hyväksytty, Adobe People Resources käynnistää sähköpostityönkulun tiedottaakseen oleellisille sidosryhmille, jotta he voivat tehdä työntekijän viimeiseen päivään johtavat tietyt toimet. Jos Adobe erottaa työntekijän, Adobe People Resources lähettää oleellisille sidosryhmille vastaavan sähköposti-ilmoituksen, kuten työntekijän työsuhteen päättämispäivämäärän ja -ajan.

Adobe Corporate Security aikatauluttaa sitten seuraavat toimet, jotta varmistetaan, että työntekijän viimeisen päivän jälkeen hänellä ei ole enää pääsyä Adoben luottamuksellisiin tiedostoihin tai toimistoihin:

- Sähköpostiin pääsyn poisto
- VPN-verkkoon etäpääsyn poisto
- Toimiston ja datakeskuksen kulkuluvan mitätöinti
- Verkkokäytön päättäminen

Esimiehet voivat pyynnöstä pyytää rakennuksen turvamiehiä saattamaan erotetun työntekijän ulos Adoben toimistosta tai rakennuksesta.

Toimitilan suojaus

Jokaisessa Adoben pääkonttorissa on vahdit, jotka suojaavat tiloja 24x7. Adoben työntekijöillä on avainkortti-kulkulupa rakennukseen sisäänpääsyä varten. Vierailijat tulevat rakennukseen pääovesta, kirjautuvat sisään ja ulos vastaanoton työntekijän kanssa. Vierailijan on pidettävä väliaikainen vierailija-kulkulupa esillä, ja hänellä on saattajana työntekijä. Adobe pitää kaikki palvelinlaitteistot, kehityslaitteet, puhelinjärjestelmät, tiedosto- ja postipalvelimet ja muut herkät järjestelmät lukittuina aina säädellyn ympäristön palvelinhuoneissa, joihin pääsee vain asianmukaisesti valtuutettu henkilöstö.

Virustorjunta

Adobe skannaa kaiken yrityksen sisääntulevan ja lähtevän sähköpostiliikenteen tunnettujen haittaohjelmauhkien varalta.

Asiakastietojen luottamuksellisuus

Adobe käsittelee aina kaikkia asiakastietoja luottamuksellisina. Adobe ei käytä tai jaa tietoja, joita on koottu asiakkaan puolesta lukuun ottamatta sopimuksen sallimia tietoja kyseisen asiakkaan sopimuksessa ja mitä Adoben käyttöehdoissa ja Adoben tietosuojakäytännössä asetetaan.

Yhteenveto

Tässä dokumentissa kuvattu Adoben ennakoiva lähestymistapa tietoturvaan ja tiukat menettelyt auttavat suojaamaan Adobe Acrobat DC:tä, Acrobat Reader DC:tä ja Document Cloud -palveluita — ja luottamuksellisia tietoja. Adobe pitää digitaalisten kokemusten tietoturvaa erittäin tärkeänä. Valvomme jatkuvasti kehittyvää uhkaympäristöä, jotta pysymme haitallisten tapahtumien edellä ja varmistamme asiakkaidemme tietojen suojauksen.

Lisätietoja, käy Adobe Trust Centerissä.

Adobe

Adobe Systems Nordic AB
Box 47, 164 93 Kista, Sverige
www.adobe.com/fi, www.adobe.com

6/19