*Laatst gewijzigd: 1 maart 2018*

# Bewijsstuk voor de beveiliging van Citrix-services

Dit Bewijsstuk voor de beveiliging van Citrix-services (het Bewijsstuk) beschrijft de technische en organisatorische beveiligingsmaatregelen die worden getroffen in verband met Citrix Cloud-services, technische-ondersteuningsservices of adviserende services in het kader van een licentie-, abonnements- of serviceovereenkomst met Citrix. Naar dit Bewijsstuk wordt verwezen in dergelijke serviceovereenkomsten (de "Overeenkomsten"). Dit Bewijsstuk geldt niet voor beta- of lab/tech preview-services, waaronder Citrix Cloud Labs. Termen met een hoofdletter hebben de betekenis die vermeld staat in de Overeenkomst of die wordt gedefinieerd in dit document, waaronder in Artikel 7, Definities, hierna.

## Artikel 1. Beveiligingsmaatregelen van Citrix

Dit artikel beschrijft de fysieke, logische en administratieve maatregelen die Citrix treft om de Services te beveiligen en de bijbehorende beveiigingsverplichtingen van de Klant. Citrix hanteert ISO/IEC 27002 als basis voor zijn servicebeveiligingsprogramma.

De maatregelen die worden beschreven in artikel 1.A gelden voor alle Services. De aanvullende maatregelen die worden beschreven in paragraaf 1.B gelden voor alle algemeen beschikbare Citrix Cloud Services (gezamenlijk "Cloudservices").

Citrix behoudt zich het recht voor om de maatregelen waarvan sprake is in dit artikel 1 te wijzigen mits de maatregelen die worden getroffen tijdens de looptijd van een service waarvoor de Klant heeft betaald minimaal dezelfde bescherming van de Klantinhoud bieden als de maatregelen vermeld in dit artikel 1 op de ingangsdatum van die looptijd.

### 1.A. Bedrijfsmatige beveiligingsmaatregelen – Alle Services

| Gebied | Maatregel(en) |
|---|---|
| Beheer van beveiligingsprogramma | **Eigenaarschap** van beveiliging. Citrix heeft één of meer beveiligingsfunctionarissen aangesteld die verantwoordelijk zijn voor de coördinatie en controle van de beveiligingsmaatregelen voor de Services.<br><br>**Beveiligingsrollen en -verantwoordelijkheden**. Citrix-personeel dat toegang heeft tot Klantinhoud heeft geheimhoudingsverplichtingen.<br><br>**Servicebeveiligingsbeleid.** Citrix hanteert een omvattend algemeen beveiligingskader (Global Security Framework, GSF), dat de overkoepelende beveiligings- en veiligheidsprincipes bevat |

| Gebied | Maatregel(en) |
|---|---|
| | die zijn vastgelegd en goedgekeurd door het uitvoerend management van Citrix. Beleidsregels vermelden beveiligingseisen op een duidelijke en beknopte manier. Standaarden definiëren het proces of de methodologie om aan beleidseisen te voldoen. Het GSF-beveiligingsprogramma ondergaat regelmatig controles en evaluaties. Citrix houdt een samenvatting van het GSF-programma bij, die het op verzoek aan klanten zal bezorgen.<br><br>**Productrisicobeheer.** Citrix voert evaluaties uit van belangrijke risicogebieden met betrekking tot de Services waaronder, louter bij wijze van voorbeeld en indien van toepassing, evaluaties van privacyrisico's, open-sourcecontroles en exportcontroleanalyses. |
| Middelenbeheer | **Middeleninventaris**. Citrix houdt een inventaris bij van door Citrix beheerde uitrusting die wordt gebruikt om de Services uit te voeren ("Middelen"). Geïdentificeerde systeemeigenaars zijn verantwoordelijk voor het bijhouden en zo nodig bijwerken van de inventaris.<br><br>**Middelen- en gegevensgebruik**<br><br>Citrix identificeert en classificeert Klantinhoud om ervoor te zorgen dat de toegang op passende wijze wordt beperkt.<br><br>Citrix legt beperkingen op voor het afdrukken van Klantinhoud en de verwijdering van gedrukte materialen die Klantinhoud bevatten.<br><br>Citrix-personeel moet gemachtigd zijn alvorens Klantinhoud op te slaan op draagbare apparaten, zich extern toegang te verschaffen tot Klantinhoud, of Klantinhoud te verwerken buiten faciliteiten die worden beheerd door Citrix of zijn serviceproviders. |
| Toegangsbeheer | **Toegangsbeleid.** Citrix houdt een register bij van beveiligingsrechten van personen die toegang hebben tot Klantinhoud en volgt het principe van minimale bevoegdheden (Least Privilege).<br><br>**Toegangsmachtiging**<br><br>Citrix houdt een register bij van personeelsleden die toegang hebben tot Citrix-systemen die Klantinhoud bevatten en werkt dit bij.<br><br>Nieuwe toegang tot systemen wordt gecontroleerd en goedgekeurd door het management voordat deze wordt verleend.<br><br>Citrix voert regelmatig controles uit van gebruikersaccounts en toegewezen machtigingen voor belangrijke systemen.<br><br>Citrix identificeert personeelsleden die gemachtigde toegang tot gegevens en bronnen mogen verlenen, wijzigen of annuleren.<br><br>Wanneer meer dan één persoon toegang heeft tot systemen die Klantinhoud bevatten, zorgt |

| Gebied | Maatregel(en) |
| --- | --- |
| | Citrix ervoor dat die personen eigen identificatoren/aanmeldingen hebben.<br><br>**Minimale bevoegdheden (Least Privilege)**<br><br>Citrix geeft alleen toegang tot Klantinhoud aan personen die deze toegang nodig hebben voor de uitvoering van hun functie.<br><br>**Integriteit en vertrouwelijkheid**<br><br>Citrix eist dat gebruikers computers en gegevens beveiligen wanneer deze onbewaakt zijn.<br><br>Citrix eist dat wachtwoorden onbegrijpelijk blijven gedurende hun volledige levenscyclus.<br><br>**Verificatie**<br><br>Citrix past de standaardmethoden van de sector toe om gebruikers die toegang proberen te krijgen tot informatiesystemen te identificeren en te verifiëren.<br><br>Daar waar verificatiemechanismen gebaseerd zijn op wachtwoorden, volgt Citrix de standaardpraktijken van de sector voor het omgaan met en beheren van wachtwoorden. Dit houdt het volgende in:<br><br>Wachtwoorden worden regelmatig vernieuwd, zoals voorgeschreven door systeemvereisten en Citrix-standaarden<br><br>Wachtwoorden moeten voldoen aan lengte- en complexiteitseisen, waaronder een minimumlengte van 8 tekens<br><br>Voor personeel geldt een verbod om wachtwoorden te delen<br><br>Gedeactiveerde of verlopen identificatoren worden niet aan andere personen verstrekt<br><br>Citrix houdt procedures aan om beschadigde of per ongeluk onthulde wachtwoorden te deactiveren.<br><br>Citrix controleert op herhaalde pogingen om toegang te krijgen tot de Services met een ongeldig wachtwoord.<br><br>Citrix gebruikt methoden die zijn ontwikkeld om de vertrouwelijkheid en integriteit van wachtwoorden te handhaven wanneer ze worden toegewezen, verspreid en opgeslagen. |
| Verliespreventie | **Kwaadaardige software**. Citrix gebruikt antivirussoftware en treft andere maatregelen om te voorkomen dat kwaadaardige software ongeoorloofde toegang krijgt tot Klantinhoud, met |

| Gebied | Maatregel(en) |
| --- | --- |
| | inbegrip van kwaadaardige software afkomstig van openbare netwerken.<br><br>**Verwijdering van media.** Citrix verwijdert media wanneer ze niet langer nodig zijn op basis van classificatie en met behulp van veilige verwijderingsprocessen. |
| Fysieke en omgevingsbeveiliging (toegangscontrole, beschikbaarheidscontrole) | **Fysieke toegang tot Citrix-faciliteiten**. Citrix geeft alleen gemachtigde personen toegang tot zijn faciliteiten. Werknemers, contractanten en gasten moeten ID-badges dragen die te allen tijde zichtbaar moeten zijn zolang zij zich in de faciliteit bevinden. Citrix bewaakt toegangspunten van faciliteiten met behulp van diverse methoden, waaronder bewakers, inbraakdetectiesystemen en CCTV-camera's.<br><br>**Bescherming tegen storingen**. Citrix gebruikt systemen ter bescherming tegen gegevensverlies als gevolg van stroomuitval of lijnstoringen, waaronder globale en redundante service-infrastructuur die wordt geconfigureerd met noodherstelsites; het evalueren van datacentra en internetserviceproviders (ISP's) om de prestaties op het gebied van bandbreedte, latentie en isolatie bij noodherstel te optimaliseren; het onderbrengen van datacentra in beveiligde faciliteiten die ISP-neutraal zijn en fysieke beveiliging, redundante voeding en redundante infrastructuur bieden; en uptime-overeenkomsten met belangrijke leveranciers.<br><br>**Gehoste datacentra.** Wanneer Citrix gecolokaliseerde datacentra van derden gebruikt voor de levering van de Services, eist Citrix dat de serviceprovider voldoet aan de fysieke en omgevingsbeveiligingseisen voor door Citrix beheerde faciliteiten of deze overtreft. Minimale beveiligingseisen omvatten, maar zijn niet beperkt tot:<br>• Beperking en beveiliging van fysieke toegang (verificatie, logboeken, controle enz.)<br>• Adequate scheiding van omgevingen<br>• Brandbestrijdings-, -detectie- en -preventiemechanismen<br>• Klimaatregelsystemen (temperatuur, vochtigheid enz.)<br><br>**Cloud Computing.** Wanneer Citrix XaaS [Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)] gebruikt voor de levering van de Services, sluit Citrix overeenkomsten met XaaS-providers om een materieel vergelijkbaar niveau van fysieke toegangscontrole te waarborgen voor zijn gehoste datacentra. |
| Toepassings- en ontwikkelingsbeveiliging | **Systeemontwikkeling en -onderhoud.** Citrix hanteert een Secure by Design-proces (veilig door ontwerp), dat standaarden en wijzigingsbeheerprocedures omvat die zijn ontworpen om te voldoen aan de beveiligingseisen van informatiesystemen, codecontroles en -tests, en de |

| Gebied | Maatregel(en) |
| --- | --- |
| | beveiligingseisen voor het gebruik van testgegevens. Dit proces wordt beheerd en gecontroleerd door een gespecialiseerd technisch beveiligingsteam, dat ook verantwoordelijk is voor ontwerpcontroles, dreigingsmodellering, handmatige codecontroles en steekproeven, en penetratietests.<br><br>**Open-sourcebeheer**. Citrix gebruikt een softwaresysteem voor het beheren van open-sourcecontroles en -goedkeuringen. Daarnaast voert Citrix regelmatig scans en audits van zijn softwareproducten uit om de naleving van open-sourceregels te controleren.<br><br>**Wijzigingsbeheer.** Citrix hanteert wijzigingsbeheerprocedures die voldoen aan de beveiligingseisen van informatiesystemen, tests, acceptatie van tests en de beveiligingseisen voor het gebruik van testgegevens. Software- en configuratiewijzigingen worden beheerd en gevolgd met behulp van standaard ticketingsystemen. |
| Beveiligde bewerkingen | **Netwerkontwerp**. Citrix past mechanismen toe om beleidsregels en standaarden op het gebied van toegangsbeheer af te dwingen voor alle Services, waaronder netwerkcontrolefuncties die de toegang tot Klantinhoud bewaken. Deze omvatten, waar passend: configuratie van een niet-vertrouwde zone tussen het internet en het interne netwerk die een beveiligingsmechanisme bevat om de toegang en ongeoorloofd verkeer te beperken; en het scheiden van web- en toepassingsservers van de overeenkomstige databaseservers in een gelaagde structuur die verkeer tussen de lagen beperkt. |
| Incidentbeheer | **Incidentrespons**. Citrix hanteert een incidentresponsprogramma dat bedoeld is om beveiligings- en veiligheidsincidenten die een impact hebben op door Citrix beheerde netwerken en/of systemen of Klantinhoud te beheersen, te analyseren, te verhelpen en te communiceren.<br><br>**Incidentmelding**. 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.<br><br>**Incidentregistratie**. Citrix houdt een register van bekende beveiligingsincidenten bij met een beschrijving van het incident, de tijdsduur, de gevolgen van het incident, de naam van de melder, aan wie het incident is gemeld en de procedure voor het herstellen van gegevens en Services, indien van toepassing. |
| Leveranciersbeheer | **Onboarding**. Citrix voert beveiligingsevaluaties uit van serviceproviders die toegang krijgen tot Klantinhoud en/of onderdelen van Services die Klantinhoud verwerken.<br><br>Citrix eist van serviceproviders die zijn verbonden met de Services dat ze voldoen aan het in deze paragraaf beschreven beveiligingsniveau voor de services die ze leveren. Serviceproviders die toegang hebben tot Klantinhoud die onder de wetgeving van de Europese Unie valt zijn verplicht om zich te certificeren volgens de EU-Amerikaanse en EU-Zwitserse |

| Gebied | Maatregel(en) |
|---|---|
| | Privacy Shield-programma's of om modelcontractbepalingen uit te voeren.<br><br>**Voortdurend onderhoud.** Serviceproviders worden regelmatig geëvalueerd op basis van de gevoeligheid van hun services en de eraan verbonden risico's.<br><br>**Offboarding.** Na beëindiging van de relatie met een leverancier is de serviceprovider verplicht alle Klantinhoud die in zijn bezit is terug te bezorgen of te waarborgen dat alle Klantinhoud veilig is vernietigd. |
| Zakelijke continuïteit en noodherstel | **Zakelijke continuïteit.** Citrix hanteert plannen voor noodgevallen en onvoorziene omstandigheden voor de faciliteiten waarin zich Citrix-informatiesystemen bevinden die Klantinhoud verwerken.<br><br>**Noodherstel.** De redundante opslag van Citrix en zijn procedures voor gegevensherstel zijn bedoeld om te proberen Klantinhoud in zijn oorspronkelijke of laatst gerepliceerde staat te reconstrueren. |
| Beveiligingsverplichtingen van de Klant | De Klant is verantwoordelijk voor het beheren van de beveiliging die niet uitdrukkelijk deel uitmaakt van de Services. Dit omvat, maar is niet beperkt tot:<br>• Het beperken van de toegang van Citrix tot Klantinhoud tot wat noodzakelijk is voor het ontvangen van de Services door de Klant.<br>• Het beschermen van zijn netwerk- en serviceonderdelen tegen storingen, inclusief het bewaken en beveiligen van zijn netwerken en computeruitrusting.<br>• Het zo nodig downloaden van Klantinhoud, zowel tijdens de looptijd van Services als na beëindiging ervan.<br>• Citrix versleutelt data in transit standaard of biedt klanten middelen om data in transit te versleutelen. Meer informatie hierover is te vinden in de productdocumentatie voor de Services. Het is de verantwoordelijkheid van de Klant ervoor te zorgen dat data in transit op de juiste wijze worden beveiligd. |

**1.B. Aanvullende beveiligingsmaatregelen voor Cloudservices**

| Gebied | Maatregel(en) |
|---|---|
| Gegevensbescherming<br><br>(Beschikbaarheidscontrole, overdrachtcontrole, gegevensverwijdering) | **Failover-procedures**. Citrix past mechanismen toe om Klantinhoud te beschermen tegen verlies van beschikbaarheid, waaronder het opslaan van kopieën van Klantinhoud op een andere plaats dan waar de hoofdcomputeruitrusting die de Klantinhoud verwerkt zich bevindt. |

| Gebied | Maatregel(en) |
|---|---|
| | **Grensoverschrijdende gegevens**. Citrix versleutelt Klantinhoud die wordt overgedragen via openbare netwerken die deel uitmaken van een Service of stelt de Klant in staat om dit te doen.<br><br>**Bewaring.** Citrix kan Klantinhoud bewaren na de looptijd van de Service en archiveren voor toegang door de klant indien dit nodig is voor juridische doeleinden. Citrix zal aan de eisen van dit Bewijsstuk voldoen tot deze Klantinhoud definitief is verwijderd. Onder voorbehoud van terugbezorging, zoals direct hieronder beschreven, is Citrix niet verplicht om Klantinhoud te bewaren na beëindiging van de Service.<br><br>**Terugbezorging.** Onder voorbehoud van beschikbaarheid en de desbetreffende beschrijving van de Services heeft de Klant dertig (30) dagen de tijd om Klantinhoud te downloaden na het verstrijken van de looptijd.<br><br>**Gegevensverwijdering**. Citrix zal Klantinhoud veilig verwijderen wanneer deze niet langer is vereist voor een rechtmatig doel. |
| Beveiligde bewerkingen | **Gebeurtenisregistratie**. In bepaalde Services verzamelt Citrix Logboeken. Logboeken kunnen toegangs-ID's, tijdstippen, toegekende of geweigerde autorisatie, diagnostische gegevens zoals tracerings- en crashbestanden en andere relevante activiteiten bevatten.<br><br>Logboeken worden gebruikt (**i**) om Services en bijbehorende analysegegevens te leveren, beveiligen, beheren, meten en verbeteren (**ii**) volgens de aanwijzingen of instructies van de Klant en zijn Gebruikers, en/of (**iii**) om aan beleidsregels van Citrix, toepasselijke wet- en regelgeving of verzoeken van de overheid te voldoen. Dit kan de controle van de prestaties, de stabiliteit, het gebruik en de beveiliging van de Services en bijbehorende onderdelen omvatten. De Klant mag deze controle niet beletten of belemmeren.<br><br>Citrix kan Logboeken aanvullen met informatie afkomstig van derden voor de hierboven vermelde doeleinden.<br><br>Logboeken mogen alleen in samengestelde vorm worden gebruikt voor doeleinden die niet in dit Bewijsstuk worden vermeld. |
| Zakelijke continuïteit en noodherstel | **Back-ups.** Tenzij anders vermeld in de desbetreffende beschrijving van de Services, worden Services onderhouden in actief-actief clusters met hoge beschikbaarheid op meerdere fysieke locaties. Bij systemen die niet in een actief-actief configuratie worden onderhouden gebeurt de back-up volgens de specifieke serviceniveaudoelstellingen van de Service. |

**Artikel 2.** **<u>Behandeling van Persoonsgegevens</u>**

Onder Persoonsgegevens wordt informatie over een geïdentificeerde of identificeerbare persoon verstaan. De Klant bepaalt welke persoonsgegevens worden opgenomen in de Klantinhoud. Bij het uitvoeren van de Services fungeert Citrix als verwerker en blijft de Klant de verwerkingsverantwoordelijke voor alle persoonsgegevens die in de Klantinhoud zijn opgenomen. Citrix verwerkt deze persoonsgegevens volgens de instructies van de Klant, zoals aangegeven in de Overeenkomst.

Meer informatie over de behandeling van persoonsgegevens die zijn onderworpen aan de Algemene Verordening Gegevensbescherming, inclusief de mechanismen voor internationale overdracht van dergelijke gegevens, is te vinden in Bewijsstuk I, Voorwaarden van de Algemene Verordening Gegevensbescherming.

**Artikel 3. Locatie van Services**

Klantinhoud kan worden overgedragen naar, opgeslagen en/of verwerkt in de Verenigde Staten of andere landen waar Citrix en/of zijn serviceproviders actief zijn. De vereisten van dit Bewijsstuk blijven gelden, ongeacht waar Citrix Klantinhoud opslaat of verwerkt.

Partijen kunnen te goeder trouw onderhandelen over eventuele verdere overeenkomsten met betrekking tot gegevensverwerking of gegevensoverdracht die nodig zijn om de rechtmatige internationale overdracht van gegevens in verband met de levering van de Services door Citrix te faciliteren.

**Artikel 4. Bekendmaking van Klantinhoud**

De Klant stemt in met de bekendmaking van Klantinhoud door Citrix zoals beschreven in deze paragraaf. Citrix kan subcontractanten en vertegenwoordigers inschakelen om Services uit te voeren. Alle eventuele subcontractanten en vertegenwoordigers krijgen alleen toegang tot Klantinhoud voor zover dit nodig is om de Services uit te voeren en moeten zich houden aan schriftelijke overeenkomsten die eisen dat ze minimaal het gegevensbeschermingsniveau bieden dat Citrix eist volgens dit Bewijsstuk, waar van toepassing. Citrix blijft te allen tijde verantwoordelijk voor de naleving van de voorwaarden van de Overeenkomst door zijn subcontractanten en vertegenwoordigers, waar van toepassing.

Citrix kan ook Klantinhoud bekendmaken aan (a) gelieerde entiteiten, voor doeleinden die stroken met de Overeenkomst; (b) in verband met een verwachte of daadwerkelijke fusie, overname, verkoop, faillissement of andere vorm van reorganisatie van een deel van of al zijn activiteiten, onder voorbehoud van de verplichting om de Klantinhoud te beschermen volgens de voorwaarden van de Overeenkomst; of (c) voor juridische doeleinden, inclusief het afdwingen van zijn rechten, opsporing en preventie van fraude, het voorkomen van schendingen van de rechten of eigendommen van Citrix, Klanten, Gebruikers of het publiek; en (c) indien het hiertoe wettelijk is verplicht, onder meer in het kader van een dagvaarding, gerechtelijk of administratief bevel, of een ander bindend instrument (gezamenlijk een “Eis”). Tenzij dit bij wet is verboden, zal Citrix de Klant onverwijld in kennis stellen van een eventuele Eis en de Klant de redelijkerwijs noodzakelijke hulp bieden om de Klant in staat te stellen tijdig op de Eis te reageren.

**Artikel 5. Verplichtingen van de Klant**

**1. Algemeen**. De Klant mag de Services slechts gebruiken en heeft er slechts toegang toe voor zover de Overeenkomst dit toestaat. De Klant moet zich houden aan alle geldende wetten tijdens het gebruik van de Services.

**2. Machtigingen.** De Klant is verantwoordelijk voor het verkrijgen van alle machtigingen die Citrix nodig heeft om de Services uit te voeren, waaronder eventueel het verstrekken van kennisgevingen en het verkrijgen van toestemmingen of licenties die Citrix nodig heeft om toegang te krijgen tot Klantinhoud en deze te verwerken zoals beschreven in dit Bewijsstuk.

**3. Regelgeving.** Het is de verantwoordelijkheid van de Klant om te bepalen of Klantinhoud al dan niet is onderworpen aan aanvullende regelgevings- of beveiligingseisen naast de eisen zoals vermeld in de Overeenkomst, waaronder dit Bewijsstuk. De Klant mag geen Klantinhoud bezorgen of opslaan die valt onder de Amerikaanse regels inzake internationale wapenhandel (International Traffic in Arms Regulations, ITAR) of soortgelijke regels van een ander land die import- of exportbeperkingen opleggen aan defensieartikelen of defensiediensten. Voorts mag de Klant geen Klantinhoud bezorgen of opslaan waarvoor aanvullende regelgevende eisen gelden, zoals beschermde gezondheidsinformatie ("PHI"), betaalkaartinformatie ("PCI"), of gegevens die van overheidswege slechts beperkt mogen worden verspreid, tenzij anders vermeld in de Klantorder en de desbetreffende servicebeschrijving en de partijen vooraf aanvullende overeenkomsten hebben gesloten (zoals een Business Associate Agreement (BAA)), wat mogelijk vereist is voor Citrix om dergelijke gegevens te verwerken. Klanten van de ShareFile-service kunnen contact opnemen met Citrix via privacy@sharefile.com om een BAA aan te vragen.

**4. Klantbeveiligingsomgeving.** De Services zijn uitsluitend bedoeld voor levering in een grotere klantbeveiligingsomgeving. De Klant moet voorzien in passende beveiligingsfunctionaliteit voor alle onderdelen die niet uitdrukkelijk worden beheerd door Citrix, met inbegrip van maar niet beperkt tot toegangscontroles, firewalls, toepassingen en netwerken die samen met de Services worden gebruikt. Zie paragraaf 1.A., Beveiligingsverplichtingen van de Klant, hierboven.

**5. Melding van beveiligingsincidenten**. Het is de verantwoordelijkheid van de Klant om eventuele beveiligingsincidenten met betrekking tot de Services en/of Klantinhoud onverwijld te melden aan Citrix zoals beschreven in artikel VI, Contactgegevens van Citrix, hieronder.

**6. Naleving door Gebruikers**. De Klant is verantwoordelijk voor de naleving van de voorwaarden van de Order en de Overeenkomst door zijn Gebruikers.

## Artikel 6. Contactgegevens van Citrix

| FUNCTIE | CONTACT |
|---|---|
| Klantondersteuning | https://www.citrix.com/contact/technical-support.html |
| Een incident melden | secure@citrix.com |
| Vermoede beveiligingsproblemen in Citrix-producten | secure@citrix.com |

## Artikel 7. Definities.

Termen met een hoofdletter in het Bewijsstuk hebben de betekenis die in de Overeenkomst of hieronder vermeld staat. In geval van een tegenstrijdigheid tussen de overige termen van de Overeenkomst en een van de definities hieronder, geldt de definitie hieronder voor dit Bewijsstuk.

**Onder Klantinhoud** worden gegevens verstaan die naar het klantaccount zijn geüpload voor opslag of gegevens in de computeromgeving van de Klant waartoe Citrix toegang heeft gekregen om Services uit te voeren.

**Logboek** is een register van gebeurtenissen die betrekking hebben op de Services, waaronder registers met statistische gegevens over de prestaties, de stabiliteit, het gebruik, de beveiliging en de ondersteuning.

**Beveiligingsincident** is een ongeoorloofde toegang tot Klantinhoud die resulteert in verlies van vertrouwelijkheid, integriteit of beschikbaarheid.