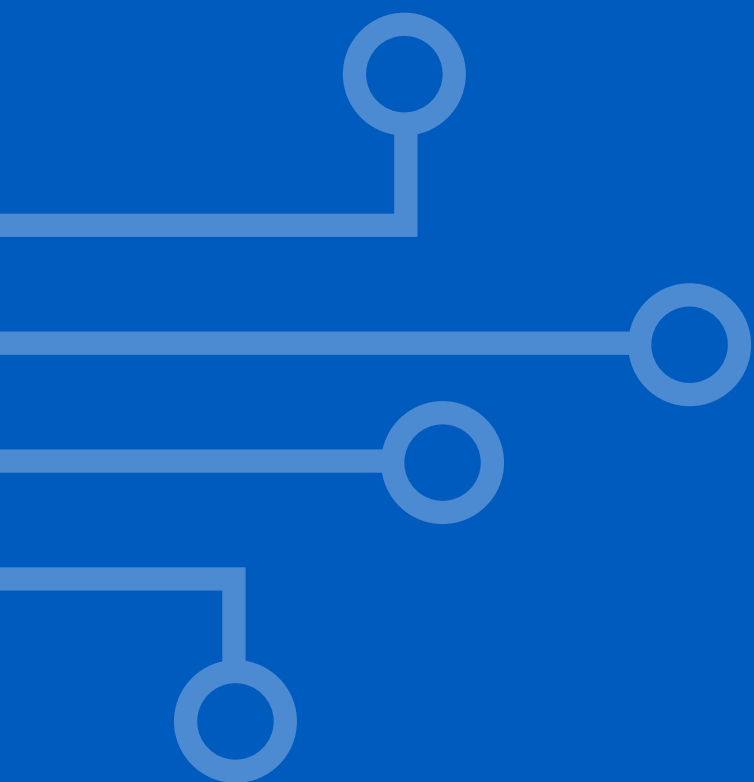




Annex VIII

Programma van Eisen



Inhoud

1	Inleiding.....	4
1.1	Doel.....	4
1.2	Situatieschets	4
1.3	Scope	4
1.3.1	Dienstencluster Workload Execution	4
1.3.2	Dienstencluster Connectiviteit.....	5
1.3.3	Dienstencluster Technische basisvoorzieningen (Eigen beheer).....	5
2	Algemene eisen	6
2.1	Algemene kenmerken	6
2.2	Kwaliteitseisen	6
2.2.1	Beschikbaarheid	6
2.2.2	Integriteit (dataprotectie)	7
2.2.3	Schaalbaarheid.....	7
2.3	Autonomie	7
2.4	Licenties	8
2.5	Beheer- en Servicelevelmanagementeisen	9
2.5.1	Uitgangspunten.....	9
2.5.2	Governance	9
2.5.3	Servicelevels.....	11
2.5.4	Proces- en ketenbeschrijving	12
2.5.5	Beheertaken van de Aanbestedende dienst	12
2.5.6	Rapportage en audit	13
2.6	Contract-, verrekenings- en facturatie-eisen	13
2.6.1	Contract(vormen)	13
2.6.2	Verrekening.....	13
2.6.3	Facturatie	13
3	Workload Execution.....	15
3.1	VM-Hosting	15
3.2	Workload Hosting.....	16
3.3	Datatransport	19
3.4	Service access control	21
3.5	Datamanagement	22
3.6	Bestandopslag	24
3.7	Raw storage.....	25
3.8	Data Recovery	26
3.9	Selfserviceportaal	27
3.10	Provisioning/Deployment Handling.....	28
3.11	Housing.....	30
4	Connectiviteit	31

4.1	Datadistributie, -inspectie en -filtering	31
4.2	Interconnection gateway	33
4.3	Netwerkbeheer.....	34
5	Technische basisvoorzieningen.....	36
5.1	Centrale Authenticatie.....	36
5.2	Network support services	36
5.3	Security monitoring	37
5.4	Health monitoring	37
5.5	Key & Certificate management.....	38
5.6	PAM	39
5.7	Bestandsuitwisseling	40

1 Inleiding

1.1 Doel

Het doel van dit Programma van Eisen is het formuleren van een samenhangend geheel van vereisten en specificaties aan de dienstverlening die Aanbestedende dienst wil betrekken uit de markt. Hierbij is de insteek dat dit primair vanuit functioneel perspectief gebeurt, in termen van (IT-)Diensten en de functies die deze Diensten realiseren. Indien nodig – als ze in de ogen van de Aanbestedende dienst essentieel zijn voor het eindresultaat, zijn daarnaast technische specificaties, standaarden en protocollen opgenomen. Het beoogde resultaat van deze aanbesteding is (een combinatie van) een optimale gebruiks- en beheerervaring en een afdoende beveiliging van (IT-)Diensten die de bedrijfsvoering zo passend mogelijk ondersteunen. Alle vereisten en specificaties die in het PvE zijn opgenomen, zijn hierop gericht. Waar mogelijk en daar waar ontwerpkeuzes niet essentieel zijn voor het resultaat, wordt beoogd aan Inschrijvers ontwerpvrijheid te geven bij de technische realisatie en wordt derhalve vanuit de Aanbestedende dienst daar geen invulling aan gegeven, maar wordt dit aan de eigenstandige verantwoordelijkheid van de Inschrijver overgelaten.

1.2 Situatieschets

De Aanbestedende dienst (de Regionale ICT-Dienst Utrecht, hierna RID genoemd) is een Gemeenschappelijke Regeling die generieke ICT-Diensten levert aan 6 gemeenten (Baarn, Soest, De Bilt, Bunnik, Utrechtse Heuvelrug, Wijk bij Duurstede) en een Sociale Dienst (RSD) in de provincie Utrecht, die in deze GR deelnemer zijn (verder in dit Programma van Eisen aangeduid met afnemers). RID ondersteunt dagelijks 2.400 gebruikers en ruim 220.000 inwoners maken gebruik van de dienstverlening. RID staat voor een strategische vernieuwing van haar IT-beheer en infrastructuur. Om de continuïteit van de dienstverlening te waarborgen, beter in te spelen op technologische ontwikkelingen en de rol van regiehouder te versterken, is besloten om het beheer van het eigen datacenter niet te continueren en over te stappen naar clouddiensten met inachtneming van het geactualiseerde Rijkscloudbeleid. Uitgangspunt hierbij is een overgang naar een Managed Private Cloudomgeving als basis, met mogelijke uitbreiding in de toekomst voor specifieke Diensten.

Een globaal overzicht van de transitie (proces en rollen Inschrijver en Aanbestedende dienst bij faciliteren van de transitie) is opgenomen in een apart document, de Transitiestrategie.

1.3 Scope

De scope van de aanbesteding betreft twee Dienstenclusters:

- Workload Execution
- Connectiviteit

Daarnaast is een Dienstencluster 'Technische basisvoorzieningen' opgenomen.

Het Dienstencluster Workload Execution omvat de Diensten die relevant zijn voor de transitie richting een Managed Private Cloudomgeving. Het Dienstencluster Connectiviteit omvat Diensten die bij voorkeur bij dezelfde leverancier worden ondergebracht via een en dezelfde aanbestedingsprocedure, maar die – als dit om wat voor reden dan ook niet tot een goede uitkomst leidt – daarna ook in een andere aanbesteding alsnog uit de markt uitgevraagd kunnen worden. Het Dienstencluster Technische basisvoorzieningen omvat die Diensten die bij de Aanbestedende dienst in beheer blijven of reeds door de Aanbestedende dienst in een eerdere procedure aan een leverancier zijn gegund. Vanwege de relatie die deze Diensten hebben met de Diensten uit de andere Dienstenclusters, zijn ze globaal beschreven, ter kennisgeving.

1.3.1 Dienstencluster Workload Execution

- VM-Hosting (platform voor uitvoering van virtuele machines)
- Workload Hosting (bieden van uitvoeringsruimte voor toepassingen)
- Datatransport (connectiviteit tussen IT-componenten, zoals applicaties, platformen, werkplekken et cetera)
- Service access control (beveiligen van ontsluiting van gebruikersinterfaces van applicaties)
- Datamanagement (gestructureerde opslag van applicatiedata)

- Bestandopslag (opslag van ongestructureerde data/bestanden)
- Raw storage (bieden van volumes voor blokopslag of blobopslag)
- Data recovery (middelen voor dataherstel na incidenten/calamiteiten)
- Selfserviceportaal (aanvraag/creatie virtuele platformen en andere componenten, rapportage)
- Provisioning/Deployment handling (geautomatiseerde uitrol van platformen, applicaties, Diensten(instanties), configuraties)
- Housing (colocatie)

1.3.2 Dienstencluster Connectiviteit

- Datadistributie, -inspectie en -filtering (datauitwisseling tussen netwerkkzones, beveiligd door inspectie en filtering)
- Interconnection gateway (koppelvlak voor verbindingen met externe netwerken/partijen)
- Netwerkbeheer (van volledig netwerk in gebruik bij Aanbestedende dienst, inclusief locaties afnemers)

1.3.3 Dienstencluster Technische basisvoorzieningen (Eigen beheer)

- Authenticatie (valideren van identiteiten van gebruikers van IT-systemen)
- Network Support Services (ondersteunende, netwerkgerelateerde Diensten, zoals Time en Naamresolutie)
- Security monitoring (bewaking van de beveiligingsstatus van IT-componenten en –ketens)
- Health monitoring (bewaking van de werking van IT-componenten en –ketens)
- Key & Certificate management (beheer van versleutelingsmechanismen)
- PAM (beveiligde, out-of-band beheertoegang)
- Bestandsuitwisseling (aansturing van data-uitwisseling tussen applicaties via bestanden)

2 Algemene eisen

2.1 Algemene kenmerken

De Aanbestedende dienst levert hoogwaardige en goed beveiligde IT-Diensten die door afnemers met een hoog cijfer worden gewaardeerd: Gemiddeld een 8,5. Deze hoge waardering is gebaseerd op een aantal factoren:

- Diensten sluiten goed aan op de behoeften van de afnemers.
- De Aanbestedende dienst is flexibel in het aanpassen van de dienstverlening op de specifieke vereisten bij verschillende deelnemers en de leveranciers van taakapplicaties die toepassingen leveren aan de deelnemers.
- Standaardmeldingen en -wijzigingen worden snel en efficiënt opgelost, met kennis van de organisatiecontext van de deelnemers.

Met de aanbesteding wordt de technische levering en het technisch beheer van een aantal Diensten belegd bij een Inschrijver. Hiermee verandert de rol van de Aanbestedende dienst, evenals de leveringsketen:

- Aanbestedende dienst verandert van uitvoeringsorganisatie naar regieorganisatie, die stuurt op kwaliteit en ketenprestaties, terwijl de Inschrijver de technische uitvoering verzorgt. De nadruk verschuift voor de Aanbestedende dienst naar bewaken, analyseren en bijsturen.
- De leveringsketen wordt uitgebreid. De Aanbestedende dienst blijft verantwoordelijk voor de Diensten als counterpart voor haar afnemers en voor het functioneel beheer ervan. Op deze manier blijft de Aanbestedende dienst een rol spelen in de keten, waarbij onder haar regie de Inschrijver verantwoordelijk is voor levering en technisch beheer.

Dit vraagt om een Inschrijver die voldoet aan de volgende kenmerken (eis):

- Een proactieve houding en een aantoonbare servicevolwassenheid,
- Een intrinsieke bereidheid tot samenwerking en continue verbetering.
- Het oog hebben voor de gehele keten, planmatig werken en tegelijkertijd beschikken over voldoende technische expertise.

Vanuit deze insteek blijft de Aanbestedende dienst in staat om haar toegevoegde waarde te leveren aan haar afnemers en deze continu te verbeteren.

2.2 Kwaliteitseisen

Aan de Diensten die worden afgenomen, worden kwaliteitseisen gesteld. De volgende kwaliteitseisen zijn algemeen geldend en intrinsiek van toepassing op iedere Dienst:

- Beschikbaarheid
- Integriteit (dataprotectie)
- Schaalbaarheid

2.2.1 Beschikbaarheid

Ten aanzien van de beschikbaarheid van Diensten hanteert de Aanbestedende dienst de volgende beschikbaarheidscategorieën, die door de Inschrijver toegepast moeten kunnen worden (eis):

	Beschikbaarheid bij incident ¹	Beschikbaarheid bij calamiteit ²	Failover-capaciteit bij incident	Failover - capaciteit bij calamiteit	RTO bij incident	RTO bij calamiteit
Standaard	X	X	0%	0%	2 dagen	2 weken
Verhoogd	√	X	50%	0%	< 1 min	2 dagen (48 uur)

Dit betekent dat Diensten met een verhoogde beschikbaarheid goed bestand dienen te zijn tegen het zich voordoen van incidenten (in de breedste zin van het woord) en minstens met de helft van de oorspronkelijke

¹ Een incident is een verstoring/uitval van een (technisch) component

² Een calamiteit is een van buiten komend onheil dat meerdere voorzieningen op een locatie treft, zoals een brand, overstroming, instorting, et cetera.

capaciteit geleverd moeten blijven worden wanneer incidenten zich voordoen. Aanbestedende dienst accepteert een hersteltijd van 2 dagen bij het zich voordoen van een calamiteit bij voorzieningen met een gegarandeerde verhoogde beschikbaarheid.

2.2.2 Integriteit (dataprotectie)

Als het gaat om integriteit, doelt Aanbestedende dienst op het correct en intact blijven van data die gerelateerd is aan / ondergebracht is bij/door Diensten in de Managed Private Cloudomgeving. Ten aanzien van deze data gelden de volgende eisen voor bescherming en herstel:

Gebeurtenis	Hersteltijd (RTO)	Maximaal dataverlies (RPO)	Aantal versies	Maximale detectietermijn
Beheer/ gebruikersincident – Ongewenste overschrijving/ verwijdering	direct	2 uur	30	30 dagen (gegarandeerde laatste actuele versie)
Technisch incident – Falend medium	direct	nihil	n.v.t.	n.v.t.
Technisch incident – Uitval opslagvoorziening	8 uur	2 dagen (nominaal 1 dag)	2	n.v.t.
Calamiteit - Uitval datacenter	8 uur	2 dagen (nominaal 1 dag)	2	n.v.t.
Calamiteit – Ransomware-aanval	1 week	2 dagen (nominaal 1 dag)	10+	n.v.t.

Indien Inschrijver verantwoordelijk is voor de opslag van data binnen een Dienst die Inschrijver levert, dient deze ervoor te zorgen dat de wijze van opslag zodanig is dat de data conform deze eisen wordt beschermd en te herstellen is (eis).

2.2.3 Schaalbaarheid

Diensten die door de Aanbestedende dienst worden afgenomen, dienen zowel op- als afgeschaald te kunnen worden, zodat de capaciteit passend is bij het gebruik ervan. Dit geldt zowel ten aanzien van groei en krimp, alsook piekbelasting (eis).

2.3 Autonomie

Aanbestedende dienst streeft een zo groot mogelijke digitale soevereiniteit na. Om dit mogelijk te maken, is het van belang om de digitale autonomie van oplossingen te waarborgen. Digitale autonomie is het vermogen om zelfstandig keuzes te maken en onafhankelijk te handelen in het digitale domein, zonder buitensporige afhankelijkheid van externe partijen. Het draait om strategische controle en risicobeheersing: de mogelijkheid om de eigen digitale infrastructuur, systemen en gegevens te beheren, zó dat men de ruimte houdt voor samenwerking en gebruik van internationale technologie, maar altijd op basis van bewuste, soevereine keuzes.

Digitale autonomie is niet vanzelfsprekend. De volgende oorzaken en dreigingen tasten de digitale autonomie aan:

Oorzaak	Dreiging
Onvoldoende rechtsbescherming Europese Economische Ruimte (EER)	<ul style="list-style-type: none"> • Toegang ontzeggen (in opdracht van vreemde overheid). • In beslag laten nemen (in opdracht van vreemde overheid). • Onbruikbaar maken (in opdracht van vreemde overheid). • Oneigenlijk gebruik (door vreemde overheid / door Inschrijver zelf). • Onmogelijk om Inschrijver sluitend te onderwerpen aan een (strikt) audit-/arbitrage-/telemetrieregime.
Teveel afhankelijkheden van een-en-dezelfde Inschrijver	<ul style="list-style-type: none"> • Diensten, gegevens en (digitale) identiteiten in beheer bij een-en-dezelfde Inschrijver. • Gegevens en encryptiesleutels/certificaten in beheer bij een-en-dezelfde Inschrijver. • Niet gecontroleerde / onveilige (beheer)toegang vanuit Inschrijver.

(Technische) samenstelling/configuratie van Diensten niet toegankelijk	<ul style="list-style-type: none"> • Functionaliteit niet over te zetten bij discontinueren dienstverlening.
Onvoldoende kennis aanwezig van / inzicht in de werking van afgenomen Diensten(complexen)	<ul style="list-style-type: none"> • Niet mogelijk om correcte werking / uitkomsten te valideren. • Niet mogelijk om bescherming tegen kwetsbaarheden te beoordelen / beveiligingsincidenten te detecteren. • Niet mogelijk om forensisch onderzoek te verrichten. • Afhankelijkheid van dienstverleners voor continuïteit dienstverlening. • Niet mogelijk om functionaliteit over te zetten naar een andere omgeving.

Om deze dreigingen te mitigeren en de digitale autonomie te waarborgen is het voor de Aanbestedende dienst van belang om de volgende maatregelen te treffen, waaraan de Inschrijver voldoet en/of volledige medewerking verleent (eis):

1. Inschrijver valt uitsluitend onder (EER)-jurisdictie en heeft geen vestigingen in een niet-EER-land.
2. Inschrijver heeft geen juridische afhankelijkheid van een moedermaatschappij of entiteit die buiten de EER is gevestigd
3. Inschrijver conformeert zich aan een informatieplicht met strikte tijdlijnen.
4. Inschrijver hanteert een vertragingsbeleid bij rechtshulpverzoeken (die voldoende tijd geeft voor het mogelijk maken van een data-evacuatie/uitvoeren exitstrategie).
5. Er is sluitende en zoveel mogelijk geautomatiseerd te executeren exitstrategie vastgelegd en geïmplementeerd. Hieraan dient de Inschrijver actief mee te werken (afgedekt met een financiële garantie die transitiekosten dekt bij afwijking van voorwaarden voor autonomie, zoals overname door een partij uit een niet-EER-land).
6. Real-time (reserve)kopie van data bij een afzonderlijke partij die uitsluitend valt onder EER-jurisdictie.
7. Genormaliseerde (reserve)kopie van bij een afzonderlijke partij die uitsluitend valt onder EER-jurisdictie.
8. Onderbrengen van digitale identiteiten bij een afzonderlijke organisatie (i.c.m. met maatregel 1).
9. Onderbrengen encryptiesleutels/certificaten bij een afzonderlijke organisatie/Inschrijver (i.c.m. maatregel 1) of bij de eigen organisatie (BYOK) .
10. Volledige onweerlegbaar authentieke logging van beheertoegang (opgeslagen bij afzonderlijke organisatie). Indien nodig i.c.m. maatregel 1.
11. Volledig gescheiden beheertoegang via afzonderlijke organisatie/Inschrijver (portal/stepping stone/PAM). Indien nodig i.c.m. maatregel 1.
12. Inschrijver conformeert zich aan het gebruik van Open Standaarden waar dit mogelijk is.
13. Audit door externe organisatie.
14. Inschrijver garandeert toegang voor externe audit.
15. Documentatie van volledige functionele decompositie van afgenomen Diensten.

2.4 Licenties

Ten aanzien van licenties gelden de volgende eisen:

Licenties besturingssystemen

De Inschrijver dient voor de levering van virtuele machines in de Managed Private Cloudomgeving de benodigde licenties voor de besturingssystemen te kunnen leveren en te beheren.

Dit betreft minimaal de volgende besturingssystemen:

- Microsoft Windows Server
- Red Hat Enterprise Linux

De licenties dienen onderdeel te kunnen zijn van de door de Inschrijver geleverde Dienst en dienen gedurende de contractperiode rechtsgeldig, compliant en passend bij het gebruik binnen de omgeving van de Aanbestedende dienst te zijn.

Alle overige softwarelicenties die binnen virtuele machines worden gebruikt, worden in beginsel door de Aanbestedende dienst zelf geleverd en beheerd (Bring Your Own License – BYOL), tenzij expliciet anders overeengekomen. Dit gaat om onder andere (maar niet beperkt tot):

- Databasesoftware (bijv. Microsoft SQL Server en Oracle Database).
- Beheer- en monitoringsoftware (bijv. Microsoft System Center).

Licenties bij Managed Platformdiensten

De Aanbestedende dienst heeft de intentie om gedurende de contractperiode aanvullende managed Diensten af te nemen naast/in plaats van de VM-Hostingdienst, zoals bijvoorbeeld Datamanagement.

Voor deze managed Diensten geldt dat (eis):

1. De Aanbestedende dienst het recht heeft om eigen softwarelicenties in te brengen (Bring Your Own License – BYOL).
2. De Inschrijver daarnaast de mogelijkheid dient te bieden om benodigde softwarelicenties als onderdeel van de managed Dienst te leveren (License Included).
3. Indien de Inschrijver licenties levert als onderdeel van de Dienst, dit transparant geprijsd dient te zijn.
4. De Aanbestedende dienst zich het recht voorbehoudt om per Dienst te bepalen of gebruik wordt gemaakt van:
 - door de Aanbestedende dienst aangeleverde licenties (BYOL), of
 - door de Inschrijver geleverde licenties als onderdeel van de managed Dienst.

De Inschrijver dient beide modellen te ondersteunen en de Aanbestedende dienst desgevraagd te adviseren over de economisch meest voordelige licentieconstructie (eis).

2.5 Beheer- en Servicelevelmanagementeisen

Voor de kwaliteit van de dienstverlening is de inrichting van beheer en Servicelevelmanagement zeer bepalend. In deze paragraaf zijn de uitgangspunten, randvoorwaarden en eisen hiervoor vastgelegd.

2.5.1 Uitgangspunten

Ten aanzien van Servicemanagement gelden de volgende (algemene) uitgangspunten (eis):

- Voor standaard uitrol- en beheeractiviteiten wordt een zo hoog mogelijke graad van automatisering gerealiseerd, zodat de dienstverlening efficiënt, voorspelbaar en schaalbaar kan worden uitgevoerd.
- Incidenten, wijzigingen, aanvragen en andere beheeractiviteiten worden geregistreerd en opgevolgd via de daarvoor ingerichte servicemanagementtooling.
- Ten aanzien van afgenomen Diensten zijn voldoende gegevens beschikbaar voor de Aanbestedende dienst om aan haar auditverplichtingen richting afnemers te kunnen voldoen. Hiervoor zijn onder andere de volgende auditnormen en -gegevens relevant:
 - ISAE3402-rapportages.
 - kwaliteits- en gebruiksgegevens
 - relevante logging- en auditgegevens met betrekking tot beheeractiviteiten en wijzigingen.
 - rapportages over incidentafhandeling en beveiligingsmaatregelen.
- De Inschrijver werkt waar nodig samen met de Aanbestedende dienst en andere betrokken partijen binnen de keten om verstoringen, wijzigingen en verbeteringen in de dienstverlening effectief te kunnen afhandelen.
- De Inschrijver adviseert vanuit de eigen technische expertise proactief om de dienstverlening op peil te houden en waar mogelijk te verbeteren.

2.5.2 Governance

Ten behoeve van de inrichting van Governance - voor een heldere taakverdeling en besturing daarvan tussen de Aanbestedende dienst als regieorganisatie en de Inschrijver, worden de volgende zaken vastgelegd (eis):

- Rollen
- Overlegstructuur
- Escalatiestructuur

2.5.2.1 Rollen

Voor een effectieve samenwerking worden duidelijke rollen ingericht aan zowel de zijde van de Aanbestedende dienst als de Inschrijver. De volgende rollen worden daarbij in ieder geval onderscheiden (eis):

Primair aanspreekpunt

De Inschrijver wijst één primair aanspreekpunt aan voor de dagelijkse afstemming met de Aanbestedende dienst.

Service Manager

De service manager is verantwoordelijk voor de tactische afstemming over de dienstverlening. Deze rol richt zich onder andere op onderwerpen zoals servicelevels, rapportages, kwaliteitsbewaking van de dienstverlening en het bespreken van mogelijke verbetermaatregelen.

Technisch specialist(en)

De Inschrijver stelt waar nodig één of meerdere technisch specialisten beschikbaar voor inhoudelijke ondersteuning bij incidenten, wijzigingen en technische vraagstukken. Deze specialisten leveren expertise op het gebied van de geleverde dienstverlening en ondersteunen bij analyse en oplossing van technische problemen.

2.5.2.2 Overlegstructuur

Tussen de Aanbestedende dienst en de Inschrijver worden periodieke overleggen ingericht om de samenwerking en de kwaliteit van de dienstverlening te bewaken (eis).

Operationeel overleg

Het operationele overleg vindt maandelijks plaats. In dit overleg worden onder andere lopende incidenten, operationele vraagstukken, wijzigingen en andere onderwerpen met betrekking tot de dagelijkse dienstverlening besproken.

Tactisch overleg (service review)

Het tactische overleg vindt per kwartaal plaats. Tijdens dit overleg worden onderwerpen besproken zoals servicelevels, rapportages, trends in de dienstverlening, structurele verstoringen en mogelijke verbetermaatregelen.

Strategisch overleg en jaarevaluatie

Het strategische overleg vindt jaarlijks plaats. In dit overleg wordt breder gekeken naar de samenwerking, de ontwikkeling van de dienstverlening, toekomstige behoeften en eventuele strategische wijzigingen. Daarnaast kan dit overleg worden gebruikt voor een periodieke evaluatie van de samenwerking tussen de Aanbestedende dienst en de Inschrijver.

2.5.2.3 Escalatiestructuur

Voor situaties waarin reguliere afstemming onvoldoende is om een vraagstuk, verstoring of knelpunt op te lossen, wordt een duidelijke escalatiestructuur gehanteerd (eis).

De Inschrijver stelt een escalatiematrix beschikbaar waarin inzicht wordt gegeven in de verschillende escalatieniveaus, de bijbehorende contactpersonen en de wijze waarop escalaties kunnen worden opgepakt. Deze escalatiestructuur ondersteunt een tijdige en passende opvolging van situaties die extra aandacht of besluitvorming vereisen.

Escalaties kunnen plaatsvinden op verschillende niveaus, bijvoorbeeld operationeel, tactisch of managementniveau, afhankelijk van de aard en impact van het vraagstuk. De exacte invulling van de escalatiestructuur en de betrokken contactpersonen worden bij aanvang van de dienstverlening in overleg tussen de Aanbestedende dienst en de Inschrijver vastgesteld en gedurende de looptijd van de overeenkomst actueel gehouden.

Het primaire aanspreekpunt is verantwoordelijk voor het coördineren van escalaties binnen de organisatie van de Inschrijver.

De Inschrijver zorgt ervoor dat de escalatiematrix gedurende de looptijd van de overeenkomst actueel blijft en dat wijzigingen in contactpersonen of escalatieniveaus tijdig worden gecommuniceerd aan de Aanbestedende dienst.

De exacte invulling van de overleggen, waaronder deelnemers, agenda en frequentie, wordt in overleg tussen de Aanbestedende dienst en de Inschrijver nader worden afgestemd.

2.5.3 Servicelevels

Ten aanzien van servicelevels geldt het volgende, op het gebied van:

- Incidentbeheer
- Wijzigingsbeheer

2.5.3.1 Incidentbeheer

De Inschrijver hanteert een prioriteringsmodel voor incidenten en verstoringen met minimaal de onderstaande classificaties (eis). De bijbehorende servicelevels zijn vastgesteld met een beperkte marge ten opzichte van de servicelevels die de Aanbestedende dienst richting haar afnemers hanteert, zodat de Aanbestedende dienst in staat blijft haar eigen dienstverlening conform afspraak te leveren.

Prioriteit	Omschrijving	Maximale responstijd	Hersteltijd (of workaround)
1 (Kritiek)	Kritieke verstoring (Dienst volledig niet beschikbaar)	15 minuten	3 uur
2 (Hoog)	Hoge impact verstoring (belangrijke functionaliteit niet beschikbaar)	30 minuten	7 uur
3 (Middel)	Beperkte verstoring: functionaliteit is gedeeltelijk beperkt maar er is een workaround beschikbaar	1 uur	14 uur
4 (Laag)	Overige meldingen, vragen of kleine verstoringen zonder directe impact op de dienstverlening	1 uur	40 uur

De genoemde responstijden en hersteltijden gelden binnen het overeengekomen venster voor de dienstverlening op basis van 7x24 uur. De exacte invulling hiervan wordt bij aanvang van de dienstverlening in overleg tussen de Aanbestedende dienst en de Inschrijver vastgesteld.

De Inschrijver rapporteert periodiek over de realisatie van de servicelevels. Deze rapportage geeft inzicht in onder andere het aantal incidenten per prioriteit, gerealiseerde responstijden en hersteltijden, eventuele overschrijdingen en mogelijke verbetermaatregelen.

2.5.3.2 Wijzigingsbeheer

De Inschrijver beschikt over een volwassen en aantoonbaar ingericht wijzigingsproces voor het plannen, beoordelen en uitvoeren van wijzigingen aan de dienstverlening. Dit proces is gericht op het gecontroleerd en beheerst doorvoeren van wijzigingen, waarbij risico's, impact op de dienstverlening en afhankelijkheden binnen de keten worden meegenomen (eis).

Het wijzigingsproces dient gebaseerd te zijn op gangbare best practices op het gebied van servicemanagement en wijzigingsbeheer, zoals beschreven in bijvoorbeeld ITIL of vergelijkbare frameworks.

De exacte inrichting van het wijzigingsproces, waaronder de classificatie van wijzigingen, beoordelingsprocedures, onderhoudsvensters en afstemming met betrokken partijen, wordt in overleg met de Aanbestedende dienst nader afgestemd.

2.5.4 Proces- en ketenbeschrijving

De Aanbestedende dienst bedient een aantal afnemers met het leveren van IT-Diensten (zie Situatieschets). In de leveringsketen blijven de volgende rollen en taken bij de Afnemende Dienst:

- Selfservicebeheer voor (eind)gebruikers. Hiermee kunnen (eind)gebruikers aanvragen en meldingen indienen, waaronder wachtwoordherstel.
- Skilled servicedesk voor (eind)gebruikers. De skilled servicedesk ondersteunt (eind)gebruikers met de volgende zaken:
 - Melden en behandelen van storingen en incidenten.
 - Informeren over de voortgang van de afhandeling van storingen en incidenten.
 - Beheren en bewaken van onderhoudsprocessen van apparatuur.
 - Doorzetten van wijzingen, incident- en probleemmeldingen naar leverancier(s).
 - Initiëren van geautomatiseerde uitrolprocessen die als standaard Dienst rechtstreeks geïntanceerd kunnen worden.
- Service Level Management, die richting (eind)gebruikers de volgende taken verzorgt:
 - Opstellen en bijhouden Producten- en Dienstenportfolio.
 - Doorzetten (met indien nodig converteren) van (kwaliteits- en gebruiks)rapportage, uitgesplitst naar afnemer.
 - Doorzetten (met indien nodig converteren) van auditrapportage.
 - Uitvoeren van contractmanagement.
 - Beheer van probleem- en escalatie-afhandeling.

De Aanbestedende dienst wil de volgende rollen en taken bij Inschrijver te beleggen (eis):

- Selfservicebeheer voor medewerkers van de regioafdeling van de Aanbestedende dienst voor het geautomatiseerd indienen van meldingen, aanvragen, wijzigingen en uitrol van (instanties van) Diensten en componenten.
- Skilled servicedesk.
- Uitvoeren van niet-standaard wijzigingen door specialisten van Inschrijver.
- Service Level Management.
- Patchmanagement en Vulnerabilitymanagement als onderdeel van de dienstverlening, gericht op het tijdig signaleren en mitigeren van beveiligingsrisico's.
- End-to-end Disaster Recoverytests (minimaal 1 keer per jaar)

De Aanbestedende dienst blijft gebruik maken van de aanwezige Service Managementtooling (TopDesk) voor het faciliteren van de volgende zaken:

- Administratie van Configuration Items (CMDB).
- Leveren van een portaal ten behoeve van selfservicebeheer van (eind)gebruikers.
- Registeren en bewaken van aanvragen, projecten, wijzigingen, meldingen, incidenten en problemen.
- Vastleggen en gebruiken van templates voor geautomatiseerde uitrol van (instanties van) Diensten en het initiëren van geautomatiseerde uitrolactiviteiten.

De Aanbestedende dienst verwacht een geautomatiseerde koppeling met Service Management- en uitroltooling voor het uitwisselen van de volgende zaken (eis):

- Registratie van door de Inschrijver opgeleverde Configuration Items.
- Terugkoppeling van (de voortgang van) de afhandeling van aanvragen, projecten, wijzigingen, meldingen, incidenten en problemen.
- Aanleveren van gegevens als input voor het kunnen vervaardigen van gebruiks- en kwaliteitsrapportage en auditrapportage.

2.5.5 Beheertaken van de Aanbestedende dienst

De Aanbestedende dienst is voornemens de volgende beheertaken zelf uit te blijven voeren:

- Functioneel beheer van voorzieningen voor het beheer van digitale identiteiten en accounts.
- Functioneel beheer van lokale authenticatievoorzieningen.
- Functioneel en beperkt technisch beheer van directory- en synchronisatievoorzieningen

- Functioneel beheer van autorisatiemodellen, groepsstructuren en basisinrichting van infrastructuurdiensten.
- Functioneel beheer van wijzigingen in infrastructuurdiensten, inclusief beheer van onderhoudsperiodes.
- Functioneel beheer van security- en autorisatiegerelateerde configuraties.
- Functioneel beheer over continuïteit, back-up en retentie.
- Functioneel beheer van patches en updates voor applicaties.
- Functioneel beheer van ketens en integraties.

2.5.6 Rapportage en audit

Inschrijver dient periodiek de volgende rapportages en gegevens op te leveren ten behoeve van rapportage aan afnemers van de Aanbestedende dienst en het opleveren van auditrapportage aan controlerende instanties (eis):

- ISAE3402-rapportage.
- kwaliteits- en (gebruiks)rapportage, uitgesplitst naar afnemer.
- rapportages over beschikbaarheid, incidentafhandeling en beveiligingsmaatregelen.

De frequentie en exacte inhoud van deze rapportages worden in overleg tussen de Aanbestedende dienst en de Inschrijver vastgesteld.

2.6 Contract-, verrekenings- en facturatie-eisen

Aanbestedende dienst heeft een aantal randvoorwaarden die gelden ten aanzien van:

- Contract(vormen)
- Wijze van verrekenen en mogelijkheden tot doorbelasting
- Facturatie

2.6.1 Contract(vormen)

Aanbestedende dienst heeft de volgende randvoorwaarden wat betreft de contractering (eis):

- Het moet mogelijk zijn om een meerjarig contract af te sluiten voor de afname van capaciteit (cpu/geheugen/opslag) en Diensten, zodat deze tegen gunstige prijscondities afgenomen kunnen worden. Hierbij wordt een contractduur van 3-4 jaar beoogd.
- Het moet mogelijk zijn om capaciteit (cpu/geheugen/opslag) en Diensten naar behoefte af te nemen (pay per use), zodat tijdelijk benodigde capaciteit op een flexibele manier op- en afgeschaald kan worden.
- Het moet mogelijk zijn om bij het reduceren van de afname van capaciteit (cpu/geheugen/opslag) en een toename van de afname van Diensten binnen een langdurig contract de toewijzing van (onderliggend) benodigde capaciteit zonder meerkosten te verschuiven.

2.6.2 Verrekening

Aanbestedende dienst heeft de volgende randvoorwaarden wat betreft verrekening (eis):

- Het moet mogelijk zijn om granulaire en gedifferentieerde kostenplaatsen te hanteren bij de verrekening van afname van capaciteit (cpu/geheugen/opslag) en Diensten (instanties, onderliggend middelenbeslag per capaciteit, additionele beheerdiensten).
- Het moet mogelijk zijn om labels toe te voegen aan afgenomen eenheden (waaronder componenten, instanties van Diensten, werkzaamheden), zodat de Aanbestedende dienst in staat is een granulaire doorbelasting toe te passen richting haar afnemers.

2.6.3 Facturatie

Ten aanzien van de facturatie heeft de Aanbestedende dienst de volgende eisen:

Inschrijver stuurt facturen digitaal in PDF (PDF/A) (doorzoekbaar) of in XML (UBL) naar: facturen@rid-utrecht.nl. Andere bestandsformaten worden niet geaccepteerd. Fysieke (papier) facturen worden niet in behandeling genomen. Inschrijver vermeldt op de factuur minimaal:

- NAW-gegevens Aanbestedende dienst.

- Contractnummer, projectnummer en/of projectomschrijving van de Aanbestedende dienst.
- Verplichtingenummer en/of factuurkenmerk van de Aanbestedende dienst.
- De geleverde eenheden (waaronder componenten, Diensten, projectwerkzaamheden, advieswerkzaamheden, beheerwerkzaamheden), uitgesplitst op basis van labels waarmee eenheden gemerkt zijn, waar van toepassing.
- Totaalbedrag exclusief BTW.
- Het BTW-bedrag.
- Totaalbedrag inclusief BTW.
- KvK-nummer.
- BTW-nummer.
- IBAN.
- Coderingen t.b.v. e-facturering (indien van toepassing).

Indien de factuur niet voldoet aan bovenstaande eisen heeft Aanbestedende dienst de mogelijkheid om niet te betalen.

3 Workload Execution

Het Dienstencluster Workload Execution omvat alle Diensten die nodig zijn voor het uitvoeren en ondersteunen van (centrale) workloads van de Aanbestedende dienst en haar afnemers.

3.1 VM-Hosting

VM-Hosting is de Dienst waarmee virtuele machines worden uitgevoerd. De Dienst biedt (in ieder geval) de volgende functies:

- Uitvoeringsplatform voor virtuele machines (platform engine.virtual machines)
- Vastleggen de inrichting/toestand van een virtuele machine ten behoeve van herstel bij (beheer)incidenten. (snapshotting.virtual machine)
- Toegang van virtuele machines tot datatransport (network access.virtual machines)
- Uitwisseling van verkeer (op laag 2) tussen virtuele machines onderling en gateways voor distributie van verkeer (access aggregation.virtual machines)
- Het bedienen van de platformen met behulp van een command line (controlling.command line.VM hosting)
- Het bedienen van de platformen met behulp van een centrale, grafische beheertool (controlling.centralized management console.VM hosting)
- Het presenteren van real-time waarden waarmee de werking en de prestaties van platformen gemeten kan worden (provisioning.platform analysis data.VM)

ID	Weging	Omschrijving	Rationale	Soort	Gerelateerd aan
VMH-01	Must	De volgende typen virtuele machines dienen in ieder geval uitgevoerd te kunnen worden: <ul style="list-style-type: none"> • VMWare virtuele machines 	Het moet mogelijk zijn om de bestaande VMWare virtuele machines 1-op-1 over te zetten van de huidige on-premises datacenteromgeving bij de Aanbestedende dienst naar de Managed Private Cloudomgeving.	Functioneel	VM-Hosting
VMH-02	Must	In de toekomst dient het mogelijk te zijn om virtuele machines en containers op een ander type platform (hypervisor) uit te voeren om kosten te besparen.	Aanbestedende dienst wil kunnen overstappen naar een platform dat kostenefficiënter is dan het huidige platform.	Functioneel	VM-Hosting
VMH-03	Must	Virtual appliances dienen geïmplementeerd te kunnen worden op basis van de volgende onderliggende platformen: <ul style="list-style-type: none"> • VMWare • Hyper-V • KVM 	Bij de Aanbestedende dienst zijn verschillende typen Virtuele Appliances in gebruik, die 1-op-1 overgezet moeten kunnen worden naar de Managed Private Cloudomgeving.	Operationeel	VM-Hosting
VMH-04	Must	De geleverde componenten dienen geschikt te zijn om eenheden met bij aanvang van het contract minimaal de volgende kentallen te ondersteunen: <ul style="list-style-type: none"> 285 VM's 900 vCPU's (toegewezen) 5TB Geheugen (toegewezen) 71 TB Opslag (toegewezen) 	Op basis van deze kentallen is een inschatting te maken van het middelenbeslag. Op de genoemde kentallen is nog geen optimalisatieslag toegepast.	Operationeel	VM-Hosting
VMH-05	Must	Licenties voor virtualisatieplatformen (hypervisors) dienen door de Inschrijver aangeleverd te kunnen worden.	Het is de verwachting dat de Inschrijver licenties tegen een gunstige prijs kan verwerven.	Operationeel	VM-Hosting
VMH-06	Must	Licenties voor besturingssystemen dienen door de Inschrijver aangeleverd te kunnen worden.	Het is de verwachting dat de Inschrijver licenties tegen een gunstige prijs kan verwerven.	Operationeel	VM-Hosting

VMH-07	Must	Platformen dienen geautomatiseerd gestopt en gestart te kunnen worden.	Om kosten te beheersen dienen systemen uit- en aangeschakeld te kunnen worden naar behoefte en benutting.	Operationeel	VM-Hosting
VMH-08	Should	Het moet mogelijk zijn om te werken met affinity rules en anti-affinity rules.	Het moet mogelijk zijn om bepaalde VM's expliciet op 1 host te laten draaien (affinity) of juist expliciet niet op 1 host (anti-affinity) voor een balans tussen optimaal middelengebruik en het voorkomen van (uitvoerings- en beveiligings)conflicten.	Operationeel / Beveiliging	Workload Hosting
VMH-09	Must	Het moet mogelijk zijn om de staat en de configuratie van een virtuele machine op een specifiek moment vast te leggen (snapshot).	Het moet mogelijk zijn om wijzigingen in inrichting en configuratie op een makkelijke en efficiënte manier terug te draaien.	Operationeel	snapshotting.virtual machine
VMH-10	Must	Minimaal de volgende items moeten geautomatiseerd bewaakt worden: <ul style="list-style-type: none"> • Processorgebruik (%) • Geheugengebruik (%) • Opslaggebruik (%) • Uptime • Systeemconnectiviteit (poll/heartbeet) • Netwerkconnectiviteit (topografie) • Bandbreedtegebruik (te filteren op verbinding/backplane) • Verkeerspatronen (te filteren op verbinding/backplane) • Blokkeringsmeldingen verkeersfiltering (te filteren op bronsysteem en protocoltypen/poortnummers) • Geldigheid certificaten (ten behoeve van encryptie) 	Weergegeven items zijn relevant voor de correcte werking van systemen.	Operationeel	provisioning.platform analysis data.VM
VMH-11	Should	Meldingen dienen op basis van de protocollen SNMP v2 en SNMP v3 opvraagbaar te zijn.	De oplossing dient te voldoen aan vigerende standaarden van de Aanbestedende dienst.	Operationeel	provisioning.platform analysis data.VM

3.2 Workload Hosting

Workload Hosting is de Dienst die ervoor zorgt dat centrale (bedrijfs)applicaties en virtualisatie- en presentatietoepassingen worden uitgevoerd. De Dienst biedt (in ieder geval) de volgende functies:

- Uitvoeringsruimte voor het draaien van code van applicaties en toepassingen (workload engine.application code).
- Het plannen en geautomatiseerd starten/pauzeren/stoppen van de uitvoering van applicaties en toepassingen (scheduling.application jobs).
- Het distribueren van applicatie-uitvoering over meerdere platformen (load balancing.application code)
- Het bedienen van de platformen met behulp van een command line (controlling.command line.workload hosting)
- Het bedienen van de platformen met behulp van een centrale, grafische beheertool (controlling.centralized management console.workload hosting)
- Het presenteren van real-time waarden waarmee de werking en de prestaties van platformen gemeten kan worden (provisioning.platform analysis data.workload hosting)

Ten aanzien van de Dienst van en de functies binnen Workload Hosting gelden de volgende (aanvullende) vereisten:

ID	Weging	Omschrijving	Rationale	Soort	Gerelateerd aan
WLH-01	Must	De volgende typen workloads dienen uitgevoerd te kunnen worden: <ul style="list-style-type: none"> • Taak/-bedrijfsapplicaties • Virtuele clientapplicaties • Webapplicaties • Databases • Bestandssystemen • Virtuele desktops (zonder GPU-capaciteit) 	Workloads die bij de Aanbestedende dienst in gebruik zijn (en nu op virtuele machines zijn geïmplementeerd) dienen in de toekomst gehost te kunnen worden vanuit de Dienst Workload Hosting.	Functioneel	Workload Hosting
WLH-02	Should	Ten behoeve van Workload Hosting is het mogelijk om containers in te richten / af te nemen conform de HAVEN-standaard.	Het moet mogelijk zijn om applicaties uit te voeren die binnen een HAVEN-container worden aangeboden, als standaard binnen het Common Ground-framework van de VNG.	Operationeel	Workload Hosting
WLH-03	Must	Per workload dient de demarcatie van verantwoordelijkheden voor beheer en lifecyclemanagement te worden afgestemd en vastgelegd.	In voorkomende gevallen ressorteren ondersteunende componenten van workloads (zoals runtime environments ten behoeve van taakapplicaties) onder de verantwoordelijkheid van leveranciers van deze workloads en vallen deze buiten de beheerverantwoordelijkheid van de Inschrijver. Hierover dient expliciet helderheid te bestaan om een effectieve samenwerking tussen Inschrijver, Aanbestedende dienst en derde leveranciers te waarborgen.	Operationeel	Workload Hosting
WLH-04	Must	Inschrijver is in ieder geval verantwoordelijk voor het uitvoeren van beheer en lifecyclemanagement op de besturingssystemen van virtuele machines. Hieronder vallen onder meer de volgende activiteiten: <ul style="list-style-type: none"> • Installatie en configuratie van besturingssystemen. • Versiebeheer. • Het uitvoeren van security updates en patches (patchmanagement). • Het toepassen en onderhouden van nader af te stemmen beveiligingsrichtlijnen (hardening). • Het monitoren van de technische staat van het besturingssysteem. 	Als kerncomponent van de Dienst Workload Hosting dient de end-to-endverantwoordelijkheid hiervoor bij de Inschrijver te berusten.	Operationeel	Workload Hosting
WLH-05	Must	Er moet een taggingschema worden opgesteld, waarbij ten minste de volgende zaken/aspecten in de tag worden vastgelegd: <ul style="list-style-type: none"> • Formele eigenaar • Creatiedatum • Verrekenmechanisme (gemeenschappelijk gebruik/toegerekend/...) 	Het moet mogelijk zijn kosten en toewijzingen van resources te traceren en te rapporteren.	Operationeel	Workload Hosting

		<ul style="list-style-type: none"> • Toepassing(en) die gebruik maakt/maken van de resource • OTAP Fase • Bedrijfsprioriteit 			
WLH-06	Should	Wanneer een hogere beschikbaarheid dan 'verhoogd' is vereist, wordt deze hogere beschikbaarheid gerealiseerd op applicatieniveau.	Op applicatieniveau is het meeste bekend ten aanzien van de stand van dataverwerking/transacties, waardoor het mogelijk is om bij failoversituatie de consistentie van de data te behouden.	Functioneel	Workload Hosting
WLH-07	Should	Wanneer een hogere beschikbaarheid dan 'standaard' is vereist en dit lukt niet op applicatieniveau, dient deze hogere beschikbaarheid gerealiseerd te worden op basis van mechanismes die door de Inschrijver standaard worden aangeboden.	Voor een correcte en kostenefficiënte werking van een failoverconfiguratie dient aangesloten te worden bij de inrichtingsprincipes van een Inschrijver.	Functioneel	Workload Hosting
WLH-08	Should	Het moet mogelijk zijn om te werken met affinity rules en anti-affinity rules	Het moet mogelijk zijn om bepaalde toepassingen expliciet op 1 VM te laten draaien (affinity) of juist expliciet niet op 1 VM (anti-affinity) voor een balans tussen optimaal middelengebruik en het voorkomen van (uitvoerings- en beveiligings)conflicten.	Functioneel	Workload Hosting
WLH-09	Must	Licenties voor virtualisatieplatformen (hypervisors) dienen door de Inschrijver aangeleverd te kunnen worden.	Het is de verwachting dat de Inschrijver licenties tegen een gunstige prijs kan verwerven.	Operationeel	Workload Hosting
WLH-10	Must	Licenties voor besturingssystemen dienen door de Inschrijver aangeleverd te kunnen worden.	Het is de verwachting dat de Inschrijver licenties tegen een gunstige prijs kan verwerven.	Operationeel	Workload Hosting
WLH-11	Must	Microsoft Defender wordt als antivirusagent gebruikt op platformen voor Workload Hosting	Microsoft Defender is de antimalwaretoepassing die in gebruik is bij Aanbestedende dienst en die noodzakelijk is voor het goed functioneren van Cyber Treath Intelligence	Beveiliging	Workload Hosting
WLH-12	Must	Virtuele machines dienen geautomatiseerd gestopt en gestart te kunnen worden.	Om kosten te beheersen dienen systemen uit- en aangeschakeld te kunnen worden naar behoefte en benutting.	Operationeel	Workload Hosting
WLH-13	Must	De volgende componenten/agents dienen standaard op managed platformen voor workloadhosting te worden aangebracht: <ul style="list-style-type: none"> • Antimalware. • Connectoren voor koppeling databases (waaronder Oracle). • Standaard middleware (zoals VCRuntime / DotNet en andere). • Monitorsoftware voor de gedane handelingen op het systeem. • App-V-client. 	Deze onderdelen zijn onmisbaar voor een correcte werking/efficiënt beheer.	Operationeel	workload engine.application code
WLH-14	Must	De inrichting van virtuele machines voldoet aan: <ul style="list-style-type: none"> • Standaardisatie naamconventie host systemen • Standaardisatie van locatie op het bestandssysteem van de 	Dit betreft gangbare beheerconventies voor efficiënt beheer.	Operationeel	workload engine.application code

		applicatie en de structuur hiervan.			
WLH-15	Must	Sizing is altijd op basis van testing. Wel met respect tot de eisen van de leverancier, daar deze over het algemeen de sizing specificaties bepaalt.	Het werkelijke gedrag en middelenbeslag van applicaties (binnen een specifieke context) kan alleen maar betrouwbaar worden bepaald aan de hand van een concrete inrichting.	Operationeel	workload engine.application code
WLH-16	Must	Minimaal de volgende items moeten geautomatiseerd bewaakt worden: <ul style="list-style-type: none"> • Uptime • Starten, pauzeren en stoppen van services/jobs/processen • Systeemconnectiviteit (poll/heartbeet) • Software-installaties (te filteren op bronsysteem) • Configuratiewijzigingen (te filteren op bronsysteem) • Netwerkconnectiviteit (topografie) • Bandbreedtegebruik (te filteren op verbinding/backplane) • Verkeerspatronen (te filteren op verbinding/backplane) • Blokkeringsmeldingen verkeersfiltering (te filteren op bronsysteem en protocoltypen/poortnummers) • Accountmodificatie (te filteren op accountsoort) • Geldigheid certificaten (ten behoeve van encryptie) 	Weergegeven items zijn relevant voor de correcte werking van workloads.	Operationeel	provisioning.platform analysis data.workload hosting
WLH-17	Should	Meldingen dienen op basis van de protocollen SNMP v2 en SNMP v3 opvraagbaar te zijn.	De oplossing dient te voldoen aan vigerende standaarden van de Aanbestedende dienst.	Operationeel	provisioning.platform analysis data.workload hosting
WLH-18	Should	Het moet mogelijk zijn om bij piekbelasting tijdelijk extra capaciteit toe te wijzen aan workloads, in volgorde van prioriteitsmarkering (label).	Het moet mogelijk zijn om piekbelasting op te vangen en daarbij meer bedrijfskritische toepassingen voorrang te geven boven toepassingen die in mindere mate bedrijfskritisch zijn.	Operationeel	workload engine.application code

3.3 Datatransport

Datatransport is de Dienst die zorgt voor uitwisseling van data tussen IT-componenten, zoals applicaties, platformen, et cetera, die zich in de Managed Private Cloudomgeving bevinden. De Dienst biedt (in ieder geval) de volgende functies:

- Leveren van toegang tot het netwerk in het managed privied cloudomgeving voor back-end systemen, waaronder virtualisatieplatform en afzonderlijke serversystemen (access.wired.back-end).
- Uitwisseling van dataverkeer binnen een compartiment/segment (afgescheiden netwerkzone) in een Managed Private Cloudomgeving/binnen een virtualisatieplatform (access.aggregation.mpc)
- Datatransport over verbindingen tussen locaties die onder de beheerverantwoordelijkheid van de Inschrijver (interconnection.mpc).
- Beheersen van toegang tot het netwerk op (virtueel) apparaatniveau (conditioning.network.access).

NB: Het uitwisselen van verkeer tussen netwerkzones is geen functie van de Dienst Datatransport, maar is voorbehouden aan de Dienst Datadistributie, -inspectie en -filtering. Dit omdat op deze manier de beveiliging van netwerkzones op een stringente en eenduidige manier is belegd.

Ten aanzien van de functies binnen Datatransport gelden de volgende (aanvullende) vereisten:

ID	Weging	Omschrijving	Rationale	Soort	Gerelateerd aan
DTR-01	Must	Routing tussen zones vindt plaats via de Dienst Datadistributie, -inspectie en -filtering	Bij uitwisseling van dataverkeer tussen zones, dient dit verkeer geïnspecteerd en indien nodig gefilterd te worden.	Beveiliging	access aggregation.data center
DTR-02	Must	De Dienst Datatransport dient OSPF te ondersteunen voor het gebruik hiervan als intern routingsprotocol, in combinatie met de Dienst Netwerkinspectie en -filtering.	Netwerkadressering van netwerkkzones dienen automatisch uitgewisseld te worden met de Dienst Netwerkinspectie en -filtering, die zorgdraagt voor de routing tussen zones binnen de Managed Private Cloudomgeving en tussen deze omgeving en (netwerk)omgevingen van deelnemers en externe partijen.	Functioneel	Datatransport
DTR-03	Must	Netwerksegmenten/-zones moeten zodanig worden ingericht dat ze als 'security boundary' functioneren.	Segmentering dient zo ingericht te zijn, dat standaard geen enkel verkeer tussen zones wordt uitgewisseld en mag derhalve niet afhankelijk zijn van aanvullende configuratie (o.a. van access lists en statische routes). Dit omdat bij misconfiguratie de kans groter wordt dat beveiligingsincidenten optreden.	Beveiliging	access aggregation.data center
DTR-04	Must	Netwerksegmenten/-zones moeten gebruikt kunnen worden als basis voor de delegatie van beheerrechten aan verschillende (derde) partijen (in combinatie met andere maatregelen)	Het moet mogelijk zijn om beheerrechten te delegeren aan verschillende partijen. Zones dienen hierbij ingezet te kunnen worden om verkeersuitwisseling te beperken.	Beveiliging	access aggregation.data center
DTR-05	Must	De netwerkvertraging tussen gekoppelde segmenten binnen een (virtuele) datacenterlocatie dient kleiner te zijn dan 2ms, gemeten tussen twee hosts	Interactie tussen applicaties dient zo weinig mogelijk hinder te ondervinden van netwerkvertraging. Aangezien interconnectie tussen locaties in veel gevallen al relatief veel vertraging introduceert, dient dit binnen een datacenterlocatie tot een minimum te worden beperkt.	Functioneel	access aggregation.data center
DTR-06	Must	De interconnectie tussen managed private cloud-datacenterlocaties dient vanuit het perspectief van de gebruiker de verschillende locaties op datalink-niveau met elkaar te koppelen.	Het moet mogelijk zijn om netwerkkzones over meerdere locaties heen als een netwerksegment te kunnen benutten.	Functioneel	interconnection.mpc
DTR-07	Must	De maximale netwerkvertraging die optreedt op de verbinding die de interconnectie tussen managed private cloud-datacenterlocaties realiseert dient kleiner te zijn dan 10ms	De totale netwerkvertraging die acceptabel is tussen hosts die zich op verschillende locaties bevinden, is 14ms. Rekening houdend met 2ms lokale vertraging, is de tolerantie voor vertraging op de verbinding tussen locaties dus maximaal 10ms.	Functioneel	interconnection.mpc

3.4 Service access control

De Dienst Service access control wordt gebruikt voor een veilige ontsluiting/toegang tot (virtuele) applicaties en systemen en ondersteunt een hoog beschikbare en schaalbare inrichting hiervan. De Dienst termineert clientessies en zet deze door naar de achterliggende (back-end) applicaties en systemen.

De Dienst biedt (in ieder geval) de volgende functies:

- Het termineren en afhandelen van applicatiesessies, zodat deze dynamisch richting back-end afgehandeld kunnen worden (session handling.application access).
- Het dynamisch routeren van sessies richting meerdere instanties van een applicatie/systeem. (distribution.application sessions).
- Het verdelen van sessies over meerdere instanties van een applicatie/systeem (load balancing.application sessions).
- Offloaden van encryptie/decryptie van applicatiesessies, zodat de sessies dynamisch afgehandeld kunnen worden (encryption handling.application sessions).
- Het bedienen van de platformen met behulp van een command line (controlling.command line.service access control)
- Het bedienen van de platformen met behulp van een centrale, grafische beheertool (controlling.centralized management console.service access control)

Ten aanzien van de functies binnen Datatransport gelden de volgende (aanvullende) vereisten:

ID	Weging	Omschrijving	Rationale	Soort	Gerelateerd aan
SAC-01	Must	De voorziening voor service access control dient (logisch) onafhankelijk van de Managed hostingomgeving(en) van de Inschrijver te functioneren	De inrichting van applicatietoegang dient eenduidig te worden gerealiseerd, ongeacht de werking van de fabric van hostingomgevingen van de Inschrijver. Hiermee wordt het makkelijker om een exit-strategie te faciliteren	Functioneel	Service Access Control
SAC-02	Must	De voorziening voor Service Access Control dient vanuit een (logisch) centrale plek te kunnen worden bediend	Deze voorziening is belangrijk voor de controle en beheersing van toegang tot het (eigen) applicatielandschap. Overzicht is essentieel voor een correcte werking. Daarnaast is centraal beheer belangrijk voor efficiëntie van dit beheer.	Functioneel, Operationeel	Service Access Control
SAC-03	Must	Wanneer de voorziening is ingericht met meerdere instanties, dient over deze instanties (cluster) heen sessiepersistentie gegarandeerd te worden.	Bij het omschakelen tussen instanties (nodes) die deze Dienst leveren, dienen eindgebruikers hiervan niets te merken in het gebruik van en de toegang tot applicaties.	Functioneel, Operationeel	Service Access Control
SAC-04	Should	Alle applicaties worden via de load balancingfunctie ontsloten (in combinatie met universele naamgeving).	De inrichting van de applicatietoegang dient eenduidig te zijn en naadloos aanpasbaar.	Functioneel, Operationeel	Service Access Control
SAC-05	Should	Applicatieverkeer wordt geïnspecteerd tijdens de afhandeling van de sessie richting back-end, gebruikmakend van de inspectie- en filterfuncties die vanuit de Dienst Datadistributie, -inspectie en -filtering geleverd worden.	Bij de sessieafhandeling wordt ook de encryptie getermineerd, wat het mogelijk maakt om verkeer intern te inspecteren.	Beveiliging	Service Access Control

3.5 Datamanagement

De Dienst Datamanagement verzorgt gestructureerde opslag van applicatiedata op basis van RDBMS-platformen. Data wordt beschermd tegen incidenten en calamiteiten door het vastleggen van transactielogs en replicatie van transacties en tabellen over nodes heen. De Dienst biedt (in ieder geval) de volgende functies:

- Centrale functie voor het (programmeerbaar) aansturen van dataverwerkingstransacties (data engine.relational data management).
- Virtuele, gestructureerde opslagruimte (tabel) voor applicatiedata (structured data store.application data tables).
- Spreiding van tabeldata over meerdere (typen) opslagmedia (tiering. application data table storage)
- Tijdelijk snel beschikbaar houden van veel geraadpleegde applicatiedata (caching.data engine).
- Replicatie van transacties ten behoeve van een redundante opslag van applicatiedata in onderscheiden instances van een data-opslagvoorziening (data replication.transactions).
- Replicatie van virtuele opslagruimtes (tabellen) ten behoeve van het inrichten van redundante opslag (data replication.application data tables).
- Invoer van gegevens via een (intern volgens een van te voren vastgesteld format gestructureerd) bestand (import.data file).
- Export van gegevens naar een (intern volgens een van te voren vastgesteld format gestructureerd) bestand ten behoeve van import in een andere data-opslagvoorziening en/of data-analyse (export.data file).
- Vastleggen van transactiegegevens ten behoeve van reconstructie van dataverwerkingstransacties, onder andere bij herstel van gestructureerde opslagruimtes/tabellen (logging.transactions.data management).
- Vastleggen van gebeurtenissen ten behoeve van auditing (logging.auditing.data management).
- Versleuteling/ontsleuteling van data in gestructureerde opslagruimtes (encryption.application data tables).
- Verbergen van gegevens in een dataset ten behoeve van privacybescherming (concealment.application data).
- Bedienfunctie in de vorm van een centrale, grafische beheertool (controlling.centralized management console.data management)
- Bedienfunctie in de vorm van een directe aansturing van de data-engine. Deze functie kan worden benut vanuit een terminal of via een grafische bedientool (zoals TOAD, SQL-developer, et cetera) (controlling.command line.data management).

Ten aanzien van de functies binnen Datatransport gelden de volgende (aanvullende) vereisten:

ID	Weging	Omschrijving	Rationale	Soort	Gerelateerd aan
DBM-01	Must	Voorzieningen voor datamanagement dienen vanuit een centrale omgeving beheerd en gemonitord kunnen worden (over meerdere typen heen)	Centraal beheer is efficiënt en voorkomt fouten, zeker in een gedistribueerd landschap.	Operationeel	Datamanagement
DBM-02	Must	Diensten voor datamanagement dienen compatibel te zijn met Oracle 19c RDBMS en MS SQL Server	De huidige inrichting van de Diensten voor datamanagement zijn gebaseerd op Oracle en MS SQL-componenten. Kentallen: Oracle databases <ul style="list-style-type: none"> • Oracle databases: 72/46/3 (productie acceptatie/test), 4,4 TB • SQL databases: 4/2 (productie/acceptatie), 750 GB 	Operationeel	Datamanagement

DBM-03	Must	Het moet mogelijk zijn om voor Oracle databases licenties uit de Centric Melody 5.0-licentieovereenkomst te gebruiken.	Om kosten te besparen dienen bestaande licentieovereenkomsten uitgenut te kunnen worden.	Financieel	Datamanagement
DBM-04	Must	Het moet mogelijk zijn om bij Point in Time Restore / herstel van transacties tot 30 dagen terug in de tijd te gaan.	Eis vanuit dataproctiemaatregelen afnamers.	Beveiliging	logging.transactions.data management
DBM-05	Could	Indien het niet mogelijk is om beprijzing via contractuele weg te verlagen, dient het mogelijk te zijn om bulk/historische data onder te brengen op een goedkoop opslagmedium	Het moet mogelijk te zijn om kosten van opslag (dynamisch) te beheersen.	Functioneel/ Operationeel	tiering. application data table storage
DBM-06	Could	Het dient mogelijk zijn om datatabellen te stretchen over meerdere data engines	Het spreiden van datatabellen over meerdere data engines is een randvoorwaarde voor het gebruik van meerdere opslagtiets	Functioneel/ Operationeel	structured data store.application data tables
DBM-07	Should	Gebruik van caching vindt alleen plaats op basis van standaard mogelijkheden binnen het platform voor datamanagement.	Er wordt binnen het applicatielandschap van de (deelnemers van de) Aanbestedende dienst geen gebruik gemaakt van geavanceerde cachingfunctionaliteit.	Functioneel	caching.data engine
DBM-08	Must	De volgende bestandsformaten dienen te kunnen worden geïmporteerd: <ul style="list-style-type: none"> • CSV-bestand • Datapump-bestand 	Zowel ETL-operaties als migraties dienen geautomatiseerd uitgevoerd kunnen worden.	Operationeel	import.data file
DBM-09	Must	De volgende bestandsformaten dienen te kunnen worden geëxporteerd: <ul style="list-style-type: none"> • CSV-bestand • Datapump-bestand 	Zowel ETL-operaties als migraties dienen geautomatiseerd uitgevoerd kunnen worden.	Operationeel	export.data file
DBM-10	Must	Ten behoeve van auditing dienen de volgende gebeurtenissen te worden vastgelegd: <ul style="list-style-type: none"> • externe transacties (transacties die niet afkomstig zijn van gekoppelde applicaties) • beheeracties 	Het beveiligingsbeleid schrijft voor dat genoemde gebeurtenissen achteraf te controleren zijn.	Beveiliging	logging.auditing
DBM-11	Must	Gegevens dienen met behulp van BYOK-mechanismes transparant versleuteld kunnen worden.	Voor de borging van digitale autonomie dient de data die is opgeslagen in een MPC-omgeving transparant versleuteld kunnen worden.	Beveiliging	(encryption.application data tables)
DBM-12	Should	Het moet mogelijk zijn om oorspronkelijke data op verschillende manieren te verbergen: <ul style="list-style-type: none"> • masking (onzichtbaar maken) • scrambling (vervangen door dummydata) 	Het dient mogelijk te zijn data te delen zonder privacygevoelige gegevens te tonen, waarbij de context bepaalt welke aanpak het meest geschikt/noodzakelijk is (masking is minder ingrijpend, maar niet altijd mogelijk, bijvoorbeeld in het geval van een export).	Privacybescherming	concealment.application data
DBM-13	Should	Het verbergen van data dient op de volgende niveaus te kunnen worden ingesteld: <ul style="list-style-type: none"> • tabel • record • kolom/veld 	Door verschil in granulariteit aan te brengen, kan het verbergen efficiënt of juist heel precies toegepast worden.	Privacybescherming	concealment.application data
DBM-14	Must	Inschrijver is in ieder geval verantwoordelijk voor het uitvoeren van beheer en lifecyclemanagement	Als kerncomponent van de Dienst Datamanagement dient de end-to-	Operationeel	Datamanagement

		op de databaseplatformen. Hieronder vallen onder meer de volgende activiteiten: <ul style="list-style-type: none"> • Installatie en configuratie van databaseplatformen. • Versiebeheer. • Het uitvoeren van security updates en patches (patchmanagement). • Het toepassen en onderhouden van nader af te stemmen beveiligingsrichtlijnen (hardening). • Het monitoren van de technische staat van databaseplatformen. 	endverantwoordelijkheid hiervoor bij de Inschrijver te berusten.		
DBM-15	Must	Lifecyclemanagement van databaseplatformen dient uitgevoerd te worden conform de releaseplanning van leveranciers.	Databaseomgevingen dienen up-to-date gehouden te worden.	Operationeel/Beveiliging	Data Management
DBM-16	Must	Lifecyclemanagement van databaseplatformen dient uitgevoerd te worden via Test/Acceptatie/Productie-fasering.	Updates dienen eerst getest te kunnen worden in minder kritieke omgevingen.	Operationeel	Data Management
DBM-17	Must	Lifecyclemanagement en uitrol van updates van databaseplatformen dient afgestemd te worden met de Aanbestedende dienst.	Het uitvoeren van lifecyclemanagement en uitrollen van updates mag de bedrijfscontinuïteit van afnemers niet in gevaar brengen.	Operationeel	Data Management

3.6 Bestandsopslag

Bestandsopslag verzorgt de semi-gestructureerde opslag van data middels een gecentraliseerd bestandssysteem. Data wordt beschermd tegen incidenten en calamiteiten door replicatie en versiebeheer van bestandssystemen en bestanden. De Dienst biedt (in ieder geval) de volgende functies:

- Opslag van databestanden (inclusief basale bestandsattributen) in mappenstructuren (file engine.application & user data).
- Versleuteling/ontsleuteling van bestanden (encryption.files)
- Replicatie van bestanden ten behoeve van een redundante opslag van bestanden in onderscheiden instances van een bestandsopslag (data replication.files).
- Functie voor het tijdelijk snel beschikbaar houden van veel geraadpleegde bestanden (data caching.files).
- Bewaren en beheren van versies van bestanden bij opslag van wijzigingen (version handling.files).
- Maken, conserveren en terugzetten van een momentopname (snapshot) van de toestand van een bestandssysteem (state preservation.file engine)file
- Geautomatiseerde aftrap van opslagbewerkingen, zoals het genereren van een snapshot (scheduling.file engine).
- Vastleggen van gebeurtenissen/opslagacties ten behoeve van auditing (logging.file engine)

Ten aanzien van de Dienst Bestandsopslag gelden de volgende (aanvullende) vereisten:

ID	Weging	Omschrijving	Rationale	Soort	Gerelateerd aan
BOS-01	Must	De Dienst biedt (in ieder geval) ondersteuning voor ontsluiting met de volgende bestandssystemen: <ul style="list-style-type: none"> • SMB2, SMB3 (CIFS) • NFS3 en NFS4 	Voor de opslag van bestanden (applicatiedatabestanden) is toegang nodig tot verschillende bestandssystemen, afhankelijk van het gebruikte	Operationeel	file engine. application & user data

		Via deze protocollen is dit type Dienst ook van buitenaf te ontsluiten.	besturingssysteem en de versie hiervan.		
BOS-02	Must	Voor bestandsopslag wordt de standaarddienst afgenomen, tenzij een applicatie hogere performancekarakteristieken vereist	Prestatiekenmerken van standaarddiensten zijn voor normale bestandstoegang voor applicaties voldoende.	Operationeel	file engine.application & user data
BOS-03	Must	Bij aanvang van het contract dient minimaal 75TB aan ruimte dient beschikbaar te zijn voor de opslag van shared data over diverse fileshares, die in gebruik zijn bij afnemers van de Aanbestedende dienst (omvang zonder compressie en/of deduplicatie).	Het moet mogelijk zijn om de hoeveelheid data die aanwezig is in de huidige omgeving over te zetten naar de Managed Private Cloudomgeving.	Operationeel	file engine.application & user data
BOS-04	Must	Logging is aanwezig voor het bijhouden van toegang tot bestandssystemen en het uitvoeren van mutaties.	Het moet mogelijk zijn om toegang en handeling ten aanzien van bestanden achteraf in te zien/te controleren. Dit heeft diverse doeleinden. Onder andere ten behoeve van beveiliging alsook het beheersen van ruimtebeslag.	Beveiliging/ Operationeel	logging.file engine
BOS-05	Must	Regelmatig wordt actief gecontroleerd en gerapporteerd of bestandssystemen nog worden benaderd, zodat geanalyseerd kan worden of overschakelen naar 'cold' opslag economische voordelen oplevert.	Om kosten voor opslag te beheersen, dienen data/bestandsets die minder actief worden benaderd op een storagetier te worden ondergebracht die economisch voordelig is ten aanzien van het ruimtebeslag	Operationeel	logging.file engine
BOS-06	Must	Het moet mogelijk zijn om een vorige versie van het bestandssysteem terug te zetten. Hiervoor wordt een keer per uur een status geconserveerd, met (in ieder geval) elk een bewaartermijn van een dag, waarvan zes instanties per dag (in ieder geval) een bewaartermijn van zeven dagen hebben en waarvan een instantie per dag (in ieder geval) een bewaartermijn van dertig dagen heeft.	Om beschermd te zijn tegen corruptie van data door onjuiste/onbevoegde bewerkingen moet het mogelijk zijn om terug te gaan naar een eerdere versie van het bestandssysteem	Operationeel/ Beveiliging	file engine. application & user data, state preservation.file engine

3.7 Raw storage

Raw Storage biedt de mogelijkheid om data rechtstreeks op te slaan in de vorm van blocks, objecten of tabellen. Deze vorm van storage wordt hiermee gebruikt door andere opslagdiensten, die een gegevens en/of bestandsstructuur bieden. De Dienst biedt (in ieder geval) de volgende functies:

- Opslaglocatie voor het opslaan van datablokken (raw storage.blocks).
- Opslaglocatie voor het opslaan van objecten (raw storage.objects).
- Opslaglocatie voor het opslaan van tabellen (raw storage.tables)
- Versleuteling/ontsleuteling van opslaglocaties encryption.raw storage unit).
- Replicatie van opslagacties ten behoeve van een redundante opslag van data in onderscheiden instances van opslagvolumes/-locaties data replication.raw storage operations).
- Geautomatiseerde aftrap van opslagbewerkingen, zoals het uitvoeren van een backup (scheduling.storage operations).
- Vastleggen van gebeurtenissen/opslagacties ten behoeve van auditing (logging.raw storage).

Ten aanzien van de Dienst Raw Storage gelden de volgende (aanvullende) vereisten:

ID	Weging	Omschrijving	Rationale	Soort	Gerelateerd aan
RST-01	Must	Dit type Dienst is van buitenaf te ontsluiten via een REST API	Opslagvoorzieningen dienen benaderbaar te zijn vanaf externe systemen (vanuit het de Managed Private Cloudomgeving gezien)	Operationeel	Raw storage

3.8 Data Recovery

De Dienst Data Recovery maakt het mogelijk om virtuele machines, datasets, bestanden en volumes te herstellen op basis van een eerder gemaakte reservekopie. Dit in aanvulling van de functies die binnen de opslagdiensten zorgen voor dataprotectie. Ook is Data Recovery te gebruiken om datasets, bestanden en volumes op een andere dan de oorspronkelijke opslaglocatie opnieuw op te bouwen. De Dienst biedt (in ieder geval) de volgende functies:

- Maken van een reservekopie van alle gegevens en bestanden van een database en daaraan gerelateerde transactielogs (backup.dataset).
- Herstellen van een database met behulp van een reservekopie met alle gegevens en daaraan gerelateerde bestanden (restore.dataset).
- Maken van een reservekopie van een of meerdere geselecteerde bestanden (backup.file).
- Herstellen van als reservekopie opgeslagen bestanden (restore.file).
- Maken van een reservekopie van een opslaglocatie (backup.raw storage unit)
- Herstellen van een opslaglocatie aan de hand van een reservekopie (restore.raw storage unit).
- Geautomatiseerd in werking stellen van backuproutines (voor het periodiek vervaardigen van een reservekopie) (scheduling.backup).
- Bedienfunctie in de vorm van een centrale, grafische beheertool (controlling.centralized management console.backup).

Ten aanzien van de Dienst Data Recovery gelden de volgende (aanvullende) vereisten:

ID	Weging	Omschrijving	Rationale	Soort	Gerelateerd aan
DRC-01	Should	De Dienst wordt vanuit een centrale omgeving bediend en gemonitord.	Ten behoeve van efficiëntie van beheer dient de Dienst vanuit een plaats te beheren zijn.	Operationeel	Data Recovery
DRC-02	Must	Het moet mogelijk zijn om te differentiëren in hersteltijden.	Sommige applicaties zijn meer bedrijfskritisch dan andere. Deze dienen voorrang te krijgen bij een calamiteit/incident, terwijl het herstel van andere applicaties kan wachten.	Operationeel	Data Recovery
DRC-03	Must	Het moet mogelijk zijn om read-only point-in-time kopieën te maken van alle opslagtypen, met een maximale bewaartermijn van 1 jaar. Deze reservekopie dient extern opgeslagen te worden door de hiervoor door Aanbestedende dienst ingerichte omgeving (OVHCloud)	Buiten de maatregelen voor databescherming (replicatie, versiebeheer) moet het mogelijk zijn om reservekopieën van data/bestandssets en volumes te maken. Deze worden op een externe locatie opgeslagen voor het faciliteren van de Exitstrategie.	Operationeel	backup.dataset backup.file backup.raw storage unit
DRC-04	Must	Read-only point-in-time kopieën kunnen worden gemaakt op basis van een van tevoren in te stellen tijdschema.	Het moet mogelijk zijn om vooraf momenten in te stellen waarop reservekopieën worden gecreëerd.	Operationeel	backup.dataset backup.file backup.raw storage unit
DRC-05	Must	Het moet mogelijk zijn voor Servicedeskmedewerkers van de Aanbestedende dienst om bestanden binnen de Dienst	De Aanbestedende dienst moet zelf in staat zijn herstelacties uit te voeren.	Operationeel	Data Recovery

		Bestandsopslag te herstellen vanuit een reservekopie.			
DRC-06	Should	Het moet mogelijk zijn voor een Servicedeskmedewerker van de Aanbestedende dienst om het herstel van een image of deel daarvan (vanuit de Dienst Applicatiehosting) geautomatiseerd uit te voeren via een selfserviceportaal.	De Aanbestedende dienst moet zelf in staat zijn herstelacties uit te voeren.	Operationeel	Data Recovery
DRC-07	Should	Het moet mogelijk zijn voor een Servicedeskmedewerker van de Aanbestedende dienst om het herstel van een dataset of deel daarvan (vanuit de Dienst Datamanagement) geautomatiseerd uit te voeren via een selfserviceportaal.	De Aanbestedende dienst moet zelf in staat zijn herstelacties uit te voeren.	Operationeel	Data Recovery

3.9 Selfserviceportaal

De Dienst Selfserviceportaal biedt de mogelijkheid aan de Aanbestedende dienst om zelfstandig, zonder tussenkomst van de Inschrijver, (standaard) servicemanagement- en beheertaken uit te voeren ten aanzien van Diensten die vanuit de Managed Private Cloudomgeving worden gerealiseerd. De Dienst biedt (in ieder geval) de volgende functies (al dan niet geïntegreerd binnen een en dezelfde omgeving):

- Aansturen Provisioning/Deployment Handlingdienst (zie paragraaf 3.10) voor het aanmaken en configureren van instanties van Diensten (deployment.service instance).
- Aansturen Provisioning/Deployment Handlingdienst voor het aanmaken en configureren van componenten (VM's, containers, storage en netwerkresources, besturingssystemen, et cetera) (deployment.component).
- Aansturen van (geautomatiseerde) herstelacties vanuit de Dienst Data Recovery (zie paragraaf 3.8).
- Beheren van instanties van Diensten (administration.service instance).
- Beheren van componenten (VM's, containers, storage en netwerkresources, besturingssystemen, et cetera) (administration.component).
- Aanvragen van (instanties van) Diensten (request.service instance).
- Aanvragen van wijzigingen op Diensten (request.service changes).
- Vastleggen en rapportage van gebeurtenissen (logging & reporting.event).
- Rapportage van voortgang van servicemanagement-, wijzigings- en beheeractiviteiten (reporting.service management & administration).
- Rapportage van incidenten (reporting.incident).
- Rapportage van compliance-status (reporting.compliance).
- Rapportage van middelengebruik en -beslag (reporting.service usage).
- Rapportage van kosten en facturatie (reporting.finance).

ID	Weging	Omschrijving	Rationale	Soort	Gerelateerd aan
SSP-01	Must	Het aanmaken en uitrollen van componenten en resources dient op basis van vooraf opgestelde scripts/templates te kunnen gebeuren.	Het moet mogelijk zijn om efficiënt, consistent en eenduidig veelvoorkomende uitrolactiviteiten uit te voeren.	Operationeel	deployment.component
SSP-02	Must	Het moet mogelijk zijn voor Aanbestedende dienst om dashboards in te richten/aan te (laten) passen op basis van aangegeven meetwaarden.	Dashboards moeten in een oogopslag de status laten zien van (uitsluitend) die meetwaarden die voor de Aanbestedende dienst relevant zijn voor de continuïteit van de levering van Diensten aan afnemers.	Operationeel	reporting.*
SSP-03	Should	Het moet mogelijk zijn de volgende rollen aan gebruikers van het Selfserviceportaal toe te kennen: <ul style="list-style-type: none"> • Servicemanager 	De Aanbestedende dienst moet bevoegdheden ten aanzien van servicemanagement en	Operationeel	Selfserviceportaal

		<ul style="list-style-type: none"> Financieel beheerder Functioneel beheerder Technisch beheerder 	beheer kunnen differentiëren op basis van de rollen die medewerkers in de organisatie bekleden.		
SSP-04	Must	Minimaal de volgende gebeurtenissen dienen te worden gerapporteerd: <ul style="list-style-type: none"> Toegang van medewerkers tot het Selfserviceportaal. Uitvoeren van servicemanagement- en beheeracties (commit). 	Ten behoeve van beveiligings- en compliancerapportage dient de Aanbestedende dienst inzicht te hebben in gebeurtenissen die impact hebben op (de wijze van functioneren van) de Managed Private Cloudomgeving.	Beveiliging	logging & reporting.event
SSP-05	Must	Het Selfserviceportaal dient via een grafische gebruikersinterface te benaderen zijn voor uitvoering van servicemanagement- en beheertaken door medewerkers	Medewerkers van de Aanbestedende dienst moeten op een intuïtieve manier taken kunnen uitvoeren.	Operationeel	Selfserviceportaal
SSP-06	Must	Het Selfserviceportaal dient via API's gekoppeld te zijn met het Servicemanagementplatform van de Aanbestedende dienst (TopDesk) voor uitvoering van geautomatiseerde servicemanagement- en beheertaken.	De Aanbestedende dienst moet vanuit het eigen Servicemanagementplatform geautomatiseerd taken kunnen uitvoeren.	Operationeel	Self-servicportaal

3.10 Provisioning/Deployment Handling

De Dienst Provisioning/Deployment Handling (Automation) maakt het mogelijk platformen, applicatie(componenten) en (instanties van) Diensten geautomatiseerd te uit te rollen (distribueren, installeren, configureren). De Dienst biedt (in ieder geval) de volgende functies:

- Geautomatiseerde uitrol van systemen en systeemconfiguraties (deployment.systems)
- Geautomatiseerde uitrol van instanties van Diensten (deployment.service instances)
- Configureerbare verwerkingseenheid van regels, in dit verband ingezet voor het aansturen van uitrolactiviteiten (rules engine.deployment).
- Het opvragen van de status van uitrolactiviteiten bij systemen (status retrieval.systems deployment).
- Gestructureerde opslag van systeemconfiguraties (data store.systems configuration).
- Vastleggen van gebeurtenissen en activiteiten van uitrolprocessen (logging.platform deployment).
- Rapporteren en genereren van meldingen van de status van uitrolactiviteiten (reporting.deployment status).
- Bedienfunctie in de vorm van een centrale, grafische beheertool (controlling.centralized management console.platform deployment & deployment handling).

Ten aanzien van de Dienst Provisioning/Deployment Handling gelden de volgende (aanvullende) vereisten:

ID	Weging	Omschrijving	Rationale	Soort	Gerelateerd aan
PDH-01	Should	De Dienst dient bij voorkeur te kunnen worden aangestuurd vanuit het servicemanagementplatform (Topdesk) van de Aanbestedende dienst op basis van gebruik van formulieren. Daarbij dienen gerealiseerde componenten (tevens) geregistreerd te worden in het servicemanagementplatform van de Aanbestedende dienst.	Het moet voor de Aanbestedende dienst mogelijk zijn om rechtstreeks instanties van Diensten en componenten geautomatiseerd te laten realiseren vanuit de eigen Servicemanagement-omgeving.	Operationeel	Provisioning/Deployment Handling
PDH-02	Must	De volgende systeemonderdelen (doelsystemen) dienen geautomatiseerd uitgerold/geconfigureerd te kunnen worden:	De geautomatiseerde uitrol dient zodanig ingericht te zijn dat alle relevante systeemcomponenten hiermee ingericht kunnen	Operationeel	Provisioning/Deployment Handling

		<ul style="list-style-type: none"> Containers virtuele machines Virtual Appliances Raw Storage (configuratie) Besturingssystemen Applicaties Agents Upgrades/patches Configuratie-instellingen 	worden en de Dienst tegelijkertijd toegepast kan worden voor geautomatiseerd onderhouden en bijwerken van systemen.		
PDH-03	Must	Provisioning / Deployment Handling dient (logisch) onafhankelijk van de platformen van de Inschrijver te functioneren.	Door de uitroldienst uniform in te richten, wordt voorkomen dat een afhankelijkheid ontstaat met een specifieke Inschrijver en wordt geborgd dat uitrol bij meerdere leveranciers vanuit eenzelfde voorziening kan worden gedaan en de scripts hetzelfde zijn, ongeacht de leverancier waar een platform uitgerold wordt.	Functioneel, Operationeel	Provisioning/ Deployment Handling
PDH-04	Must	De voorziening voor Provisioning / Deployment Handling dient gekoppeld te zijn aan het servicemanagementsysteem	Met uitrolactiviteiten worden nieuwe systemen gecreëerd en bestaande systemen gewijzigd. Om ervoor te zorgen dat het servicemanagementsysteem beschikt over actuele data ten aanzien van systemen, dienen deze gegevens vanuit de uitrolvoorziening geautomatiseerd gerapporteerd te worden.	Functioneel, Operationeel	reporting.deployment status
PDH-05	Must	De volgende zaken dienen meegegeven worden bij uitrolrapportage richting het servicemanagementsysteem: <ul style="list-style-type: none"> Omgeving waarbinnen een systeem is uitgerold/bijgewerkt Initiator van de uitrolactie Resourcegebruik als resultante van uitrolactie Beoogde/maximale levensduur van het systeem. 	Bij rapportage van uitrolactiviteiten is het belangrijk dat de context en de (beheer)impact wordt meegegeven en traceerbaar is.	Operationeel	reporting.deployment status
PDH-06	Must	Het resultaat van uitrolactiviteiten dient bij de volgende processen/Diensten geautomatiseerd aangemeld te worden: <ul style="list-style-type: none"> Back-up Monitoring Antimalwarevoorziening Kostenregistratie Service Management Facturatie 	Na uitrol dienen platformen volledig in beheer genomen te kunnen worden en moeten derhalve opgenomen worden in de hiervoor ingerichte processen.	Operationeel	reporting.deployment status
PDH-07	Must	Het moet mogelijk zijn standaard uitrolscripts te combineren met (afzonderlijk op te voeren) systeemvariabelen, zoals: <ul style="list-style-type: none"> Systeemparameters en – configuratie (op VM- en besturingssysteemniveau) Beschikbaarheids-/Schaalbaarheidslevels Storage account/storage tiers (incl. keys) 	Uitrolprocessen dienen zo gestandaardiseerd mogelijk ingericht te kunnen worden, zonder het genereren van nieuwe code te vereisen.	Operationeel	rules engine.systems deployment

3.11 Housing

Voor het plaatsen van componenten van de Aanbestedende dienst waarmee de (netwerk)Diensten Datadistributie, -inspectie en -filtering en Interconnectiviteit worden gerealiseerd, is de Dienst Housing benodigd. De volgende voorzieningen dienen via deze Dienst beschikbaar te worden gesteld:

- Afsluitbare 19" rack-space, minimaal 20U hoogte-eenheden, inbouwdiepte minimaal 1000mm.
- 230V redundante stroomvoorziening (aangesloten op noodstroom).
- PDU. Wens: met mogelijkheid om per aansluiting op afstand een power off/on uit te voeren.
- Klimaatconditionering.
- Patchpaneel voor fysieke connectiviteit met externe netwerken (waaronder internet, Diginet, Eurofiber glasvezelring RID).
- Netwerkconnectiviteit met de Managed Private Cloudomgeving.

Voor medewerkers van Aanbestedende dienst en/of onderaannemers dient de housingfaciliteit 24x7 fysiek toegankelijk te zijn.

4 Connectiviteit

Het Dienstencluster Connectiviteit bevat Diensten die datatransport tussen verschillende locaties leveren en beveiligen. Dit betreft de locaties van de Inschrijver, locaties van (deelnemers van) de Aanbestedende dienst en locaties van externe leveranciers. Tevens omvat dit perceel de Dienst waarmee tweede- en derdelijnsbeheer voor de totale netwerkinfrastructuur wordt geleverd, behoudens de Dienst waarmee het datatransport binnen de Managed Private Cloudomgeving wordt geleverd. Deze Dienst (Datatransport) valt onder het Dienstencluster Workload Execution.

Er zijn verschillende manieren waarop de realisatie van Diensten binnen dit perceel kan worden ingevuld, waarbij aan Inschrijvers wordt gevraagd voor welke variant zij kiezen:

1. Inschrijver voert de Diensten Datadistributie, -inspectie en -filtering en Interconnection gateway uit met eigen componenten.
2. Inschrijver maakt gebruik van bestaande componenten voor de Diensten Datadistributie, -inspectie en -filtering en Interconnection gateway uit met eigen componenten, ondergebracht met behulp van de Dienst Housing uit het Dienstencluster Workload Execution. Deze variant heeft de voorkeur van Aanbestedende dienst.

4.1 Datadistributie, -inspectie en -filtering

De Dienst Datadistributie, -inspectie en -filtering zorgt voor de distributie van verkeer tussen veiligheidszones en netwerksegmenten. Tijdens het uitwisselen van verkeer tussen veiligheidszones en netwerksegmenten, wordt het verkeer geïnspecteerd en gefilterd (op applicatieniveau). De Dienst wordt (in ieder geval) gerealiseerd door de volgende functies:

- Uitwisseling van dataverkeer tussen compartimenten in de Managed Private Cloudomgeving (distribution.mpc).
- Analyse van dataverkeer op basis van applicatiekenmerken (data scanning.application level).
- Filteren van dataverkeer op applicatieniveau (traffic filtering.application level).
- Termineren van kopiesessies ten behoeve van ontsleuteling en (payload)inspectie.
- Het ontsleutelen (verwijderen van encryptie) van verkeer dat ten behoeve van beveiliging versleuteld is (decryption.data transport).
- Register met regels en verkeerspatronen ten behoeve van filtering van verkeer (configuration register.application level rule base).

Indien deze Dienst wordt uitgevoerd met andere dan de bestaande componenten, dienen deze componenten deze functionaliteit te bieden, evenals het geval is bij de bestaande componenten.

Indien deze Dienst wordt uitgevoerd met andere dan de bestaande componenten, zijn de volgende vereisten van toepassing, zoals deze ook geboden worden door de bestaande componenten:

ID	Weging	Omschrijving	Rationale	Soort	Gerelateerd aan
DIF-01	Should	Voor het uitvoeren van de Dienst worden componenten hergebruikt van de Aanbestedende dienst.	Het is economisch om bestaande componenten die onlangs in gebruik zijn genomen te hergebruiken. Voor de interoperabiliteit van de netwerkvoorzieningen over alle locaties heen is het efficiënt en wat betreft de inrichting het meest consistent om de huidige configuratie in zijn geheel te behouden.	Functioneel	Datadistributie, -inspectie en -filtering
DIF-02	Must	Indien deze Dienst wordt gerealiseerd met componenten van de Aanbestedende Dienst, dan dienen deze ondergebracht te kunnen worden in de vorm van colocatie	Indien componenten van de Aanbestedende dienst worden gebruikt, dient het mogelijk te zijn om housingfaciliteiten te gebruiken die zich	Functioneel	Datadistributie, -inspectie en -filtering

		(housing) op locatie van de Managed Private Cloudomgeving.	geografisch op dezelfde locatie bevinden als de Managed Private Cloudomgeving, ten behoeve van (fysieke) connectiviteit en het beperken van netwerkvertraging.		
DIF-03	Must	Als routeringsprotocol wordt OSPF ondersteund .	OSPF is binnen on premises netwerkimplementaties een standaard routeringsprotocol dat nodig is voor dynamische route-informatie.	Functioneel	distribution.mpc
DIF-04	Must	Als routeringsprotocol wordt BGP ondersteund .	BGP is op het internet en richting verschillende (andere) externe netwerken het standaard routeringsprotocol dat nodig is voor dynamische route-informatie.	Functioneel	distribution.mpc
DIF-05	Must	Ten behoeve van het gebruik van virtuele netwerken (VLAN's) over locaties heen ('stretched VLAN's') dient VXLAN-technologie toegepast te worden.	In de huidige situatie wordt VXLAN toegepast voor het over locaties heen definiëren en gebruiken van virtuele netwerken. Voor een naadloze transitie is het nodig dat deze technologie ook in de Managed Private Cloudomgeving beschikbaar is.	Functioneel	distribution.mpc
DIF-06	Should	Bij een redundante inrichting van 'routing interfaces' wordt een virtueel IP-adres toegepast dat hosts op een gerouteerd segment als gateway-adres gebruiken.	Bij een storing op een fysieke 'routing interface' dient een andere interface de functie over te kunnen nemen, indien aanwezig.	Functioneel	distribution.mpc
DIF-07	Must	Analyse van datastromen is mogelijk.	Op dit punt in het netwerk komen veel verkeersstromen samen, het is belangrijk voor inzicht in het verkeer dat op dit punt inzicht kan worden verkregen. Hiervoor is het van belang dat verkeer ondanks SSL-encryptie toch kan worden geïnspecteerd.	Operationeel	distribution.mpc, session handling.parallel scanning, encryption.data transport
DIF-08	Must	Filterregels worden uitgevoerd op een centrale locatie, te weten de (virtuele) appliance(s) die hiervoor wordt/worden ingezet. Het aanbrengen van de filterregels in (een) platform-fabric(s) wordt voorkomen.	Voor de consistentie en beheerbaarheid van filterregels is het essentieel dat op een centrale plek worden toegepast.	Operationeel	traffic filtering.application level
DIF-09	Must	Verkeersfiltering wordt op een centrale plek beheerd en gemonitord	Voor efficiënt beheer en snelle aanpasbaarheid is het essentieel dat filterregels op een plek worden bijgehouden.	Operationeel	traffic filtering.application level
DIF-10	Must	Analyse van applicatiekenmerken van verkeer gebeurt op basis van patronen/signatures die door de fabrikant van de filteroplossing worden aangeleverd, inclusief autodeployment met door de fabrikant aangeleverde voorkeursopties wat betreft opvolging.	Het herkennen van malafide verkeerspatronen vergt een dermate specialistische expertise dat het niet kosteneffectief is om hier zelf in te voorzien of dit van een beheerpartij te verwachten.	Operationeel	data scanning.application level
DIF-11	Must	Bij het onderbreken van versleutelde sessies ten behoeve van interne inspectie met behulp van decryptie/encryptie zijn de richtlijnen/aanbevelingen van de	Lokale overheidsdiensten conformeren zich aan ICT-Beveiligingsrichtlijnen van de overheid.	Beveiliging	session handling.encrypted traffic

		Factsheet TLS-interceptie van het NCSC van toepassing.			
--	--	--	--	--	--

4.2 Interconnection gateway

De Dienst Interconnection gateway levert het knooppunt waarmee op een beveiligde manier data kan worden uitgewisseld met externe netwerken. Tijdens het uitwisselen van verkeer tussen externe netwerken wordt het verkeer geïnspecteerd en gefilterd (op protocolniveau). Ook zorgt de Dienst voor versleuteling van data tijdens het transport van en naar externe netwerken. De Dienst wordt (in ieder geval) gerealiseerd door de volgende functies:

- Datatransport over een glasvezelverbinding die geconnecteerd is aan de glasvezelring die bij de Aanbestedende dienst in gebruik is (leverancier: Eurofiber) (interconnection.fibre-ring).
- Datatransport over een glasvezelverbindingen die geconnecteerd zijn met externe netwerken (o.a. Internet, DigiNetwerk) (interconnection.external environments.*).
- Uitwisseling van dataverkeer tussen locaties (distribution.external connections).
- Filteren van dataverkeer op protocolniveau (netwerk- en sessie-ID's) (traffic filtering.protocol level).
- Register met regels ten behoeve van filtering van verkeer (configuration register.protocol level rule base).
- Leveren van een koppelvlak voor het termineren van een virtuele, versleutelde netwerkverbinding (tunnel) ten behoeve van interconnectiviteit over een niet-vertrouwd netwerk (o.a. internet) (tunnel endpoint.interconnection).
- Versleuteling/ontsleuteling van gegevens voor het veilig uitwisselen van data over een netwerkverbinding (data transport).

Indien deze Dienst wordt uitgevoerd met andere dan de bestaande componenten, dienen deze componenten deze functionaliteit te bieden, evenals het geval is bij de bestaande componenten.

Indien deze Dienst wordt uitgevoerd met andere dan de bestaande componenten, zijn de volgende vereisten van toepassing, zoals deze ook geboden worden door de bestaande componenten:

ID	Weging	Omschrijving	Rationale	Soort	Gerelateerd aan
IGW-01	Must	De Dienst is redundant ingericht over twee locaties, te weten de locatie waar de managed private hosting-omgeving zich bevindt en een van de locaties van de Aanbestedende dienst (Doorn)	Om ervoor te zorgen dat vanuit de locaties van deelnemers altijd dataverkeer kan worden uitgewisseld met externe partijen (ook wanneer de Managed Private Cloudomgeving niet beschikbaar is), dienen deze ook direct vanuit de glasvezelring van RID-Utrecht bereikbaar te zijn.	Functioneel	Interconnection Gateway
IGW-02	Must	De verbinding met de glasvezelring die bij de Aanbestedende dienst in gebruik is, dient zodanig redundant te zijn ingericht dat de locatie(s) van de Managed Private Cloudomgeving topologisch in deze ring worden opgenomen.	De locatie(s) van de Managed Private Cloudomgeving dienen bereikbaar te blijven als een (enkele) verbinding niet meer beschikbaar is. De ringtopologie zorgt voor meerdere paden, die vanuit iedere locatie beschikbaar zijn.	Functioneel	Interconnection.fibre-ring
IGW-03	Must	Met de volgende externe partijen/netwerken dient datatransport over een glasvezelverbinding mogelijk te zijn: <ul style="list-style-type: none"> • Internet • Diginet 	De deelnemers van de Aanbestedende dienst dienen dataverkeer uit te kunnen wisselen met deze externe partijen/netwerken ten behoeve van de werking van de applicaties die zij in gebruik hebben.	Functioneel	interconnection.external environments.*
IGW-04	Must	De maximale netwerkvertraging die optreedt op de verbinding die de	De totale netwerkvertraging die acceptabel is tussen hosts	Functioneel	interconnection.fibre-ring,

		interconnectie tussen de managed private cloud-datacenterlocaties realiseert en de glasvezelring die bij de Aanbestedende dienst in gebruik is, evenals die de verbinding realiseren met externe netwerken, dient kleiner te zijn dan 10ms	die zich op verschillende locaties bevinden, is 14ms. Rekening houdend met 2ms lokale vertraging, is de tolerantie voor vertraging op de verbinding tussen locaties dus maximaal 10ms.		interconnection.external environments.*
IGW-05	Must	Als routeringsprotocol wordt BGP ondersteund.	BGP is binnen (publieke, virtuele) datacenters het standaard routeringsprotocol dat nodig is voor dynamische route-informatie.	Functioneel, Operatie	distribution.external connections
IGW-06	Must	Analyse van datastromen is mogelijk.	Op dit punt in het netwerk komen veel verkeersstromen samen, het is belangrijk voor inzicht in het verkeer dat op dit punt inzicht kan worden verkregen.	Operatie	distribution.external connections
IGW-07	Must	Filterregels worden uitgevoerd op een centrale locatie, te weten de (virtuele) appliance(s) die hiervoor wordt/worden ingezet. Het aanbrengen van de filterregels in (een) platform-fabric(s) wordt voorkomen.	Voor de consistentie en beheerbaarheid van filterregels is het essentieel dat op een centrale plek worden toegepast.	Functioneel, Operatie	traffic filtering.protocol level
IGW-08	Must	Verkeersfiltering wordt op een centrale plek beheerd en gemonitord.	Voor efficiënt beheer en snelle aanpasbaarheid is het essentieel dat filterregels op een plek worden bijgehouden.	Functioneel, Operatie	traffic filtering.protocol level
IGW-09	Must	Voor de toepassing van versleuteling van datatransport zijn de NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) van toepassing, minimaal op veiligheidsniveau VOLDOENDE.	Lokale overheidsdiensten conformeren zich aan ICT-beveiligingsrichtlijnen van de overheid.	Beveiliging	encryption.data transport
IGW-10	Must	(Distributed) Denial of Service-aanvallen dienen te worden gedetecteerd en geïsoleerd bij verkeersstromen waar dit niet al upstream wordt uitgevoerd.	DDoS-aanvallen tasten de normale werking van het datatransport (in ernstige mate) aan en dienen zo snel mogelijk onschadelijk gemaakt te worden. Voldaan dient te worden aan BIO-richtlijn 13.1.2.4.	Beveiliging	distribution.external connections

4.3 Netwerkbeheer

Aanbestedende dienst wil ten aanzien van het beheer van de volledige netwerkinfrastructuur (op eigen locaties en die van de afnemers) de volgende activiteiten uit laten voeren (wens):

- Monitoring - Het actief bewaken van de correcte werking van apparatuur en protocollen, het opvangen van storingsmeldingen van apparatuur en het verzamelen van gebruiks- en meetgegevens.
- Probleemonderzoek - Het achterhalen van storingsbronnen door het interpreteren, koppelen en analyseren van storingsmeldingen van apparatuur en gebruiks- en meetgegevens.
- Alarmering - Het op de hoogte stellen van medewerkers van de Aanbestedende dienst van (ernstige) verstoringen, conform de afgesproken rolverdeling, zoals aangegeven in paragraaf 2.5.2.
- Uitvoeren wijzigingen/wijzigingsverzoeken - Het aanpassen van configuraties van apparatuur op basis van (functioneel of technisch gedefinieerde) aanvragen.
- Uitvoeren updates systeemsoftware en -patches - Het bijwerken van systeemsoftware van apparatuur op basis van met de Aanbestedende dienst afgestemd lifecycle- en patchmanagement, op basis van lifecycleplanningen van leveranciers en actuele dreigingen.

- Vervanging van apparatuur bij defecten.
- Maken reservekopieën configuraties/instellingen - Het veiligstellen van configuraties door periodiek (minstens 1 keer per week) incrementeel vastleggen van configuratie- en instellingenbestanden op een externe locatie.
- Bijhouden netwerkdocumentatie - Het documenteren van wijzigingen door deze incrementeel te verwerken in de bestaande netwerkdocumentatie.
- Technisch advies en ondersteuning - Op afroep beschikbaar stellen van specialistische kennis bij vraagstukken van functionele en/of technische aard ten aanzien van de werking van de netwerkinfrastructuur.

Ten aanzien van deze beheerwerkzaamheden zijn de Servicelevels van toepassing, zoals vastgelegd in paragraaf 2.5.3.

Toegang voor de Aanbestedende dienst tot de netwerkbeheerdienst wordt zo mogelijk integraal ondergebracht in de Dienst Selfserviceportaal, zoals gedefinieerd in paragraaf 3.9. Indien het niet mogelijk is om dit als integraal onderdeel in deze Dienst onder te brengen, dan wordt hiervoor een aparte instantie van een Selfserviceportaal ingericht, conform de definitie in paragraaf 3.9.

Een gedetailleerd technisch ontwerp van de huidige netwerkinrichting wordt op aanvraag toegestuurd. In dit technisch ontwerp is een uitputtend overzicht opgenomen van de gebruikte technische apparatuur, de gebruikte protocollen en de topografie en technische inrichting van de volledige netwerkinfrastructuur, zoals deze in gebruik is bij de Aanbestedende dienst.

5 Technische basisvoorzieningen

Een aantal voorzieningen binnen het ecosysteem van de Aanbestedende dienst is ondersteunend van aard en cruciaal voor de werking ervan. Omdat hiervan gemeenschappelijk gebruik gemaakt wordt en dat ook in de toekomst zo moet zijn, blijven deze voorzieningen rechtstreeks onder de verantwoordelijkheid van de Aanbestedende dienst vallen en maken deze geen deel uit van de aanbesteding. Om duidelijkheid te scheppen in samenhang en de manier waarop hiermee Diensten voor Workload Execution en Connectiviteit worden ondersteund, beheerd en beveiligd, is in dit hoofdstuk een beschrijving van deze Diensten opgenomen, inclusief de eisen die aan de Inschrijver worden gesteld ten behoeve van de werking van deze voorzieningen.

5.1 Centrale Authenticatie

Voordat gebruikers Diensten kunnen afnemen of bronnen kunnen raadplegen, moet zo ondubbelzinnig mogelijk worden vastgesteld of de digitale identiteit waarmee ze dit doen hoort bij de gebruiker die als natuurlijk persoon hieraan gekoppeld is. Daarom is het nodig om als basisvoorziening binnen het ecosysteem de authenticatie (identiteitsvalidatie) goed te regelen.

De Dienst Centrale Authenticatie maakt het mogelijk voor medewerkers en die onder de beheerverantwoordelijkheid van Aanbestedende dienst vallen aan te melden de Digitale Werkomgeving van de Aanbestedende dienst en op applicaties die door leveranciers beschikbaar worden gesteld (meestal in de vorm van een SaaS-applicatie). Door deze Dienst in te zetten in combinatie met een externe (SaaS-)applicatie hoeven gebruikers slechts een keer in te loggen (ofwel op een interne werkplek, of bij een willekeurige externe applicatie) om toegang te krijgen tot alle applicaties die bij deze Dienst zijn aangesloten (Single Sign On). De Dienst is erop ingericht om zoveel als mogelijk MFA (multifactorauthenticatie) toe te passen, waarbij de digitale identiteit van gebruikers op meerdere manieren kan worden geverifieerd.

5.2 Network support services

Ten behoeve van het goed functioneren van apparatuur binnen de netwerkinfrastructuur zijn een aantal ondersteunde netwerkdiensten in gebruik en beheer bij de Aanbestedende dienst:

- Naamresolutie (DNS)
- Automatische netwerkconfiguratie (DHCP)
- Tijdssynchronisatie (NTP).

Voor naamresolutie middels DNS worden in de huidige situatie Microsoft Windows Server Domain Controllers ingezet. Deze zijn autoritatief voor de interne DNS-domeinen. Alle interne systemen maken hier gebruik van. Naamresolutieverzoeken voor externe domeinen worden doorgestuurd naar de DNS-infrastructuur van de internetprovider en Logius (Diginetwerk). Apparaten van (gast)gebruikers die verbinden via GovRoam en PublicRoam hebben geen toegang tot de interne DNS-servers en maken gebruik van Google DNS.

Voor automatische netwerkconfiguratie zijn verschillende systemen in gebruik:

- 2 DHCP-servers op basis van Microsoft Windows Server voor interne serverplatformen
- 2 DHCP-servers op basis van Microsoft Windows Server voor endpoints (bedraad).
- Lokale Fortinet FortiGate voor endpoints op draadloze netwerken.

Tijdsynchronisatie vindt plaats middels de ESXi-hosts als interne primaire tijdbron. Zij synchroniseren rechtstreeks met pool.ntp.org. De Microsoft Windows Server Domain Controllers fungeren als secundaire tijdsbron, die met de ESXi-hosts synchroniseren en zelf als gedistribueerde bron fungeren voor Windows Memberservers, Red Hat-servers, de Fortinet netwerkapparatuur en fat clients. Een aantal systemen synchroniseert rechtstreeks met pool.ntp.org, waaronder een PowerStorage opslagvoorziening en diverse IoT-apparaten.

Het is de bedoeling om deze voorzieningen in de toekomst te consolideren naar een integrale DDI-Dienst, die ofwel intern gerealiseerd, ofwel als Clouddienst afgenomen zal worden. In ieder geval dient deze Dienst onafhankelijk van en overkoepelend over alle omgevingen ingericht te worden.

5.3 Security monitoring

Huidige situatie Security Monitoring

De Aanbestedende dienst maakt gebruik van een externe leverancier voor Security Monitoring en Security Operations Center (SOC) dienstverlening. Deze leverancier verzorgt onder andere netwerkdetectie, security monitoring en incident response. De SOC-Dienst maakt gebruik van een cloudgebaseerd SIEM-platform voor het verzamelen, analyseren en correleren van security-gerelateerde loggegevens. De Aanbestedende dienst heeft de intentie om gedurende de looptijd van de overeenkomst gebruik te blijven maken van deze bestaande SOC-dienstverlening.

Dit betekent in ieder geval dat (eis):

- Inzicht moet zijn in netwerkverkeer voor monitoring door middel van technieken zoals (R)SPAN, netwerk TAPs, packet brokers, vSwitch-mirroring of vergelijkbare methoden.
- Het (inzicht in het) netwerkverkeer origineel, onbewerkt en ongefilterd dient te zijn.
- Het aanbieden van inzicht in netwerkverkeer via ERSPAN niet is toegestaan.
- De bestaande SOC-leverancier toegang dient te krijgen tot relevante componenten van de omgeving via een door de Aanbestedende dienst beheerde VPN-oplossing of via een site-to-site VPN-verbinding.

Detectie en logging

De Inschrijver dient te faciliteren dat loggegevens van IT-systemen, security devices, platformcomponenten en applicaties van en/of in gebruik bij de Aanbestedende dienst beschikbaar kunnen worden gesteld aan het SIEM-platform van de Aanbestedende dienst.

Dit houdt in ieder geval in dat (eis):

- Loginformatie in onbewerkte en ongefilterde vorm beschikbaar gesteld moet worden voor ingestie in het SIEM-platform dat bij de Aanbestedende dienst in gebruik is.
- Dit tevens geldt voor loggegevens afkomstig uit eventuele shared services die door de Inschrijver voor de Aanbestedende dienst worden geleverd.
- Technische koppelingen te realiseren moeten zijn voor het ontsluiten van logging vanuit onder andere infrastructuurcomponenten, netwerkvoorzieningen en platformdiensten.

Integraties en API-koppelingen

De Inschrijver dient te faciliteren dat geleverde (platform)Diensten, componenten en securityapparaten via API-koppelingen geïntegreerd kunnen worden met het SIEM-platform en andere securitytools van de Aanbestedende dienst (eis).

Security Response

De Aanbestedende dienst behoudt de mogelijkheid om via haar SOC geautomatiseerde response-acties uit te voeren op IT-systemen, security devices en applicaties binnen de afgenomen Diensten. Indien de Inschrijver shared services levert, dient het mogelijk te zijn dat dergelijke response-acties ook kunnen worden uitgevoerd op de fysieke of virtuele omgevingen die specifiek voor de Aanbestedende dienst zijn ingericht. De Inschrijver dient hiervoor de benodigde technische integraties en toegangsmechanismen te faciliteren (eis).

5.4 Health monitoring

De Dienst Health Monitoring maakt het mogelijk om de status te bewaken van de Diensten die vanuit de Managed Private Cloudomgeving geleverd worden, de componenten die die Diensten realiseren en de overige Diensten die bij de Aanbestedende dienst in gebruik zijn en de hieraan gerelateerde componenten. Dit om tijdig te kunnen reageren op (dreigende) incidenten en storingen, zodat actief beschikbaarheid en integriteit van voorzieningen geborgd kunnen worden vanuit beheer. De volgende items worden met behulp van de Dienst bewaakt:

- Processorgebruik (%)

- Geheugengebruik (%)
- Opslaggebruik (%)
- Uptime
- Starten, pauzeren en stoppen van services/jobs/processen
- Systeemconnectiviteit (poll/heartbeet)
- Applicatiefouten (te filteren op bronsysteem en ernst)
- Software-installaties (te filteren op bronsysteem)
- Configuratiewijzigingen (te filteren op bronsysteem)
- Netwerkconnectiviteit (topografie)
- Bandbreedtegebruik (te filteren op verbinding/backplane)
- Verkeerspatronen (te filteren op verbinding/backplane)
- Blokkeringsmeldingen verkeersfiltering (te filteren op bronsysteem en protocoltypen/poortnummers)
- Accountmodificatie (te filteren op accountsoort)
- Geldigheid certificaten (ten behoeve van encryptie)

De Dienst biedt de volgende functies:

- Ophalen van loggegevens bij bronsystemen die bewaakt worden.
- Het opvragen van metingen/meldingen van sensoren binnen bronsystemen die bewaakt worden.
- Analyse van dataverkeer op basis van applicatiekenmerken.
- Normaliseren, correleren en analyseren van monitoringgegevens.
- Gestructureerde opslag van genormaliseerde loggegevens.
- Opslagmedium voor onbewerkte loggegevens die verzameld zijn.
- Alarmering bij healthincidenten.
- Real-time rapportage van healthstatus.
- Periodieke (verzamel)rapportage van healthstatus en -gebeurtenissen.
- Bedienfunctie in de vorm van een centrale, grafische beheertool.

De Inschrijver dient voor de werking van de voorziening van Health Monitoring de benodigde technische integraties en toegangsmechanismen te faciliteren (eis). Uiteraard is de Inschrijver zelf eindverantwoordelijk voor het functioneren en de beschikbaarheid van de door de Inschrijver geleverde Diensten, inclusief alle geautomatiseerde voorzieningen die de Inschrijver hiervoor zelf in gebruik heeft en/of wenst te hebben. Dit betekent ook dat er geen afhankelijkheid mag bestaan van de door de Aanbestedende dienst gebruikte Health Monitoringdienst bij de Inschrijver.

5.5 Key & Certificate management

Huidige situatie Key & Certificate Management

De Aanbestedende dienst beschikt over een eigen Public Key Infrastructure (PKI) voor het beheer van cryptografische sleutels en certificaten. Deze PKI is gebaseerd op een self-signed certificaatautoriteit die draait op virtuele servers binnen de huidige virtuele infrastructuur.

De PKI-omgeving wordt gebruikt voor onder andere:

- Uitgifte en beheer van interne certificaten voor systemen en Diensten.
- Beheer van cryptografische sleutels.
- Ondersteuning van beveiligde communicatie binnen de infrastructuur.

Het beheer van deze PKI-omgeving wordt uitgevoerd door beheerders van de Aanbestedende dienst.

Naast de interne PKI maakt de Aanbestedende dienst gebruik van certificaten van externe certificaatautoriteiten (third-party/public certificates) voor publiek toegankelijke Diensten. Het beheer en de lifecycle van deze certificaten wordt eveneens door de Aanbestedende dienst uitgevoerd.

Uitgangspunten voor de nieuwe omgeving

De Aanbestedende dienst behoudt de regie over het beheer van cryptografische sleutels en certificaten. De Inschrijver dient de aangeboden infrastructuur- en platformdiensten zodanig in te richten dat het gebruik van de bestaande PKI-omgeving wordt ondersteund.

Dit houdt in ieder geval in dat (eis):

- De interne virtuele PKI-servers binnen de aangeboden infrastructuur kunnen worden gehost.
- Beheerders van de Aanbestedende dienst beheer kunnen uitvoeren op deze PKI-omgeving.
- Systemen en Diensten binnen de infrastructuur gebruik kunnen maken van certificaten die door de PKI van de Aanbestedende dienst zijn uitgegeven.
- Het gebruik van een door de Inschrijver beheerde PKI- of certificaatdienst niet verplicht wordt gesteld.

Toekomstige ontwikkeling

De huidige PKI-implementatie wordt door de Aanbestedende dienst beschouwd als functioneel maar niet optimaal ingericht. Gedurende de looptijd van de overeenkomst kan de Aanbestedende dienst besluiten deze omgeving te herontwerpen of te optimaliseren. De Inschrijver dient in dat kader, indien gevraagd, ondersteuning te kunnen bieden bij het verbeteren of moderniseren van de PKI-inrichting, waarbij de regie over het key- en certificaatbeheer bij de Aanbestedende dienst blijft (eis).

5.6 PAM

Huidige situatie Privileged Access Management

De Aanbestedende dienst maakt gebruik van een centrale Privileged Access Management (PAM) oplossing op basis van Delinea Secret Server in de vorm van een SaaS-Dienst.

Deze oplossing wordt gebruikt voor:

- Beheren en opslaan van privileged accounts en credentials (password vault).
- Gecontroleerd verstrekken van verhoogde rechten aan beheerders.
- Faciliteren van gecontroleerde remote toegang tot systemen.
- Verstrekken van tijdelijke toegang voor interne beheerders en externe partijen (derden).

Toegang tot systemen binnen de huidige datacenteromgeving vindt plaats via deze PAM-oplossing. Beheerders authenticeren zich via de PAM-oplossing waarna vanuit deze oplossing toegang wordt verkregen tot de virtuele machines die zij willen benaderen.

Uitgangspunten voor de nieuwe omgeving

De Aanbestedende dienst blijft gedurende de looptijd van de overeenkomst gebruik maken van de bestaande PAM-oplossing. De Inschrijver dient de dienstverlening zodanig in te richten dat integratie met deze PAM-oplossing mogelijk blijft.

Dit houdt in ieder geval in dat (eis):

- Beheer- en onderhoudstoegang tot virtuele machines via de PAM-oplossing van de Aanbestedende dienst moet kunnen plaatsvinden.
- De omgeving van de Inschrijver geen beperkingen oplegt aan het gebruik van de bestaande PAM-oplossing.

- Waar nodig technische integratie mogelijk is middels protocollen zoals RDP, SSH of andere gangbare beheerprotocollen.
- De PAM-oplossing gebruikt kan blijven worden voor het beheren en roteren van wachtwoorden van privileged accounts.
- Toegang op afstand voor externe partijen via de PAM-oplossing ondersteund blijft.

Verantwoordelijkheden

De Aanbestedende dienst blijft verantwoordelijk voor het beheer en de configuratie van de PAM-oplossing. De Inschrijver is verantwoordelijk voor het faciliteren van de benodigde technische integraties en toegangsvoorzieningen binnen de aangeboden infrastructuur- en platformdiensten (eis).

5.7 Bestandsuitwisseling

Huidige situatie Bestandsuitwisseling

De Aanbestedende dienst maakt gebruik van een externe third-party oplossing voor het uitwisselen van bestanden tussen systemen. Deze oplossing faciliteert zowel interne als externe bestandsuitwisseling, waaronder:

- Uitwisseling tussen interne systemen.
- Uitwisseling met externe organisaties.
- Uitwisseling met systemen in Cloudomgevingen.

In een beperkt aantal gevallen wordt voor deze uitwisseling gebruik gemaakt van een versleutelde site-to-site (S2S) VPN-verbinding.

De huidige oplossing wordt beheerd door de Aanbestedende dienst zelf.

Uitgangspunten voor de nieuwe omgeving

De Aanbestedende dienst blijft in eerste instantie gebruik maken van de bestaande oplossing voor bestandsuitwisseling en blijft verantwoordelijk voor het functioneel en technisch beheer daarvan.

De Inschrijver dient de aangeboden infrastructuur zodanig in te richten dat integratie met deze bestaande oplossing mogelijk blijft. Dit houdt in ieder geval in dat (eis):

- De bestandsuitwisselingsoplossing toegang heeft tot de aangeboden infrastructuur, zodat systemen hiermee bestanden kunnen uitwisselen.
- Netwerkconnectiviteit mogelijk is met de externe dienstverlener die deze oplossing levert.
- Waar nodig ondersteuning wordt geboden voor beveiliging van netwerkverbindingen, waaronder versleuteling van site-to-site VPN-verbindingen.

Toekomstige ontwikkeling

De huidige oplossing voor bestandsuitwisseling wordt door de Aanbestedende dienst als basaal functionerend, maar suboptimaal beschouwd. Gedurende de looptijd van de overeenkomst kan de Aanbestedende dienst besluiten deze functionaliteit te herzien of te optimaliseren.

De Inschrijver dient desgevraagd ondersteuning te kunnen bieden bij het verbeteren of moderniseren van de inrichting van de faciliteiten voor bestandsuitwisseling (eis). Dit kan onder meer betrekking hebben op:

- Het adviseren over verbeterde of gestandaardiseerde oplossingen voor veilige bestandsuitwisseling.
- Het faciliteren van integratie met interne systemen, externe partijen en Cloudomgevingen.
- Het ondersteunen bij migratie naar een toekomstbestendige oplossing.

De regie over de keuze en inrichting van de oplossing blijft hierbij bij de Aanbestedende dienst.