citrix.

Beveiligingsdocument voor Citrix-services

Versie 2.1
Van kracht sinds donderdag
1 juli 2021

Inhoud

Toepassingsgebied 3

Beveiligingsprogramma en beleidskader 3

Toegangscontrole 4

Systeemontwikkeling en onderhoud 5

Activabeheer 6

HR-beveiliging 7

Operationele beveiliging 7

Versleuteling 9

Fysieke beveiliging 9

Bedrijfscontinuïteit en noodherstel 10

Reactie bij incidenten 11

Leveranciersbeheer 11

Naleving 12

Klantenaudits en -vragen 13

Contactgegevens van Citrix 13

In dit Beveiligingsdocument voor Citrix-services (het 'Document') vindt u een beschrijving van de beveiligingscontroles die zijn geïmplementeerd in verband met de prestaties van Citrix Cloud-services, technische ondersteuningsservices of adviesservices (de 'Services') die aan klanten worden geleverd onder de betreffende licentie- en/of serviceovereenkomst van Citrix en de toepasselijke bestelling voor de Services (samen de 'Overeenkomst'). Bèta- of lab/tech-previewservices (waaronder Citrix Cloud Labs) en interne Citrix 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. 'Klantinhoud' betekent gegevens die voor opslag naar het klantaccount zijn geüpload of gegevens in de computeromgeving van de Klant waarvoor toegang kan worden verleend aan Citrix om Services uit te voeren. 'Logboeken' betekent records van Services, inclusief maar niet beperkt tot gegevens en informatie over prestaties, stabiliteit, gebruik, beveiliging, ondersteuning en technische informatie over apparaten, systemen, gerelateerde software, services of randapparaten die betrokken zijn bij het gebruik van Services door de Klant.

1. Bereik

In dit document worden de administratieve, fysieke en technische beveiligingscontroles beschreven die Citrix gebruikt om de vertrouwelijkheid, integriteit en beschikbaarheid van de Services te handhaven. Deze controles zijn van toepassing op de operationele en servicesystemen en -omgevingen van Citrix. Citrix gebruikt ISO/IEC 27002 als basis voor het beveiligingsprogramma voor diensten en heeft industrie-specifieke certificeringen en evaluaties verkregen voor bepaalde diensten. U vindt meer informatie hierover in de sectie "Privacy en naleving" van het Citrix Trust Center.

Citrix werkt continu aan de versterking en verbetering van de beveiligingsprocedures en behoudt zich het recht voor om de hierin beschreven controles te wijzigen. Eventuele wijzigingen doen geen afbreuk aan het beveiligingsniveau tijdens de betreffende termijn van Services.

2. Beveiligingsprogramma en beleidskader

Citrix heeft een beveiligingsprogramma en beleidskader die zijn vastgelegd en goedgekeurd door het hoger en leidinggevend management van Citrix voor diverse zakelijke gebieden in het hele bedrijf.

2.1 Toezicht op beveiligingsrisico's

Het Citrix 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

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

Het programma past erkende kaders uit de sector toe, zoals ISO/IEC 31000 en ISO/IEC 27005.

2.3 Informatiebeveiliging

Citrix 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 reacties bij incidenten, waaronder onderzoek, beheersing en herstel.

2.4 Fysieke en omgevingsbeveiliging

Het Citrix Security-team, samen met het faciliteitenmanagement, houdt toezicht op de fysieke toegang tot de Citrix-faciliteiten.

3. Toegangscontrole

Citrix vereist 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. Citrix volgt het principe van minimale bevoegdheden, of beveiliging op basis van rollen, zodat de toegang van gebruikers 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 te bieden tegen fraude en fouten.

3.1 Nieuwe accounts, rollen en toegangsaanvragen

Citrix vereist een formele aanvraag voor toegang tot bedrijfssystemen of -gegevens. Elk verzoek tot toegang vereist minstens de goedkeuring door de manager van de gebruiker. Hij bevestigt de functie en toegang van de gebruiker. Toegangsbeheerders bevestigen dat de nodige goedkeuringen werden verkregen voordat toegang tot systemen of gegevens wordt verleend.

3.2 Accountbeoordeling

Citrix onderhoudt en updates een record met beveiligingsbevoegdheden voor medewerkers en contractanten die toegang hebben tot Citrix-systemen met Klantinhoud. Het principe van minimale bevoegdheden wordt toegepast.

Citrix voert 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

Citrix vereist dat gebruikerstoegang meteen 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

Citrix vereist meervoudige verificatie voor externe toegang tot Citrix-systemen door medewerkers en dwingt de volgende wachtwoordafhandelings- en managementprocedures af:

- Wachtwoorden moeten regelmatig gewijzigd worden zoals opgelegd door de systeemvereisten van Citrix.
- 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.
- Citrix handhaaft procedures om wachtwoorden te deactiveren die abusievelijk zijn onthuld
- Citrix controleert op pogingen om toegang te krijgen tot de Services met een ongeldig wachtwoord neemt automatisch actie om herhaalde pogingen te blokkeren

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

- Citrix vereist dat wachtwoorden worden verborgen (gehasht) gedurende hun levenscyclus
- Citrix verbiedt het delen van wachtwoorden

4. Systeemontwikkeling en onderhoud

Citrix handhaaft een beveiligingsproces op basis van ontwerp, inclusief 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 opgevolgd door een gespecialiseerd beveiligingsteam. Dit team is ook verantwoordelijk voor de beoordeling van het ontwerp, bedreigingsmodellering, de handmatige herziening van code, steekproefsgewijze controle en penetratietesten.

4.1 Principes van veilige ontwerpen

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

Citrix gebruikt 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. Citrix heeft 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

Het beheersproces voor veranderingen van infrastructuur en software van Citrix komt tegemoet aan de beveiligingsvereisten en vereist dat veranderingen van software en infrastructuur geautoriseerd worden, formeel gedocumenteerd worden, getest (zoals toepasselijk), beoordeeld en goedgekeurd worden voor ze in de productieomgeving aangewend kunnen 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 te migreren naar productie is beperkt tot geautoriseerd personeel.

5. Activabeheer

5.1 Beheer van fysieke en virtuele activa

Citrix handhaaft een dynamische inventaris van door Citrix beheerde fysieke en virtuele systemen die worden gebruikt om de Services uit te voeren ('Serviceactiva'). Systeemeigenaren zijn verantwoordelijk voor het onderhoud en bijwerken van hun Serviceactiva volgens Citrix-beveiligingsstandaarden.

Er zijn formele verwijderingsprocedures van kracht om de veilige verwijdering van Citrix- en klantengegevens te begeleiden. Citrix verwijdert 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.

Technologische Citrix-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 voldoen aan de vereisten van beveiligheidsbeleidsregels en -standaarden van Citrix
- Computers en gegevens zonder toezicht beveiligen

5.3 Gegevensretentie

Klantinhoud die is opgeslagen als onderdeel van Citrix Cloud-services 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 van Citrix. De zakelijke gedragscode van Citrix vereist dat alle medewerkers en contractanten de Citrix-beveiligingsbeleidsregels en -standaarden volgen, en komt specifiek tegemoet aan de bescherming van vertrouwelijke informatie evenals persoonlijke informatie van Citrix-klanten, -partners, -leveranciers en -medewerkers.

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

Citrix gebruikt momenteel achtergrondscreeners voor alle nieuwe medewerkers overal ter wereld en vereist hetzelfde voor alle personeel van externe leveranciers, tenzij dit beperkt wordt door de plaatselijke wetgeving of de arbeidswetgeving.

6.2 Training

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

6.3 Afdwinging

Van alle medewerkers wordt vereist dat ze voldoen aan de 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

Citrix heeft netwerk- en systeembeveiligingsstandaarden gedocumenteerd die zijn ontworpen om ervoor te zorgen dat netwerken en systemen veilig worden geconfigureerd. Vereiste procedures onder deze standaarden omvatten, maar zijn niet beperkt tot:

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

Citrix vereist de implementatie van antimalwaresoftware op servers en werkstations en scant 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

Citrix verzamelt 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.

Logboeken kunnen op identificeerbare wijze worden gebruikt (i) voor het leveren, beveiligen, beheren, meten en verbeteren van de Services en bijbehorende analysen, (ii) zoals verzocht door de Klant of zijn eindgebruikers, en/of (iii) voor naleving van Citrix-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. Klanten kunnen deze controle niet blokkeren of belemmeren.

Meer informatie over klantinhoud en de behandeling van logboeken vindt u in het Citrix Trust Center, sectie Privacy en naleving. Deze sectie bevat verschillende witboeken over logboeken bij Citrix.

7.3 Certificaten, toegangsgegevens en het beheer van geheime informatie

Citrix heeft een beleid inzake de levenscyclus van certificaten, toegangsgegevens en geheime informatie om de beveiliging, beschikbaarheid en vertrouwelijkheid ervan te waarborgen. Hoeders van geheime informatie moeten gedocumenteerd worden en formeel erkennen dat zij de verantwoordelijkheden van personeel dat geheime informatie beheert aanvaarden.

Hun verantwoordelijkheden omvatten, maar zijn niet beperkt tot:

- Certificaten moeten uitgegeven worden door een erkende certificeringsinstantie.
- Cryptografische sleutels mogen niet opgeslagen of doorgegeven worden in onbewerkte tekst en moeten sterke, goedgekeurde cryptografische protocollen gebruiken.
- Toegangsgegevens en geheime informatie moeten minstens een keer per jaar veranderd worden en opgeslagen worden in een goedgekeurd speciaal instrument voor authenticatiebeheer.

7.4 Kwetsbaarheidsbeheer

Citrix monitort applicaties en systemen op kwetsbaarheden met regelmatige geautomatiseerde scanning op kwetsbaarheid en poortscanning. Volledig geauthentiseerde scans worden minstens een keer per maand uitgevoerd op toestellen in het netwerk, onderdelen van de applicatieserver, fysieke en virtuele servers en eindpunten.

De geïdentificeerde kwetsbaarheden moeten binnen een bepaalde periode aangepakt worden. De periode is afhankelijk van de ernst van de kwetsbaarheden en van de aanbevelingen van de leverancier. Wanneer er geen patch, update of permanente bestrijding beschikbaar is, moeten geschikte tegenmaatregelen genomen worden om het risico dat deze kwetsbaarheid gebruikt zal worden te beperken.

8. Versleuteling

8.1 Bescherming van gegevens tijdens overdracht

Citrix 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 rust

Citrix vereist dat alle werkplekken die gebruikt worden om diensten te verlenen minstens versleuteld zijn met volledige schijfversleuteling van 128 bit. Klantinhoud mag niet op draagbare toestellen opgeslagen worden tenzij ze versleuteld zijn.

Sommige clouddiensten versleutelen standaard bepaalde gegevens en bieden ook andere versleutelingsfuncties aan die klanten kunnen gebruiken. In de van toepassing zijnde documentatie inzake clouddiensten op docs.citrix.com vindt u meer informatie.

9. Fysieke beveiliging

9.1 Citrix-faciliteiten

Citrix handhaaft 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 gadegeslagen
- ID-badges zijn vereist voor medewerkers, contractanten en gasten en moeten op elk moment zichtbaar worden gedragen tijdens de aanwezigheid in de faciliteit
- Security beheert en controleert toegang tot de faciliteiten na de 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 beschikken de Citrix-faciliteiten over:

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

Datakasten in kantoren zijn beschermd via badgetoegang en -controle.

9.2 Datacenters

Behalve de controles van de Citrix-faciliteiten die hierboven zijn beschreven, implementeert Citrix voor eigen en beheerde faciliteiten extra controles in de datacenters die worden gebruikt om de Services te leveren.

Citrix gebruikt systemen die zijn ontworpen om te beschermen tegen gegevensverlies vanwege stroomstoringen of interferentie van leidingen, inclusief 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 Citrix datacenters of cloudservices van derden gebruikt voor de levering van de Services, huurt Citrix providers in die voldoen aan de fysieke en omgevingsbeveiligingsvereisten van Citrix-faciliteiten of deze overtreffen.

10. Bedrijfscontinuïteit en noodherstel

10.1 Bedrijfscontinuïteit

Citrix 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.

Citrix voert minstens om de 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 goed op jaarbasis, of als er zich aanzienlijke organisatorische wijzigingen voordoen.

Citrix houdt plannen in geval van nood en onvoorziene gebeurtenissen aan voor alle Citrix-faciliteiten. In het geval faciliteiten niet beschikbaar zijn, krijgen medewerkers de mogelijkheid om extern te werken in andere Citrix-faciliteiten of op de locatie van hun keuze. Aanvullende herstelstrategieën worden in de BCP's gedocumenteerd waar toepasselijk.

10.2 Noodherstel

Citrix probeert 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 Citrix-bedrijfssystemen en -gegevens. Citrix 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, inclusief 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. Reactie bij incidenten

Citrix houdt een reactieplan bij cyberbeveiligingsincidenten aan dat nauwkeurig de processen beschrijft voor het detecteren, rapporteren, identificeren, analyseren en reageren op beveiligingsincidenten die van invloed zijn op door Citrix beheerde netwerken en/of systemen of Klantinhoud. Training in reactie 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 Citrix vaststelt dat Klantinhoud die het beheert aan een Beveiligingsincident is blootgesteld, wordt de Klant hiervan binnen de wettelijk verplichte termijn op de hoogte gebracht. De kennisgeving van Citrix beschrijft, indien bekend, de aard van het incident, de tijdsperiode en de mogelijke impact op de Klant.

Citrix houdt een record aan van elk Beveiligingsincident.

12. Leveranciersbeheer

Citrix 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 Citrix wordt vereist door dit Document, voor zover van toepassing. Citrix blijft 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 Citrix die toegang kunnen krijgen tot klantinhoud in het Citrix Trust Center.

12.1 Onboarding

Het Citrix-risicobeheerprogramma voor derden biedt een systematische benadering van het beheer van de beveiligingsrisico's die het gebruik van externe leveranciers met zich meebrengt. Citrix tracht beveiligingsrisico's te identificeren, te analyseren en te beperken voordat wordt begonnen met de werving van dergelijke derden.

Citrix sluit overeenkomsten af met leveranciers om relevante beveiligingsmaatregelen en -verplichtingen te documenteren die consistent zijn met wat is bepaald in dit Document.

12.2 Continue beoordeling

Citrix voert 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 de wijzigingen geen extra of overbodig risico inhouden.

12.3 Offboarding

Citrix streeft 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 opzeg vereist is). De inkooporganisatie van het bedrijf coördineert de beëindiging van de bestaande relaties om ervoor te zorgen dat de bedrijfsgegevens en -activa van Citrix beveiligd zijn en correct worden verwerkt.

13. Compliance

13.1 Behandeling van persoonsgegevens

Persoonsgegevens bestaan uit informatie die is gerelateerd aan een geïdentificeerde of identificeerbare persoon. De Klant bepaalt welke persoonsgegevens worden opgenomen in de Klantinhoud. Bij het uitvoeren van de Services fungeert Citrix als gegevensverwerker en de Klant blijft de datacontroller voor persoonsgegevens die zijn opgenomen in de Klantinhoud. Citrix onderneemt actie op basis van de instructies van de Klant 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 gegevensverwerkingsovereenkomst van Citrix.

13.2 Locatie van Services

Klanten van Citrix Cloud Services behouden controle over de keuze van de geografische locatie van de omgeving van hun Cloud Services (*zie ook de geografische overwegingen over Citrix Cloud*). Op geen enkel moment tijdens het betreffende Cloud Services-abonnement zal Citrix de geografische locatie van de omgeving die door de Klant is gekozen, zonder de toestemming van de Klant wijzigen. Het is mogelijk dat sommige clouddiensten 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 diensten te kunnen leveren.

13.3 Openbaarmaking van Klantinhoud

Citrix kan Klantinhoud openbaar maken voor zover de wet dit vereist, inclusief als reactie op een dagvaarding, een gerechtelijk of administratief bevel of een ander bindend instrument (elk een 'Vordering'). Tenzij de wet dit verbiedt, zal Citrix de Klant onmiddellijk op de hoogte stellen van de Vordering en hem de hulp bieden die hij redelijkerwijs nodig heeft om tijdig op de Vordering te kunnen reageren.

13.4 Beveiligings- en regelgevingsvereisten van Klanten

De diensten zijn ontworpen om binnen een ruimere IT-omgeving bij klanten geleverd te worden. Klanten behouden dus de volledige verantwoordelijkheid voor alle beveiligingsaspecten die niet uitdrukkelijk door Citrix beheerd worden, inclusief maar niet beperkt tot de technische integratie met de diensten, het beheer en de controle van toegang door gebruikers, en alle applicaties en netwerken die klanten kunnen gebruiken in combinatie met de diensten.

Het blijft de verantwoordelijkheid van klanten om te bepalen of hun gebruik van de diensten, inclusief het verlenen van toegang tot klantinhoud aan Citrix als onderdeel van de diensten, onderworpen is aan regelgeving of veiligheidsvereisten die niet zijn opgenomen in de Overeenkomst, inclusief 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 de verwerking van dergelijke gegevens door Citrix.

14. Klantenaudits en -vragen

Citrix zal tot eenmaal per jaar op auditverzoeken reageren in de vorm van antwoorden op risicobeoordelingen van de klant. Klanten kunnen ook te allen tijde toegang krijgen tot het Citrix Due Diligence-pakket voor een bijgewerkt beveiligingspakket en een vragenlijst. Het Citrix Due Diligence-pakket werd gemaakt om vragen van klanten rond beveiliging te beantwoorden en bevat onmiddellijk beschikbare beveiligingsinformatie, inclusief een Standardized Information Gathering (SIG) Lite-vragenlijst van Share Assessments voor elk product. De SIG-vragenlijst is de vragenlijst die door onze klanten het meest gebruikt wordt. Hij wordt in alle sectoren gebruikt. Het Due Diligence-pakket kan worden gedownload vanuit het Citrix Trust Center.

15. Citrix-contactgegevens

Functie	Contactgegevens
Klantenondersteuning	https://www.citrix.com/contact/technical-support.html
Een beveiligingsincident melden	secure@citrix.com
Vermoedelijke kwetsbaarheden in Citrix-producten	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
Hoofdkantoor | 851 Cypress Creek Road Fort Lauderdale, FL 33309, Verenigde Staten Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, Verenigde Staten