Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

KANS

Kader Acceptatie Nieuwe Systemen

April 2025

Versie	1.7.2
Datum	9 april 2025
Status	Definitief

Colofon

DG Organisatie Bedrijfsvoering Rijk
SSC-ICT

Koningskade 4 Den Haag

Contactpersoon CTO Office | Team Architectuur

Introductie

KANS (Kader Acceptatie Nieuwe Systemen) beschrijft de voorwaarden waaraan nieuwe en bestaande applicaties en technologische ontwikkelingen moeten voldoen om aangeboden te worden binnen de ICT omgeving en het verzorgingsgebied van SSC-ICT. Let wel, deze voorwaarden gelden ook bij vernieuwing of LCM van bestaande omgevingen.

KANS volgt de structuur van de SSC-ICT Producten en Diensten Catalogus 2025 (PDC 2025).

De voorwaarden zijn conform de PDC onderverdeeld in de volgende hoofdstukken:

1. Documentgegevens
2. Inleiding
3. Rijkswerkomgeving - Digitale werkomgeving
4. Rijkswerkomgeving - Persoonlijke devices
5. Locatie Gebonden Services
6. Applicaties
7. Hosting
8. Housing
9. Security
10. Supporting services

Aan de hand van de indeling in domeinen wordt dienstverlening beschreven (in de PDC 2025). in dit KANS document staan de actuele technische standaarden en aansluitvoorwaarden. Let op: De PDC 2025 is leidend in de beschrijving van diensten en de serviceniveaus.

Dit document geeft huidige stand van zaken weer en staat niet op zichzelf, de technische standaarden zijn voortdurend in ontwikkeling. Het document bevat informatie voor een klant of leverancier over de technische standaarden van dienstverlening van SSC-ICT. Voor een goede inschatting van de mogelijkheden binnen de bestaande SSC-ICT dienstverlening wordt een intakegesprek met de klant sterk aanbevolen.

De SSC-ICT-organisatie ziet het als haar verantwoordelijkheid om het beheer van de technische infrastructuur zo goed mogelijk te doen, maar stelt zich ook ten doel om deze zo efficiënt mogelijk in te richten en daarover een inzichtelijke kostprijs af te geven.

Voor het bereiken van efficiency – en daarmee een zo laag mogelijke kostprijs - probeert SSC-ICT-schaalvoordelen te benutten. Dat kan onder meer door (het beheer van) de technische infrastructuur te centraliseren, te standaardiseren en te consolideren. De beschreven standaarden zijn van toepassing tenzij er zwaarwegende argumenten om hier van af te wijken.

SSC-ICT zet zich in om bouwstenen te realiseren waarbij een optimale afweging wordt gemaakt tussen kosten, kwaliteit, veiligheid en generieke toepasbaarheid. Standaardisatie en hergebruik van generieke componenten mag er niet toe leiden dat een concessie wordt gedaan aan het (per systeem) vereiste beveiligingsniveau.

1 Documentgegevens

1.1 Revisies

Op dit document zijn de volgende revisies toegepast:

Versie	Status	Datum	Wijzigingen
1.3.1	Concept	15-12-2016	Opzet conform PDC
1.3.2	Concept	15-12-2016	Versie voor goedkeuring AB
1.4	Definitief	2-12-2020	Versie voor publicatie SSC-ICT
1.4.1	Concept	23-02-2022	Versie voor commentaar
1.4.2	Concept	15-03-2022	Versie voor goedkeuring AB Verwerkt commentaar FredvL, Rein Hennen, FredvdK en Paul Slats.
1.4.3	Concept	23-03-2022	Versie voor goedkeuring AB
1.5	Definitief		Versie voor publicatie SCC-ICT
1.5.1	Concept	12-12-2022	Versie met consolidatie van commentaren Rein Hennen, Onno Hoogeveen en Orhan Reyhan.
1.5.2	Concept	12-12-2022	Wijzigingen doorgevoerd
1.5.3	Concept	08-02-2023	Wijzigingen H5 en H7 besproken met domein architecten en doorgevoerd
1.6	Definitief	15-02-2023	Versie 1.6 vastgesteld in Architectuurboard
1.7	Definitief	12-03-2025	Update 1e kwartaal 2025 vastgesteld in Architectuurboard
1.7.1	Definitief	12-03-2025	Aanpassing jaartal par. 3.1 (2025 i.p.v. 2024) + toevoeging A13 in par. 3.3
1.7.2	Concept	09-04-2025	Aanscherping A13 (pagina 11)

1.2 Goedkeuring

Dit document behoeft de volgende goedkeuringen:

Versie	Datum goedkeuring	Naam	Functie	Paraaf
1.0	07-03-2018	Helmer de Vries	Architectuurboard	
1.1	26-09-2018	Helmer de Vries	Architectuurboard	
1.2	27-2-2019	Helmer de Vries	Architectuurboard	
1.3	27-11-2019	Helmer de Vries	Architectuurboard	
1.4	02-12-2020	Helmer de Vries	Architectuurboard	
1.5	23-03-2022	Helmer de Vries	Architectuurboard	
1.6	15-02-2023	Helmer de Vries	Architectuurboard	
1.7	12-03-2025	Helmer de Vries	Architectuurboard	

1.3 Distributie

Dit document is verstuurd aan:

Versie	Datum verzending	Naam	Functie
1.0	14-03-2018	Joost van Duinen	Publicatie
1.2	27-2-2019	Joost van Duinen	Publicatie
1.3	08-10-2019	Joost van Duinen	Publicatie
1.4	2-12-2020	Joost van Duinen	Publicatie
1.5	maart-2022	Joost van Duinen	Publicatie
1.6	15-02-2023	Joost van Duinen	Publicatie
1.6.3	November 2023	Joost van Duinen	Concept
1.7	12 Maart 2025	Roman Sarghandoy	Publicatie
1.7.1	13 Maart 2025	Roman Sarghandoy	Publicatie
1.7.2	xx April 2025	Roman Sarghandoy	Publicatie

2 Inleiding

2.1 Doel van het document

Deze specificatie is opgesteld als kader beschrijft de technische- en aansluitvoorwaarden waar applicaties en technische componenten aan moeten voldoen om aangeboden of gebruikt te kunnen worden binnen de ICT omgeving en het verzorgingsgebied van SSC-ICT.

Afnemers van SSC-ICT diensten dienen dit als kader te hanteren.

Onder afnemers worden verstaan: Verzorgingsgebied (Klanten), Leveranciers van software en hardware, Projecten en Afdelingen van SSC-ICT die onderling diensten afnemen.

Het document heeft onderstaande doelen:

- Informatiebron voor (potentiële) afnemers over de inrichting van de dienstverlening en de gebruikte technische services en standaarden.
- Informatiebron voor ontwikkelaars van applicaties over de gebruikte technische services, technische standaarden en beveiligingsrichtlijnen.
- Kader voor kwaliteitscontrole tijdens en na oplevering aan de beheerorganisatie.
- Toelichten en scherpstellen van relevante begrippen.

2.2 Opbouw van dit document

SSC-ICT was de afgelopen jaren ingericht in vier domeinen. De structuur van dit document volgt die indeling per domein. De organisatie die de genoemde diensten levert bestaat uit de huidige Business Units, die indeling kan als gevolg van de transitie nog wijzigen.

De business services van SSC-ICT zijn onderverdeeld in de huidige vier domeinen: Persoonlijke Werkomgeving, Locatiegeboden diensten, Housing en Hosting en Applicaties.

Onder *Rijkswerkomgeving – Digitale werkomgeving* (Hoofdstuk 3) valt de digitale werkomgeving. Hier worden de aansluitvoorwaarden beschreven die van toepassing zijn op de digitale werkomgeving.

Onder *Rijkswerkomgeving -Persoonlijke devices* (Hoofdstuk 4) vallen de persoonlijke devices, Steeds meer ambtenaren krijgen persoonlijke devices, zoals een smartphone of een laptop, waarmee zij tijd-, plaats- en apparaat onafhankelijk kunnen werken. Deze diensten maken deel uit van het domein Rijkswerkomgeving en zijn toe te wijzen aan individuele ambtenaren.

Locatie gebonden services (Hoofdstuk 5) maakt het binnen de Rijkskantoren mogelijk dat er steeds flexibeler wordt gewerkt en het aantal vaste werkplekken wordt verminderd. Er is dan ook steeds minder vaak een duidelijk aanwijsbare gebruiker van een aantal ICT-faciliteiten. Denk hierbij aan faciliteiten als wifi en printers. Alle services die verbonden zijn met een gebouw, zijn opgenomen in het domein Locatie gebonden services.

Het domein *Applicaties* (Hoofdstuk 6) heeft zich gespecialiseerd in het applicatiebeheer van de verschillende applicaties om de afnemers nog beter te kunnen helpen.
De vier servicedomeinen bevatten verschillende ondersteunende diensten die van belang zijn om de services uit de verschillenede domein veilig te kunnen leveren vanuit opgelegde kaders. De kosten voor deze ondersteunende processen zijn niet direct aan een service toe te rekenen en worden over alle diensten omgeslagen.

Binnen *Hosting* (Hoofdstuk 7) worden alle technische diensten zoals servercapaciteit, databases, opslag en de benodigde netwerkkoppelingen geleverd die ervoor zorgen dat alle applicaties die binnen het verzorgingsgebied gebruikt worden.

Binnen *Housing* (Hoofdstuk 8) worden alle technische aansluitvoorwaarden voor de levering van vloer en kastruimte in het datacenter en de benodigde netwerkkoppelingen beschreven

Het domein Security (Hoofdstuk 9) beschrijft de standaarden en richtlijnen die gehanteerd worden bij het proces van informatiebeveiliging en security dienstverlening.

Hoofdstuk 10 *Supporting services* legt de relatie naar de ondersteunde diensten in de PDC.

2.3 Relatie met andere documenten

Voor het opstellen van dit document zijn onderstaande bronnen gebruikt.

1. **SSC-ICT Producten en Diensten Catalogus 2025:** De Producten- & Diensten Catalogus (PDC) is een beschrijving van de dienstverlening waarmee SSC-ICT haar klanten in 2025 van dienst zal zijn.
2. **Architectuur principes en bouwblokken:** De architectuur van SSC-ICT's dienstverlening is vastgelegd in de Architectuur Wiki. De Wiki is opgebouwd volgens de TOGAF methode waar stapsgewijs bouwblokken worden afgeleid uit basisprincipes die door het DMT zijn vastgesteld.
3. **High Level Designs van Bouwblokken:** Deze documenten geven aanvullende informatie over de gerealiseerde infrastructuur die van belang is voor het maken van de juiste keuzes. Deze zijn gekoppeld aan de architectuur bouwblokken in de Architectuur Wiki[1].
4. **Beveiliging – BIO**: Het technisch normenkader met betrekking tot de beveiliging is vastgelegd in de BIO wat staat voor Baseline Informatiebeveiliging Overheid en is gebaseerd op ISO27001/27002. De BIO is per 1 januari 2019 verplicht en vervangt voor de gemeenten, waterschappen, provincies en het Rijk respectievelijk de BIG, BIWA, IBI en de BIR (Baseline Informatiebeveiliging Rijksdienst).

[1] Deze wikipagina's zijn bereikbaar via de DWR werkomgeving met voldoende rechten op de architectuur Wiki. (i.e. de rol van technisch of solution architect)

3 Rijkswerkomgeving (RWO) - Digitale Werkomgeving (DWR)

SSC-ICT levert als dienstverlener aan gebruikers werkplekfunctionaliteit, de Rijkswerkomgeving (RWO) DWR, Digitale Werkomgeving Rijk - in zijn rol als ICT-dienstverlener voor gebruikers (IDV-G). De werkplek wordt verder aangeduid als werkomgeving omdat de werkomgeving ontkoppeld is van zijn fysieke component. De werkplek duidt de combinatie bureau, scherm en het toegangsdevice aan in een rijkskantoor, een persoonlijk device zoals een managed laptop of een privé device (BYOD). Als we spreken over de aangeboden functionaliteit, dan spreken we over de werkomgeving. De huidige versie van DWR, DWR Next, is een 'klassieke' werkomgeving die met on-premises middelen wordt beheerd en beveiligd en waarbij gebruikers tot hun applicaties en data toegang krijgen via een VPN-verbinding. DWR Next is in de basis geschikt voor gebruik t/m. BBN2, Dep-V.

De details over de dienstverlening als leverancier van de werkomgeving staan omschreven in de Servicecatalogus SSC-ICT. De hieronder opgenomen specificaties dienen als referentie voor applicaties die een relatie hebben met de werkomgeving.

SSC-ICT streeft naar verbetering van de digitale toegankelijkheid van Business Services, die geboden worden aan eindgebruikers. Daarom zijn in de diverse hoofdstukken van dit document ook verwijzingen opgenomen naar regelgeving en richtlijnen voor digitale toegankelijkheid

3.1 Relatie met PDC

Voor de dienstverlening geldt in beginsel dat al hetgeen is beschreven in de PDC 2025 Hoofdstuk 3 "Rijkswerkomgeving- Digitale Werkomgeving" van toepassing is.

DWR Next is echter doorontwikkeld in het kader van lifecycle management én vernieuwing tot DWR2.0. De vervanging van DWR Next door DWR 2.0 zal naar verwachting vanaf medio 2025 gefaseerd voor de afnemers plaats gaan vinden; DWR Next is dan vanaf enig moment niet meer afneembaar.

Voor de aansluitvoorwaarden van DWR 2.0 zal te zijner tijd in 2025 een update van KANS plaatsvinden, maar in het kader van de afhandeling van bijvoorbeeld changes kunnen aanvullende voorwaarden worden gesteld. E.e.a. ook om bij de afnemers migratie issues naar DWR 2.0 te voorkomen.

3.2 Aansluitvoorwaarden Rijkswerkomgeving

De kern voor het kunnen ontsluiten van applicaties op de werkomgeving is het in juli 2022 vastgestelde rijksbrede IDWOR kader 8 – Werkplekonafhankelijkheid van klantapplicaties:

- Buiten een 'moderne browser' mag er geen andere afhankelijkheid van de werkplek zijn, met andere woorden de updates van de werkplek mogen geen invloed hebben op de werking van de applicatie. Dit is, volledigheidshalve, van toepassing voor alle koppelvlakken/koppelingen en integraties met de werkomgeving (plugins, extensions, middleware en frameworks) zoals Flash, Silverlight, Java, DotNet, maar ook koppelingen met Outlook, Excel of Word die een werkplekcomponent nodig hebben en dus potentieel problemen kunnen veroorzaken;
- Webapplicaties functioneren onafhankelijk van de gekozen browser met ondersteuning voor de in de markt 'gangbare browsers', zoals: Chrome, Edge, Safari en Firefox. Hierbij mag er ook geen afhankelijkheid zijn met een specifieke versie van een browser. De applicatie moet met iedere recente versie van een moderne browser overweg kunnen. Zowel op een Windows, Mac of Linux-device, alsook op een mobile device (smartphone

of tablet). Moderne browsers worden in een hoog tempo doorontwikkeld: ook daarop moet de webapplicatie permanent worden bijgehouden om te blijven voldoen aan deze laatste standaarden;
- Een applicatie heeft geen harde afhankelijkheid met andere applicaties in- of op het device, koppelingen met andere applicatie(componenten) dient te geschieden op basis van (open) standaarden en moeten plaatsvinden vanuit het backend op basis van gedefinieerde API's. Een voorbeeld ter verduidelijking: de Exchange-koppeling niet realiseren met een plugin voor Outlook op de werkplek, maar via EWS met de Exchangeserver;
- Applicatieverkeer dient versleuteld te zijn conform de richtlijnen van het NCSC voor TLS (https://www.ncsc.nl/documenten);
- Er moet verplicht gebruik worden gemaakt van relevante (open) standaarden, gemakshalve wordt verwezen naar de lijst met open standaarden van het Forum Standaardisatie (https://www.forumstandaardisatie.nl/open-standaarden) en het gebruik van de webstandaarden die zijn gedefinieerd door het W3C (https://www.w3.org/standards/) en de IETF (https://www.ietf.org/standards/) wordt sterk aanbevolen;
- Webapplicaties dienen gebruik te maken van authenticatie/ autorisatieprotocollen OpenID Connect (OIDC), Oauth en/of SAML in de versies zoals te vinden op de site van het Forum Standaardisatie;
- Webapplicaties die benaderbaar zijn voor andere organisaties binnen de rijkdienst dienen gebruik te maken van de SSOn-federatie. Dat wil zeggen aangesloten te zijn op SSOn of op een daaraan gelieerde en verbonden departementale authenticatie(SSO)voorziening binnen de SSOn-federatie. Zie verder de SSOn kaders;
- Applicaties binnen één cloud SaaS-ecosysteem mogen gebruikmaken van B2B concepten binnen dat SaaS-ecosysteem.

CIO Rijk is verantwoordelijk voor dit kader en publiceert een actuele online lijst met (generieke) uitzonderingen.

Als een applicatie niet op de lijst met generieke uitzonderingen staat en van de afspraken in dit kader moet worden afgeweken, dient – in samenwerking met SSC-ICT – vooraf overleg met CIO Rijk te worden gevoerd (*Comply or Explain*). Contact met CIO Rijk over IDWOR kader 8 kan via: postbusidwor@rijksoverheid.nl

Afwijkingen zijn daarbij vanuit de optiek van SSC-ICT (tijdelijk) mogelijk indien:

- een bepaalde functionaliteit een Must is in MoSCoW-termen;
- de applicatie / het extra component de enige manier is om deze functionaliteit te leveren en er ook geen acceptabel te achten workaround voor handen is;
- de applicatie / het extra component van een gerenommeerde leverancier afkomstig is (denk hier met name aan het kunnen leveren van adequate support als een standaard component van de werkomgeving niet kan worden voorzien van een update of upgrade vanwege de applicatie/het extra component);
- de applicatie / het extra component is ondertekend door een geldig certificaat (code signing) van een vertrouwde certificeringsinstantie.

In voorkomende gevallen dienen bij toegestane afwijkingen nadere formele afspraken met de klant/afnemer gemaakt te worden over de applicatie als maatwerkvoorziening, denk bijvoorbeeld aan het toch updaten van een standaard component van de werkomgeving waardoor de applicatie / het extra component niet meer werkt, totdat (via de klant/afnemer) een werkende update van de applicatie / het extra component in productie kan worden genomen.

Niet alle applicaties vragen om dienstverlening op het gebied van hosting. Indien er enkel sprake is van software die op een desktop kan worden geïnstalleerd, dus zonder backend en

databases, moet een applicatie voor de ontsluiting via de digitale werkomgeving gepackaged worden. Om deze dienst te kunnen leveren is de eis die aan een applicatie vanuit SSC-ICT wordt gesteld, eenvoudig weg dat de applicatie compatibel is met de gehanteerde Citrix versie, de distributie-methodiek en de Microsoft Windows-werkomgeving die wordt geleverd. In tegenstelling tot de hosting-dienstverlening, waarbij meerdere versies van besturingssystemen e.d. kunnen worden ondersteund is hier de eis veel meer eendimensionaal.

3.3 Aanvullende technische aansluitvoorwaarden Rijkswerkomgeving

A - Algemeen	
A1	Een applicatie heeft minimale rechten nodig op de werkomgeving om te kunnen functioneren voor de eindgebruiker, verhoogde of systeemrechten (administrator) rechten zijn derhalve niet toegestaan.
A2	Applicaties welke geïnstalleerd worden komen altijd in "C:\Program Files" of "C:\Program Files (x86)". Verhoogde systeemrechten zijn niet toegestaan op deze locatie.
A3	Een applicatie heeft geen functionaliteit op het gebied van Telemetry, Customer Experience Improvement Programs, Diagnostics en dergelijke of deze kan aantoonbaar worden uitgeschakeld in de configuratie van de applicatie. Uitzonderingen hierop moeten worden goedgekeurd met uitgevoerde DPIA en zo nodig een IB risico-analyse.
A4	Tijdelijke bestanden die nodig zijn voor het functioneren van een applicatie (logging, cache etc) worden in bekende standaard folders weggeschreven (%Variabele paden%). Applicaties moeten voldoen aan de Microsoft ontwikkelstandaarden. (Zie https://docs.microsoft.com/en-us/windows/win32/win_cert/certification-requirements-for-windows-desktop-apps).
A5	Licenties zijn niet gebonden aan specifieke machines, activatie van een applicatie wordt op basis van concurrent aantal gebruikers of specifiek toegekend aan de gebruiker. Er wordt geen gebruik gemaakt van voorzieningen zoals dongles om de applicatie te activeren of te laten functioneren.
A6	Applicatie-instellingen zijn op gebruikersniveau in te regelen, applicatie-instellingen zijn niet actief wanneer de ingelogde gebruiker geen rechten heeft op de betreffende applicatie.
A7	Wanneer een applicatie een verbinding nodig heeft naar het internet moet het internetverkeer via een proxy kunnen worden afgehandeld. Het gebruik van extra VPN-clients vanaf een werkomgeving om een externe omgeving te benaderen is niet toegestaan; dergelijke voorzieningen moeten via een site-to-site-voorziening worden ingevuld.
A8	Authenticatie gebeurt op basis van de huidige ingelogde gebruikers credentials op basis van federatieve identiteiten. Voor nieuwe toepassingen is authenticatie via AD-Trust niet toegestaan. De bestaande AD-Trusts worden zoveel mogelijk verwijderd en vervangen door federatieve koppelvlakken op basis van SAML en OIDC. Nieuwe AD-Trusts worden niet meer gelegd.
A9	Het benaderen van een applicatieserver en/of bronnen gebeurt altijd op basis DNS met een verwijzing naar een FQDN, gebruik van harde verwijzingen naar IP-adressen zijn niet toegestaan.
A10	Koppeling met of gebruik van een persoonlijk Microsoft account is niet toegestaan.
A11	Universal Windows Platform (UWP) Apps worden aangeboden via Ivanti of SCCM en kunnen niet rechtstreek vanaf de Publieke Microsoft Store geïnstalleerd worden.
A12	Functionele cloud services zoals bv. Opslag in de cloud kunnen worden uitgezet of dienen de eindgebruiker dusdanig duidelijk te zijn dat er buiten het vertrouwde domein data wordt gedeeld dat van een bewuste actie van de eindgebruiker kan worden gesproken.

A13	Wachtwoorden mogen niet onversleuteld in de configuratie van applicaties voorkomen. Basic authenticatie, waarbij credentials in clear text of via eenvoudige encoding (zoals Base64) worden verzonden is niet toegestaan voor enige toepassing, dienst of systeem.
A14	Voor netwerkauthenticatie wordt de IEEE 802.1X standaard gebruikt. Hiervoor worden op de managed werkomgeving devices 802.1X device certificaten geïnstalleerd.
B - Life Cycle Management en Ondersteuning	
B1	Life Cycle Management van Basis en Basis+ applicaties is de verantwoordelijkheid van SSC-ICT. Life Cycle Management van klant-specifieke applicaties is de verantwoordelijkheid van de applicatie eigenaar. Applicaties zijn te allen tijde ondersteund door een leverancier. Patch management (security fixes) wordt uitgevoerd onder goedkeuring van SSC-ICT.
B2	Applicatie ondersteuning voor een volgende release in het General Availability Channel voor Windows 10 Enterprise moet binnen maximaal 90 dagen na RTM worden geleverd door leverancier / ontwikkelaar van de applicatie. Zie paragraaf 3.3.1 voor ondersteunde Windows versies.
C - Distributie van applicatie	
C1	Voor de distributie van applicaties wordt het principe 'Virtueel tenzij' gehanteerd. Standaard worden Applicaties door middel van virtualisatietechnieken op de werkomgeving aangeboden: Microsoft Application Virtualization (App-V).
C2	Applicaties die geïnstalleerd worden op de werkomgeving kunnen niet automatisch bijgewerkt worden. Het gebruik van Auto-update is niet toegestaan.
C3	Mobiele applicaties die binnen de beveiligde container moeten functioneren moeten worden ontwikkeld en onderhouden met de door BlackBerry beschikbaar gestelde SDK's.
C4	Mobiele apps mogen alleen gedistribueerd worden als deze ondertekend zijn met een vertrouwd certificaat.
D - Webbrowser	
D1	Op de werkomgeving wordt Microsoft Edge als primaire browser en Mozilla Firefox ESR als extra browser aangeboden. Hierbij is Edge de standaard browser; Google Chrome kan alleen op speciaal verzoek via een NSK/RfC aangevraagd worden.
D2	Het gebruik van browser add-ons, plugins, extensions en dergelijke is in beginsel niet toegestaan op basis van IDWOR kader 8. Indien als toegestane exceptie een klantapplicatie toch een integratie met een browser moet hebben moet deze, zoals in het IDWOR Kader is aangegeven, zijn ondertekend door een geldig certificaat (Code Signing) van een vertrouwde certificeringsinstantie. Hierbij is de klant/aanvrager zelf verantwoordelijk voor het aanleveren en het beheer over de geldigheid van het certificaat.
E - Office integratie	
E1	Het gebruik van Office add-ons, add-ins, plugins, extensions, VBA, macro's en dergelijke is in beginsel niet toegestaan op basis van IDWOR kader 8. Indien als toegestane exceptie een applicatie toch een integratie met Office componenten moet hebben moet deze, zoals aangegeven in H3.1 van het IDWOR Kader, zijn ondertekend door een geldig certificaat (Code Signing) van een vertrouwde certificeringsinstantie. Hierbij is de klant/aanvrager zelf verantwoordelijk voor het aanleveren en het beheer over de geldigheid van het certificaat.
E2	Office 365 ProPlus wordt uitsluitend aangeboden in een 64-bits mode. Dit betekent dat op basis van IDWOR kader 8 toegestane (zie H3.1) integraties in Office zoals Add-ins ook beschikbaar moeten zijn in een 64-bits versie aangezien 32-bits versies niet compatibel zijn.
E3	Gebruikte certificaten zijn ondertekend door een vertrouwde certificeringsinstantie bij voorkeur een PKI-O certificaat. Voor het Windows platform moet de Root CA zijn

	opgenomen in de 'Microsoft Trusted Root Certificate Program'. Zie voor een actuele lijst van root CA's: https://aka.ms/trustcertpartners.
E4	Het berichten platform is primair toegankelijk ten behoeve van Office functionaliteiten ("Outlook voor de eindgebruikers") en secundair, binnen de grenzen van deze functionaliteiten, voor het applicatielandschap. Voor het applicatielandschap zijn drie interfaces in gebruik: - EWS (secure Exchange Web Services), poort 443. Ondersteuning voor de EWS API wordt stapsgewijs door Microsoft uitgefaseerd. Gebruik van EWS is daarom alleen in overleg met SSC-ICT mogelijk en hooguit voor 'native' commando's, niet voor *notification subscriptions*. Voor Exchange Online (Microsoft 365) zal in de toekomst worden overgegaan naar Microsoft Graph. - SMTP (Simple Mail Transfer Protocol), poort 25 - IMAP (Internet Message Access Protocol), poort 993. IMAP wordt in beginsel alleen toegestaan voor Linux applicaties. Alle bewerkingen via deze interfaces dienen te voldoen aan het bewaarbeleid voor e-mail van de rijksoverheid. Belangrijkste eisen hierbij zijn dat van ontvangen en verzonden berichten de inhoud of de metadata niet aangepast mogen worden. Dat mail eventueel wel uitgezonderd kan worden van archivering of binnen 10 weken verwijderd kan worden. Voor applicatie systemen zal dit in afstemming met de departementale zorgdrager voor e-mail archivering ingeregeld moeten worden.
E5	Klantspecifieke Teams Apps vallen onder IDWOR kader 8 en worden derhalve gezien als koppeling/integratie met de werkomgeving. Afwijkingen voor een exceptie van CIO Rijk zijn vanuit het perspectief van SSC-ICT alleen mogelijk onder de volgende voorwaarden: - De Team App voldoet aan de voorwaarden van het Microsoft 365 App Compliance Program; - De Teams App mag geen gebruik maken van Office 365 Connectors, maar moet van Power Automate of Microsoft Graph.
F -Overig	
F1	Aparte drivers voor bijvoorbeeld het aansluiten van additionele randapparatuur moeten voldoen aan de Windows Hardware Quality Labs (WHQL)-eisen van Microsoft.
F2	Wanneer op basis van een toegestane exceptie voor IDWOR kader 8 (zie H3.1) gebruik wordt gemaakt van frameworks (bijvoorbeeld .Net en C++) dient de applicatie actief onderhouden te worden om te blijven werken met (security-)updates en upgrades van het onderliggende framework die op de werkomgeving worden doorgevoerd.
G - Printing	
G1	Follow-me printing van Xerox in combinatie met Equitrack is de standaard.
G2	Gebruik van Rijkspas of Pin is verplicht voor het ophalen van printopdrachten. Printen kan alleen vanuit de gebruiker worden geïnitieerd. Direct printing is niet toegestaan.
G3	Anoniem printen (direct vanuit een applicatie) is niet toegestaan.

H – Externe Mail Relay	
De Externe Mail Relay (EMR) stelt 3e partijen in staat om mail te versturen namens de ministeries.	
H1	De EMR is compliant aan de pas toe of leg uit lijst van het forum standaardisatie. Op deze mail zal het beveiligingsbeleid van de overheid worden toegepast en zal op virussen en malicious code worden onderzocht

H2	De EMR koppeling is alleen beschikbaar voor leveranciers van maildiensten en Cloud maildiensten die in opdracht werken van een ministerie.
H3	Voor het gebruik van de EMR worden 2 varianten aangeboden: **1.** Een verbinding naar emr.ssonet.nl op poort 25 en we spreken af welk e-mail adres gebruikt wordt, en in de e-mail onderwater dien je een shared secret te plaatsen wat wij kunnen herkennen. **2.** Men verbind naar emr.ssonet.nl op poort 587 en men gebruikt een door SSC-ICT verstrekt username en wachtwoord

3.4 Relevante Technische standaarden voor de Werkomgeving

3.4.1 Algemene ondersteunde standaarden

Onderstaande lijst is deels gebaseerd op de lijst van open standaarden welke wordt gepubliceerd door het Forum Standaardisatie, zie voor overige standaarden: https://www.forumstandaardisatie.nl/open-standaarden.

Type	Versie	Status	Omschrijving
Certificaten	Minimaal SHA-2	Productie	De ondersteuning voor SHA-1 in o.a. Microsoft producten is niet meer aanwezig.
Block Cipher	AES		Sleutellengte AES-128 (advies) AES-192 of AES-256 (voor zware toepassingen)
Hash Functie	SHA-256 Bitlengte		Hash functie compatibel met TLS 1.2 en TLS 1.3 SHA-384 en SHA-512 zijn alternatieven
Protocol (TLS)	Minimaal TLS 1.2 Voorkeur is TLS 1.3	Productie	https://www.forumstandaardisatie.nl/standaard/tls
Protocol (SMB)	Minimaal SMB v3	Productie	Oudere SMB versies (met name SMB v1) worden niet ondersteund en zijn uitgeschakeld op het Windows besturingssysteem.

3.4.2 Werkomgeving besturingssysteem

OS	Type	Versie	Status	Toelichting
Microsoft	Windows 10, 64 bits – Enterprise SKU	N(-1), nu 22H2	Productie	Windows 10 wordt End of Life (EoL) en wordt vervangen door Windows 11 (DWR 2.0)
Apple	iOS (BYOD & COPE) iPadOS (BYOD & COPE)	N(-1), nu v18	Productie	Geplande release door Apple is jaarlijks in september, ondersteuning door SSC-ICT voor Q4 later dat jaar. Installatie van updates door eindgebruikers. Lite managed Werkomgeving.

Android	BYOD & COPE	N(-1), nu v15	Productie	Jaarlijks update van OS, ondersteuning door SSC-ICT later dat jaar. Installatie van updates door eindgebruikers. Lite managed Werkomgeving.

3.4.3 Digitale Werkomgeving Online

Platform	TS	Versie	Status	Toelichting
Windows	Persistente Desktop	Windows 10 & 11 GAC	Productie	Werkomgeving waar veranderingen aan het applicatie landschap bewaard blijven. (Managed Laptop, Special, O&T-werkomgeving / Persistent VDI)
Windows	Niet-Persistente Desktop	Windows 10 & 11 GAC	Productie	Werkomgeving die bij iedere herstart weer gereset wordt naar de default waarden. (Non persistent VDI)

3.4.4 Digitale Werkomgeving Light

Voor ontwikkeling van interne beveiligde apps voor de mobiele werkomgeving moet gebruik worden gemaakt van BlackBerry Dynamics.

Service	TS	Versie	Status	Toelichting
Mobile Device Management	BlackBerry Unified Endpoint Management (UEM)	N-1, nu 12.x	Productie	Endpoint Management (MDM en MAM) van smartphones en tablets (Android en iOS)

3.4.5 Applicatie Distributie DWO

Voor de distributie van applicaties wordt het principe 'Virtueel tenzij' gehanteerd. Standaard worden Applicaties door middel van virtualisatie technieken op de werkomgeving aangeboden (Microsoft Application Virtualization, App-V).

Platform	TS	Versie	Status	Toelichting
Windows	Microsoft AppV Via Ivanti Workspace Control	5.x	Productie	Gevirtualiseerde software die on demand gestreamd wordt naar de werkomgeving
Windows	Microsoft MSI-X via Microsoft Intune		Gepland	Gevirtualiseerde software die middels de techniek application layering, streaming install of middels een lokale installatie gedistribueerd kan worden.
Windows	MSI/Unattended – Win32 Via Microsoft SCCM		Productie	Software die in het image van Windows 10 of Windows server 2016 opgenomen wordt of gedistribueerd wordt naar de persistent desktop.

Windows	Universal Windows Platform (UWP) App's		Nog geen Productie	Geen ondersteuning
Windows 10 GAC Enterprise	Citrix Published App's		Productie	Legacy applicaties worden aangeboden als een Published app.
iOS & Android	SSC-ICT Appstore (Public en custom apps)		Productie	Specifieke bedrijfsapplicaties worden aangeboden middels BlackBerry UEM. Voor publieke apps wordt een verwijzing aangeboden naar publieke store.

3.4.6 Basisplus Applicaties

Type	TS	Versie	Status	Toelichting
Applicatie	Basis	Zie PDC	Productie	Software die voor alle gebruikers beschikbaar zijn gesteld en door SSC-ICT actueel worden gehouden.
Applicatie	Basis Plus	Zie PDC	Productie	Software die door diverse ministeries te gebruiken zijn waarbij de kosten voor licenties, packaging, distributie en beheer per gebruiker doorberekend wordt en door SSC-ICT actueel worden gehouden.
Applicatie	Specifiek (Maatwerk)	Zie PDC	Productie	Software die alleen door een ministerie gebruikt wordt, of door een specifieke gebruikersgroep binnen dat ministerie.

4 Rijkswerkomgeving – Persoonlijke Devices

4.1 Relatie met PDC

Voor de dienstverlening geldt dat al hetgeen is beschreven in de PDC 2025 Hoofdstuk 4 "Rijkswerkomgeving- Persoonlijke Devices" van toepassing is.

5 Locatie Gebonden Services (LGS) Business Services

Voor de dienstverlening in Rijkskantoren geldt dat de meest recente RijksPDC Gebouwgebonden ICT diensten (https://www.samenwerkruimten.nl/teamsites/idwor/Gedeelde%20%20documenten/Forms/AllItems.aspx) leidend is. Tevens kunnen er, behoudens de door LGS en Facilitaire dienstverlening geleverde diensten, geen applicaties landen in een kantooromgeving. Applicaties landen in het datacenter. Op de (Rijks)kantoorlocaties zijn geen technische ruimtes meer die applicatie-hosting (aan anderen dan de voor de het Pand verantwoordelijke IT dienstverlener (de IDV-P) kunnen bieden, noch personeel om die te onderhouden).

5.1 Relatie met PDC

Voor de dienstverlening geldt dat al hetgeen is beschreven in de PDC 2025 Hoofdstuk 5 "Locatie Gebonden Services" van toepassing is.

5.2 Aansluitvoorwaarden locatie gebonden services

5.2.1 Kiosk pc

Kader Kiosk pc	
1	De kiosk pc wordt uit gefaseerd en is niet meer te bestellen.

5.2.2 Telefonie

Kader Session Border Controller	
1	SSC-ICT biedt de klanten de mogelijkheid om een eigen telefooncentrale te koppelen aan het interne SBC-landschap. SSC-ICT maakt gebruik van een S**ession** B**order** C**ontroller (SBC) van AudioCodes** welke door middel van meerdere redundante SIP-verbindingen zijn *gekoppeld met het netwerk van een externe telecomprovider.* Deze koppeling tussen de SBC van SSC-ICT en het netwerk van **de externe telecomprovider**, en daarmee met het **public switched telephone network (PSTN)**, heeft een verhoogde beschikbaarheid van 99,999%. De SBC routeert **uitsluitend** op basis van internationaal E**.**164 formaat**.** **De SBC routeert alleen de secure versie van SIP en RTP (SSIP / SRTP).**
2	SBC is ingericht conform zero trust (mutual TLS). De versleuteling gebeurt op basis van (minimaal) TLS versie 1.2.
3	Externe telefonie providers worden op netwerkniveau gekoppeld op basis van (E)BGP peering. Dit maakt het mogelijk om verkeer te routeren van telefonie provider van/naar het SSC-ICT datacenter netwerk.
Kader fysieke telefoontoestellen in kantoren	
1	In kantoren worden geen fysieke toestellen geplaatst op werkplekken. Er zijn enkele uitzonderingen, zoals recepties en beveiliging.
2	Uitzonderingen worden bepaald door CIO-Rijk. Door het plaatsen van een fysieke telefoon, zorgt ervoor dat de werkplek niet gebruikt kan worden door anderen. Deze zal dan uit de te boeken werkplek mix gehaald moeten worden.
3	Fysieke telefoontoestellen zijn geclassificeerd als onvertrouwd apparaat. Het plaatsen van een fysiek toestel vereist een internetverbinding die gebruikt wordt om te communiceren met de telefoniecentrale van SSC-ICT in het OverheidsDataCenter.

4	Fysieke telefoontoestellen en andere unified communicatie dienstverleningen kunnen alleen afgenomen worden als ook de werkomgeving afgenomen wordt.

5.2.3 Netwerkauthenticatie

Kader Netwerkauthenticatie	
1	Voor netwerkauthenticatie – toegang tot het netwerk - wordt de IEEE802.1X standaard gebruikt op basis van (802.1x) device certificaten.
2	IEEE802.1x certificaat gebaseerde toegang geldt voor alle devices in een (rijks)kantoor. Dit geldt voor alle locatie gebonden apparatuur zoals printers, videoconferencing schermen, kiosk-pc, werkplekken van de IDV-G's, et cetera.
3	De (802.1x) device certificaten moeten automatisch vernieuwd worden als deze verlopen. Dit is de verantwoordelijkheid van leverancier van de desbetreffende dienst.

Toekomst:

- Manufacturer Installed Certificate (MIC) wordt op een aantal devices standaard geleverd door de leverancier. Dit MIC certificaat is factory installed en kan niet gewijzigd worden. Onderzocht gaat worden of dit opgenomen kan worden in het ontwerp voor rijkskantoren.

5.2.4 Afdrukken en scannen

Kader Afdrukken en scannen	
1	De multi-functionele printers in een kantoor zijn bedoeld voor het afdrukken van documenten door gebruikers in een kantoor.
2	IDV-G’s dienen aan te sluiten op het rijksbrede print platform.
3	De werkplekken kunnen niet rechtstreeks een printer benaderen.

5.2.5 Ontwikkelingen:

- Nieuwe printer aanbesteding is gestart in 2025.
- Nieuwe print platform is gereed medio 2025/2026.

6 Applicaties

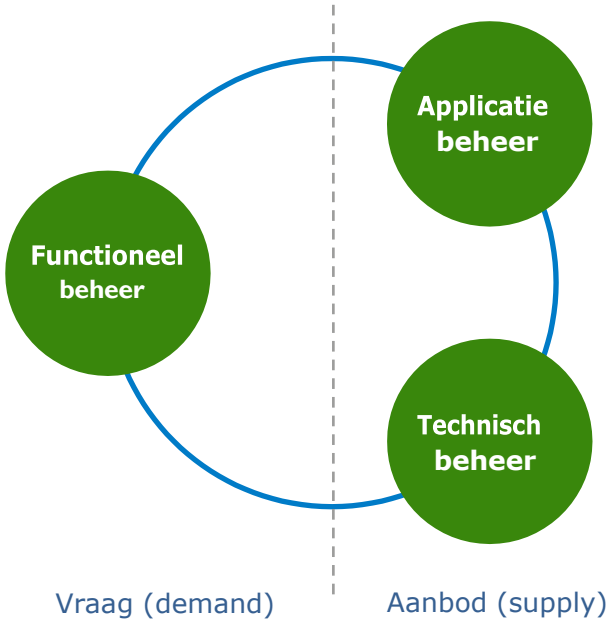
6.1 Relatie met PDC

Voor de dienstverlening geldt dat al hetgeen is beschreven in de PDC 2025 Hoofdstuk 8 “Applicaties” van toepassing is.

6.2 Beheer aansluitvoorwaarden

6.2.1 Achtergrond van de aansluitvoorwaarden

De dienstverlening op het gebied van de hosting van applicaties bestaat feitelijk uit het leveren van technisch beheer. Het doel van dit beheermodel is een efficiënt en effectief managementsysteem te bieden voor het beheer van informatiesystemen. De essentie ervan is dat voor wat betreft IT-beheer drie deelgebieden worden onderkend: functioneel, technisch en applicatiebeheer. Onze dienstverlening op het gebied van hosting heeft dus enkel betrekking op het technisch beheer uit dit model.



Functioneel beheer is de beheervorm die alle beheertaken omvat die nodig zijn in het kader van het gebruik van informatiesystemen. Aangezien gebruik zich richt op de functionaliteit, zoals het invoeren, manipuleren, verkrijgen, transporteren en opslaan van gegevens, wordt gesproken van functioneel beheer.

Applicatiebeheer betreft het ontwikkelen en onderhouden van applicatiesoftware (zowel voor maatwerktoepassingen als pakketten). Er kunnen zich tal van situaties voordoen waardoor wijzigingen in de oorspronkelijke applicatieprogrammatuur of gegevensbankstructuren moeten worden aangebracht. De aanleiding kan liggen in veranderende eisen vanuit het gebruik, maar ook in het aanpassen van de programmatuur aan het samenwerken met de ondersteunde versies van gekoppelde systemen en vanuit de infrastructuur. Telkens wanneer zich zo'n situatie voordoet, wordt applicatie-onderhoud uitgevoerd. Daarom is het belangrijk om voorwaarden te hanteren waaraan een applicatie moet voldoen, zodat deze 'gemakkelijk' onderhouden kan worden.

Technisch beheer bevat als beheervorm alle taken die nodig zijn voor het installeren, accepteren en operationeel maken en houden van informatiesystemen en technische infrastructuren. Onder technisch beheer valt ook het optimaliseren van de verwerkingsprocessen en het aanbrengen van wijzigingen in de technische infrastructuur als gevolg van fouten, uitbreiding of vervanging. Het technische beheer is met name gericht op het technische platform, bestaande uit apparatuur met bijbehorende basisprogrammatuur, en de operationalisering van de hierop gebouwde informatiesystemen.

Vanwege de samenloop van de diverse beheerrollen is het voor SSC-ICT noodzakelijk om voorwaarden te stellen aan de opdrachtgever die betrekking hebben op deze samenloop.

6.2.2 Aansluitvoorwaarden functioneel beheer en applicatie beheer

Aansluitvoorwaarden functioneel beheer	
1	Het functioneel beheer voor een applicatie moet helder en eenduidig belegd zijn door de opdrachtgever. Hierbij moet duidelijk zijn op welke wijze SSC-ICT in het geval van vragen, meldingen en storingen contact kan krijgen met functioneel beheer.
2	Inhoudelijke vragen omtrent gehoste specifieke applicaties moeten primair door functioneel beheer worden beantwoord. Dit is geen onderdeel van het technisch beheer.
3	Bij incidenten die betrekking hebben op de werking van de applicatie neemt functioneel beheer het voortouw in de troubleshooting en zorgt ervoor dat de applicatiebeheerder hierbij wordt betrokken.
4	Functioneel beheer deelt jaarlijks een beheerplan met SSC-ICT waarin vooraf wordt afgestemd welke wijzigingen zijn voorzien en inzichtelijk wordt gemaakt hoe de applicatie blijft aansluiten op ondersteunde versies van de gekoppelde en infrastructurele systemen.

Aansluitvoorwaarden applicatiebeheer	
1	De applicatiebeheerder is verantwoordelijk voor een duidelijke beschrijving van de eisen waaraan de infrastructuur moet voldoen en moet aangeven dat deze eisen passen binnen de door SSC-ICT ondersteunde infrastructurele toepassingen.
2	De applicatiebeheerder is verantwoordelijk voor een heldere installatie-instructie van de programmatuur en de eisen die worden gesteld aan de inrichting van de infrastructuur ten aanzien van koppelingen.
3	De applicatiebeheerder zorgt, waar noodzakelijk, voor een mogelijkheid om binnen de applicatie rechten aan beheerders en gebruikers toe te wijzen. Rechten op de infrastructurele producten (admin-rechten e.d.) zijn enkel voorbehouden aan SSC-ICT.
4	De applicatiebeheerder is beschikbaar om bij incidenten die betrekking hebben op de werking van de applicatie de troubleshooting uit te voeren. De eigenaar van de applicatie is de opdrachtgever voor zowel het functioneel en het applicatie beheer. Daarom zal bij een intake van een te hosten applicatie de eigenaar moeten aantonen aan de eisen te voldoen en zal er jaarlijks een beheerplan moeten worden overlegd om aan te tonen dat blijvend aan de eisen wordt voldaan.

Naast de aansluitvoorwaarden voor het functioneel en applicatie beheer is het uiteraard zaak dat SSC-ICT als technisch beheerder niet alleen de dienstverlening op dat specifieke gebied borgt, maar ook informatie verstrekt via de opdrachtgever die nodig zijn voor alle partijen om hun verantwoordelijkheden waar te maken. Die informatie betreft:

Aansluitvoorwaarden applicatiebeheer

1	Een jaarlijks te updaten opsomming van de door SSC-ICT ondersteunde IAAS-producten en ondersteunde versies die ten grondslag liggen aan de dienstverlening op het gebied van hosting en waartoe deze dienst zich ook beperkt. Hiervan afwijkende IAAS-producten zullen in de infrastructuur van SSC-ICT niet worden toegestaan.
2	Een jaarlijks te updaten opsomming van de PAAS-producten en ondersteunde versies van de aan de hosting ten grondslag liggende dienstverlening. Hiervan afwijkende PAAS-producten kunnen worden gehost, maar worden dan beschouwd als onderdeel van de applicatie-programmatuur
3	Jaarlijks zal SSC-ICT publiceren hoe de lifecycleplanning voor de IAAS- en PAAS-producten eruitziet, zodat de andere beheerverantwoordelijken hierop kunnen anticiperen.

Indien om wat voor reden dan ook een gehoste applicatie niet meer kan voldoen aan de eis om aan te sluiten op de door SSC-ICT ondersteunde versies van de IAAS- en PAAS-producten, dan wordt de dienstverlening ten principale op het moment van beëindigen van de ondersteuning gestopt. Een eventuele verlenging van de dienstverlening op het gebied van hosting kan enkel plaatsvinden door extra afspraken met de leverancier, het langer borgen van de kennis van verlopen versies binnen de beheerorganisatie bij SSC-ICT en door de applicatie omwille van beveiliging te isoleren van de reguliere omgeving. Een dergelijke verlenging is geen automatisme en hier kan ook niet als recht door de opdrachtgever een beroep op worden gedaan. In uitzonderlijke omstandigheden kunnen hierover als maatwerk tegen een hoger tarief en met een initiële investering voor de extra te nemen maatregelen voor een korte periode afspraken over worden gemaakt. De randvoorwaarde vanuit SSC-ICT is dat deze verlenging nooit ten koste mag gaan van de andere dienstverlening die wel binnen de aansluitvoorwaarden wordt verleend.

6.2.3 Aansluitvoorwaarden beheeromgeving (B-Next)

SSC-ICT bouwt een nieuwe beheeromgeving (B-Next), dit platform komt in de loop van 2025 beschikbaar. Vanuit deze centrale beheeromgeving zullen alle klantapplicaties en de daartoe ondersteunende diensten beheerd moeten kunnen worden.

Bij deze omgeving horen de volgende aansluitvoorwaarden wat betreft het beheer.

Algemeen	
1	Applicaties en de daarvoor beschikbare beheersoftware voldoen aan de normen van de NORA, BIO, AVG en verplichte rijks-standaarden
2	Applicaties voldoen aan de guidelines, standaarden, policies en procedures welke zijn ingevuld door het vigerende SSC-ICT informatie beveiligingsbeleid.
3	Autorisaties en expliciete toegang wordt verleend op basis van een door de beheersorganisatie vastgestelde autorisatiematrix.
4	Applicaties voldoen aan de door SSC-ICT gestelde richtlijnen voor logging en monitoring.
5	Vooraf is bekend welke poorten en protocollen gebruikt moeten worden om beheer uit te kunnen voeren op een applicatie.
6	Beheer op afstand wordt voor alle klanten centraal vanuit de B-Next omgeving in het ODC Rijswijk gedaan door gebruik van een beheer VDI. Er zijn geen andere beheermethodes toegestaan.

7	In de B-Next beheeromgeving wordt voor alle klantomgevingen een virtuele beheerwerplek gecreëerd. Andere methoden voor beheer zijn niet toegestaan.

Voor de Beheerwerkplek (beheerVDI) worden aanvullende eisen gesteld:

Virtuele beheerwerkplek (in de B-Next omgeving)	
1	Voor software die op de VDI beschikbaar gesteld wordt om de beheerwerkzaamheden uit te voeren is de KANS toets voor de reguliere DWR-Next werkplek leidend (paragraaf 3.1).
2	Ontwikkelwerkzaamheden zijn niet toegestaan op de beheer VDI, hiervoor kunnen OT-werkplekken worden geleverd (zie PDC).
3	Het gebruik van RDP is niet toegestaan. Indien toch noodzakelijk moeten de CIS richtlijnen voor beveiliging van RDP sessies worden gevolgd.
4	Scripts worden beschouwd als Software, die moet het software kwaliteitscontrole proces volgen.
5	De BeheerVDI heeft geen toegang tot internet.
6	De beheer software moet door de leverancier ondersteund worden en de meest recente versie moet gebruikt waar mogelijk.
7	De beheer software moet gecontroleerd kunnen worden of dit de versie is die de leverancier beschikbaar gesteld; onder andere via een checksum.
8	Software dient uit een vertrouwde bron te komen. Een vertrouwde leverancier met ondertekend met een certificaat door de leverende partij.

6.3 Standaarden Federatieve Identity Management Services

Directory services voorzien in zoeken, identificeren, authenticatie en autorisatie van verschillende informatieobjecten zoals servers, websites, identiteiten (gebruikers) groepen en configuraties. Het gebruik van Directory Services is verplicht voor alle bouwblokken.

Service	TS	Versie	Status	Toelichting
Accounts	Microsoft Active Directory	2016	Productie	Standaard bouwsteen voor Kerberos en op SAML gebaseerde authenticatie. Waarbij Kerberos alleen gebruikt wordt binnen de werkplekomgeving voor desbetreffende klant en niet daar buiten.
SAML-Bridge	Microsoft Active Directory Federation Services	2012 R2 / ADFS 3.0	Productie	Protocoltransformatie tussen WS* en SAML
Attribuut	Microsoft Active Directory LDS	2016	Productie	Standaard bouwsteen voor beheer van applicatie-gebonden attributen
Federatie	OpenConext	-	Bouw	Standaard bouwsteen voor federatieve authenticatie op

				basis van SAML, OAuth en OpenID
Rijksdirectory	DIRX Directory / DIRX Identity	8.3 /8.4	Productie	Rijksbrede directory voor identiteiten van rijskmedewerkers voor het gebruik in rijksbrede applicaties
Azure AD, met UPN=emailadres	Microsoft Entra ID	MS Azure actieve versie	MS Cloud dienst	Cloud based directory voor hybride cloud Identiteiten (Office 356). Deze hybride identiteiten worden gesynchroniseerd vanuit de on-presmisse klant Active Directories. Voor gebruik van Entra ID geldt dat hier uitsluitend gebruik van kan worden gemaakt indien de UPN (User Principal Name) gelijk is aan het primaire emailadres van een gebruiker.

6.4 Technische Standaarden Rijksoverheid

SSC-ICT conformeert zich aan de rijksbrede open standaarden past deze toe in zijn producten. De lijst van rijksbrede open standaarden is te vinden op de website van het Bureau Forum Standaardisatie: https://www.forumstandaardisatie.nl/lijst-open-standaarden.

Digitale toegankelijkheid

Ieder een moet informatie en diensten van de overheid kunnen bereiken en gebruiken. Dat geldt ook voor digitale informatie en diensten. Daarom moeten de websites en (mobiele) apps van overheidsorganisaties verplicht toegankelijk zijn.

De mate van digitale toegankelijkheid heeft directe gevolgen voor eindgebruikers in het verzorgingsgebied van SSC-ICT en is cruciaal voor een kleine groep[2] die afhankelijk is van invoer en of uitvoer anders dan muis en beeldscherm.

Er is een wet voor digitale toegankelijkheid. De Wet Digitale Overheid (WDO) Deze wet vraagt het volgende van overheidsinstanties:

- Maak je digitale kanalen toegankelijk:
- Publiceer toegankelijkheidsverklaringen
- Blijf verbeteren:

De Wet Digitale Overheid is de wettelijke grondslag voor het Besluit digitale toegankelijkheid overheid. (2018)

Overheidsinstanties zijn zelf verantwoordelijk voor de toegankelijkheid van hun digitale dienstverlening. Zij moeten dit uitleggen in hun toegankelijkheids-verklaringen. Het ministerie

[2] De totale groep mensen met een sensorische, motorische of verstandelijke beperking in Nederland is aanzienlijk. Geschat op 4,5 mln. mensen op een totale bevolking van 18 mln.

van Binnenlandse Zaken en Koninkrijksrelaties werkt aan interbestuurlijk toezicht. Dit is opgenomen in de Wet digitale overheid.

Open standaarden

Ontwikkelde programmatuur mag alleen bij hoge uitzondering gebruik maken van gesloten standaarden. Gebruik van gesloten standaarden dient vooraf gemeld te worden met een motivatie voor het waarom en mag alleen na expliciete toestemming worden ingezet.

In de architectuurwiki zijn in de beschrijvingen de standaarden opgenomen voor de architectuur bouwblokken en technische services

Web	Standaard	Versie	Status	Toelichting
Opmaak	HTML	5.0	Aanbevolen	Opvolger van XHTML
Opmaak	XHTML	1.1	Aanbevolen	
Opmaak	CSS	2.1/3.0	Aanbevolen	http://www.w3.org/Style/CSS/
	XML	1.0	Aanbevolen	Opmaaktaal voor gestructureerde gegevens
Communicatie	HTTP	1.1/2.0	Verplicht	IETF
Beveiliging	HTTPS en HSTS		Aanbevolen	RFC2818, RFC6797
Publicatie	RDF	1.1	Aanbevolen	W3C publicatie gestructureerde gegevens

Digitale Toegankelijheid	Standaard	Versie	Status	Toelichting
Publicatie	EN 301 549		Verplicht	Europese standaard voor de digitale toegankelijkheid voor mensen met een beperking.
Richtlijnen	WCAG 2.1	2.1	Verplicht	Moet worden toegepast op het aanbieden van web-gebaseerde informatie-, interactie-, transactie- en participatiediensten.
Wetgeving	Wet Digitale Overheid	01-07-2023	Verplicht	Wettelijke grondslag voor besluit digitale toegankelijkheid
Besluit	Besluit digitale toegankelijkheid overheid	2018	Verplicht	Overheidsinstanties maken hun websites en mobiele applicaties toegankelijk door toepassing van standaard EN 301 549

Beveiliging	Standaard	Versie	Status	Toelichting
Transport	TLS	<= 1.1	Uitgefaseerd	Onveilig /kwetsbaar
	TLS	1.2	Verplicht	Standaard voor transportbeveiliging
	TLS	1.3	Aanbevolen	Standaard voor transportbeveiliging

Beveiliging	Standaard	Versie	Status	Toelichting
Authenticatie	SAML	2.0	Verplicht	Standaard raamwerk voor uitwisseling van authenticatie- en autorisatie-gegevens
	OAuth	2.0	Aanbevolen	autorisatiestandaard voor met web gebaseerde applicaties die gegevens uitwisselen met behulp van API's
	OIDC		Aanbevolen	OIDC bouwt voort op OAuth 2.0. Het maakt het mogelijk om andere authenticatievoorzieningen middels een routeringsvoorziening te ontsluiten.
	~~FIDO~~			

Applicatie	Standaard	Versie	Status	Toelichting
Ontwikkeling	Javascript			
Ontwikkeling	ASP.NET	3.0, 3.5, 4.0		
Ontwikkeling	C#	3.0, 3.5, 4.0		
	JSON			JavaScript Object Notation (JSON) uitwisselen van datastructuren
	SCIM	2.0		REST protocol API voor creatie en beheer van identiteit gegevens op het web.
	Microsoft Graph	N	Gepland	Platform voor applicatieve interfacing met Microsoft 365

.

7 Hosting

7.1 Relatie met PDC

Voor de dienstverlening geldt dat al hetgeen is beschreven in de PDC 2025 Hoofdstuk 7 "Hosting" van toepassing is.

7.2 Standaarden

7.2.1 Omgevingen

De term "Omgeving" wordt gebruikt in de context van O-, T-, A-, P- E omgeving. Functioneel gezien is een omgeving een verzameling systemen met een bepaalde classificatie binnen een Tenant. Omgevingen kunnen alleen services van elkaar gebruiken als zij eenzelfde classificatie hebben. Voorbeelden:

- Productie-werkplekken kunnen alleen met Productiesystemen communiceren.
- Applicatie servers in Acceptatie mogen alleen koppelen met servers van andere Acceptatie applicaties.

SSC-ICT biedt klanten een O-T-A-P-(E) omgeving aan. Indien SSC-ICT verantwoordelijk is voor het beheer van een applicatie in de Productie omgeving en daar garanties afgeeft over diensten niveaus en life cycle management dient er altijd een Acceptatie omgeving voor die applicatie aanwezig te zijn (of binnen zeer korte tijd opgestart kunnen worden).

De applicaties van klanten wordt ondersteund door basis infrastructuur diensten uit het Nuts compartiment. Het Nuts compartiment is een voorziening die onderdeel is van de basis infrastructuur, waar diensten in staan die alle servers gebruiken, zoals Active Directory, NTP, DHCP, Log collectoren, etc.

	Bevat	Functie	Beheer	Ondersteuning
Productie	Productie data	Release in beheer nemen Wijzingen doorvoeren	SSC-ICT	
Acceptatie	Voor productie representatieve data	Release vrijgeven voor productie Wijzigingen testen	SSC-ICT	
Test	Test Datasets	Release vrijgeven voor Acceptatie Wijzigingen testen	Tenant Testteam	
Ontwikkel	Ontwikkel Datasets	Bouw aan volgende functionele release	Tenant Ontwikkelteam	
Educatie	Voor productie representatieve data	Opleiden gebruikers	Functioneel beheerders / Opleiders	

Omgevingen bestaan uit compartimenten. Een compartiment is een door toegangsregels en filtering afgeschermd netwerk waarop systemen zijn aangesloten die een vergelijkbare rol vervullen of data van eenzelfde vertrouwelijks niveau bevatten. Veel voorkomende compartiment zijn bijvoorbeeld Presentatie-Applicatie-Data. Compartimenten geven invulling aan de BIO definities van "Koppelvlakken". Compartimenteren is dus een technische maatregel om aan beveiligingscriteria te kunnen voldoen.

Compartiment in ACI[3]	Bevat	Functie	Beheer	Voorbeeld
Presentatie	Presentatie systemen	Aanbieden van functionaliteit aan gebruikers	SSC-ICT	Web servers, load balancers, front-end servers
Applicatie	Applicatie systemen	Aanbieden van applicatie functionaliteit aan presentatiesystemen	SSC-ICT	Applicatie servers
Data	Data systemen	Dataopslag ten behoeve van de applicatie systemen	SSC-ICT	Databases, Storage en File systemen

Let wel: In voorkomende gevallen kunnen compartimenten gecombineerd worden als de applicatie de drielaags structuur niet ondersteund. Er is dan de mogelijkheid presentatie-applicatie te combineren: PA. Ook bestaat de mogelijkheid om applicatie en data compartimenten te combineren: AD. Tenslotte kan er voor er voor applicaties die monolithisch zijn een PAD compartiment ingericht worden.

7.2.2 Load-balancing

Het bouwblok Load Balancer vult de functie reverse proxy en verdeling van verkeer over de (applicatie- of web)servers. De load balancer wordt ingezet in server farms waarbij de werklast wordt verdeeld over meerdere servers. Door servers toe te voegen is schaalbaarheid volgens het "scale-out" principe mogelijk. Een ander voordeel is de mogelijkheid om serverbeheer uit te voeren zonder onderbreking van de dienstverlening. (wel met enig verlies van capaciteit).

Het ODC Rijswijk heeft een standaard technische service voor load-balancing. Er zijn aparte fysiek gescheiden load balancers voor het DCLAN en de DMZ.

Service	TS	Versie	Status	Toelichting
Load balancing	Big IP F5	-	Productie	Standaard bouwsteen in ODC
	Dynamic traffic control	-	In ontwikkeling	Onderdeel van Infoblox bouwsteen
	Cisco ACE	-	Verouderd	

7.2.3 Proxy, Reverse Proxy, SSL Off-loading

Het ODC Rijswijk heeft een centrale voorziening voor proxy-support en SSL-off-loading. Er een proxy voorziening voor het DCLAN, voor situaties waar vertrouwde connecties een proxy nodig hebben.

Proxy functionaliteit wordt ingezet waar volgens het BIR er sprake is van een koppelvlak tussen zones met een verschillend vertrouwelijkheidsniveau en waar dientengevolge sessie ontkoppeling een eis is.

Service	TS	Versie	Status	Toelichting
(Reverse) Proxy	Big IP F5	-	Productie	Standaard bouwsteen in ODC

[3] Cisco ACI is de software defined netwerktechnologie waarmee (o.a.) netwerkcompartimenten worden gebouwd.

7.2.4 Server besturingssysteem

Alle nieuwe servers worden virtueel gerealiseerd, tenzij specifieke omstandigheden dit verhinderen. Het virtuele server platform biedt ontkoppeling van fysieke hardware en software: Hierdoor hebben hardware storingen en wijzigingen (w.o. vervanging) veel minder impact op de bovenliggende software lagen en kan het datacenter als geheel kosteneffectief en flexibel worden ingezet.

Platform	TS	Versie	Status	Toelichting
Windows	Windows Server	2012 R2 (64 bits)	Uitfaseren voor 1-1-2023	Wordt niet meer uitgeleverd en ondersteund
Windows	Windows server	2016 (64 bits)	Uitfaseren voor 1-1-2024	Wordt niet meer uitgeleverd en ondersteund
Windows	Windows server	2019 (64 bits)	Uitfaseren voor 1-1-2025	Wordt niet meer uitgeleverd
Windows	Windows server	2022 (64 bits)	Productie	Ondersteund tot 2027
Windows	Windows server	2022 CORE (64 bits)	Productie	Ondersteund tot 2027
Windows	Windows server	2025 (64 bits)	In ontwikkeling	Gepland 2025
Linux	Red Hat Enterprise Linux	7.x (64 bits)	Verouderd	Uitfaseren
Linux	Red Hat Enterprise Linux	8.x (64 bits)	Verouderd	Uitfaseren
Linux	Red Hat Enterprise Linux	9.x (64 bits)	Productie	Tot medio 2027
Linux	Red Hat Enterprise Linux	10.x (64 bits)	In ontwikkeling	Leverbaar vanaf 2026
Oracle Linux	Oracle Enterprise Linux unbreakable	6.x (64 bits)	Verouderd	Extended support ends Dec 2024 Voor toepassing i.c.m. Oracle database
Oracle Linux	Oracle Enterprise Linux unbreakable	7.x (64 bits)	Verouderd	Premier support ends Dec 2024 Extended support ends Jun 2028 Voor toepassing i.c.m. Oracle database
Oracle Linux	Oracle Enterprise Linux unbreakable	8.x (64 bits)	Productie	Premier support ends July 2029 Extended support ends Jun 2032 Voor toepassing i.c.m. Oracle database
Oracle Linux	Oracle Enterprise Linux unbreakable	9.x (64 bits)	Productie	Premier support ends July 2032 Extended support ends Jun 2035 Voor toepassing i.c.m. Oracle database

Voor Redhat (Linux) Installaties is het type minimal (Image), SElinux en de firewall moeten aan staan. Aanvullende software moet via Yum uit de beschikbare RedHat repositories (via satellite)

komen. (i.v.m. updates uit een vertrouwde bron)
De applicatie moet om kunnen gaan met de OS-en "Productie" status uit de tabel. De software mag geen verstoringen aan de applicatie geven. Java, Apache en Tomcat is beschikbaar vanuit de Redhat repository (Alle gebruikte software komt uit een repo, geen losse rpm's)

7.2.5 Virtuele servers

Voor servers geldt de ontwerpregel "OR-15 Servers Virtueel"

Het virtualisatieplatform zorgt voor een laag tussen de fysieke hardware en het besturingssysteem. De hypervisor zorgt voor een bundeling van onderliggende hardwareresources waardoor een efficiënter gebruik van de hardware mogelijk is.

Rationale: Inzet van virtualisatie zorgt voor een efficiënter gebruik van hardware en biedt betere beschikbaarheid, onderhoudbaarheid en fail-over mogelijkheden.

Platform	TS	Versie	Status	Toelichting
Windows /Linux	VMware VSphere	6.7	Verouderd	Wordt niet als IaaS of PaaS geleverd aan afnemers.
Windows / Linux	VMware vSphere	7	Productie	Wordt niet als IaaS of PaaS geleverd aan afnemers.
Windows / Linux	VMware vSphere	8	Bouw	Wordt niet als IaaS of PaaS geleverd aan afnemers.

7.2.6 Web Servers

Platform	Type	Versie	Status	Toelichting
Windows	Internet Information Services	7.5	Uitfaseren	Wordt niet meer ondersteund
Windows	Internet Information Services	8.5	Uitfaseren	Wordt niet meer ondersteund
Windows	Internet Information Services	10.0	Verouderd	Versie behorend bij Windows server 2016 Wordt niet meer uitgeleverd
Windows	Internet Information Services	10.0	Productie	Versie behorend bij Windows Server 2022 Versie Windows server 2019 wordt niet meer uitgeleverd
Linux (RHEL)	Apache	Laatste versie uit de REPO	Productie	

Techniek; PHP, Apache (httpd) en Apache/Tomcat worden alleen op het SSC-ICT Red Hat Linux platform aangeboden.

7.2.7 Database platform

Platform	TS	Versie	Status	Toelichting
Oracle Linux	Oracle DBMS	18C	Verouderd	

Oracle Linux	Oracle DBMS	19C	Productie	Mainstream Support tot 2024 Extended support tot 2027
Oracle Linux	Oracle DBMS	21C	Bouw	
Windows	MSSQL	2016	Verouderd	End of mainstream support juli 2021
Windows	MSSQL	2017	Verouderd	End of mainstream support november 2022
Windows	MSSQL	2019	Productie	Mainstream support tot juli 2025
Linux/..	MariaDB	5.5	Productie	Special meegeleverd als onderdeel van de applicatie
Oracle Linux	PostgreSQL	12.X	Productie	
Oracle Linux	PostgreSQL	13.X	Productie	

7.2.8 Storage en backup

De technische standaarden NFS over ethernet IP, LUN over Fibre Channel (SAN) en CIFS over LAN bepalen hoe en op welke storage hosts aangesloten worden.

Storage wordt in de volgende vormen aangeboden:

- Block opslag aangesloten op een Fiber Channel (SAN) netwerk
- File opslag aangesloten op een IP netwerk met de protocollen NFS en CIFS
- Software defined opslag op het VMware VSAN platform

Op grond van de ontwerpregels Servers Virtueel en afgeleid principe Exit strategie wordt storage aangeboden via een virtualisatie laag.

Platform	TS	Versie	Status	Toelichting
File based Storage	NetApp	-	Productie	CIFS en NFS
Block based Storage	EMC & HDS	-	Productie	
Storage Virtualisatie	IBM SVC	-	Productie	Ten behoeve van virtualisatie block based storage
Storage Virtualisatie	VMware VSAN	-		Ten behoeve van virtualisatie van lokale of direct gekoppelde storage

N.B: De dienstverleningen afspraken met betrekking tot Storage zijn in “H 11.12 Back-up en restore” van de Producten- & Dienstencatalogus 2025 opgenomen.

Platform	TS	Versie	Status	Toelichting
Backup	Commvault	11.x	Productie	Generiek, B-next
	EMC DDboost	n.v.t	Productie	Oracle DB backup
	Rubrik CDM	7.0	Productie	VM backup, shared en JenV
	Dataprotector		Productie	BuZa en JenV

7.3 OS Hardening

Voor alle eerdergenoemde componenten (Operating Systemen, Webservers en Databases) geldt dat ze volgens de laatste, vastgestelde best-practice security baselines (gebaseerd op bijvoorbeeld CIS, STIG) worden gehardenend. Hardening houdt in dat zoveel mogelijk niet-noodzakelijke services zijn uitgeschakeld en/of verwijderd worden, waardoor wordt voldaan aan de eisen uit de BIO teneinde de beveiliging van de componenten te verbeteren. Hardening kan in sommige gevallen van invloed zijn op het functioneren van geïnstalleerde applicatie(s) en

vergt derhalve zorgvuldig testen. In uitzonderlijke gevallen kan een exceptie worden aangevraagd en vastgesteld. Periodiek wordt over de mate van hardening, i.c. compliance met betreffende security baseline, gerapporteerd. Meer informatie over hardening van componenten kan worden verkregen via SCC-ICT relatiemanagement."

Dit betekent dat bij oplevering van componenten security updates en patches zijn geïnstalleerd binnen de periode die is overeengekomen conform het vigerende beveiligingsbeleid. Binnen het OS worden verschillende instellingen aangepast om te voldoen aan de security eisen.

Lokale firewalls, zoals die deel uitmaken van de meeste OS distributies, mogen gebruikt worden om functies ontoegankelijk te maken, maar andere methodes zoals het uitschakelen van services en listeners op netwerkpoorten zijn ook acceptabel.

SSC-ICT hanteert de StiG benchmarks (https://public.cyber.mil/stigs/) als richtlijn voor hardening van het OS en de daarop gebaseerde (applicatie)servers. Verder wordt OS hardening uitgevoerd met het oog op de inzet van de (applicatie)server. Er wordt gewerkt met een risicoanalyse op basis van een kwetsbaarheden scan.

7.4 Toekomst

7.4.1 Container dienstverlening

We verwachten vanaf het derde kwartaal van 2025 container diensten te kunnen leveren en de dienstbeschrijving daarvan opgenomen te hebben in de PDC.

Daarbij maken we onderscheid tussen container dienstverlening voor:

- Off-The-Shelf aangeleverde containers die kunnen landen op het beoogd SUSE Rancher platform
- het leveren van containers diensten voor "Cloud Ready / Cloud-native" applicatie ontwikkeling (door afnemers) op basis van een Kubernetes platform met additionele tooling voor CI/CD en Selfservice, beoogd platform is RedHat OpenShift

7.4.2 AI dienstverlening

We verwachten in de loop van 2025 AI dienstverlening te ontwikkelen en de dienstbeschrijving daarvan opgenomen te hebben in de PDC.

Daarbij willen we voor onze afnemers AI diensten op een veilige wijze beschikbaar maken in ons datacenter, door een eigen 'on-premises' variant te ontwikkelen van generatieve AI zoals ChatGTP of Co-pilot. We onderscheiden drie diensten:

- API: een API-voorkant voor afnemers om ontwikkelaars en toepassingen te laten communiceren met Large Language Models (LLMs) in ODC Rijswijk.
- Chat: een AI-chat middels RAG, met een gestandaardiseerde grafische voorkant, voor het communiceren met LLM's in ODC Rijswijk.
- Search: een AI-zoekdienst voor het doorzoeken van inhoud in bestandsbronnen aangeleverd door afnemers, en het beantwoorden van vragen

De AI dienstverlening moet voldoen aan de rijksbrede en Europese kaders en wetten, om de risico's verbonden met het gebruik van generatieve AI te minimaliseren.

8 Housing Business Services

8.1 Relatie met PDC

Voor de dienstverlening geldt dat al hetgeen is beschreven in de PDC 2025 Hoofdstuk 6 "Housing" van toepassing is.

8.2 Housing

Het ODC Rijswijk voldoet aan de eisen die aan een tier-3 datacenter worden gesteld, te weten:

- 99,982% beschikbaarheid
- Jaarlijks niet meer dan 1,6 uur downtime t.g.v. datacenter
- Redundante distributie paden, d.w.z. apparatuur heeft dubbele voedingen en alle aansluitingen zijn dubbel en onafhankelijk uitgevoerd.
- Fout tolerant, alle voorzieningen zoals stroom en koeling zijn N+1 keer aanwezig
- Bestand tegen een stroomonderbreking van 72 uur.

Elk datacenter heeft een redundante connectie met een eigen Internetprovider. Evenzo zijn er redundante connecties met de Haagse Ring en met Internet. Voor Internet wordt gebruik gemaakt van de providers Tele2 en KPN en voor specifieke kantoorlocaties wordt gebruik gemaakt van de provider BT.

De datacenters ODC Rijswijk en locatie Korte Voorhout zijn onderling gekoppeld op een breedbandig laag 3 netwerk. Laag 2 koppelingen worden niet ondersteund.

Standaard dienstverlening conform PDC 2025 zoals opgenomen in H6

8.3 Aansluitvoorwaarden Housing

Bij het verlenen van diensten stelt SSC-ICT voorwaarden waaraan een opdrachtgever bij zowel de start van de dienstverlening als tijdens de exploitatiefase moet blijven voldoen.

Deze voorwaarden zijn opgesteld voor de dienstverlenings- domeinen Housing, Hosting en Rijkswerkomgeving, omdat hier sprake is van een koppelvlak met departement specifieke ICT.

8.3.1 Achtergrond van de aansluitvoorwaarden

Dienstverlening op het gebied van housing wordt geleverd vanuit het ODC Rijswijk. Om een solide basis te vormen voor de verdere ICT-dienstverlening is het ODC ontworpen en ingericht als een Tier-3 datacenter. Hiermee voldoet het datacenter aan de volgende eisen:

- 99,982% beschikbaarheid
- Jaarlijks niet meer dan 1,6 uur downtime
- Redundante distributiepaden: apparatuur heeft dubbele voedingen en alle aansluitingen zijn dubbel en onafhankelijk uitgevoerd
- Fout-tolerant: alle voorzieningen zoals stroom en koeling zijn N+1 keer aanwezig
- Bestand tegen een stroomonderbreking van 72 uur
- 7x24 uur beveiligingspersoneel aanwezig

Om die solide basis vanuit de inrichting van het datacenter door te trekken hanteren we de volgende inrichtingsprincipes op de computervloer:

- De in het ODC gebruikte racks (kasten waarin de servers kunnen worden geplaatst) zijn voorzien van gestructureerde bekabeling en een redundante stroomvoorziening.
- Ieder rack heeft een maximale hoogte van 47 hoogte-eenheden, een breedte van 80 centimeter, een diepte van 120 centimeter en is maximaal 240 centimeter hoog. Een aantal hoogte-eenheden wordt gebruikt voor het aanleggen van de gestructureerde bekabeling.
- De voorste en de achterste stijlen van de 19-inch racks staan 74 centimeter uit elkaar. De bovenste 5 en de onderste 3 hoogte-eenheden worden gereserveerd voor datacenter-voorzieningen. Apparatuur wordt vanaf hoogte-eenheid 4 tot maximaal 38 geplaatst (maximale rackvulling 70%).
- Het plaatsen van klant-eigen racks is niet toegestaan.
- Apparatuur wordt geplaatst door of onder begeleiding van floormanagement van het ODC.

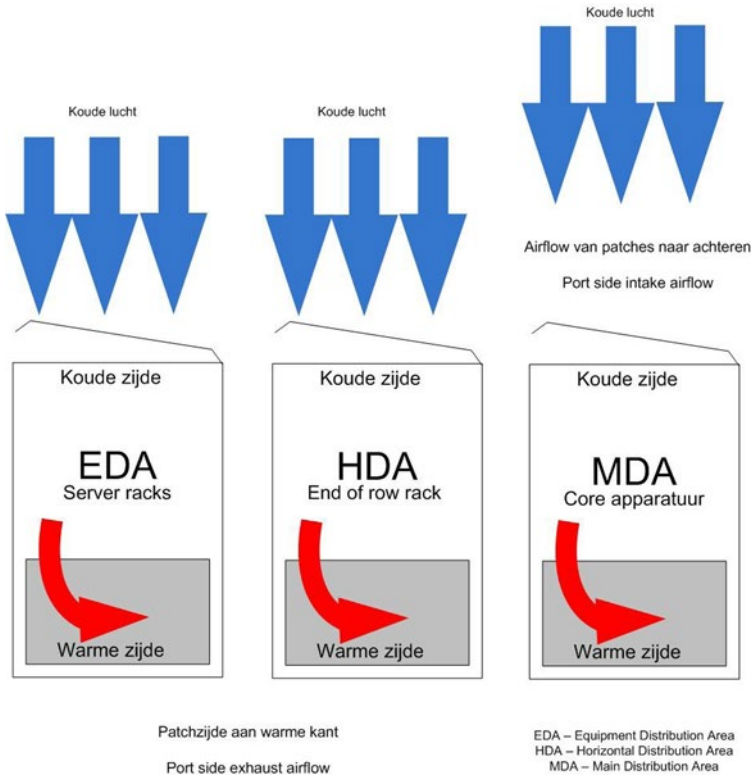
8.3.2 Aansluitvoorwaarden voor afnemers

Om de in deze PDC aangeboden dienstverlening te kunnen leveren en het serviceniveau te kunnen borgen, stellen wij de volgende voorwaarden aan zowel het proces als de apparatuur die wij of onze klanten willen plaatsen in het ODC. Ten aanzien van de procesgang zijn de eisen:

- De apparatuur wordt geplaatst door of onder begeleiding van ODC Floormanagement (ODC FMT).
- Het aansluiten van de apparatuur wordt uitgevoerd door ODC FMT met kabels geleverd vanuit ODC Rijswijk (zie tabel 1 kabeloverzicht).
- UTP-connectiviteit is alleen beschikbaar binnen de rijen. Connectiviteit tussen rijen is op basis van multimode glasvezel.
- Buiten de 19-inch kast wordt er gebruik gemaakt van de gestructureerde bekabeling van het ODC Rijswijk.
- Het afleveren van de apparatuur dient op straatniveau plaats te vinden. Er is geen laadperron of heftruck aanwezig

Voor de apparatuur zijn de volgende eisen van kracht:

- De luchtstroom van de apparatuur moet van de voorzijde naar de achterzijde van de kast gaan (zie Figuur 1 Airflow datacenter).
- De apparatuur moet voorzien zijn van actieve ventilatoren.
- De apparatuur moet met de netwerkaansluitingen naar de patchzijde van de kast geplaatst worden. In een zone is er altijd maar één patchzijde. In de EDA rijen (zie de afbeelding hieronder) is dit aan de warme kant.
- De apparatuur heeft redundante netvoedingen. Indien dit niet het geval is moet er door SSC-ICT een automatic transfer switch (ATS) geplaatst worden (1 hoogte-eenheid). Hier zijn extra kosten aan verbonden.
- De apparatuur moet ‘rackmount’ zijn volgens de specificaties van de 19-inch kast die SSC-ICT hanteert. De maximale afmetingen van de apparatuur zijn 19 inch breed en 100 centimeter lang.
- De apparatuur moet waterpas in de kast hangen. Indien dit niet het geval is, moet er ter ondersteuning een legplank geplaatst worden (1 hoogte-eenheid). Hier zijn extra kosten aan verbonden.
- De luchtinlaat van de apparatuur moet aansluiten op de voorkant van het rack. Indien dit niet kan moet het mogelijk zijn om air ducts te kunnen plaatsen, bij voorkeur vanuit de leverancier. Hierbij moet patchen wel mogelijk blijven. Indien het ODC Rijswijk de air ducts levert zijn hier extra kosten aan verbonden.
- Direct patchen tussen de kasten is niet toegestaan. Hiervoor kan gestructureerde bekabeling worden aangevraagd. Hier zijn extra kosten aan verbonden en de levertijd is minimaal 8 weken na aanvraag.



Figuur 1 Airflow datacenter

Naast deze eisen gelden de volgende voorkeuren voor te plaatsen apparatuur:

- Netwerk redundant aangesloten. Het ODC beschikt over een redundante netwerk-infrastructuur. De voorkeur is om hiervan gebruik te maken.
- Remote management aansluiting UTP 1000Mb. Om het aantal personen op zaal zoveel mogelijk in te perken geniet het de voorkeur dat de apparatuur is voorzien van remote management.

Aansluitvoorwaarden netwerk:

- De netwerk capaciteit op het datacenter kent beperkingen. Om hier verstandig mee om te gaan wordt onderscheid gemaakt tussen laag/medium en hoog volume verkeer;
- Housing klanten nemen netwerkcapaciteit af in lage of medium volumes. Voor die diensten worden zij gekoppeld via het Basis koppelnetwerk;
- ODC Houders nemen hoge netwerkcapaciteit af van het ODC. Hoog volume netwerkcapaciteit wordt buiten het Basiskoppelnetwerk om gerealiseerd met een directe verbinding naar de Housing omgeving.

Contractpartij	Neemt af	Behoefte	Koppeling	Kosten
Housing Klant	PoD / Kast / RackUnit	Laag / Medium volume verkeer naar aangesloten netwerken in ODC Rijswijk	Basiskoppelnetwerk	Per Mb
ODC Houder	PoD / Kast	Hoog Volume verkeer tussen ODC's	Directe koppeling buiten BKN om	Uren realisatie connectiviteit

8.3.3 Vertrouwelijkheid

PDC 2025: Het beveiligingsbeleid toegepast op de dienstverlening van SSC-ICT is, tenzij expliciet anders is overeengekomen, BIO2017, BBN2.

Housing biedt standaard dienstverlening tot en met Departementaal Vertrouwelijk (Dep-V). Niveau BBN2. Voor specifieke klanten kan met inzet van aanvullende EU en NATO maatregelen BBN3 niveau worden bereikt

9 Security

9.1 Relatie met PDC

Voor de dienstverlening geldt dat al hetgeen is beschreven in de PDC 2025 Hoofdstuk 9 "Security" van toepassing is.

Het lijnmanagement is verantwoordelijk voor informatiebeveiliging. Risicomanagement speelt hierbij een belangrijke rol. Voor de generieke dienstverlening van SSC-ICT is de Baseline Informatiebeveiliging Overheid (BIO) leidend.

Voor de verwerking van persoonsgegevens geldt daarbij de Algemene Verordening Gegevensbescherming (AVG).

9.2 Baseline Informatiebeveiliging Overheid (BIO)

De BIO is een normenkader voor informatiebeveiliging en voorziet in het basisniveau voor informatiebeveiliging waar alle overheidspartijen aan moeten voldoen. Dit is gebaseerd op de actuele, internationale standaarden voor informatie- beveiliging, de ISO 27001 en 27002, en vergemakkelijkt het uitwisselen van gegevens tussen departementen, uitvoerings- organisaties en andere overheden en verhoogt het onderlinge vertrouwen in elkaars beveiliging.

De BIO kent 3 basisbeveiligingsniveaus. De baseline die voor de generieke ICT-dienstverlening wordt toegepast op het gebied van Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) is (M/M/M). Deze BIV-classificatie komt overeen met BBN2 en dat betekent dat de informatie die verwerkt mag worden is gerubriceerd als Departementaal Vertrouwelijk. Deze DEP-V informatie wordt preventief beschermd tegen alle dreigingen met uitzondering van geavanceerde dreigingen, zoals Advanced Persistent Threats (APT's), afkomstig van statelijke actoren of beroepscriminelen. Daarvoor geldt een bescherming achteraf: zij dienen te kunnen worden gedetecteerd, waarop vervolgens passend gereageerd moet worden.

De basisclassificatie voor persoonsgegevens (P-classificatie) is "geen" tenzij anders is aangegeven door de eigenaar. Voor de overige informatiesystemen wordt door de eigenaar bepaald wat de BIV-classificatie en de P-classificatie is.

Indien een informatiesysteem een hogere BIV-classificatie heeft dan de baseline van SSC-ICT dan leidt dit tot aanvullende maatregelen en afspraken met de opdrachtgever die worden vastgelegd.

9.3 Algemene Verordening Gegevensbescherming

SSC-ICT verwerkt iedere dag persoonsgegevens, voor diverse doeleinden. Op al deze verwerkingen is de privacywetgeving van toepassing, in het bijzonder de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG).

In het kader van de dienstverlening zoals omschreven in de PDC verwerkt SSC-ICT persoonsgegevens ten behoeve van afnemers. Dit doet SSC-ICT in de rol van verwerker in de zin van de AVG. De klant bepaalt het doel van (waarom) en de middelen voor (hoe) de verwerking van persoonsgegevens en is daarmee de verwerkingsverantwoordelijke.

Naast de rol van verwerker vervult SSC-ICT ook de rol van verwerkingsverantwoordelijke. Dit doet wij voornamelijk voor de eigen interne bedrijfsvoering, denk aan de personeels-en klantadministratie. In een enkel geval is sprake van gezamenlijke verwerkingsverantwoordelijkheid tussen ofwel SSC-ICT en de klant, ofwel meerdere klanten onderling.

Verwerkingsverantwoordelijke en verwerker verschaffen elkaar tijdig alle nodige informatie en verlenen medewerking om de verplichtingen uit geldende privacy wet- en regelgeving uit te

voeren. Omdat SSC-ICT tot dezelfde rechtspersoon behoort als de klant, namelijk de Staat der Nederlanden, kan er in dit geval geen (verwerkers)overeenkomst gesloten worden. Deze verplichtingen dienen daarom vastgelegd te worden in (verwerkers)afspraken.

9.4 NIS2 Richtlijn

De Network and Information Security directive, of NIS2-richtlijn, is de opvolger van de NIS-richtlijn. Deze is vastgesteld door de Europese Unie en bedoeld om de cyberbeveiliging en de weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren. De NIS2 vergroot de reikwijdte van de eerste richtlijn door meer sectoren te omvatten. Daarnaast stelt de richtlijn strengere beveiligingsnormen en meldingsvereisten voor incidenten. De NIS2 wordt momenteel naar Nederlandse wetgeving vertaald.

De richtlijn stuurt op risico's die netwerk- en informatiesystemen bedreigen, zoals cyberbeveiligingsrisico's. De komst van de NIS2-richtlijn moet bijdragen aan meer Europese harmonisatie en een hoger niveau van cybersecurity bij bedrijven en organisaties. Het is de opvolger van de eerste NIS-richtlijn, de NIB, die in Nederland in 2016 is opgenomen in de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni).

De NIS2-richtlijn richt zich op sectoren die al onder de eerste NIS-richtlijn vallen, en op een aantal nieuwe sectoren. Een belangrijk verschil met de eerste richtlijn is dat de sector Overheid er nu ook binnen valt.

Onderdelen van de centrale overheid (Rijksoverheid en zelfstandige bestuursorganen) vallen onder de NIS2-richtlijn als essentiële entiteiten.

Welke verplichtingen schrijft de NIS2-richtlijn voor?

- Zorgplicht – De richtlijn bevat een zorgplicht die entiteiten verplicht om zelf een risicobeoordeling te doen. Op basis daarvan nemen zij passende maatregelen om hun diensten zoveel mogelijk te waarborgen en de gebruikte informatie te beschermen.
- Meldplicht – De richtlijn schrijft voor dat entiteiten incidenten binnen 24 uur bij de toezichthouder moeten melden. Het gaat om incidenten die de verlening van de essentiële dienst sterk (kunnen) verstoren. Een cyberincident moet ook bij het Computer Security Incident Response Team (CSIRT) gemeld worden. Dit team kan vervolgens hulp- en bijstand leveren. Factoren die een incident meldingswaardig maken, zijn bijvoorbeeld het aantal personen dat door de verstoring is geraakt, de tijdsduur van een verstoring en de mogelijke financiële verliezen.
- Toezicht – Organisaties die onder de richtlijn vallen, komen ook onder toezicht te staan. De NIS2-richtlijn schrijft voor dat een onafhankelijk toezichthouder (buiten eventueel interbestuurlijk toezicht) naar de naleving van de verplichtingen uit de richtlijn kijkt. Zoals de zorg- en meldplicht. Momenteel wordt bekeken onder welke toezichthouder de sector Overheid komt te vallen (dit is nog niet bekend) en wat het toezicht inhoudt. Het is de bedoeling om gebruik te maken van bestaande verantwoordingsstructuren. Ook wordt gestreefd naar harmonisering van deze verantwoordingsstructuren. Bevindingen uit onderzoeken naar toezicht in opdracht van het ministerie van BZK in 2019 en 2022 worden hierin meegenomen.

Wat kunnen organisaties alvast doen om zich voor te bereiden?

Het voldoen aan bestaande kaders voor informatiebeveiliging bij de overheid, waaronder de Baseline Informatiebeveiliging Overheid (BIO), vormt de basis om invulling te geven aan de zorgplicht die uit NIS2 volgt. Het volgen van de huidige verplichtingen is dus een belangrijk beginpunt.

Voor overheidsinstanties geldt dat de invulling van de NIS2-zorgplicht zoveel mogelijk langs de lijnen van bestaande kaders zal gebeuren. Organisaties die voorheen nog niet aan de bestaande kaders voor informatiebeveiliging voldeden, hebben hier vanuit NIS2 nu wel verplichting toe.

10 Supporting Services

10.1 Relatie met PDC

Voor de dienstverlening geldt dat al hetgeen is beschreven in de PDC 2025 Hoofdstuk 10 “Supporting services” van toepassing is.