Rijksdienst Caribisch Nederland

CANS - Document SSO CN/ICT

CANS: Criteria Acceptatie Nieuwe Systemen

Colofon

Informatie	CANS - document
Uitgevoerd door	SSO CN/ICT
Versie	2.0
Datum	01-12-2024
Status	Concept

Inleiding

CANS (Criteria Acceptatie Nieuwe Systemen) beschrijft de voorwaarden waaraan nieuwe applicaties en technologische ontwikkelingen moeten voldoen om aangeboden te kunnen worden binnen de ICT omgeving van SSO CN/ICT.

Deze voorwaarden zijn onderverdeeld in de volgende domeinen:

- Datacenter
- Hosting
- Werkomgeving

Deze domeinen bestaan uit beschrijving van de dienstverlening, de gedefinieerde technische standaarden en aansluitvoorwaarden.

Let op: dit document geeft huidige stand van zaken weer, maar staat niet op zichzelf. Het document is basis voor een discussie met de klant of leverancier over de dienstverlening van SSO CN/ICT.

1 Documentgegevens

1.1 Revisie

Op dit document zijn de volgende revisies toegepast:

Versie	Status	Datum	Wijzigingen
0.1	Concept	22-05-2018	Compleet nieuwe opzet
0.2	Concept	11-07-2018	Besproken met SB
0.3	Concept	06-08-2018	NWB aanpassingen ingevoerd
0.4	Concept	28-08-2018	SB aanpassingen toegevoegd
0.5	Concept	31-08-2018	TAB aanpassingen toegevoegd
0.6	Concept	19-09-2018	Opmerkingen verwerkt
1.0	Definitief	07-01-2019	Definitief gemaakt
1.1	Definitief	01-03-2020	Aanpassingen doorgevoerd
2025	Concept	01-12-2024	Grondige revisie

1.2 Goedkeuring

Versie	Datum goedkeuring	Naam	Functie	Paraaf
1.0	07-01-2019	Farley Silvano	Teamleider ICT	
1.1				
2025	15-12-2024	Arjen Dekker	Hoofd ICT	

Inhoudsopgave

2 Inleiding

2.1 Doel van het document

Deze specificatie is opgesteld als kader voor applicaties die in de SSO CN/ICT datacenters moeten "landen". Afnemers van SSO CN/ICT datacenter diensten dienen dit kader te hanteren.
Applicaties dienen niet alleen aan technische eisen te voldoen, maar ook aan eisen die voortkomen uit Architectuur en Informatiebeveiliging, hetgeen in een volgende versie van dit document wordt opgepakt.
Het document was redelijk gedateerd. In december 2024 is het met name op technisch vlak up-to-date gebracht. In een volgend stadium wordt het document herschreven, waarschijnlijk vanuit het CIO Office.

Onder afnemers wordt verstaan: Verzorgingsgebied (Klanten), Leveranciers van software en hardware, Projecten en Afdelingen van SSO CN/ICT die onderling diensten afnemen.

Het document heeft onderstaande doelen:

- Toelichten en scherpstellen van relevante begrippen.
- Informatiebron voor (potentiële) afnemers over de inrichting van de ICT-infrastructuur.
- Kwaliteitscontrole tijdens en na oplevering aan de beheerorganisatie.

2.2 Opbouw van dit document

De eerste hoofdstukken van dit document zijn gewijd aan het definiëren en verklaren van de gebruikte begrippen. Vervolgens worden de begrippen toepasbaar gemaakt voor de gewenste situatie.

3 Introductie

SSO CN/ICT ziet het niet alleen 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 en veilig als mogelijk in te richten.

Voor het bereiken van die efficiency – en daarmee een zo laag mogelijke kostprijs - probeert SSO CN/ICT schaalvoordelen te benutten. Dat kan onder meer door (het beheer van) de technische infrastructuur te centraliseren, te standaardiseren en te consolideren. Deze efficiencyslag is niet alleen uit te voeren bij de zogenaamde generieke systemen (standaard producten), maar ook bij de specifieke systemen (maatwerk), die immers doorgaans wel uit generieke componenten oftewel bouwstenen zijn opgebouwd[1]. Bij standaardisatie en consolidatie moet ook worden gedacht aan protocollen, programmeertalen en diensten van derden.

De kosten voor het technisch beheer van een specifiek systeem worden bepaald door de hoeveelheid bouwstenen die voor deze benodigd zijn. Bijvoorbeeld, een systeem dat gebruik maakt van dure componenten zoals een serverplatform, een database, een web voorziening en twee verschillende client applicaties, zal duurder zijn dan een eenvoudige webapplicatie.

SSO CN/ICT zal zich inzetten om bouwstenen te realiseren waarbij een optimale afweging wordt gemaakt met betrekking tot kosten, kwaliteit, veiligheid en generieke toepasbaarheid.

[1] Bij bouwstenen van ICT systemen moet worden gedacht aan: hardware platform, besturingssysteem, databasemanagement, email dienst, DMZ, opslagcapaciteit, clientdistributie etc.

4 Datacenter

4.1 Datacenter configuratie

SSO CN/ICT heeft de beschikking over twee datacentra, te weten DAC en FTV.
De hosting van de (bedrijfs)applicaties vindt plaats in deze datacentra en is ten aanzien van opslag en rekencapaciteit 100% redundant ingericht.

4.2 Begrippen

4.2.1 Patroon

Een patroon beschrijft hoe een aantal bouwblokken samen een bepaalde functionaliteit leveren. Patronen hebben tot doel om gelijksoortige functionaliteit op eenzelfde manier te realiseren. Dit vereenvoudigt beheer.

In het kader van dit document wordt patroon gebruikt voor de configuratie van bouwblokken, maatregelen en ontwerprichtlijnen die het tezamen mogelijk maken dat applicaties kunnen landen in het Datacenter.

4.2.2 Omgeving

De term "Omgeving" wordt meestal gebruikt in de context van OTAP omgeving (Ontwikkel, Test, Acceptatie en Productie). Functioneel gezien is een omgeving een verzameling systemen met een bepaalde classificatie.
Omgevingen kunnen alleen services van elkaar gebruiken als zij eenzelfde classificatie hebben. Voorbeeld: Productie-werkplekken kunnen alleen met Productiesystemen communiceren.

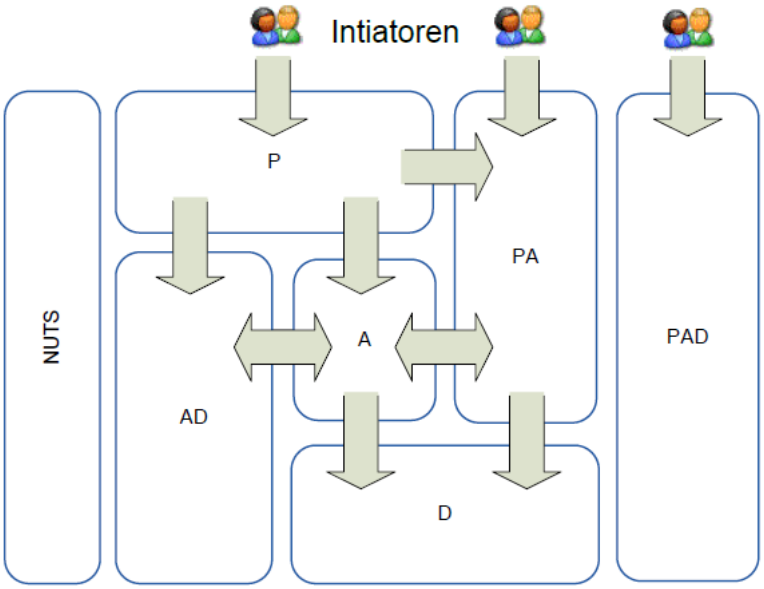
4.2.3 Applicatie Tiers

Met "Tiering" wordt bedoeld de manier waarop een systeem over servers is verdeeld. Tiering is van belang voor de schaalbaarheid en beheerbaarheid van systemen. Tiering heeft ook een relatie met mogelijkheden die er zijn om een systeem te verdelen over verschillende netwerk compartimenten. "Tiers" die van belang zijn voor de indeling in compartimenten zijn:

- Presentatie – de interface van een applicatie naar de afnemers;
- Applicatie – waar de logica van een systeem zich bevindt;
- Data – waar opslaan van informatie plaatsvindt.

4.2.4 Compartimenten

Omgevingen bestaan uit Compartimenten. Een compartiment is een 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 en Data. Compartimenteren is een technische maatregel om aan beveiligingscriteria te kunnen voldoen.



De functies “Presentatie”, ”Applicatie” en “Data” worden onderscheiden. Echter systemen zijn niet altijd zo gemakkelijk op te knippen. De gecombineerde rollen “Presentatie/Applicatie”, “Applicatie/Data” en “Presentatie/Applicatie/Data” komen ook voor. Verkeerstromen tussen compartimenten is mogelijk onder de voorwaarde dat deze “eenrichtingsverkeer” zijn van een van de “P” compartimenten naar een van de “D” compartimenten.
Voor applicaties is de functie van een systeem of server maatgevend voor het compartiment waar het in landt. Dit in tegenstelling tot de software die gebruikt wordt. Database software wat geen of alleen tijdelijk (bijv. data queues of caching gedurende dataverwerking) informatie bevat ter ondersteuning aan de applicatie logica hoort niet in een datacompartiment thuis.

4.2.5 DMZ

De DMZ of (ge)Demilitariseerde Zone is het “niemandsland” tussen on- of semi-vertrouwde verbindingen en het beschermde interne netwerk.

Een DMZ heeft eenzelfde opbouw in omgevingen en compartimenten als het interne netwerk, echter de systemen die er staan hebben andere (lagere) vertrouwelijkheidsniveaus. Met eenzelfde opbouw wordt bereikt dat applicaties op eenzelfde wijze kunnen worden gecompartimenteerd, ongeacht of een deel ervan in de DMZ staat.

4.2.6 Vertrouwelijkheid

Informatie is geclassificeerd in een aantal categorieën (labels) om aan te kunnen geven hoe met de vertrouwelijke gegevens omgegaan mag worden. Deze regelgeving heeft zowel betrekking op wat personen met de informatie mogen doen, als op hoe de systemen waar de informatie op wordt verwerkt geplaatst, beveiligd en ingericht.
Er zijn verschillende categorieën, waarvan de belangrijkste zijn “Staatsgeheim” ook wel afgekort STG-G en “Departementaal vertrouwelijk” afgekort Dep-V.

Het SSO CN ICT /Datacenter biedt standaard dienstverlening tot en met Departementaal Vertrouwelijkheid (Dep-V)

5 Hosting

5.1 Introductie

SSO CN/ICT biedt klanten een TAP omgeving (Test, Acceptatie en Productie) aan. De applicaties van klanten worden 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, etc.

Omgeving	Functie	Beheer
Productie	Release in beheer nemen Wijzigingen doorvoeren	SSO CN/ICT
Acceptatie	Release vrijgeven voor productie Gebruikers Acceptatie Testen	SSO CN/ICT
Test	Release vrijgeven voor Acceptatie Technische test (POC)	SSO CN/ICT

5.2 Server besturingssysteem

De applicatie moet om kunnen gaan met een up-to-date Server besturingssysteem plus software Het installeren van Security en functionele updates voor het OS en software mag geen verstoringen aan de applicatie geven.

Platform	SYSTEEM	Versie	Status	Beheer
Server besturingssysteem	Windows Server	2012 R2 (64 bits)	Verouderd	SSO CN/ICT
	Windows Server	2016	Productie	SSO CN/ICT
	Windows Server	2019	Productie	SSO CN/ICT
	Windows Server	2022	Productie	SSO CN/ICT

5.3 Server Virtualisatie

Alle nieuwe servers worden virtueel gerealiseerd, tenzij specifieke omstandigheden dit verhinderen.

Het virtualisatieplatform zorgt voor een laag tussen de fysieke hardware en het besturingssysteem. 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. Het zorgt voor een bundeling van onderliggende hardware resources 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 failover mogelijkheden.

Platform	SYSTEEM	Versie	Status	Toelichting
Virtualisatieplatform	VMWare vSphere	8	Productie	

5.4 Database

Platform	SYSTEEM	Versie	Status	Toelichting
Microsoft Windows	MSSQL	2016	Productie	In cluster

5.5 Web Servers

Platform	SYSTEEM	Versie	Status	Toelichting
Windows	Internet Information Services	8.5	Productie	
	Internet Information Services	10	Productie	
	Apache Tomcat	9	Productie	

5.6 Storage en back-up

Het bouwblok storage en backup definieert de functionele eisen met betrekking tot het opslaan van centrale gegevens (storage) en de reserve kopieën (back-up) van deze gegevens ten behoeve van het veilig stellen van gegevens tegen het verlies van gegevens als gevolg van storingen, fouten, security incidenten of andere calamiteiten.

De storage en backup bouwsteen voorziet niet in een archieffunctie van gegevens om bijvoorbeeld aan bewaarplichten te voldoen. Daar moet de applicatie zelf in voorzien. De archief functie binnen de applicatie kan dan wel gebruik maken van de storage en back-up bouwstenen.

5.6.1 Implementatie Storage

SSO CN/ICT heeft een storage oplossing welke een Block based opslag via een FC netwerk. Deze opslag wordt door de Virtualisatie omgeving gebruikt voor het hosten van de Virtuele servers.

5.6.2 Implementatie back-up

Backups worden periodiek gemaakt en dienen vervolgens voor een bepaalde termijn bewaard te worden..

Frequentie	Type	Bewaartermijn
Dagelijks	Incremental	2 weken
Wekeliijks	Full	4 weken
Maandelijks	Full	1 jaar

Backups worden ter beveiliging bewaard volgens het WORM principe (Write Only Read Many)

5.7 Loadbalancing, Proxy, Reverse Proxy, SSL Off-loading

F5 Big-IP

De Big-IP van F5 is een ADC (Application Delivery Controller) en geeft ons de mogelijkheid om netwerkverkeer te controleren, door het netwerkverkeer inzichtelijk te maken (proxy), te inspecteren, versleutelen en ontsleutelen en te verdelen. Met de Big-IP zorgen wij ervoor dat onze applicaties en (web) servers altijd en overal beschikbaar en beveiligd zijn.

Loadbalancing

De F5 Big-IP Load Balancer vervult de functie van Reverse Proxy en het verdelen van verkeer over de (applicatie- of web) server. Met een Load Balancer wordt de werklast verdeelt over meerdere servers. Door servers toe te voegen in een pool is schaalbaarheid mogelijk. Een ander grote voordeel is om serverbeheer uit te voeren zonder onderbreking van de dienstverlening.

Proxy

Proxy functionaliteit wordt ingezet waar volgens de BIO er sprake is van een koppelvlak tussen zones met een verschillend vertrouwelijkheidsniveau en waar als gevolg daarvan sessie ontkoppeling een eis is.

SSL Off-loading

Middels SSL Off-loading op de Big-IP Loadbalancers wordt de veiligheid van de (applicatie- of web) server gewaarborgd en worden de achterliggende servers ontlast van het encrypten en decrypten van het verkeer.

Service	SYSTEEM	Versie	Status	Toelichting
Load balancing	Big IP F5		Productie	
(Reverse) Proxy	Big IP F5		Productie	
SSL Off-loading	Big IP F5		Productie	

5.8 Directory 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	SYSTEEM	Versie	Status	Toelichting
Directory Services	Microsoft Active Directory	2012R2	Productie	
	Microsoft Active Directory	2016	Productie	RSC-BES.NL
	Microsoft Active Directory	2022	Productie	FRD.BENET.NL

5.9 OS Hardening

Servers worden gehard conform het hiertoe opgestelde hardeningsbeleid. Dit betekent tevens dat bij oplevering systemen security updates en patches zijn geïnstalleerd binnen de periode die is overeengekomen conform het vigerende beveiligingsbeleid.
Lokale firewalls, zoals die deel uitmaken van de meeste OS distributies (Windows Firewall), zullen gebruikt worden om functies ontoegankelijk te maken, maar andere methodes zoals het uitschakelen van services en listeners op netwerkpoorten zijn ook acceptabel.

5.10 Technische Standaarden

SSO CN/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 Forum Standaardisatie: https://www.forumstandaardisatie.nl/lijst-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.

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	1.2	Aanbevolen	
Publicatie	Digitale Toegankelijkheid	2.0	Verplicht	

Beveiliging	Standaard	Versie	Status	Toelichting
Transport	TLS	1.2	Verplicht	Indien v1.3 niet beschikbaar
Transport	TLS	1.3	Verplicht	

Beveiliging	Standaard	Versie	Status	Toelichting
Authenticatie	Kerberos		Productie	Voor Windows systemen
Authenticatie	Entra ID EA		Productie	Voor SaaS en Virtual applicances
Authenticatie	ADFS		Verouderd	Wordt uitgefaseerd

Voor de interne Windows omgeving bieden we Kerberos als standaard aan.
Voor connectie met externe systemen (lees SaaS) of niet-Windows systemen (Virtual Appliances) is er federatieve SSO mogelijk via Entra Enterprise Applications (SAML, OAuth of OPenID).

6 Werkomgeving

SSO CN/ICT levert als ICT-dienstverlener aan gebruikers werkplekfunctionaliteit. De werkplek duidt de combinatie bureau, scherm en toegangsdevice aan in een rijkskantoor. Als we spreken over de aangeboden functionaliteit dan spreken we over de werkomgeving.

De details over de dienstverlening als leverancier van de werkomgeving staan omschreven in de Producten- en Diensten Catalogus (PDC). De hieronder opgenomen specificaties dienen als referentie voor applicaties die een relatie hebben met de werkomgeving.

6.1 Account

Met een werkomgeving account (gebruikersaccount) krijgt de gebruiker toegang tot de volgende basisfunctionaliteit.

- Digitale Identiteit (Account) die toegang verschaft tot een bedrijfsnetwerk
- Persoonsafhankelijke toegangsverlening tot generieke en gemeenschappelijke toepassingen en specifieke bedrijfstoepassingen
- Optioneel: Externe Toegang tot de werkomgeving in combinatie met een mobiel toegangsdevice en token.

Service	SYSTEEM	Versie	Status	Toelichting
User Account	Active Directory User Account PWD	-	Productie	
Token SW	Account plus Fortitoken	-	Productie	

6.2 Toegang

Een werkomgeving is toegankelijk met een toegangsdevice in combinatie met een account. Toegang is standaard mogelijk vanaf een toegangsdevice in een rijkskantoor, of extern vanaf een RCN toegangsdevice, in combinatie met account met een token.

Service	SYSTEEM	Versie	Status	Toelichting
Interne toegang		-	Productie	
Telewerken	Account plus Fortitoken	-	Productie	Alleen voor managed laptops

6.3 Werkomgeving besturingssysteem

OS	Type	Versie	Status	Toelichting
Windows 10	64 bits		Productie	

6.4 Werkomgeving applicaties

De werkomgeving wordt voorzien van een aantal standaard applicaties en dit is uitbreidbaar met niet-standaard applicaties. Voor beide categorieën wordt verwezen naar de bijlagen in de Producten- en Diensten Catalogus (PDC).

6.5 Software distributie

Het image wat gebruikt wordt bij de uitrol van Windows 10 inclusief bijbehorende applicaties en stuurprogramma's voor de hardware wordt modulair opgebouwd.
Dit houdt in dat de installatie van een werkplek is opgebouwd uit diverse stappen.
Als er nieuwe software en/of hardware uit komt is, dan hoeft er geen nieuw image gemaakt te worden, maar kan er een stap gewijzigd en/of toegevoegd worden aan de bestaande uitrol.
De impact op de uitrol van nieuwe systemen is minimaal en het risico op fouten wordt daardoor beperkt.

Het applicatielandschap is opgebouwd uit twee verschillende lagen: Basis en Basis+.
Basis applicaties zijn standaard op alle werkplekken beschikbaar.
Basis+ applicaties zijn beschikbaar op aanvraag, eventueel i.c.m. een licentie.
Het uitgangspunt is dat applicaties worden aangeboden middels App-V.

App-V (Applicatie Virtualisatie) houdt in dat een applicatie niet lokaal geïnstalleerd wordt op een werkplek, maar dat de applicatie in een virtuele omgeving (bubbel) beschikbaar wordt gesteld op de werkplek.
Dit zorgt ervoor dat een werkplek geen last heeft van "vervuiling" van verschillende applicaties en de updates hiervan alsmede eventuele compatibiliteit issues.

In het geval dat applicaties niet compatible zijn met App-V kan er bij uitzondering gekozen worden voor een lokale installatie.

6.6 Technische aansluitvoorwaarden SSO CN / ICT werkomgeving

Algemeen

1.	Een applicatie krijgt minimale rechten op de werkplek om te kunnen functioneren voor de eindgebruiker, verhoogde of systeemrechten (administrator) rechten zijn derhalve niet toegestaan.
2.	Tijdelijke bestanden die nodig zijn voor het functioneren van een applicatie (logging, cache etc) worden in bekende standaard folders weggeschreven (%temp%). Applicaties moeten voldoen aan de Microsoft ontwikkelstandaarden
3.	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.
4.	Applicatiebestanden die nodig zijn voor het functioneren van de applicatie (.EXE, .DLL) moeten zijn ondertekend met een geldig certificaat van de leverancier.
5.	Het benaderen van een applicatieserver gebeurt altijd op basis van een FQDN DNS naam, gebruik van harde verwijzingen naar IP adressen is niet toegestaan.
6.	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. Verder vindt geen activering/licentiecheck via internet of "de cloud" plaats.
7.	Applicatie instellingen zijn op gebruikersniveau in te regelen. Applicatie instellingen zijn niet actief wanneer de ingelogde gebruiker geen rechten heeft op de betreffende applicatie.
8.	Wanneer een applicatie een verbinding nodig heeft naar het internet moet het internetverkeer via een proxy kunnen worden afgehandeld. Authenticatie gebeurt op basis van de huidige ingelogde gebruikers credentials.

Servers

9.	Applicaties mogen niet onnodig en niet langer dan noodzakelijk onder een systeemaccount (een privileged user zoals administrator of root) draaien. Direct na het uitvoeren van handelingen waar hogere rechten voor nodig zijn, wordt weer teruggeschakeld naar het niveau van een gewone gebruiker (een unprivileged user);

10.	Servers worden zodanig ingericht dat gebruikers alleen toegang hebben tot toepassingen en geen toegang kunnen krijgen tot het besturingssysteem en data;
11.	Servers voor opslag zijn ingericht volgens het 'deny all except'-principe. Dit betekent dat toegang tot bestanden en informatie alleen wordt verleend als een toegangsregel dit expliciet toestaat;
12.	Services, websites en webapplicatie draaien onder een service account. Dit is standaard een domein account
13.	Data van (bedrijfs-)applicatie dient gescheiden te zijn van data van het besturingssysteem.

Database

14.	Gebruikers mogen niet beschikken over database-accounts.
15.	Databasemanagementsysteem dienen zodanig te zijn geconfigureerd dat gebruikers in databasemanagementsysteem opgenomen databases c.q. informatieverzamelingen alleen via applicatiefuncties kunnen benaderen, niet rechtstreeks m.b.v. cliënt software.
16.	Het zou niet mogelijk kunnen zijn om rechtstreeks queries op productiedatabases uit te voeren via Query Analyzer of SQL-plus of andere, vergelijkbare tools om de functionaliteit van een applicatie te onderhouden. Daar moet de applicatie zelf te allen tijde in voorzien.
17.	Database moet te migreren zijn naar een hogere versie van het platform.
18.	Databases die in het beheer van SSO CN / ICT zijn worden, ter ontwikkeling, troubleshoot of anders NIET naar de software leverancier opgestuurd
19.	Beheerwerkzaamheden op databases, datawarehouses en servers worden alleen uitgevoerd door SSO CN /ICT.
20.	Het gebruik van de user 'SA' (system administrator), of SQL Servergebruikers met rollen zoals sysadm, setupadmin, diskadmin etc door applicaties is niet toegestaan
21.	Authorisatie vindt plaats via Active Directory groepen. Users, dbo, db_accesadmin, db_backupoperator, db_securityadminen, db_ddladmin mogen geen sysadminrechten hebben(SA) of SA zijn.
22.	Database moet van shared hosting gebruik kunnen maken

Life Cycle Management en Ondersteuning

23.	Voor applicaties moet door de leverancier actief life cycle management en patch management (security fixes) worden uitgevoerd en ondersteund.
24.	Applicatie ondersteuning voor een volgende release van Windows Server moet worden geleverd door leverancier/ ontwikkelaar van de applicatie
25.	Applicatie ondersteuning voor een volgende release van Windows Desktop moet worden geleverd door leverancier/ ontwikkelaar van de applicatie
26.	Applicatie ondersteuning voor een volgende release van Windows SQL Server moet worden geleverd door leverancier/ ontwikkelaar van de applicatie

Distributie van applicatie

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

Webbrowser

28.	Op de werkplek worden Internet Explorer en Frontmotion Firefox als standaard browsers aangeboden. Eenapplicatie moet functioneren met minimaal één van deze browsers.

29.	Het gebruik van IE browser extensions en plugins moet zoveel mogelijk worden beperkt. Indien een invoegtoepassing (Active-X plugin) wordt gebruikt moet deze ondersteund zijn met de Enhanced Protected Mode. Dit betekent dat de plugin zowel 32- als 64 bits architectuur moet ondersteunen.
30.	Het gebruik van de Mozilla Firefox extensions en plugins moet worden beperkt op basis van WebExtensions-API's en “Ask to Activate”.

Office integratie

31.	Indien een applicatie een integratie met Office componenten heeft (b.v. VBA / Macro) moeten deze zijn ondertekend door een geldig certificaat (Code Signing) van een vertrouwde certificeringsinstantie.
32.	Voor het gebruik van certificaten wordt gebruik gemaakt van een vertrouwde certificeringsinstantie.

7 Applicatie Architectuur

1.	Applicatie dient een audit trail bevatten. Dit om te allen tijde te kunnen zien welke aanpassingen door welke gebruiker zijn uitgevoerd. Deze audit trail moet via de applicatie bekeken kunnen worden.
2.	Wachtwoorden mogen alleen encrypted in de configuratie voorkomen. Het heeft de voorkeur gebruik te maken van Windows Integrated authenticatie waarbij er helemaal geen wachtwoorden in de configuratie hoeven voor te komen