ORACLE

Oracle beleid voor cloudhosting en levering

Datum van inwerkingtreding: februari 2024; versie 3.6

INHOUDSOPGAVE

OVERZICHT

Dit *Oracle beleid voor cloudhosting en levering* beschrijft (het 'leveringsbeleid') de Oracle Cloud Services die door u zijn besteld. Dit leveringsbeleid kan verwijzen naar andere beleidsdocumenten voor Oracle Cloud, elke verwijzing naar 'klant' in dit leveringsbeleid of in zulke andere beleidsdocumenten worden geacht te verwijzen naar 'u' zoals dit in uw order is gedefinieerd. Alle verplichtingen in dit leveringsbeleid zijn van toepassing op Cloud Services voor productie tenzij anders aangegeven.

Verwijzingen in dit leveringsbeleid naar een Cloud Services' "datacenterregio" verwijst naar de geografische regio die in uw order voor dergelijke services is gespecificeerd of, indien van toepassing, de geografische regio die u hebt geselecteerd bij het activeren van de instance van dergelijke services. Voor de doeleinden van de datacenterregio die van toepassing is op uw bestelde Cloud Services, zijn de volgende definities van toepassing:

- "Europa" verwijst naar de lidstaten van de Europese Unie, het Verenigd Koninkrijk en Zwitserland gezamenlijk; en
- "APAC" verwijst naar de geografische regio Azië-Pacific, met uitzondering van China, aangezien Oracle geen datacenters in China heeft.
- "Noord-Amerika" verwijst naar geografische regio's bestaande uit het vasteland van de Verenigde Staten van Amerika en Canada; behalve wanneer de entiteit die Cloud Services afneemt ervoor kiest om initieel geleverd te worden in het land Mexico. In dat geval verwijst Noord-Amerika naar de geografische regio's bestaande uit het vasteland van de Verenigde Staten van Amerika, Canada en Mexico.

In het kader van de door u bestelde Oracle Cloud Services zal uw content worden opgeslagen in de datacenterregio die van toepassing is op dergelijke services. Oracle kan uw content kopiëren naar andere locaties binnen de geïdentificeerde datacenterregio ter ondersteuning van gegevensredundantie. Woorden die in dit leveringsbeleid met een hoofdletter worden geschreven maar niet verder gedefinieerd zijn in dit leveringsbeleid, hebben de betekenis die in de Oracle overeenkomst, uw order of het beleid hieraan is toegekend. Dit leveringsbeleid wordt tweemaal per jaar bijgewerkt.

Uw order of de Service Specifications van Oracle (zoals gedefinieerd in uw overeenkomst voor Oracle Cloud Services, waaronder Oracle Cloud Services Pillar-documentatie, Service Descriptions en aanvullende definities in de Oracle Cloud Services overeenkomst) kunnen aanvullende details of uitzonderingen bevatten met betrekking tot specifieke Oracle Cloud Services. De Oracle Cloud Service Pillar-documentatie, de Service Descriptions en de programmadocumentatie voor Oracle Cloud Services zijn beschikbaar op www.oracle.com/contracts.

De Oracle Cloud Services worden geleverd onder de voorwaarden van de Oracle overeenkomst, uw order, en Service Specifications die van toepassing zijn voor dergelijke services. De levering van de Cloud Services door Oracle is afhankelijk van het naleven door u en uw gebruikers van uw

verplichtingen en verantwoordelijkheden die in deze documenten en het daarin opgenomen beleid zijn bepaald. Dit leveringsbeleid, en de documenten waarnaar hierin wordt verwezen, kunnen naar eigen goeddunken van Oracle worden gewijzigd; wijzigingen in het beleid van Oracle zullen echter niet leiden tot een materiële vermindering van het niveau van de prestaties, de beveiliging of beschikbaarheid van de Cloud Services die tijdens de Service Period van uw order worden geleverd.

Oracle Cloud Services worden geleverd door datacenters of externe leveranciers van infrastructuurservices die door Oracle zijn ingehuurd, met uitzondering van Oracle Cloud bij klantenservices. Oracle Cloud bij klantenservices zijn openbare Cloud Services die worden geïmplementeerd in ons datacenter of in een extern datacenter dat door u wordt ingezet. U kunt deze services standalone aankopen of ze kunnen geïmplementeerd worden als onderliggend platform voor andere Oracle Cloud Services. Voor Oracle Cloud bij klantenservices zal Oracle bepaalde hardwarecomponenten leveren aan uw datacenter, waaronder apparatuur voor een gateway, die Oracle nodig heeft om deze services te bedienen. U bent ervoor verantwoordelijk om voldoende ruimte, stroom en koeling te verschaffen voor implementatie van de Oracle-hardware (inclusief de externe gateway-apparatuur) en te zorgen voor een passende netwerkverbinding zodat Oracle Cloud Operations de services kan benaderen. Oracle is als enige verantwoordelijk voor onderhoud van de Oracle-hardwarecomponenten (inclusief gateway-apparatuur).

Dit leveringsbeleid is niet van toepassing op Oracle BigMachines Express of andere dergelijke Oracle Cloud aanbiedingen zoals aangegeven door Oracle in uw order of de van toepassing zijnde Service Descriptions.

1. ORACLE CLOUD BEVEILIGINGSBELEIDSLIJN

1.1 Beveiligingspraktijken ten aanzien van Oracle-informatie – Algemeen

Oracle past beveiligingscontroles en -praktijken voor Oracle Cloud Services toe die zijn ontworpen voor de bescherming van de vertrouwelijkheid, integriteit en beschikbaarheid van uw content die door Oracle wordt gehost in uw Oracle Cloud Services en voor de bescherming van uw content tegen enige ongeoorloofde verwerkingsactiviteiten zoals verlies of onwettige vernietiging van gegevens. Oracle probeert voortdurend om deze beveiligingscontroles en -praktijken te versterken en te verbeteren.

Oracle Cloud Services worden uitgevoerd onder praktijken die voldoen aan ISO/IEC 27002 (praktijkcode voor informatiebeveiligingscontroles) waaruit een uitgebreide set controles is geselecteerd. Oracle Cloud Services voldoen aan 800-53 en 800-171 van de National Institute of Standards and Technology (“NIST”).

De Oracle Cloud beveiligingspraktijken ten aanzien van informatie bepaalt beveiligingsgebieden die van toepassing zijn op Oracle Cloud Services en het gebruik van deze Oracle Cloud Services.

De beveiligingspraktijken ten aanzien van Oracle-informatie zijn van toepassing op Oracle-personeel (inclusief werknemers, aannemers en tijdelijke werknemers), evenals eventueel aanvullend beleid waaraan hun dienstverband of de services die zij Oracle leveren onderhevig zijn.

Oracle past een holistische aanpak van informatiebeveiliging toe. Hierbij wordt een meerlaagse beveiligingsstrategie toegepast en vullen beveiligingspraktijken en procedures ten aanzien van netwerken, besturingssystemen, databases en software elkaar aan, waarbij krachtige interne controles, governance en toezicht worden toegepast.

Voor die Oracle Cloud Services die u in staat stellen om uw beveiligingshouding te configureren, bent u, tenzij anderszins aangegeven, verantwoordelijk voor het configureren, uitvoeren, onderhouden en beveiligen van de besturingssystemen en andere gerelateerde software van deze geselecteerde Oracle Cloud Services (inclusief uw content) die niet door Oracle wordt geleverd. U bent verantwoordelijk voor het handhaven van passende beveiliging, bescherming en back-up van uw content. Hieronder kan het gebruik van encryptietechnologie vallen om uw content te beschermen tegen onbevoegde toegang en het routinematig archiveren van uw content.

1.2 Fysieke beveiligingsmaatregelen

Oracle neemt maatregelen om te voorkomen dat onbevoegden toegang krijgen tot de computerfaciliteiten waarin uw content wordt gehost, zoals het gebruik van beveiligingspersoneel, beveiligde gebouwen en aangewezen datacenters. Oracle biedt beveiligde computerfaciliteiten voor zowel kantoorlocaties als infrastructuur van de productiecloud. Algemene controles tussen kantoorlocaties en door Oracle beheerde co-locaties/datacenters omvatten momenteel onder andere:

- Fysieke toegang vereist autorisatie en wordt bewaakt
- Alle werknemers en bezoekers moeten duidelijk zichtbaar officiële identificatie dragen op de locatie
- Bezoekers moeten een bezoekersregister tekenen en worden begeleid en/of geobserveerd zolang zij zich op de locatie bevinden
- Bezit van sleutels/toegangskaarten en de mogelijkheid van toegang tot de locaties worden bewaakt. Personeel waarvan het dienstverband bij Oracle wordt beëindigd moet sleutels/kaarten inleveren

Aanvullende fysieke beveiligingsmaatregelen zijn van toepassing op door Oracle beheerde Cloud-datacenters. Dit omvat onder andere de volgende maatregelen:

- Locaties worden via camerabewaking (CCTV) bewaakt
- Ingangen zijn voorzien van fysieke barrières om te voorkomen dat voertuigen ongeautoriseerde toegang krijgen
- Ingangen worden 24 uur per dag, 365 dagen per jaar bemand door beveiligingspersoneel dat visuele identificatie uitvoert en het escorteren van bezoekers regelt
- Voorzorgsmaatregelen met betrekking tot omgevingsgevaren
- Elke fysieke verplaatsing van apparatuur wordt beheerd op basis van persoonlijk ingediende ontvangstbewijzen en andere geautoriseerde procedures voor wijzigingenbeheer.
- Netwerkkabels beschermen met kabeldoorvoeren en, waar mogelijk, routes door openbare gebieden te vermijden

Deze sectie is niet van toepassing op Oracle Cloud bij klantenservices. U moet uw eigen beveiligde computerfaciliteiten bieden voor het hosten en uitvoeren van de aan de Oracle Cloud bij klantenservice gerelateerde hardware (inclusief de gateway-apparatuur) en netwerkverbindingen die vereist zijn om de Oracle Cloud bij klantenservices te bieden.

1.3 Toegangscontroles voor het systeem

Het Oracle-beleid vereist dat de volgende controles worden toegepast: authenticatie met wachtwoorden en/of multifactorauthenticatie, gedocumenteerde autorisatiecontroles en toegangsregistratie. Alle externe toegang tot het Oracle Cloud netwerk door personeel dat toegang heeft tot uw content wordt beperkt door het gebruik van een Virtual Private Network dat gebruik maakt van multifactorauthenticatie. Naast het verplichte gebruik van een Virtual Private Network, voert Oracle, voordat Oracle personeel toegang krijgt tot het Oracle Cloud netwerk, controles uit op de toestand van apparaten en heeft Oracle controles ingesteld, zoals bastionhosts. Oracle verbiedt (zowel aan de hand van beleidslijnen en technische controles) het gebruik van persoonlijke apparaten om toegang te verkrijgen tot het Oracle Cloud netwerk de Oracle Cloud Services.

Voor Cloud Services gehost door Oracle: (i) logins op Cloud Services worden gelogd en (ii) logische toegang tot de datacenters wordt beperkt en beschermd.

1.4 Toegangscontroles voor gegevens

Voor servicecomponenten beheerd door Oracle is de toegang van Oracle tot uw content beperkt tot geautoriseerd personeel.

Met betrekking tot Oracle personeel dat toegang heeft tot de Oracle Cloud Services (inclusief uw content die zich in de Cloud Services bevindt) dwingt Oracle Role Based Access Controls (RBAC) af en hanteert Oracle de toegangsbeheerprincipes van "need to know", "minste toegangsrechten" en "scheiding van taken". Daarnaast biedt Oracle een mechanisme waarmee u de toegang van uw gebruikers tot de Cloud Services en tot uw content kunt controleren.

1.5 Gebruikersencryptie voor externe verbindingen

Uw toegang tot Oracle Cloud Services vindt plaats via een beveiligd communicatieprotocol dat door Oracle wordt geleverd. Als toegang plaatsvindt via een TLS-verbinding (Transport Layer Security), moet die verbinding geschikt zijn voor ten minste 128-bits encryptie. De private sleutel die wordt gebruikt om de cijfersleutel te genereren, bestaat uit ten minste 2048 bits. TLS wordt geïmplementeerd of kan worden geconfigureerd voor alle web based TLS-gecertificeerde applicaties die bij Oracle worden gebruikt. Het wordt aanbevolen de nieuwste beschikbare browsers die voor Oracle-programma's zijn gecertificeerd, die compatibel zijn met hogere codeersterkten en beter zijn beveiligd, te gebruiken om verbinding te maken met web based programma's. De lijst van gecertificeerde browsers voor elke release van Oracle Cloud Services zal beschikbaar worden gesteld via een voor u toegankelijke portal of in de bijbehorende Service Description voor de Oracle Cloud Services. In sommige gevallen wordt een versleutelde verbinding niet geaccepteerd door een site van derden, zoals een socialemediaservice, die u wilt integreren met de Oracle Cloud Service. Voor Oracle

Cloud Services waarbij HTTP-verbindingen met de site van derden door Oracle worden toegestaan, zal Oracle dergelijke HTTP-verbindingen, naast de HTTPS-verbinding, mogelijk maken.

1.6 Invoercontrole

De bron van uw content valt onder uw controle en uw verantwoordelijkheid, en de integratie van uw content in de Oracle Cloud Services wordt door u beheerd.

1.7 Scheiding van gegevens en netwerk

Uw content wordt logisch of fysiek gescheiden van de content van andere klanten die in de Oracle Cloud Services worden gehost. Alle Oracle Cloud netwerken zijn gescheiden van de zakelijke netwerken van Oracle.

1.8 Vertrouwelijkheid en training

Het Oracle personeel is onderworpen aan vertrouwelijkheidsovereenkomsten en moet bij indiensttreding een cursus in bewustwording van informatiebescherming volgen. Daarna moet al het Oracle personeel periodiek een cursus volgen in overeenstemming met het van toepassing zijnde beleid voor bewustwordingscursussen op het gebied van beveiliging en privacy.

1.9 Beheer van bedrijfsmiddelen

Oracle is verantwoordelijk voor de bescherming en de inventaris van de Cloud Services-bedrijfsmiddelen van Oracle. De verantwoordelijkheden kunnen bestaan uit het beoordelen en autoriseren van toegangsaanvragen voor mensen met een zakelijke behoefte en het bijhouden van een inventaris van bedrijfsmiddelen.

U bent verantwoordelijk voor de bedrijfsmiddelen die u beheert en die gebruikmaken van of integreren met de Oracle Cloud Services, inclusief het bepalen van de juiste informatieclassificatie voor uw content en of de gedocumenteerde controles die Oracle Cloud Services bieden geschikt zijn voor uw content. U moet alle vereiste toestemmingen of andere wettelijke rechtsgronden hebben of verkrijgen met betrekking tot het verzamelen en gebruiken van door betrokkenen verstrekte informatie, met inbegrip van dergelijke toestemmingen of andere wettelijke rechtsgronden die nodig zijn om de Cloud Services te leveren.

1.10 Intern Oracle-informatiebeveiligingsbeleid

Het Oracle Cloud beveiligingsbeleid ten aanzien van informatie bepaalt beveiligingsgebieden die van toepassing zijn op Oracle Cloud Services en uw gebruik van Oracle Cloud Services. Oracle personeel is onderworpen aan de zakelijke informatiebeveiligingsbeleidslijn van Oracle en eventuele aanvullende beleidsregels die van toepassing zijn op hun tewerkstelling of de diensten die zij aan Oracle leveren. Het Information Security Program ("ISP") van Oracle bestaat uit gedocumenteerd beleid dat rekening houdt met risicofactoren, waaronder cyber- en beveiligingsfactoren, met bijbehorende afgeleide procedures, normen en richtlijnen die nodig zijn voor een effectieve uitvoering van het beleid. De ISP van Oracle is ontworpen om de vertrouwelijkheid, integriteit, privacy, continuïteit en beschikbaarheid van uw content die door Oracle wordt gehost in uw Cloud Services te waarborgen door middel van

effectieve beveiligingsbeheerpraktijken en -controles. De ISP van Oracle wordt jaarlijks geëvalueerd door het Oracle Security Oversight Committee en indien nodig bijgewerkt.

1.11 Interne beveiligingsevaluaties en uitvoering

Oracle gebruikt interne processen voor het regelmatig testen, beoordelen, evalueren en handhaven van de effectiviteit van de technische en organisatorische beveiligingsmaatregelen die in deze sectie worden beschreven.

1.12 Externe evaluaties

Oracle kan onafhankelijke evaluaties uitvoeren op Oracle Cloud Services en daarvoor derden inschakelen, en dat voor de volgende gebieden (de scope van zulke evaluaties kan per service en land verschillen):

- SOC-1-rapporten (gebaseerd op Statement on Standards for Attestation Engagements (SSAE) nr. 18) en/of SOC-2-rapporten (gebaseerd op Trust Services Criteria)
- Overige beveiligingstests door onafhankelijke derden om de effectiviteit van administratieve en technische controles te evalueren.

Relevante informatie uit deze evaluaties kan beschikbaar worden gesteld aan klanten.

1.13 Oracle softwareveiligheidswaarborgen

Oracle Software Security Assurance (OSSA) is de methodologie van Oracle voor het inbouwen van beveiliging in het ontwerp, de build, de tests en het onderhoud van haar services, of ze nu op locatie door klanten worden gebruikt of via de Oracle Cloud worden geleverd. Het OSSA-programma wordt beschreven op https://www.oracle.com/corporate/security-practices/assurance/.

1.14 Beveiligingslogs

Logs worden gegenereerd voor beveiligingsrelevante activiteiten op besturingssystemen. Systemen worden geconfigureerd om standaard beveiligingsactiviteiten, toegang tot informatie of programma's, systeemgebeurtenissen zoals waarschuwingen, consoleberichten en systeemfouten te loggen. Oracle evalueert logbestanden voor forensische doeleinden en incidenten; geïdentificeerde abnormale activiteiten worden opgenomen in het incidentbeheersingsproces. Beveiligingslogs worden opgeslagen in het Security Information and Event Management-systeem (of gelijkwaardig systeem) in een oorspronkelijke, ongewijzigde indeling en bewaard in overeenstemming met het interne beleid van Oracle. Dergelijk logs worden online bewaard voor minstens één jaar. Deze logs worden bewaard en gebruikt door Oracle voor onze interne beveiligingsactiviteiten in het kader van de Oracle Cloud Services.

1.15 Andere beveiligingsgerelateerde verplichtingen van klant

U bent verantwoordelijk voor:

- Het implementeren van uw eigen uitgebreide beveiligingssysteem en operationeel beleid, normen en procedures op basis van uw op risico's gebaseerde beoordelingen en bedrijfsvereisten
- Het garanderen dat apparaten van eindgebruikers voldoen aan vereisten ten aanzien van webbrowser en minimale netwerkbandbreedte voor toegang tot de Oracle Cloud Services.
- Het beheren van beveiligingscontroles van clientapparaten, zodat antivirus- en malwarecontroles worden uitgevoerd op gegevens en bestanden voordat gegevens worden geïmporteerd in of geüpload naar de Oracle Cloud Services.
- Het onderhouden van door klant beheerde accounts in navolging van uw beleid en beste beveiligingspraktijken
- Daarnaast bent u voor Oracle Cloud bij klantenservices verantwoordelijk voor het volgende:
    - Geschikte fysieke beveiliging en netwerkbeveiliging
    - Beveiligingsmonitoring om het risico van realtime bedreigingen te verminderen en ongeautoriseerde toegang tot uw Oracle Cloud Service vanuit uw netwerken te voorkomen; dit omvat inbraakdetectiesystemen, toegangscontroles, firewalls en alle andere netwerkmonitoring, en alle beheertools die door u worden beheerd.

2. ORACLE CLOUD SERVICE CONTINUÏTEITSBELEID

2.1 Strategie inzake hoge beschikbaarheid van Oracle Cloud Services

Oracle zet de Cloud Services in op een veerkrachtige computerinfrastructuur die ontworpen is om de beschikbaarheid en continuïteit van de services te handhaven in het geval van een incident dat van invloed is op de services. Datacenters die Oracle gebruikt om Oracle Cloud Services te hosten hebben component- en stroomredundantie met back-upgeneratoren, en Oracle kan redundantie op een of meer lagen implementeren, inclusief netwerkinfrastructuur, programmaservers, databaseservers en/of opslag.

2.2 Back-upstrategie van Oracle Cloud Services

Oracle maakt periodiek back-ups van uw content in uw instance van de Oracle Cloud Services met als enig doel het verlies van gegevens te beperken in het geval van een incident. Back-ups worden opgeslagen op de primaire locatie die wordt gebruikt om de Oracle Cloud Services te leveren en kunnen ook worden opgeslagen op een alternatieve locatie voor redundantiedoeleinden. Een back-up wordt doorgaans online of offline bewaard gedurende een periode van ten minste 60 dagen na de datum waarop de back-up is gemaakt. In principe worden uw gegevens niet namens u door Oracle geüpdatet, ingevoegd, verwijderd of teruggezet. Bij uitzondering kan Oracle na schriftelijke goedkeuring u ondersteunen bij het terugzetten van gegevens die u hebt verloren als gevolg van uw eigen acties.

Voor Cloud Services die u in staat stellen back-ups te configureren in overeenstemming met uw eigen beleid, bent u verantwoordelijk voor het uitvoeren van back-ups en het herstellen van uw content.

Daarnaast moedigen we u aan om een bedrijfscontinuïteitsplan te ontwikkelen en de continuïteit van uw eigen activiteiten te waarborgen in het geval van een calamiteit.

2.3 Oracle Business Continuity

Oracle zal gedurende de duur te allen tijde een plan handhaven dat betrekking heeft op de interne bedrijfsvoering van Oracle met als doel de verstoring van de dienstverlening te minimaliseren indien zich een ramp, verstoring of geval van overmacht voordoet ("BC-plan").

Het BC-plan formuleert, documenteert en implementeert processen, procedures en maatregelen om te zorgen dat de beveiligingsbepalingen die van toepassing zijn op de Oracle Cloud Services niet worden aangetast indien een beroep wordt gedaan op het BC-plan. Het doel van het BC-plan is onder meer te voorzien in veerkracht voor de interne bedrijfsvoering van Oracle voor de continuïteit en het onderhoud van de Oracle Cloud Services, ongeacht de oorzaak.

3. ORACLE CLOUD SERVICENIVEAU-OVEREENKOMST

3.1 Uren van beschikbaarheid

De Oracle Cloud Services zijn ontworpen om 24 uur per dag, 7 dagen per week, 365 dagen per jaar beschikbaar te zijn, met uitzondering van onderhoudsperioden, upgrades van technologie en zoals anders wordt uiteengezet in de Oracle overeenkomst, de order en deze *Oracle Cloud serviceniveau-overeenkomst*.

3.2 Servicebeschikbaarheid

Vanaf de activering van uw Oracle Cloud Service probeert Oracle het beoogde servicebeschikbaarheidsniveau of de beoogde service-uptime van 99,9% te behalen. Dit is in overeenstemming met de bepalingen in de Cloud Service Pillar-documentatie voor de van toepassing zijnde Cloud Service (of een ander beoogd beschikbaarheidsniveau of andere beoogde uptime die in dergelijke documentatie door Oracle voor de Cloud Service is aangegeven).

Het voorgaande is afhankelijk van uw naleving van de door Oracle aanbevolen minimale technische configuratievereisten voor toegang tot en gebruik van de Oracle Cloud Services vanaf uw netwerkinfrastructuur en uw gebruikerswerkstations zoals uiteengezet in de programmadocumentatie voor de van toepassing zijnde Oracle Cloud Services.

3.2.1 Meting van beschikbaarheid

Aan het einde van elke kalendermaand van de Service Period meet Oracle het servicebeschikbaarheidsniveau door het verschil tussen het totale aantal minuten in de maandelijkse meetperiode en enige ongeplande onderbreking te delen door het totale aantal minuten in de meetperiode, en het resultaat vervolgens te vermenigvuldigen met 100 om tot een percentage te komen.

$$\left(\frac{Number\ of\ minutes\ in\ the\ month - Number\ of\ minutes\ of\ unplanned\ downtime}{Number\ of\ minutes\ in\ the\ month}\right) * 100$$

Aantal minuten in een maand van 30 dagen = 30 dagen * 24 uur per de dag * 60 minuten per uur

Aantal niet geplande minuten in de maand = minuten niet geplande onderbreking zoals gedefinieerd in de sectie "*Definitie van niet geplande onderbreking*".

Voorbeeld: juni heeft 30 dagen = 30*24*60 = 43.200 minuten in de maand

Als er in de maand juni 90 minuten ongeplande onderbreking optreedt, is de vergelijking als volgt:

$((43{,}200 - 90)/43.200) * 100$ = 99,8% serviceniveaubeschikbaarheid

3.2.2 Rapportage van beschikbaarheid

Oracle zal u statistieken verstrekken over het servicebeschikbaarheidsniveau voor Oracle Cloud Services die u hebt aangeschaft in uw order, ofwel via selfservice ofwel via een service request dat u bij Oracle indient en waarin u om de statistieken verzoekt.

3.2.3 Servicecredits

U kunt servicecredits ontvangen indien het beoogde servicebeschikbaarheidsniveau of de beoogde service-uptime voor de Oracle Cloud Services die u hebt aangeschaft in uw order onder het/de gedefinieerde beoogde servicebeschikbaarheidsniveau of beoogde service-uptime dat/die van toepassing zijn op dergelijke services. Servicecredits worden bepaald in de Oracle Cloud Service Pillar-documentatie of Service Descriptions die van toepassing zijn op de door u aangekochte Oracle Cloud Services. Niettegenstaande de bepalingen van dit artikel, als uw order bij Oracle of de Service Specifications die van toepassing zijn op uw order voor een bepaalde Oracle Cloud Service recht geeft op een hoger bedrag aan servicecredits, dan kunt u de servicecredits ontvangen onder de bepaling die voorziet in het hoogste bedrag aan servicecredits voor u, maar u kunt geen servicecredits ontvangen onder meerdere bepalingen voor hetzelfde event.

3.3 Definitie van ongeplande onderbreking

Oracle Cloud Services worden geïmplementeerd in veerkrachtige computingfaciliteiten met veerkrachtige infrastructuur, redundante netwerkverbindingen en stroom voor elke hostingfaciliteit.

"Ongeplande uitvaltijd" betekent elk moment waarop een probleem met de Cloud Services uw connectiviteit verhindert. Ongeplande uitvaltijd omvat geen momenten waarop de Cloud Services of een component van de Cloud Services niet beschikbaar is als gevolg van: (i) gepland onderhoud, (ii) omstandigheden buiten de controle van Oracle en andere gevallen van overmacht (bijv. uitval ingeleid op uw verzoek, uitval veroorzaakt door niet-Oracle infrastructuur zoals elektrische, netwerk-, telecommunicatie- of andere connectiviteitsapparatuur, beveiligingsaanvallen, natuurrampen of politieke gebeurtenissen), (iii) enig handelen of nalaten van u, uw gebruikers of een derde (anders dan agenten en aannemers van Oracle die Oracle heeft ingeschakeld om de van toepassing zijnde Oracle Cloud Services uit te voeren) of (iv) enige opschorting door Oracle toegestaan onder uw Oracle overeenkomst of uw order. Daarnaast omvat ongeplande uitvaltijd met betrekking tot Oracle Cloud bij klantenservices ook geen uitvaltijd of andere onbeschikbaarheid (i) van uw datacenter (bijv. als gevolg

van onderhoud) of (ii) buiten de on-site uren zoals gedefinieerd onder uw order voor personeel van Oracle Cloud Operations in uw datacenter.

3.4 Bewaking

Oracle gebruikt diverse softwaretools voor het bewaken van de beschikbaarheid en prestaties van de Oracle Cloud Services en de werking van infrastructuur- en netwerkcomponenten. Oracle bewaakt geen niet door Oracle beheerde componenten die u gebruikt in de Oracle Cloud Services, zoals niet-Oracle applicaties, en pakt ook geen afwijkingen aan die daarmee worden ervaren.

3.4.1 Bewaakte componenten

Oracle bewaakt de hardware die de Oracle Cloud Services ondersteunt, en genereert waarschuwingen met betrekking tot bewaakte netwerkcomponenten, zoals CPU, geheugen, opslag, database en andere componenten. Het operationeel personeel van Oracle Cloud bewaakt alle waarschuwingen die betrekking hebben op afwijkingen van de door Oracle gedefinieerde drempels en volgt standaard operationele procedures voor het onderzoeken en oplossen van onderliggende problemen.

3.4.2 Tools voor bewaking en tests bij de klant

Oracle staat u toe beperkte functionele tests voor Oracle Cloud Services uit te voeren in uw testinstance. Specifieke regels voor testen kunt u vinden in de programmadocumentatie.

Oracle voert regelmatig penetratie- en kwetsbaarheidstests en beveiligingsbeoordelingen uit op Cloud-infrastructuur, -platforms en -toepassingen om de algemene beveiliging van Cloud Services te valideren en te verbeteren. De Oracle Cloud Services programmadocumentatie beschrijft waar en hoe u componenten die u beheert of aanmaakt in Oracle Cloud Services kunt beoordelen of testen, inclusief niet-Oracle applicaties, niet-Oracle databanken, overige van toepassing zijnde niet-Oracle software, code, of het gebruik van data-scrapingtools.

Oracle behoudt zich het recht voor om de toegang tot enige tool of technologie die de richtlijnen in deze sectie of de van toepassing zijnde Oracle Cloud Services programmadocumentatie schendt te verwijderen of uit te schakelen zonder enige aansprakelijkheid jegens u.

4. ORACLE CLOUD BELEID VOOR CHANGE MANAGEMENT

4.1 Oracle Cloud Change Management en onderhoud

Oracle Cloud Operations voert wijzigingen door in de hardware infrastructuur, besturingssoftware, productsoftware en ondersteunende applicatiesoftware van de cloud die door Oracle als onderdeel van de Oracle Cloud Services worden geleverd, om de operationele stabiliteit, beschikbaarheid, beveiliging, prestaties en actualiteit van de Oracle Cloud Services te behouden. Oracle volgt formele change management procedures om wijzigingen te controleren, te testen en goed te keuren voorafgaand aan toepassing in de service.

Wijzigingen die via de change management procedures worden doorgevoerd, omvatten systeem- en serviceonderhoud, upgrades, updates en klantspecifieke wijzigingen. De Oracle Services Cloud

change management procedures zijn ontwikkeld om serviceonderbreking tijdens het doorvoeren van wijzigingen te minimaliseren.

Oracle reserveert specifieke onderhoudsperioden voor wijzigingen waarbij de Oracle Cloud Service gedurende die perioden mogelijk niet beschikbaar kan zijn. Oracle probeert te zorgen dat de change management procedures worden uitgevoerd tijdens geplande onderhoudswindows (waarvan Oracle u vooraf op de hoogte zal brengen), met inachtneming van perioden met weinig dataverkeer en geografische vereisten.

Oracle zal een voorafgaande kennisgeving verstrekken van aanpassingen aan de planning van de onderhoudswindows. In het geval van klantspecifieke wijzigingen en upgrades zal Oracle, waar haalbaar, de onderhoudsperioden met u coördineren.

Voor wijzigingen die naar verwachting een onderbreking van de services zullen veroorzaken, wordt de duur van de onderhoudsperioden voor gepland onderhoud niet meegenomen in de berekening van het aantal minuten ongeplande uitvaltijd in de maandelijkse meetperiode voor het servicebeschikbaarheidsniveau (raadpleeg de bovenstaande *Oracle Cloud serviceniveau-overeenkomst*). Oracle levert commercieel redelijke inspanningen om het gebruik van deze gereserveerde onderhoudsperioden te minimaliseren en om de duur van de onderhoudsactiviteiten die een serviceonderbreking veroorzaken te minimaliseren.

Voor Oracle Cloud Services die u in staat stellen onderhoudsactiviteiten uit te voeren, bent u verantwoordelijk voor het configureren en onderhouden van de besturingssystemen en andere gerelateerde software.

4.1.1 Kritiek beveiligingsonderhoud

Oracle kan vereist zijn kritiek beveiligingsonderhoud uit te voeren om de beveiliging van de Oracle Cloud Services te beschermen. Kritiek beveiligingsonderhoud is vereist om in te grijpen bij een urgente situatie (bv. een beveiligingslek) met betrekking tot de Oracle Cloud Service of Oracle infrastructuur die niet kan worden aangepakt tenzij met een noodinterventie. Oracle tracht het gebruik van kritiek beveiligingsonderhoud te beperken en, voor zover redelijk onder de omstandigheden, om 24 uur van tevoren te melden dat kritiek beveiligingsonderhoud nodig is dat een serviceonderbreking vereist buiten de geplande onderhoudsperioden.

4.1.2 Datacentermigraties

Oracle kan uw Oracle Cloud Services geïmplementeerd in de datacenters die Oracle inschakelt migreren tussen productiedatacenters binnen dezelfde datacenterregio zoals nodig geacht door Oracle of in het geval van disaster recovery. Oracle zal, in het geval van datacentermigraties anders dan disaster recovery, u een kennisgeving van minimaal 30 dagen bezorgen.

4.2 Softwareversiebeheer

4.2.1 Software-updates

Oracle vereist van alle klanten van Oracle Cloud Services dat zij de softwareversies van de Oracle Cloud Services actueel houden met de softwareversies die Oracle als ondersteunde releases aanduidt voor dergelijke Oracle Cloud Services. Software updates zijn vereist voor de Oracle Cloud Services om de versies actueel te houden. De verplichtingen van Oracle volgens dit leveringsbeleid (inclusief het *Oracle Cloud servicecontinuïteitsbeleid,* de *Oracle Cloud serviceniveau-overeenkomst* en het *Oracle beleid voor Cloud Support*) zijn afhankelijk van het actueel houden door u van de ondersteunde versie van uw Oracle Cloud Services. Oracle is niet verantwoordelijk voor problemen met prestaties, functionaliteit, beschikbaarheid of beveiliging van Oracle Cloud Services die een mogelijk een gevolg zijn van het gebruik van oudere versies.

4.2.2 Einde levensduur

Oracle zal uitsluitend de ondersteunde releases van een Oracle Cloud Service hosten en ondersteunen. Alle andere versies van de Oracle Cloud Service zullen worden beschouwd als 'einde levensduur' (End of Life; EOL). U moet een update van de Oracle Cloud Services uitvoeren naar de laatste versie voorafgaand aan de EOL van een bepaalde versie. U erkent dat het niet uitvoeren van de update voorafgaand aan de EOL van een Oracle Cloud Service-versie ertoe kan leiden dat een update automatisch door Oracle wordt uitgevoerd of dat de Oracle Cloud Services worden opgeschort. Onder bepaalde omstandigheden waarbij een Oracle Cloud Service-versie de EOL bereikt en Oracle geen geüpdatete versie beschikbaar stelt, kan Oracle een daaropvolgende Oracle Cloud Service aanwijzen en u vereisen daarnaar over te stappen.

5. BELEID VOOR ORACLE CLOUD SUPPORT

De ondersteuning die in dit *Beleid voor Oracle Cloud Support* wordt beschreven, is uitsluitend van toepassing op Oracle Cloud Services en wordt door Oracle geleverd als onderdeel van dergelijke Oracle Cloud Services ingevolge uw order. Oracle kan aanvullende ondersteunende service-aanbiedingen voor de Oracle Cloud Services beschikbaar stellen, die u tegen aanvullende vergoeding kunt bestellen.

5.1 Voorwaarden voor Oracle Cloud Support

5.1.1 Ondersteuningsvergoedingen

De vergoedingen die u betaalt voor de Oracle Cloud Services ingevolge uw order, omvatten de ondersteuning die in dit *Beleid voor Oracle Cloud Support wordt beschreven*. Bijkomende vergoedingen zijn van toepassing op aanvullende Oracle-ondersteuningsservices die door u worden aangeschaft.

5.1.2 Ondersteuningsperiode

Oracle Cloud-ondersteuning is beschikbaar na de startdatum van de Oracle Cloud Services en eindigt na afloop of beëindiging van de services (de 'ondersteuningsperiode'). Oracle is niet verplicht om na

afloop van de ondersteuningsperiode de ondersteuning te bieden die in dit beleid voor Oracle Cloud Support wordt beschreven.

5.1.3 Technische contactpersonen

De technische contactpersonen fungeren als enige tussenpersoon tussen u en Oracle voor ondersteuning voor Oracle Cloud Services. Dergelijke technische contactpersonen moeten, op zijn minst, initiële basistraining hebben gevolgd en, waar nodig, aanvullende training geschikt voor de specifieke rol of implementatiefase, gespecialiseerd service-/productgebruik en migratie. Uw technische contactpersonen moeten kennis hebben van de Oracle Cloud Services om problemen met het systeem te helpen oplossen en Oracle bij te staan bij het analyseren en oplossen van service requests. Wanneer een service request wordt ingediend, moet uw technische contactpersoon een basisbegrip hebben van het probleem dat wordt ondervonden en de mogelijkheid om het probleem te reproduceren om Oracle bij te staan bij het diagnosticeren en achterhalen van het probleem. Om onderbreking in Oracle-ondersteuning voor Oracle Cloud Services te voorkomen, moet u Oracle op de hoogte stellen zodra de verantwoordelijkheden van de technische contactpersoon worden overgedragen op een andere persoon.

5.1.4 Oracle Cloud Support

Oracle Support voor Oracle Cloud Services bestaat uit:

- Diagnose van problemen met de Oracle Cloud Services.
- Commercieel redelijke inspanningen om gemelde en verifieerbare fouten in de Oracle Cloud Services op te lossen, zodat deze Oracle Cloud Services in elk materieel opzicht functioneren zoals beschreven in de bijbehorende Service Specifications
- Ondersteuning tijdens Change Management activiteiten beschreven in het *Oracle Cloud Change Management beleid* (zie hierboven)
- 24 uur per dag, 7 dagen per week assistentie bij technische service requests
- 24 uur per dag, 7 dagen per week toegang tot een Cloud Customer Support Portal opgezet door Oracle en live telefonische ondersteuning om service requests vast te leggen
- Toegang tot community forums
- Niet-technische assistentie door de klantenservice tijdens normale Oracle-werkuren (8:00 tot 17:00) plaatselijke tijd van het land.

5.2 Systemen voor klantondersteuning voor Oracle Cloud

5.2.1 Oracle Cloud Customer Support Portal

Oracle biedt ondersteuning voor de Oracle Cloud Service die door u is verkregen, onder een order, via de Cloud Customer Support Portal (ondersteuningsportal), die voor die bepaalde Cloud Service is opgezet. Hoewel Oracle Cloud Support en de portals (inclusief delen van de services die zij kunnen leveren) deel kunnen uitmaken van uw order, vormen ze geen aanbod van Oracle Cloud Service en kunnen ze wereldwijd worden geleverd, waarbij toegang tot deze portals valt onder de gebruiksvoorwaarden die op de van toepassing zijnde portalwebsites zijn geplaatst, en die kunnen

worden gewijzigd. Wanneer dergelijke portals u toestaan om informatie te uploaden, bent u ervoor verantwoordelijk dat u en uw gebruikers geen door de overheid uitgegeven identificatienummers of gezondheids-, financiële, betaalkaart-, gecontroleerde niet-geclassificeerde informatie of andere gevoelige persoonlijke informatie in dergelijke portals plaatsen, tenzij uitdrukkelijk anders is toegestaan volgens de voorwaarden van de ondersteuningsportal of uw van toepassing zijnde Cloud Services order. Toegang tot de ondersteuningsportal is beperkt tot uw aangewezen technische contactpersonen en andere geautoriseerde gebruikers van de Oracle Cloud Services. Waar van toepassing, worden op de ondersteuningsportal ondersteuningsdetails geplaatst voor uw aangewezen technische contactpersonen om het gebruik van Oracle ondersteuning voor Oracle Cloud Services mogelijk te maken. Ondersteuningsmeldingen en -waarschuwingen die relevant zijn voor uw service requests worden op de ondersteuningsportal geplaatst.

5.2.2 Live telefonische ondersteuning

Uw technische contactpersonen hebben toegang tot live telefonische ondersteuning via de telefoonnummers en de contactgegevens die op de ondersteuningswebsite van Oracle staan aangegeven op https://www.oracle.com/support/contact.html.

5.3 Severity-definities

Service requests voor Cloud Services kunnen door uw aangewezen technische contactpersonen worden ingediend via de ondersteuningsportal. Het severity-niveau van een service request moet worden gebaseerd op uw input en zal gebaseerd zijn op de volgende severity-definities:

5.3.1 Severity 1 (Kritieke uitval)

Uw productiegebruik van de Oracle Cloud Services is gestopt of wordt zo sterk gehinderd dat u niet redelijk kan blijven werken. U ervaart een volledige onderbreking van de service. De getroffen werking is van cruciaal businessbelang en het betreft een noodsituatie. Een service request met severity 1 heeft één of meer van de volgende kenmerken:

- Gegevens beschadigd
- Een essentiële gedocumenteerde functie is niet beschikbaar
- De service 'hangt' gedurende onbepaalde tijd, waardoor sprake is van onacceptabele of oneindige vertraging ten aanzien van resources of respons
- De service crasht en blijft dat herhaaldelijk doen na pogingen tot opnieuw opstarten
- Beveiligingsincident met mogelijke gevolgen voor de vertrouwelijkheid, integriteit of beschikbaarheid van de service

Oracle zal redelijke inspanningen leveren om binnen vijftien (15) minuten te reageren op service requests met severity 1. Gedurende de periode waarin Oracle bezig is met het afhandelen van een service request met severity 1, gaat u ermee akkoord om uw technische contactpersoon 24 uur per dag en 7 dagen per week beschikbaar te stellen. Oracle zal 24 uur per dag, 7 dagen per week werken totdat de service request met severity 1 is opgelost, of totdat een redelijke workaround is ingesteld, een goedgekeurd actieplan is ingesteld of de contactpersoon van de klant niet meer 24 uur per dag en 7 dagen per week beschikbaar is. U moet Oracle binnen deze 24x7-periode een technische

contactpersoon toewijzen om te helpen bij het verzamelen van gegevens, het uitvoeren van tests en het toepassen van fixes. U moet de severity-classificatie zorgvuldig kiezen, zodat geldige severity 1-situaties de benodigde resources krijgen toegewezen door Oracle.

5.3.2 Severity 2 (Aanzienlijk verminderde functionaliteit)

U ervaart een ernstig verlies van service. Belangrijke functies van de Oracle Cloud Services zijn niet beschikbaar en er is geen acceptabele workaround, maar de activiteiten kunnen op een beperkte manier doorgaan.

5.3.3 Severity 3 (Technisch probleem)

U ervaart een beperkt serviceverlies. De impact is een ongemak, waarvoor mogelijk een workaround nodig is om de functionaliteit te herstellen.

5.3.4 Severity 4 (Algemene assistentie)

U verzoekt om informatie, uitbreiding of toelichting van documentatie met betrekking tot de Oracle Cloud Services, maar er is geen sprake van een impact op de werking van een dergelijke service. U ervaart geen verlies van service.

5.4 Verandering van severity-niveau van service request

5.4.1 Initieel severity-niveau

Wanneer een service request wordt aangemaakt, zal Oracle een eerste severity-niveau van de service request vastleggen op basis van de bovenstaande severity-definities en/of uw input. De initiële focus van Oracle, bij het aanmaken van een service request, is het oplossen van de onderliggende problemen van de service request. Het severity-niveau van een service request kan worden aangepast zoals hieronder wordt beschreven.

5.4.2 Verlagen van service-requestniveaus

Naarmate het werk aan het onderliggende probleem vordert en het huidige toegewezen severity-niveau van het probleem niet meer gerechtvaardigd is op basis van de huidige impact op de werking van de van toepassing zijnde Oracle Cloud Service, wordt het severity-niveau verlaagd tot het severity-niveau dat de huidige impact het best weerspiegelt.

5.4.3 Upgraden van service-requestniveaus

Als tijdens het service-requestproces, het toewijzen van een hoger severity-niveau, dan het huidig toegewezen severity-niveau aan het probleem gerechtvaardigd is op basis van de huidige impact op de productiewerking van de van toepassing zijnde Oracle Cloud Service, wordt het severity-niveau verhoogd tot het severity-niveau dat de huidige impact het best weerspiegelt.

5.4.4 Handhaving van definities van severity-niveaus

U zal ervoor zorgen dat de toewijzing en aanpassing van een toegekend severity-niveau juist gebaseerd is op de huidige impact op de productiewerking van de van toepassing zijnde Oracle Cloud Service.

5.5 Escalatie van service request

Voor door u geëscaleerde service requests zal de ondersteuningsanalist van Oracle de Oracle service request escalation manager, die verantwoordelijk is voor het beheer van de escalatie, inschakelen. De service request escalation manager van Oracle zal met u samenwerken om een actieplan te ontwikkelen en de juiste Oracle-resources toe te wijzen. Als het onderliggende probleem van de service request onopgelost blijft, kunt u contact opnemen met de Oracle service request escalation manager om de service request te evalueren en te verzoeken dat deze geëscaleerd wordt naar het volgende niveau bij Oracle. Om een oplossing voor een geëscaleerde service request mogelijk te maken, moet u contactpersonen doorgeven binnen uw organisatie van hetzelfde niveau als de contactpersonen bij Oracle waarnaar de service request is geëscaleerd.

6. ORACLE CLOUD SCHORSINGS- EN BEËINDIGINGSBELEID

6.1 Beëindiging van Oracle Cloud Services

Gedurende een periode van 60 dagen na het einde van de Service Period voor de Cloud Services of, indien van toepassing, de periode van 60 dagen na uw beëindiging van Cloud Services die u verbruikt in een Pay-as-You-Go-model, na het einde van de bijbehorende Service Period, zal Oracle, via veilige protocollen en in een gestructureerd, machineleesbaar formaat, uw content die zich in de Cloud Services bevindt beschikbaar stellen, of het servicesysteem toegankelijk houden, zodat u gegevens kunt ophalen.

Voor gratis proefversies en pilots van Cloud Services zal Oracle uw content beschikbaar stellen voor een periode van 30 dagen na afloop van de proefversie of pilot. Tijdens deze ophaalperiode is de Oracle Cloud serviceniveau-overeenkomst niet van toepassing en mag het servicesysteem niet worden gebruikt voor productieactiviteiten. Oracle is niet verplicht om uw content te behouden na deze periode van ophaalperiode.

Als u assistentie nodig heeft van Oracle om toegang te verkrijgen tot of kopieën van uw content, moet u een service request indienen in de ondersteuningsportal.

Het ophalen van gegevens en enige gerelateerde assistentie door Oracle is niet van toepassing op Oracle Cloud Services waarbij uw content niet wordt opgeslagen. U bent ervoor verantwoordelijk dat als deze services afhankelijk zijn van afzonderlijke Cloud Services, zoals Storage Cloud Service of Database Cloud Services, voor de opslag van gegevens, die afzonderlijke Cloud Services een geldige duur moeten hebben tot aan het einde van de service die wordt beëindigd om het ophalen van gegevens mogelijk te maken, of voor het anderszins nemen van gepaste actie om een back-up te maken van uw content of deze anderszins apart op te slaan terwijl de productie Oracle Cloud Services nog actief zijn vóór het einde van de Service Period.

Na het verstrijken van de ophaalperiode zal Oracle uw content van de Cloud Services verwijderen (tenzij anders vereist door de van toepassing zijnde wetgeving).

Waar het Oracle Cloud bij klantenservices betreft, moet u alle Oracle Cloud bij klantenservice gerelateerde hardwarecomponenten (inclusief de gateway-apparatuur), die door Oracle zijn geleverd,

beschikbaar stellen zodat Oracle deze kan ophalen. Dergelijke componenten moeten in goede staat zijn en in dezelfde toestand als bij de aanvang van Oracle Cloud bij klantenservices, onderhevig aan redelijke slijtage als gevolg van gepast gebruik.

7 GEBRUIK VAN SERVICES

Het is uw verantwoordelijkheid ervoor te zorgen dat de toegang tot en het gebruik van de verworven Oracle Cloud Services, en het voordeel dat wordt verkregen van dergelijke Cloud Services, enkel voorbehouden zijn aan en bestemd zijn voor gebruikers in landen overeenkomstig het Global Trade Compliance beleid van Oracle dat beschikbaar is op https://www.oracle.com/corporate/security-practices/corporate/governance/global-trade-compliance.html.