Cloud Software Group Beveiligingsdocument voor services

Versie 3.0

Met ingang van 30 september 2022

Inhoud

In dit Beveiligingsdocument voor services van Cloud Software Group, Inc. ('Cloud Software Group', 'we', 'ons' of 'onze') (het 'Document') vindt u een beschrijving van de beveiligingscontroles die zijn geïmplementeerd in verband met de prestaties van cloudservices, technische ondersteuningsservices of adviesservices (de 'Services') die aan klanten ('Klant', 'u' of 'uw') worden geleverd onder de betreffende licentie- en/of serviceovereenkomst van Cloud Services Group en de toepasselijke bestelling voor de Services (samen de 'Overeenkomst'). Bèta- of lab/tech-previewservices (waaronder Cloud Labs) en onze interne IT-systemen die niet zijn betrokken bij de levering van Services, vallen buiten het bereik van dit Document.

Termen met een hoofdletter hebben de betekenis die in de Overeenkomst is vermeld of die hierin is gedefinieerd. Onder 'Klantinhoud' wordt gegevens verstaan die we openen of ontvangen of die u verzendt of uploadt voor opslag of verwerking zodat we Services kunnen verlenen. Het bevat ook eigendomsrechtelijk beschermde technische informatie over uw omgeving, zoals systeem- of netwerkconfiguraties en de besturingselementen die u selecteert. 'Logboeken' betekent informatie over prestaties, stabiliteit, gebruik, beveiliging, ondersteuning, hardware, software, services of randapparaten die betrokken zijn bij het gebruik van onze producten of Services.

1. Bereik

In dit document worden de administratieve, fysieke en technische beveiligingscontroles beschreven die we gebruiken om de vertrouwelijkheid, integriteit en beschikbaarheid van onze Services te handhaven. Deze controles zijn van toepassing op onze operationele en servicesystemen en -omgevingen. Cloud Software Group gebruikt ISO/IEC 27002 als basis voor het beveiligingsprogramma voor Services en heeft industrie-specifieke certificeringen en evaluaties voor bepaalde Services verkregen. Aanvullende informatie is beschikbaar in de sectie 'Privacy en naleving' van ons Trust Center.

We werken continu aan de versterking en verbetering van de beveiligingsprocedures en behouden ons het recht voor om de hierin beschreven controles te wijzigen. Eventuele wijzigingen doen geen afbreuk aan het beveiligingsniveau tijdens de betreffende termijn van de Services.

2. Beveiligingsprogramma en beleidskader

Cloud Software Group heeft een beveiligingsprogramma en beleidskader die zijn vastgelegd en goedgekeurd door het hoger en leidinggevend management van voor diverse zakelijke gebieden in het gehele bedrijf.

2.1 Toezicht op beveiligingsrisico's

Het Cyber Risk Oversight Committee (CROC) regelt de activiteiten voor beveiligingsrisicobeheer. Het CROC bestaat uit management en leidinggevenden in diverse functies. Het leidinggevende team evalueert het lidmaatschap van de commissie op jaarbasis om te bepalen of alle zakelijke en operationele gebieden goed zijn vertegenwoordigd.

Het CROC komt minstens een keer per kwartaal bijeen en biedt instructies, inzicht en richting voor het identificeren, beoordelen en aanpakken van

beveiligingsrisico's in zowel de bedrijfswerking als de infrastructuur voor de levering van services.

2.2 Beveiligingsrisicobeheer

Cloud Software Group maakt gebruik van een programma voor beveiligingsrisicobeheer dat potentiële bedreigingen voor onze producten en services en onze infrastructuur identificeert, het belang van de risico's van die bedreigingen beoordeelt, risicobeperkende strategieën ontwikkelt en met onze technische en productteams samenwerkt om deze strategieën te implementeren.

2.3 Informatiebeveiliging

Cloud Software Group heeft een Chief Information Security Officer (CISO) aangewezen, die verantwoordelijk is voor de strategie, naleving en afdwinging van beveiligingstoezicht en beleid. De Director of Security Monitoring and Response leidt het proces voor respons bij incidenten, waaronder onderzoek, beheersing en herstel.

2.4 Fysieke en omgevingsbeveiliging

Het beveiligingsteam van Cloud Software Group houdt toezicht op de fysieke toegang tot onze faciliteiten.

3. Toegangscontrole

We vereisen het gebruik van toegangscontrolemaatregelen die zijn ontworpen om ervoor te zorgen dat de juiste rechten worden toegewezen en onderhouden voor toegang tot bedrijfssystemen, activa, gegevens en faciliteiten om te beschermen tegen potentiële schade, inbreuken of verlies. We volgen het principe van minimale bevoegdheden, of beveiliging op basis van rollen, zodat de toegang van de gebruiker wordt beperkt tot alleen dat wat nodig is om functies of rollen uit te voeren.

Managers ontwerpen rollen om de juiste scheiding van verplichtingen te bieden, waarbij taken en bevoegdheden worden gedistribueerd onder meerdere mensen om bescherming tegen fraude en fouten te bieden.

3.1 Nieuwe accounts, rollen en toegangsaanvragen

Cloud Software Group vereist een formele aanvraag voor toegang tot bedrijfssystemen of -gegevens. Elk verzoek voor toegang vereist minimaal de goedkeuring door de manager van de gebruiker. Hij bevestigt de functie en toegang van de gebruiker. Toegangsbeheerders bevestigen dat de nodige goedkeuringen zijn verkregen voordat toegang tot systemen of gegevens wordt verleend. Het principe van minimale bevoegdheden wordt toegepast.

3.2 Accountbeoordeling

We voeren minimaal tweejaarlijkse beoordelingen van gebruikersaccounts uit en wijst bevoegdheden voor belangrijke systemen toe. Wijzigingen die zijn vereist als resultaat van de beoordelingen, zijn onderhevig aan een formeel toegangsaanvraagproces om te bevestigen dat de gebruiker en de rol van de gebruiker toegang tot relevante systemen vereisen.

3.3 Verwijdering van accounts, rollen en toegang

We vereisen dat gebruikerstoegang onmiddellijk wordt uitgeschakeld, ingetrokken of verwijderd bij melding van de wijziging of beëindiging van de rol van een gebruiker (indien van toepassing), de voltooiing van de overeenkomst door de gebruiker of het vertrek van de gebruiker bij het bedrijf.

Aanvragen voor toegangverwijdering worden gedocumenteerd en bijgehouden.

3.4 Referenties

Cloud Software Group vereist meervoudige verificatie voor externe toegang tot onze systemen door medewerkers en dwingt de volgende wachtwoordafhandelings- en managementprocedures af:

- Wachtwoorden moeten regelmatig geroteerd worden zoals opgelegd door onze systeemvereisten.

- Wachtwoorden moeten aan de vereisten inzake lengte en complexiteit voldoen, met inbegrip van een combinatie van cijfers, speciale karakters, hoofdletters en kleine letters en een minimum aantal karakters, waarbij gewone woorden of woordenboekwoorden niet toegelaten zijn.
- Gedeactiveerde of verlopen gebruikers-ID's worden niet aan andere personen toegewezen.
- We handhaven procedures om wachtwoorden te deactiveren die abusievelijk zijn onthuld.
- We controleren op pogingen om met een ongeldig wachtwoord toegang te krijgen tot de Services en nemen automatisch actie om herhaalde pogingen te blokkeren.

Cloud Software Group gebruikt procedures die zijn ontworpen om de vertrouwelijkheid en integriteit van wachtwoorden te handhaven wanneer ze worden toegewezen, gedistribueerd of opgeslagen, zoals:

- Vereisen dat wachtwoorden gedurende hun levenscyclus worden verborgen (gehasht) en/of gecodeerd.
- Verbieden van het delen van wachtwoorden

4. Systeemontwikkeling en onderhoud

We handhaven een beveiligingsproces op basis van ontwerp, waaronder standaarden en procedures voor wijzigingsbeheer die zijn ontworpen om tegemoet te komen aan beveiligingsvereisten van informatiesystemen, codebeoordeling en -tests en beveiliging voor het gebruik van testgegevens. Dit proces wordt beheerd en gecontroleerd door een gespecialiseerd beveiligingsteam dat ook verantwoordelijk is voor de beoordeling van het ontwerp, bedreigingsmodellering, de handmatige herziening van code, steekproefsgewijze controle en penetratietesten.

4.1 Principes van veilige ontwerpen

Cloud Software Group heeft formele methodologie voor de levenscyclus van systeemontwikkeling aangenomen die ontwikkeling, verwerving, implementatie en onderhoud van gecomputeriseerde informatiesystemen en gerelateerde technologievereisten regelt.

We gebruiken een op software gebaseerd systeem om beoordelingen en goedkeuringen van Open Source te beheren. Dit omvat het uitvoeren van periodieke scans en audits van de softwareproducten. We hebben gedocumenteerde beleidsregels, beschikbaar voor alle medewerkers, omtrent het gebruik van Open Source, evenals training voor ontwikkelaars en hun beheer van aanbevolen procedures voor Open Source.

4.2 Wijzigingsbeheer

Ons beheersproces voor wijzigingen van de infrastructuur en software komt tegemoet aan de beveiligingsvereisten en vereist dat veranderingen van infrastructuur en software geautoriseerd worden, formeel gedocumenteerd worden, getest (zoals toepasselijk), beoordeeld en goedgekeurd worden voordat ze in de productieomgeving aangewend worden. Infrastructuur- en softwarewijzigingen worden beheerd en bijgehouden met behulp van werkbeheersystemen.

Het proces voor wijzigingsbeheer is op geschikte wijze gescheiden en toegang om wijzigingen naar productie te migreren is beperkt tot geautoriseerd personeel.

5. Activabeheer

5.1 Beheer van fysieke en virtuele activa

Cloud Software Group handhaaft een dynamische inventaris van de fysieke en virtuele systemen die we beheren en gebruiken om de Services uit te voeren ('Serviceactiva'). Systeemeigenaren zijn verantwoordelijk voor het onderhoud en bijwerken van hun Serviceactiva volgens onze beveiligingsstandaarden.

Er zijn formele verwijderingsprocedures van kracht om de veilige verwijdering van Cloud Software Group- en klantengegevens te begeleiden. We verwijderen gegevens indien ze niet langer vereist zijn op basis van de classificatie en met behulp van verwijderingsprocessen die zijn ontworpen om te vermijden dat gegevens opnieuw worden samengesteld of gelezen.

Onze technologische activa worden opgeschoond en verwijderd wanneer ze niet langer nodig zijn in hun toegewezen gebied. Technologische activa omvatten maar zijn niet beperkt tot individuele computerapparatuur, multifunctionele computerapparatuur, opslagapparatuur, beeldvormingsapparatuur en netwerkapplicaties. Verwijdering wordt gecoördineerd door Global Security Risk Services en Information Security.

5.2 Toepassings- en systeembeheer

Toepassings - en systeemeigenaren zijn verantwoordelijk voor de beoordeling en classificatie van de gegevens die ze opslaan, raadplegen, verwijderen of overbrengen. Als onderdeel van controles worden medewerkers en contractanten vereist het volgende te doen:

- Klantinhoud classificeren als onderdeel van de hoogste twee categorieën van vertrouwelijke Citrix-informatie en de geschikte toegangsbeperkingen toepassen.
- Het afdrukken van Klantinhoud beperken en gedrukte materialen in veilige containers verwijderen.
- Geen zakelijke of vertrouwelijke informatie opslaan op apparaten die niet aan de vereisten van beveiligheidsbeleidsregels en -standaarden van Citrix voldoen.
- Onbeheerde computers en gegevens beveiligen.

5.3 Gegevensretentie

Klantinhoud die is opgeslagen als onderdeel van onze cloudservices is toegankelijk voor de Klant gedurende beperkte tijd na beëindiging van Services en wordt vervolgens verwijderd (met uitzondering van back-upexemplaren) nadat een verwijderingsbevestiging naar de klant is verzonden. Aanvullende gegevens worden geboden in de documentatie voor specifieke services. Klantinhoud kan ook worden bijgehouden na beëindiging van de services indien vereist voor juridische doeleinden. Citrix voldoet aan de vereisten van dit Document tot dergelijke Klantinhoud definitief is verwijderd.

6. HR-beveiliging

De beveiliging van Klantinhoud is een van de hoofdvereisten voor alle medewerkers en contractanten. Onze zakelijke gedragscode van vereist dat alle medewerkers en contractanten de onze beveiligingsbeleidsregels en -standaarden volgen, en komt specifiek tegemoet aan de bescherming van vertrouwelijke informatie evenals persoonlijke informatie van klanten, -partners, -leveranciers en -medewerkers.

Alle medewerkers en -contractanten zijn onderworpen aan de vertrouwelijkheidsovereenkomsten die van toepassing zijn op klantinformatie.

De organisatie Cloud Software Group Security informeert medewerkers ook regelmatig over onderwerpen die zijn gerelateerd aan informatie- en fysieke beveiliging om het beveiligingsbewustzijn over specifieke onderwerpen te onderhouden.

6.1 Achtergrondscreening

We maken momenteel gebruik van achtergrondscreeners voor alle nieuwe medewerkers overal ter wereld en vereisen hetzelfde voor alle personeel van externe leveranciers, tenzij dit door de plaatselijke wetgeving of de arbeidswetgeving wordt beperkt.

6.2 Training

Alle medewerkers worden vereist om training te volgen voor gegevensbescherming en bedrijfsbeleidsregels die zijn ontworpen om de beveiliging van onze vertrouwelijke informatie, inclusief vertrouwelijke informatie van onze klanten, partners, leveranciers en medewerkers, te handhaven. De training omvat de privacyprocedures en principes die van toepassing zijn op de afhandeling van persoonlijke informatie door medewerkers, met inbegrip van de behoefte om beperkingen op het gebruik, de toegang, het delen en het bewaren van persoonlijke informatie op te leggen. Leden van de technische organisatie volgen training die de veilige ontwikkeling, architectuur en versleuteling omvat.

6.3 Afdwinging

Van alle medewerkers wordt vereist dat ze voldoen aan onze beleidsregels en standaarden inzake beveiliging en privacy. Niet-naleving is onderworpen aan disciplinaire acties, waaronder de beëindiging van het dienstverband.

7. Operationele beveiliging

7.1 Netwerk- en systeembeveiliging

Cloud Software Group heeft netwerk- en systeembeveiligingsstandaarden gedocumenteerd die zijn ontworpen om ervoor te zorgen dat netwerken en systemen veilig worden geconfigureerd. Vereiste procedures onder deze standaarden zijn met inbegrip van maar niet beperkt tot:

- Standaardinstellingen en/of accounts wijzigen of uitschakelen.
- Gecontroleerd gebruik van beheerderstoegang.
- Serviceaccounts beperken voor alleen het doel waarvoor ze zijn gemaakt.
- Instellingen voor logboekregistratie en waarschuwingen die geschikt zijn voor audits.

We vereisen de implementatie van antimalwaresoftware op servers en werkstations en scannen het netwerk op schadelijke software.

Netwerkcontroles regelen toegang tot Klantinhoud. Deze omvatten, zoals toepasselijk: het configureren van een tussenliggende niet-vertrouwde zone tussen het internet en het interne netwerk dat beveiligingsmechanismen bevat om toegang en ongeautoriseerd verkeer te beperken; netwerksegmentering om ongeautoriseerde toegang tot Klantinhoud te voorkomen; en het scheiden van web- en toepassingsservers van de bijbehorende databaseservers in een gelaagde structuur die verkeer tussen de lagen beperkt.

7.2 Logboekregistratie

We verzamelen Logboeken om de juiste werking van de Services te bevestigen, om ondersteuning te bieden bij het oplossen van systeemproblemen en om onze netwerken en Klantinhoud te beschermen en

te beveiligen. Logboeken kunnen toegangs-ID, tijd, autorisatie verleend of geweigerd, diagnostische gegevens zoals tracerings- en crashbestanden, en andere relevante informatie en activiteit bevatten.

We verzamelen en gebruiken Logboeken (i) voor het leveren, beveiligen, beheren, meten en verbeteren van de Services, (ii) zoals verzocht door de Klant of zijn eindgebruikers, (iii) voor facturering, accountbeheer, interne rapportage en productstrategie, en/of voor naleving van overeenkomsten, beleidsregels, toepasselijke wetgeving, voorschriften of verzoeken door de overheid. Hiervoor kunnen de prestaties, de stabiliteit, het gebruik en de beveiliging van de Services en gerelateerde onderdelen worden gecontroleerd. Logboeken kunnen toegangs-ID, tijd, autorisatie verleend of geweigerd, diagnostische gegevens zoals tracerings- en crashbestanden, en andere relevante informatie en activiteit bevatten. Klanten kunnen deze controle niet blokkeren of belemmeren.

Meer informatie over klantinhoud en de behandeling van logboeken vindt u in ons Trust Center Cloud Assurance Data Protection & Security section welke verschillende witboeken over logboeken bij Citrix-cloudservices bevat.

7.3 Beheer van certificaten, referenties en geheimen

Cloud Software Group handhaaft beleid dat de levenscyclus van certificaten, referenties en geheimen bestrijkt om bescherming, beschikbaarheid en vertrouwelijkheid te waarborgen. Geheimhouders moeten gedocumenteerd zijn en formeel verklaren dat zij de verantwoordelijkheden als geheimhouder aanvaarden.

Verantwoordelijkheden zijn met inbegrip van maar niet beperkt tot:

- Certificaten moeten worden afgegeven door een erkende certificaatautoriteit.
- Cryptografische sleutels mogen niet in platte tekst worden opgeslagen of overgedragen en moeten gebruik maken van sterke goedgekeurde cryptografische protocollen.
- Referenties en geheimen moeten ten minste eenmaal per jaar worden geroteerd en worden opgeslagen in een goedgekeurde tool voor verificatiebeheer met bevoegdheden.

7.4 Kwetsbaarheidsbeheer

Wij controleren toepassingen en systemen op kwetsbaarheden met geautomatiseerde kwetsbaarheids- en poortscans op regelmatige basis

Geïdentificeerde kwetsbaarheden moeten worden verholpen volgens een tijdschema dat afhangt van de ernst van de kwetsbaarheid en de aanbevelingen van de leverancier. In gevallen dat er geen patch, update of permanente beperking beschikbaar is, worden passende tegenmaatregelen genomen om het risico op misbruik van de kwetsbaarheid te verminderen.

8. Versleuteling

8.1 Bescherming van gegevens tijdens overdracht

Cloud Software Group heeft veilige overdrachtsprotocollen geïmplementeerd voor de overdracht van informatie via openbare netwerken die onderdeel zijn van de Services. De Services worden beschermd door versleuteling en toegang via internet wordt beschermd door TLS-verbindingen.

8.2 Bescherming van gegevens in ruste

Wij eisen dat alle werkstations die worden gebruikt om Services te verlenen, worden gecodeerd met een minimum van 128-bits volledige schijfversleuteling. Klantinhoud mag niet worden opgeslagen op een draagbaar apparaat, tenzij deze is versleuteld.

Sommige cloudservices versleutelen standaard bepaalde gegevenselementen en

bieden mogelijk ook andere versleutelingsfuncties die klanten kunnen implementeren. Raadpleeg de toepasselijke documentatie van de cloudservices voor aanvullende informatie.

9. Fysieke beveiliging

9.1 Faciliteiten

We handhaven de volgende controles die zijn ontworpen om ongeautoriseerde toegang tot een faciliteit te voorkomen:

- Toegang tot faciliteiten is beperkt tot geautoriseerde personen.
- Bezoekers moeten zich registreren in een digitaal bezoekerslogboek en moeten op elk moment worden vergezeld of geobserveerd.
- ID-badges zijn vereist voor medewerkers, contractanten en gasten en moeten tijdens aanwezigheid in de faciliteit op elk moment zichtbaar worden gedragen.
- Security beheert en controleert toegang tot de faciliteiten na sluitingstijd.
- Bewakers, inbraakdetectie en/of CCTV-camera's bewaken de ingangen van gebouwen, laad- en loszones en openbare ruimten - (mechanismen voor het bewaken van toegang kunnen verschillen tussen faciliteiten, afhankelijk van de faciliteit en locatie).

Bovendien bieden de faciliteiten van de Cloud Software Group:

- Systemen of apparaten voor brandbestrijding en -detectie.
- Systemen of apparaten voor klimaatregeling (temperatuur, vochtigheid, enz.).
- Toegankelijke hoofdafsluiting of afscheidingskleppen voor water.
- Nooduitgangen en vluchtroutes.

Datakasten in kantoren zijn beschermd via badgetoegang.

9.2 Datacenters

Behalve de controles van de faciliteiten die hierboven zijn beschreven, implementeren we voor faciliteiten die eigendom zijn van Cloud Software Group of die door Cloud Software Group worden beheerd extra controles in de datacenters die worden gebruikt om de Services te leveren.

We gebruiken systemen die zijn ontworpen om te beschermen tegen gegevensverlies vanwege stroomstoringen of interferentie van leidingen, waaronder de globale en redundante service-infrastructuur die is ingericht met locaties voor noodherstel. Datacenters en internetserviceproviders (ISP's) zijn geëvalueerd om de prestaties betreffende bandbreedte, latentie en isolatie bij noodherstel te optimaliseren.

Datacenters bevinden zich in faciliteiten die netwerkneutraal zijn en bieden fysieke beveiliging, redundante voeding, redundantie van de infrastructuur en beschikbaarheidsovereenkomsten van belangrijke leveranciers.

Wanneer we gebruikmaken van datacenters of cloudservices van derde voor de levering van de Services, huren we providers in die aan de fysieke en omgevingsbeveiligingsvereisten van onze faciliteiten voldoen of deze overtreffen.

10. Bedrijfscontinuïteit en noodherstel

10.1 Bedrijfscontinuïteit

Cloud Software Group plant op strategische wijze de continuïteit van de bedrijfsactiviteiten tijdens ongunstige of verstorende situaties en ontwerpt systemen om ervoor te zorgen dat de Services tijdens dergelijke gebeurtenissen blijven functioneren.

We voeren minstens elke twee jaar een bedrijfsimpactanalyse (BIA) op afdelingsniveau uit, met elk jaar een beoordeling. De BIA wordt gebruikt om een bedrijfscontinuïteitsplan (BCP) per afdeling te maken, dat voor elke afdeling de resourcevereisten, herstelparameters en -methoden, verplaatsingsbehoeften en de veiligheidsmaatregelen identificeert en documenteert die tijdens het hele proces zijn vereist om mislukkingen of hiaten te vermijden. Het hoger management van elke afdeling evalueert het BCP en keurt het op jaarbasis goed, of als er zich aanzienlijke organisatorische wijzigingen voordoen.

We onderhouden plannen in geval van nood en onvoorziene gebeurtenissen voor al onze faciliteiten. In het geval faciliteiten niet beschikbaar zijn, krijgen medewerkers de mogelijkheid om extern te werken in andere Cloud Software Group faciliteiten of op de locatie van hun keuze. Aanvullende herstelstrategieën worden waar van toepassing in de BCP's gedocumenteerd.

10.2 Noodherstel

We proberen de impact van service- of operationele onderbrekingen te minimaliseren door processen en controles te implementeren die zijn ontworpen om te zorgen voor stabiel en ordelijk herstel van onze bedrijfssystemen en -gegevens. Cloud Software Group implementeert redundantie voor alle missiekritische systemen, gegevens en infrastructuur. Het noodherstelplan gebruikt de evaluatie die in de BIA is uitgevoerd, zoals hierboven vermeld, om hersteltijdparameters, methoden, prioriteiten en veiligheidsmaatregelen te identificeren en te documenteren die tijdens het hele proces zijn vereist om mislukkingen of hiaten te vermijden.

Het plan schetst de algemene structuur en benadering om kritieke systemen en gegevens te herstellen, met inbegrip van maar niet beperkt tot:

- Rollen en verantwoordelijkheden van personen of teams.
- Contactgegevens voor essentiële medewerkers of derden.
- Trainingsvereisten en plannen voor essentiële medewerkers.
- Hersteldoelstellingen, herstelprioriteiten en succesmetrieken.
- Schema van volledig herstel.

Het hoger management evalueert het noodherstelplan en keurt het goed op jaarbasis, of als er zich aanzienlijke organisatorische wijzigingen voordoen.

11. Incident respons

Cloud Software Group onderhoudt een responsplan bij cyberbeveiligingsincidenten dat nauwkeurig de processen beschrijft voor het detecteren, rapporteren, identificeren, analyseren en reageren op beveiligingsincidenten die van invloed zijn op door ons beheerde netwerken en/of systemen of Klantinhoud. Training in respons bij een beveiligingsincident en het testen ervan vinden minstens eenmaal per jaar plaats.

'Beveiligingsincident' betekent ongeautoriseerde toegang tot Klantinhoud met

het verlies van de vertrouwelijkheid, integriteit of beschikbaarheid als gevolg. Als we vaststellen dat Klantinhoud die wij beheren aan een Beveiligingsincident is blootgesteld, wordt u hiervan binnen de wettelijk verplichte termijn op de hoogte gebracht. Onze kennisgeving beschrijft, indien bekend, de aard van het incident, de tijdsperiode en de mogelijke impact voor u.

We houden een record aan van elk Beveiligingsincident.

12. Leveranciersbeheer

Cloud Software Group kan gebruikmaken van subcontractanten en vertegenwoordigers om Services te leveren. Aan subcontractanten en vertegenwoordigers wordt alleen toegang tot Klantinhoud verleend voor zover dit nodig is om de Services uit te voeren en zij zijn gebonden aan schriftelijke overeenkomsten die vereisen dat zij minstens het niveau van gegevensbeveiliging bieden dat van ons wordt vereist door dit Document, voor zover van toepassing. We blijven te allen tijde verantwoordelijk voor de naleving van de voorwaarden van de overeenkomst door de subcontractanten en vertegenwoordigers, voor zover van toepassing. Er bevindt zich een lijst van subverwerkers van Cloud Software Group die toegang tot Klantinhoud kunnen hebben in Ons Trust Center.

12.1 Onboarding

Ons risicobeheerprogramma voor derden voorziet in een systematische benadering van het beheer van de beveiligingsrisico's die het gebruik van externe leveranciers met zich meebrengt. We proberen beveiligingsrisico's te identificeren, te analyseren en te beperken voordat met de werving van dergelijke derden wordt begonnen.

Cloud Software Group sluit overeenkomsten af met leveranciers om relevante beveiligingsmaatregelen en -verplichtingen te documenteren die consistent zijn met hetgeen in dit Document is bepaald.

12.2 Continue beoordeling

We voeren periodieke beoordelingen van de beveiligingsrisico's uit om te zorgen dat de beveiligingsmaatregelen gedurende de relatie met de leverancier gehandhaafd blijven. Wijzigingen in services die worden geleverd of wijzigingen in bestaande contracten vereisen een beoordeling van de beveiligingsrisico's om te bevestigen dat deze wijzigingen geen extra of overbodig risico inhouden.

12.3 Offboarding

We streven ernaar om de inkooporganisatie van het bedrijf minstens 90 dagen op voorhand op de hoogte te stellen van de intentie om een relatie met een leverancier stop te zetten of minstens 90 dagen voor een contract met een leverancier afloopt (tenzij een vroegere opzegging vereist is). De inkooporganisatie van het bedrijf coördineert de beëindiging van de bestaande relaties om te bevestigen dat onze bedrijfsgegevens en -activa beveiligd zijn en correct worden verwerkt.

13. Naleving

13.1 Behandeling van persoonsgegevens

Persoonsgegevens bestaan uit informatie die aan een geïdentificeerde of identificeerbare persoon is gerelateerd. U bepaalt welke persoonsgegevens worden opgenomen in de Klantinhoud. Bij het uitvoeren van de Services

fungeren we als gegevensverwerker en blijft u de datacontroller voor persoonsgegevens die zijn opgenomen in de Klantinhoud. We ondernemen actie op basis van uw instructies betreffende de verwerking van dergelijke persoonsgegevens, zoals bepaald in de Overeenkomst.

Verdere informatie over de behandeling van persoonsgegevens die zijn onderworpen aan de Algemene verordening gegevensbescherming, inclusief de mechanismen die worden aangewend voor de internationale overdracht van dergelijke gegevens, wordt aangeboden in de Cloud Software Group Addendum over Gegevensverwerking.

13.2 Locatie van Services

Klanten van Cloud Services behouden controle over de keuze van de geografische locatie van de omgeving van hun Cloud Services. Op geen enkel moment tijdens het betreffende Cloud Services-abonnement zullen we de geografische locatie van de omgeving die door u is gekozen, zonder uw toestemming wijzigen. Het is mogelijk dat sommige cloudservices de keuze van bepaalde geografische locaties niet toelaten en dat Klantinhoud, als onderdeel van de algemene dienstverlening, overgedragen wordt naar de Verenigde Staten of andere landen waarin Citrix en/of dienstverleners van Citrix actief zijn om de nodige Services te kunnen leveren.

13.3 Openbaarmaking van Klantinhoud

We kunnen Klantinhoud openbaar maken voor zover dit wettelijk verplicht is, onder andere om te voldoen aan een dagvaarding, een gerechtelijk of administratief bevel of een ander bindend instrument (elk een 'Vordering'). Tenzij de wet dit verbiedt, stellen we u onmiddellijk op de hoogte van de Vordering en bieden we u de hulp die u redelijkerwijs nodig hebt om tijdig op de Vordering te kunnen reageren.

13.4 Beveiligings- en regelgevingsvereisten van Klanten

Klanten behouden dus de volledige verantwoordelijkheid voor alle beveiligingsaspecten die niet uitdrukkelijk door Citrix beheerd worden, met inbegrip van maar niet beperkt tot de technische integratie met de Services, het beheer en de controle van toegang door gebruikers, en alle applicaties en netwerken die Klanten kunnen gebruiken in combinatie met de Services.

Het blijft uw verantwoordelijkheid om te bepalen of uw gebruik van de Services, inclusief het verlenen van toegang tot Klantinhoud aan ons als onderdeel van de Services, onderworpen is aan regelgeving of veiligheidsvereisten die niet zijn opgenomen in de Overeenkomst, met inbegrip van dit Document. Klanten moeten er daarom voor zorgen dat zij geen Klantinhoud indienen of opslaan die is onderworpen aan wetten die specifieke controles opleggen die niet in dit Document zijn opgenomen, waaronder mogelijk de Amerikaanse International Traffic in Arms Regulations (ITAR) of soortgelijke regelgeving van een land die de import of export van defensieproducten of -services beperkt, beschermde gezondheidsinformatie, betaalkaartinformatie, of gegevens met gecontroleerde distributie op grond van overheidsvoorschriften, tenzij dit in de Overeenkomst en de betreffende Servicebeschrijving is bepaald en de partijen vooraf aanvullende overeenkomsten hebben gesloten (zoals een HIPAA-overeenkomst voor zakenrelaties) die nodig zijn voor onze verwerking van dergelijke gegevens.

14. Naleving Klantenaudits en -aanvragen

Cloud Software Group reageert tot eenmaal per jaar op auditverzoeken in de vorm van antwoorden op risicobeoordelingen van de Klant. Klanten kunnen

ook te allen tijde toegang krijgen tot ons Due Diligence-pakket voor een bijgewerkt beveiligingspakket en een vragenlijst. Ons Due Diligence-pakket werd gemaakt om vragen van klanten rond beveiliging te beantwoorden en bevat onmiddellijk beschikbare beveiligingsinformatie, met inbegrip van een Standardized Information Gathering (SIG) Lite-vragenlijst van Share Assessments voor onze cloudservices. Het Due Diligence-pakket kan worden gedownload vanuit ons Trust Center in Sectie Cloudverzekering Gegevensbescherming en -beveiliging.

15. Contactgegevens

Functie	Contactgegevens
Klantenondersteuning	https://www.citrix.com/contact/technical-support.html
Een beveiligingsincident melden	secure@citrix.com
Vermoedelijke kwetsbaarheden in onze Services	https://www.citrix.com/about/trust-center/ (Klik op de knop 'Een beveiligingsincident melden'.

Enterprise Sales
Noord-Amerika | +1-800-424-8749 Wereldwijd | +1 408-790-8000

Locaties
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States