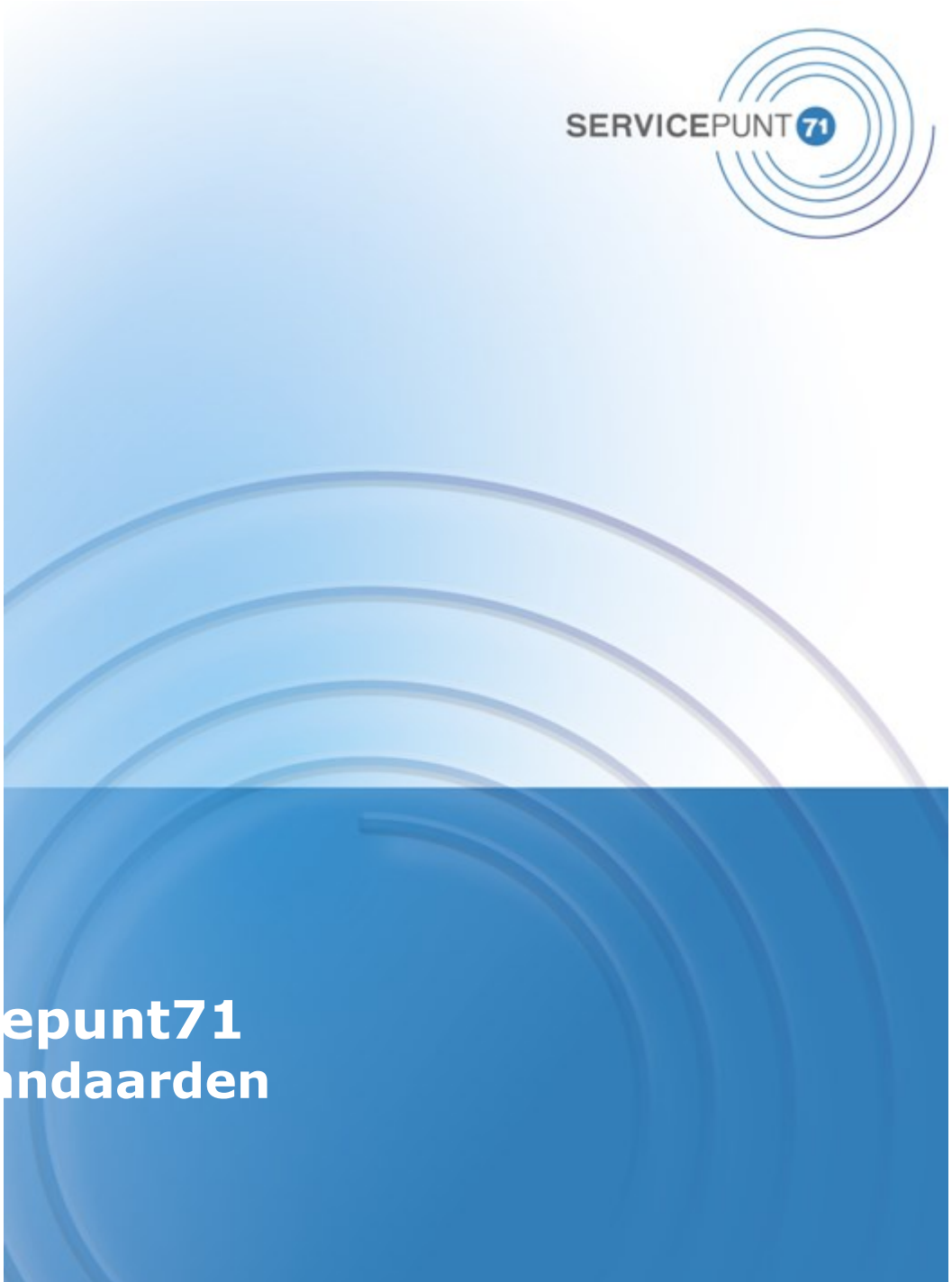
eerd naar S.



epunt71
ndaarden

Auteur: Servicepunt 71 Team Infra

Onderwerp: Standaarden ICT - Servicepunt71

Aantal pagina's: 62

Datum: 15 augustus 2017

Versie: 3.20

Verklarende woordenlijst

De terminologie in de ICT-branche is niet altijd eenduidig, daarom is hieronder een woordenlijst opgenomen.

Begrip	Omschrijving
Beheerbaarheid	De mate van een systeem om deze in operationele staat te brengen en te houden.
Beheersbaarheid	Het in toom houden van een systeem, de mogelijkheid om het geheel te kunnen overzien.
Besturingssysteem	Het operating system van een device waarop alle applicaties draaien.
Calamiteit	Een gebeurtenis die een service of systeem zodanig verstoort dat veelal aanzienlijke maatregelen moeten worden genomen (een uitwijk) om het originele werkingsniveau te herstellen.
Failover	Het overschakelen naar een redundant of stand-by omgeving.
Image	Een template waarmee een device voorzien kan worden van een operating system en optioneel een set van applicaties.
Infrastructuur	Het geheel van IT componenten die de basis vormt waarop de (business)applicaties draaien, zoals netwerk, storage en computersystemen.
Patchlevel	De versie van een systeem inclusief systeemonderdelen na het uitrollen van patches.
Principe	Een fundamentele waarde of stelling dat dient als basis voor een systeem.
RPO	Het recovery point objective definieert de hoeveelheid dataverlies die acceptabel is. Het is het tijdstip waarvan data moet worden hersteld, bekeken vanaf het tijdstip dat data niet meer beschikbaar is.
RTO	De recovery time objective definieert de tijd die nodig is om systeem functionaliteit te herstellen.
Service window	Periode waarin onderhoudswerkzaamheden uitgevoerd kunnen worden.
Slipstreamen	Het offline bijwerken van een image met driver(s) of update(s).

Inhoudsopgave

Hoofdstuk 1 Inleiding

1.1 Aanleiding

De exploitatie en het beheer van de Informatie en Communicatie Technologie (ICT)-infrastructuur van de deelnemende gemeenten en van het Servicepunt71 zelf, zijn van bedrijf kritische aard. De primaire dienstverlening aan de burger en het ondersteunen van de bedrijfsprocessen binnen de gemeenten zijn ondenkbaar zonder de beschikbaarheid van ICT- middelen. Daarom dient de beschikbaarheid van deze middelen te zijn gewaarborgd. De service eenheid ICT is hiervoor verantwoordelijk.

Om de informatiserings- en automatiseringstaak voor de gemeentelijke organisaties adequaat te kunnen uitvoeren heeft de service eenheid ICT standaarden opgesteld voor de ICT-infrastructuur. Deze omvatten de te hanteren standaarden voor technische oplossingen, waarbij hardware en software wordt gebruikt. Het doel van de ICT-standaarden is, naast het bereiken van een hoge beschikbaarheid en continuïteit van de ICT-dienstverlening, ook het beter in de hand houden van de kosten die de ICT-infrastructuur met zich meebrengt. Daarnaast kunnen de ICT-standaarden bijdragen aan een snellere afhandeling van de aanbesteding en invoering van nieuwe applicaties.

Alle producten en diensten, die de service eenheid ICT van Servicepunt71 kan aanbieden, zijn vastgelegd in de Producten en Diensten Catalogus. De standaarden, die de service eenheid ICT hanteert om de producten en diensten te kunnen realiseren, worden in dit document beschreven.
De snelle ontwikkelingen in het ICT-vakgebied en in de eisen en wensen van de deelnemende gemeenten vereisen dat de standaarden mee-evolueren. De service eenheid ICT zal het document dan ook minimaal twee keer per jaar actualiseren.

1.2 Doelstelling

Het is van groot belang dat de binnen de gemeentelijke organisaties aanwezige apparatuur goed met elkaar kan communiceren. Daarnaast moet onderhoud tegen redelijke kosten kunnen plaatsvinden. Vergaande standaardisatie en regelgeving is een belangrijk middel om dit in de hand te houden. Een belangrijke regel is daarom dat de deelnemende gemeenten alle aanschaf van ICT middelen laten plaatsvinden via de Service eenheid ICT. De Service eenheid ICT mag alleen compatibele en vooraf gekwalificeerde componenten inkopen; deze zijn in de Producten en Diensten Catalogus opgenomen. Dit document is bedoelt als richtlijn voor zowel de klanten die gebruik maken van de diensten die Servicepunt71 levert als ook voor de leveranciers van ICT middelen en diensten.

Hoofdstuk 2 Samenvatting standaarden

Dit hoofdstuk geeft een globaal overzicht van de bij Servicepunt71 gehanteerde standaarden. Voor detailinformatie is raadplegen van de diverse hoofdstukken noodzakelijk.

Hoofdstuk 3 Technische Architectuur Principes

Dit hoofdstuk is een beknopte samenvatting van het document 'MEREL Architectuurprincipes'. Dit document is een product van de Werkgroep Regionale Architectuur, zoals beschreven in het document *MEREL-architectuurvisie 2016-2018.* Dit architectuurproduct is opgesteld als onderdeel van het programma Versterken Regionale I-Samenwerking (VRIS).

De architectuur principes welke relevant zijn voor de in dit document beschreven technische standaarden worden onderstaand beknopt beschreven. De omschrijving (Rationale) is geheel of gedeeltelijk overgenomen, de implicaties niet. **Voor de volledige teksten en informatie dient het originele document geraadpleegd te worden.**

3.1 Gebruik Standaarden

De Leidse regio is geen op zichzelf staand eiland. Dat geldt ook voor onze informatievoorziening. Steeds vaker zijn onze gemeenten onderdeel van organisatie overstijgende ketens. Om het samenwerken binnen deze ketens te vergemakkelijken zijn landelijke of sectorale standaarden ontwikkeld. Wij maken hier gebruik van en wijken alleen af als dat echt niet anders kan.

Standaard 1.	We maken gebruik van standaarden (zie 'MEREL Architectuurprincipes' voor meer informatie.

3.2 Informatiebeveiliging

Informatie moet beschikbaar zijn voor de juiste personen. Veel informatie is openbaar toegankelijk, maar dit geldt niet voor alle informatie. Binnen de werkprocessen van de gemeenten worden ook vertrouwelijke en privacygevoelige gegevens gebruikt. In deze gevallen mag niet iedereen alles weten of gegevens aanpassen. Verder moet informatie beschermd worden tegen ongewenste invloeden van buitenaf. Het bepalen van de benodigde beveiligingsmaatregelen van gegevens en informatie vindt plaats aan de hand van dataclassificatie en risicoanalyse. Hiervoor wordt gebruik gemaakt van de richtlijnen vanuit de IBD (Informatie Beveiligingsdienst).

Standaard 2.	Onze informatie is adequaat beveiligd.

3.3 Hergebruik

Vooral in verband met de kosten als met de beheerlast willen we het aantal applicaties in de regio binnen de perken houden. Als het gaat om onze informatievoorziening kiezen we niet langer voor 'probleempje-systeempje', maar maken we gebruik van landelijk gedefinieerde standaard generieke componenten. We verwachten ook van de markt dat ze zich naar deze standaarden voegt.
Als regio kiezen we voor gezamenlijke oplossingen die we op eenzelfde manier gebruiken. Dubbelingen in functionaliteit worden voorkomen. Reeds aanwezige functionaliteit wordt hergebruikt mits deze past binnen de architectuurkaders. Bij de gezamenlijke inkoop kiezen we altijd eerst voor standaardpakketten voordat we maatwerk laten ontwikkelen. Maatwerk leidt altijd tot hogere kosten en vraagt meer werk rond onderhoud en beheer. Standaardpakketten worden om dezelfde redenen in principe niet aangepast. Dit alles moet leiden tot lagere TCO in de regio.

Standaard 3.	We gebruiken standaard generieke informatiesystemen die we gezamenlijk aanschaffen en beheren.

3.4 Goed beheerbare ICT-oplossingen

Bij het ontwerpen, aanschaffen en inrichten van ICT-oplossingen houden we er vanaf het begin rekening mee dat de oplossingen ook onderhouden en beheerd moet worden. Bekeken over de gehele levensduur van een oplossing vormt het beheer uiteindelijk het grootste deel van de kosten. Het is dus zaak om het onderhouden en beheren van een systeem niet nodeloos ingewikkeld te maken. Dit leidt uiteindelijk tot lagere beheerkosten en een hogere gebruikerstevredenheid.
We zorgen er ook voor dat de medewerkers die het systeem gaan onderhouden en beheren tijdig betrokken worden en voldoende kennis en ervaring kunnen opdoen.

Standaard 4.	We gebruiken alleen goed te beheren ICT-oplossingen.

3.5 Toegang tot informatievoorziening

Medewerkers willen op allerlei momenten, plaatsen en manieren toegang kunnen krijgen tot de voor hen relevante functionaliteit en informatie. In toenemende mate willen zij daar ook via hun mobiele apparaten toegang tot hebben. Het invullen van deze behoeften zorgt er tevens voor dat de gemeente een aantrekkelijke werkgever is. Het biedt medewerkers meer flexibiliteit in hun werken. Het verhoogt de productiviteit, maakt efficiënter gebruik van gebouwcapaciteit mogelijk en voorkomt onnodig reizen. Het draagt daarmee ook bij aan een meer duurzame gemeente.

Standaard 5.	Applicaties zijn locatie-, tijd- en apparaat onafhankelijk beschikbaar.

3.6 Gemeentelijke gegevens zijn beschikbaar via generieke koppelvlakken

Gegevensuitwisseling tussen interne en externe applicaties dient over gestandaardiseerde koppelvlakken plaats te vinden. We beperken het aantal verschillende typen koppelvlakken. Dit leidt tot eenvoudiger beheer en een verhoging van de informatieveiligheid door beperkte set aan soorten koppelingen. Het gebruik van generieke koppelvlakken voorkomt bovendien te grote afhankelijkheid van leveranciers en leverancier specifieke oplossingen.

Standaard 6.	Gemeentelijke gegevens zijn beschikbaar via generieke koppelvlakken.

3.7 Standaard ICT-infrastructuur

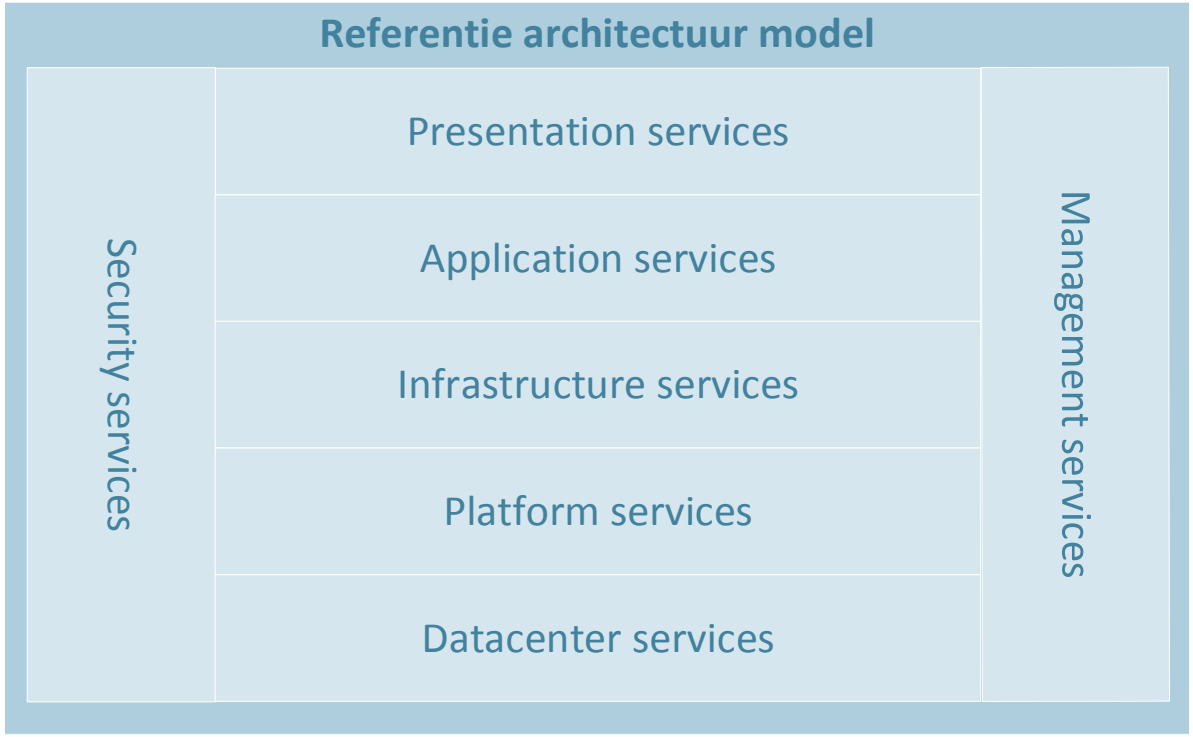
De gemeenten in de regio gebruiken een gezamenlijke ICT-omgeving, onder meer vanwege het kostenvoordeel dat hierdoor mogelijk is. Door de ICT-infrastructuur uniform en gestandaardiseerd in te richten kan dit schaalvoordeel maximaal worden benut. Dit maakt het bovendien eenvoudiger om garanties te geven over serviceniveaus.
Deze gezamenlijke infrastructuur is schaalbaar zodat veranderingen in het aantal deelnemende organisaties en veranderingen in het gebruik binnen deze organisaties eenvoudig opgevangen kunnen worden. Door een schaalbare ICT-infrastructuur in te richten kunnen dit soort ontwikkelingen snel worden ondersteund en worden desinvesteringen zo veel mogelijk voorkomen.
Redundantie in de gemeenschappelijk ICT-infrastructuur voorkomt het stilvallen van bedrijfsprocessen door het voorkomen van uitval in de informatievoorziening. Redundantie is een belangrijk middel om de beschikbaarheid van de infrastructuur te verhogen. Ook gegevensverlies wordt er mee voorkomen.

Standaard 7.	Onze ICT-infrastructuur is gestandaardiseerd, schaalbaar en redundant.

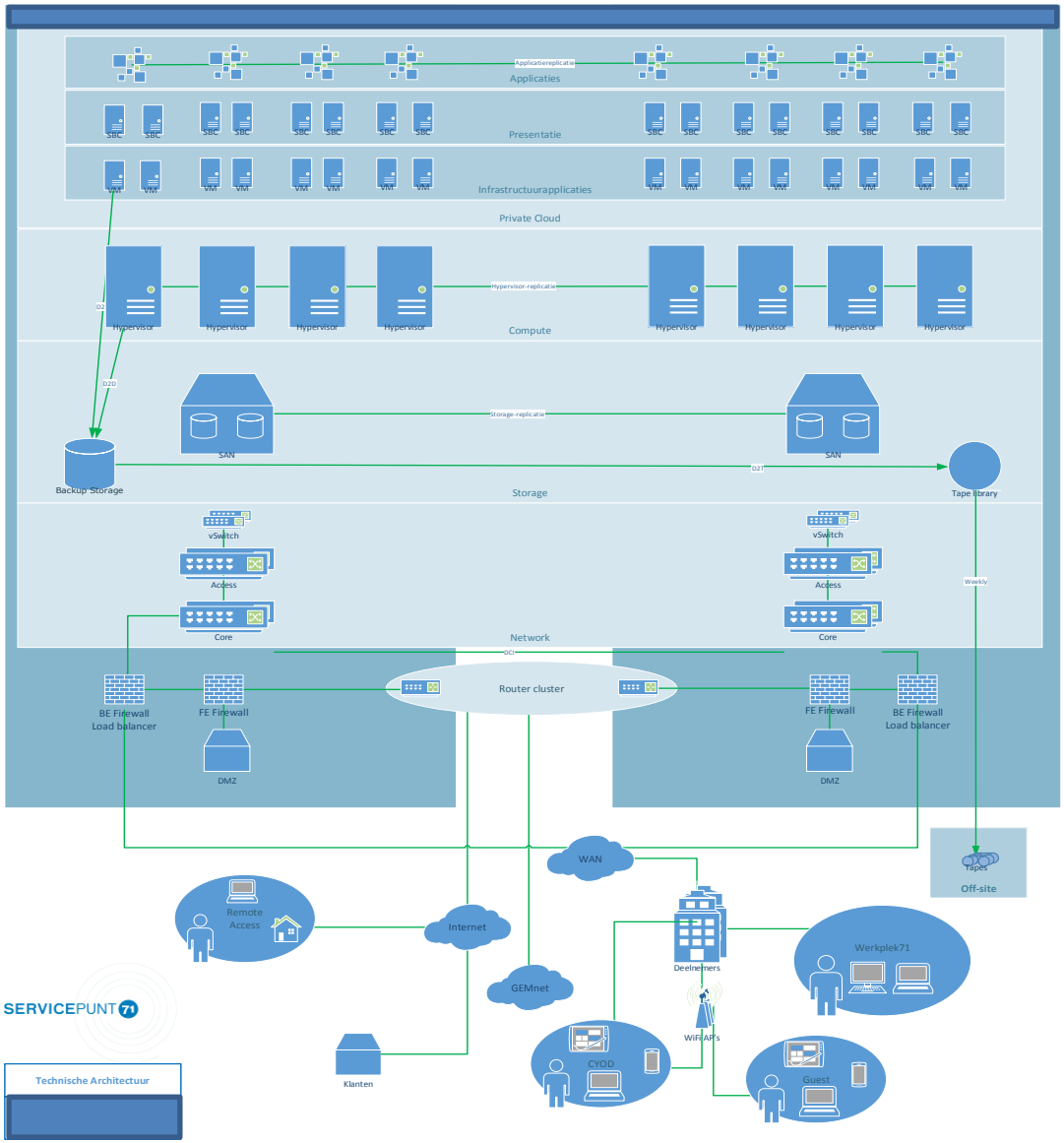
Hoofdstuk 4 Technische infrastructuur

4.1 Referentie architectuur

De technische infrastructuur van het Servicepunt en de deelnemende gemeenten is ingericht met als leidraad een hoge graad van standaardisatie in technische oplossingen om op die wijze een zo hoog mogelijke beschikbaarheid tegen zo laag mogelijke kosten te kunnen bieden. Daarnaast zijn, om een zo hoog mogelijke continuïteit te kunnen garanderen, cruciale componenten uit de infrastructuur dubbel uitgevoerd en op een andere locatie beschikbaar gemaakt. De technische infrastructuur is opgebouwd uit de volgende lagen:



4.2 Blauwdruk technische architectuur



Figuur 1 Blauwdruk Technische Architectuur

Bij deze blauwdruk horen een 50-tal richtlijnen. Deze zijn na te lezen in de technische architectuur.

Hoofdstuk 5 ICT Standaarden

5.1 Naamgevingsconventie

Een eenduidige naamconventie van de systemen en actieve componenten bij het Servicepunt71 is essentieel om de omgeving goed te kunnen beheren. Het voorkomt verwarring en miscommunicatie. Om deze reden zijn alle componenten zoals gebruikers, servers, printers, switches en dergelijke volgens vaststaande afspraken naamgegeven.

Standaard 8.	Voor de naamgeving van alle componenten dient de naamgevingsconventie zoals beschreven in 'Bijlage 1 Naamgevingsconventie' aangehouden te worden.

5.2 Datacenter services

De infrastructuur van het Servicepunt71 heeft een hoge beschikbaarheid nodig. Hiervoor is een twin datacenter gerealiseerd. Dit maakt het mogelijk om uit te wijken van het ene datacenter naar het andere datacenter met minimale risico en beheerinspanning. Hiermee kan de technische infrastructuur hoog beschikbaar worden gemaakt. De Main Equipment Rooms (MER) zijn gesitueerd in twee geografisch gescheiden locaties in de stad. Beide ruimtes zijn voorzien van dubbel uitgevoerde airco units, UPS systeem, noodaggregaat, gasblusinstallatie, toegangscontrole systeem en camerasysteem.

Standaard 9.	Voor eisen rondom de datacenters van Servicepunt 71 dienen de voorschriften zoals weergegeven in 'Bijlage 2 Datacenter Services' aangehouden te worden.

Replicatie

Om een applicatie of dienst hoog beschikbaar te maken over meerdere datacenters zal datareplicatie plaats moeten vinden. Dit kan op twee niveaus. Van hoog naar laag zijn dit:

1. Op applicatieniveau, bijvoorbeeld Active Directory, Exchange DAG, SQL Mirroring, Oracle RAC, etc.;
2. Op hypervisor niveau met behulp van Hyper-V Replica;

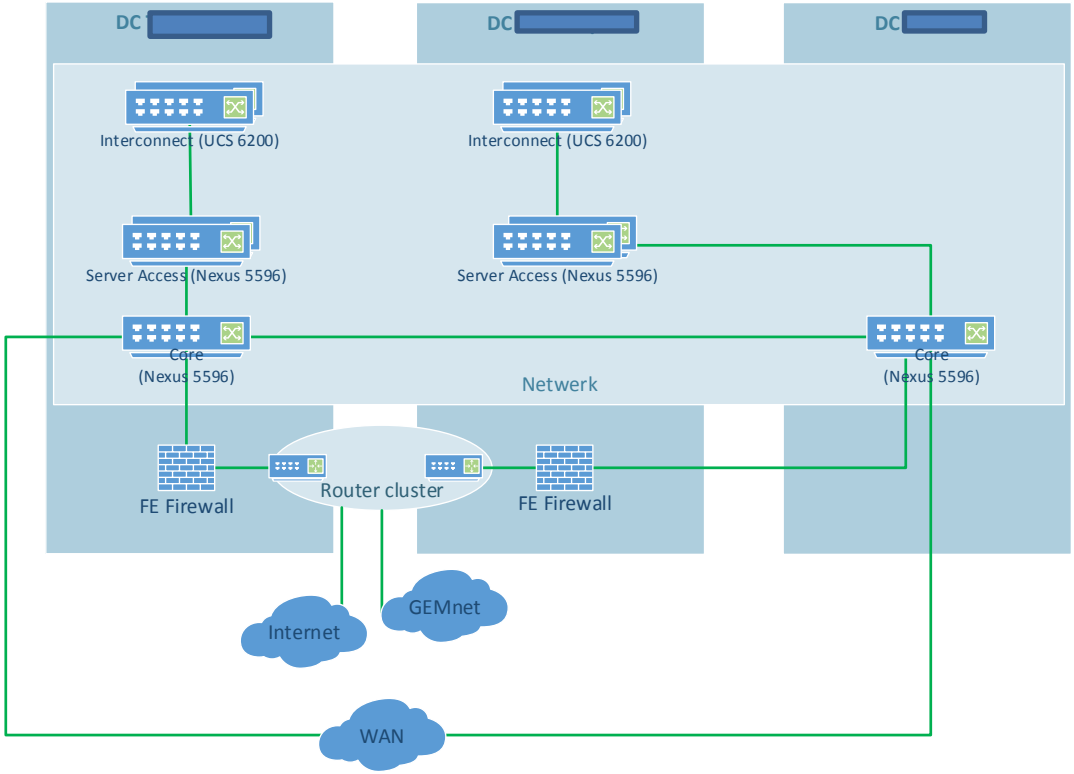
Standaard 10.	Bij het Servicepunt71 wordt alleen gebruik gemaakt van replicatie op applicatie- en hypervisor niveau. In het geval van Hyper-V replicatie geldt een Restore Point Objective (RPO) van 15 minuten. Voor kleiner RPO waarden is replicatie op applicatie niveau noodzakelijk.

5.3 Platform services

Standaard 11.	De platform services zijn gebaseerd op het Cisco/NetApp FlexPod concept met hierop gebruikmaking van servervirtualisatie op basis van Microsoft Hyper-V 2016 en 2012 . Nieuwe componenten moeten in deze infrastructuur passen.

5.3.1 Network

De bestaande zes Cisco Nexus 5596 switches vormen de netwerk core.



Figuur 2 Core network

De deelnemers zijn met de datacenters verbonden door middel van een fiber netwerk of met een site to site VPN op basis van een internetverbinding. Om een beschikbaarheid van 99,5% te realiseren zijn de fiberverbindingen met de datacenters redundant uitgevoerd.

5.3.2 Storage

De storageomgeving is opgebouwd uit twee NetApp SAN controllers per datacenter. Centrale storage wordt vanaf de NetApp's in 2 tiers aangeboden te weten; High Performance Storage en High Capacity storage.

Het ontsluiten van data aan applicaties vindt plaats op basis van het SMB protocol , en door middel van het aanbieden van NTFS volumes en Windows (DFS) Shares.

Backup en restore
Het Servicepunt71 maakt gebruik van Tivoli Storage Manager (TSM). Backups worden met een agent gemaakt op verschillende niveaus:

- Op machine niveau;
- Op database niveau voor Oracle servers;
- Op exchange niveau.

De backup infrastructuur is gebaseerd op de 3-2-1 regel waarbij er drie kopieën zijn van de data op twee verschillende media waarvan één off-site. Doordat de tapes wekelijks off-site worden gehaald ontstaat er geen gap in de dataretentie.

Client systemen worden niet meegenomen in de backup. Dit geldt ook voor serversystemen die niet in beheer zijn bij het Servicepunt71.

5.3.3 Compute

Het FlexPod concept maakt gebruik van Cisco UCS blades.

Standaard Server Operating System

- Het standaard server operating systeem bij Servicepunt71 voor nieuwe servers is Microsoft Windows Server 2016. Centrale Firewall welke is voorzien van scanning en security opties.

Standaard 12.

Daar waar dit niet mogelijk is – door bijvoorbeeld een beperking van applicatiesoftware – zal er door middel van een uitzondering gebruik worden gemaakt van een ander (ouder) server OS. Hierbij wordt gebruik gemaakt van de N-1 regel. Dat wil zeggen dat Windows Server 2008 SP1 nog mogelijk is, maar zonder Service Pack of Server 2008 en lager niet. Tevens zal deze uitzondering op de ICT roadmap worden geplaatst om zo snel mogelijk te worden gemigreerd naar het standaard OS

Server virtualisatie
Vanwege het standaardisatie principe en om complexiteit te verlagen is zal primair gebruik worden gemaakt van server virtualisatie op basis van Microsoft Hyper-V.

5.4 Infrastructure services

- De services die in deze laag beschikbaar zijn, worden via gevirtualiseerde servers aangeboden;
- Elke server is voorzien van beveiligings- en beheer tools. Deze tools worden alleen door Servicepunt71 ICT medewerkers beheerd.

5.4.1 Database Services

Standaard 13.	Er zijn twee typen database server systemen in de infrastructuur opgenomen: Oracle en Microsoft SQL.

- Oracle database versie 12.op Oracle Linux.
- Microsoft SQL database versie 2012 AlwaysOn Cluster.
- Beide database typen zijn hoog beschikbaar.
- Gebruik van Oracle heeft de voorkeur voor applicaties die belangrijke gemeentelijke processen ondersteunen.
- Gebruik van een volledige Oracle client met gebruik van TNSnames heeft de voorkeur ivm HA beschikbaarheid,
  Een connectie string met daarin beide database (productie)servers mag ook.
  Andere database oplossingen, inclusief standalone inrichtingen van Oracle en SQL (Express), worden niet toegestaan.

5.4.2 E-mail Services

Standaard 14.	De e-mail service is gebaseerd op Microsoft Exchange 2010.

- Om een hoge beschikbaarheid van de e-mail voorziening te kunnen garanderen, is deze hoog beschikbaar uitgevoerd in de vorm van een DAG cluster.
- Microsoft Outlook 2010 is de standaard e-mail client.
- Externe toegang wordt geboden met Outlook Web Access en Outlook Mobile Access op mobiele apparaten die dit ondersteunen.
- De Outlook voorziening is onder andere beveiligd met cloud bassed E-mail antivirus/antispam Filter.
- Verkeer tussen clients en mailserver is beveiligd op basis van SSL met behulp van certificaten.
- De mailservers staan geen (open/) relay toe, tenzij specifiek opgenomen

5.4.3 File Services

Standaard 15.	File services is opgebouwd rond het Distributed File System (DFS) van Microsoft, dat via een cluster beschikbaar wordt gemaakt. Shares worden aangeboden op basis van het SMB protocol

5.4.4 Print Services

Standaard 16.	Printfaciliteiten zijn gestandaardiseerd op multifunctionele apparatuur, waarmee men kan kopiëren, printen en scannen, in zwart-wit en kleur;

a.	Waar het follow-me principe is geïnstalleerd, kan gekozen worden om de output op elk willekeurige apparaat uit te printen, dat aangesloten is op het netwerk. De prints kunnen enkel met behulp van de toegangspas of persoonlijke code worden afgedrukt.

5.4.5 Web Service

Standaard 17.	De Webservices zijn gebaseerd op: IIS op basis van Windows Server 2016, Oracle IAS op Linux.

Afhankelijk van de applicatie wordt deze op het desbetreffende platform geïnstalleerd. Er zijn meerdere Webservers op één server omgeving beschikbaar. Op deze wijze kunnen interne Web services onafhankelijk van elkaar gestopt en gestart worden en kunnen er geen conflicten tussen de Web-applicaties optreden. Webservers die diensten aanbieden aan het Internet worden ontsloten via de reverse proxy.

5.4.6 Netwerk Services

De volgende ondersteunende netwerk services zijn geïmplementeerd:
- ADDS 2012 (Active Directory Domain Services);
- DNS (Domain Name Service);
- DHCP (Dynamic Host Configuration Protocol);
- NTP (Network Time Protocol).

- DFS-N
- ADFS 2016
- Azure AD connect

Standaard 18.	De volgende Active Directory services zijn in gebruik: Active Directory Domain Services (ADDS) 2012 , DNS, DHCP, NTP, DFS, ADFS 2016. Het domain functional level is Server 2008 .

Omdat deze services maximaal beschikbaar moeten zijn om het netwerk en de applicaties te kunnen gebruiken, zijn de servers waarop ze draaien hoog beschikbaar gemaakt door middel van replicatie.

5.4.7 Load Balancing

- De loadbalancing voor ADFS, SBC en Exchange wordt verzorgd door Cisco ACE load balancers in High Availability opstelling
- De volgende diensten worden geloadbalanced:

Standaard 19.	Load balancing diensten moeten via de Cisco ACE aangeboden worden. Er wordt geen gebruik gemaakt van Windows NLB.

5.5 Application services

Het applicatielandschap van Servicepunt71 is divers. Er zijn applicaties die beschikbaar moeten zijn voor alle deelnemers en een aantal applicaties zijn specifiek voor een deelnemer. Ook zijn er applicaties die niet geschikt zijn voor de SBC omgeving. Deze zijn beschikbaar gemaakt voor de fat clients.

Standaard 20.	Applicaties worden beschikbaar gesteld via een centrale werkplek omgeving gebaseerd op een Citrix XenApp 7 werkplekomgeving (Microsoft Windows Server 2008).

5.5.1 Applicatie levels

Om het applicatielandschap in te delen zijn de applicaties opgedeeld in de volgende levels:

- Level 0: Kantoorautomatisering (KA) applicaties. Deze zijn voor alle gebruikers beschikbaar op alle werkplekken;
- Level 1: Bedrijfsvoering applicaties. Deze applicaties zijn generiek voor alle deelnemers, maar zijn maar voor een deel van de gebruikers beschikbaar gebaseerd op zijn of haar rol, functie of afdeling;
- Level 2: Vak applicaties. Deze applicaties zijn specifiek voor één deelnemer, maar zijn maar voor een deel van de gebruikers beschikbaar gebaseerd op zijn of haar rol, functie of afdeling;
- Level 3: Special applicaties. Dit zijn bedrijfsvoering applicaties of vak applicaties met een beperking waardoor ze alleen op het fat client platform aangeboden kunnen worden.

Standaard 21.	Applicaties worden gepackaged.

a.	Hierbij is er een voorkeur om dit met behulp van applicatievirtualisatie te doen, hiervoor wordt Microsoft App-V 4. technologie gebruikt;
b.	Distributie van applicaties vindt plaats via RES producten en is een taak van de SE ICT.

5.5.2 Infrastructuurapplicaties

Infrastructuurapplicaties zijn operationeel in de backend infrastructuur. Ze leveren een dienst aan de gebruiker via een KA of Vak applicatie op de client. Dit volgens het client-server model. Bijvoorbeeld de applicatie Exchange levert de dienst e-mail via de client-applicatie Outlook.

5.5.3 Vakinhoudelijke applicaties

Binnen de Service eenheid ICT wordt voortdurend gewerkt aan een groot aantal projecten, die (bijna) altijd leiden tot het in productie nemen van applicaties en de onderliggende infrastructuur of het doorvoeren van wijzigingen daarop. Om dit op een verantwoorde manier te kunnen doen, is het noodzakelijk dat aan een aantal randvoorwaarden wordt voldaan.

Iedere invoering van nieuwe (of sterk gewijzigde) functionaliteit van applicaties en infrastructuur, met uitzondering van updates & patches (herstel van fouten in de bestaande software) moet projectmatig plaatsvinden. Afhankelijk van de impact van een wijziging wordt deze als project of als activiteit uitgevoerd. De Service eenheid ICT zorgt ervoor dat de toepassing beschikbaar is, zodat gebruikers deze kunnen testen en in productie nemen. De functionaliteit van de toepassing is de verantwoordelijkheid van de applicatie-eigenaar en de functioneel beheerder.

Inhoudelijk, functioneel beheer van applicaties is de verantwoordelijkheid van het organisatieonderdeel dat de applicatie aanschaft. Technisch beheer is altijd de verantwoordelijkheid van de Service eenheid ICT. Alvorens een nieuwe (of sterk gewijzigde) applicatie aan het bedrijfsnetwerk kan worden toegevoegd, dient vastgesteld te worden of de software voldoet aan de eisen die de infrastructuur stelt. Als uitgangspunt daarbij gelden de vastgestelde standaarden ICT. Daarnaast worden er ook eisen vanuit beheer gesteld. Om het voor beheer mogelijk te maken een applicatie of een infrastructurele voorziening op een verantwoorde manier in beheer te nemen is het noodzakelijk dat aan deze eisen wordt voldaan. Bij een voorgenomen besluit tot aanschaf van een nieuwe (of sterk gewijzigde) toepassing dient ICT in de gelegenheid te worden gesteld om vast te stellen dat deze aan alle eisen voldoet.

5.6 Presentation services

Standaard 22.	De kern van de presentation services bestaat uit Server Based Computing (SBC) op basis van Citrix XenApp .

a.	Het aanbieden van applicaties gebeurt vanuit een centrale omgeving, waarbij op diverse lagen virtualisatie wordt toegepast;
b.	Het uitgangspunt is dat applicaties getest en geschikt zijn voor een SBC-omgeving;
c.	Voor de afwijkende applicaties wordt een beslisboom gebruikt, waarin wordt aangeven op welke wijze de applicatie het beste aangeboden kan worden;
d.	Als een applicatie niet geschikt is voor SBC, dan beperkt dit het aantal gebruikers dat de applicatie kan gebruiken.

5.6.1 OTAP

Standaard 23.	Voor elke bedrijfstoepassing moet, in principe, een testomgeving beschikbaar zijn. Daarbij wordt de OTAP[1] aanpak gehanteerd, waarbij verschillende activiteiten in gescheiden omgevingen worden uitgevoerd om mogelijke verstoringen van productie en andere test processen te voorkomen.

OTAP beschrijving:

- **Ontwikkel** - omgeving waar software (maatwerk) en inrichtingsmodellen ontwikkeld worden;
- **Test** - omgeving waar vastgesteld wordt of de ontwikkelde software goed functioneert binnen de kaders van de infrastructuur. Specifieke eigenschap van deze omgeving is dat deze zonder verstorende invloeden van andere applicaties en netwerk beschikbaar kan zijn om het technisch testen zo zuiver mogelijk kunnen laten verlopen;
- **Acceptatie** - omgeving waar de functioneel beheerder eventueel samen met een aantal toekomstige gebruikers de goede werking van de applicatie test. Specifieke eigenschap van deze omgeving is dat deze identiek is aan de productie omgeving om het testen zo natuurgetrouw mogelijk te laten zijn;
- **Productie** - omgeving waar de bedrijfsapplicatie hoog beschikbaar is voor de gebruikers.

Aangezien er vrijwel uitsluitend standaard applicaties worden aangeschaft, zullen er geen Ontwikkel- en Testomgevingen nodig zijn, maar volstaat het om naast de Productie-omgeving een Acceptatie-omgeving in te richten, waarbij geprobeerd wordt de productie-omgeving zo goed mogelijk na te bootsen. Doel van de acceptatie-omgeving is, te verzekeren dat een nieuwe of aangepaste applicatie naar behoren functioneert in de standaard infrastructuur en daarmee goed integreert zonder de operationele omgeving te verstoren. Wijzigingen op applicaties worden daarom eerst aangebracht in de acceptatie-omgeving. Deze omgeving biedt de mogelijkheid:

- Voor de gebruikers om de applicatie grondig functioneel te testen zonder de operationele omgeving te verstoren;
- Om fouten in de productie-omgeving te kunnen reproduceren en mogelijke oplossingen te kunnen testen.

5.6.2 De standaard werkplek typen

De standaard werkplek is op Windows gebaseerd. De volgende types zijn in gebruik:

Werkplek type	Hardware	Opmerking
Thin Client	Igel, UD5, model	'Normale' gebruiker
Desktop	Dell Optiplex	Waar applicatievirtualisatie niet mogelijk is.
Laptop	<selectie lopend>	Mobiele toepassingen
Workstation	<selectie lopend>	Zware toepassingen
Surface Tablet	Microsoft Surface Pro	Kleine schaal t.b.v. flexwerk /

[1] Bron: Wikipedia. Ontwikkeling Test Acceptatie en Productie, afgekort OTAP is de naam van een methodiek die wordt gebruikt in de ICT. De hoofdwoorden in de naam geven de fases aan die onder andere in de softwareontwikkeling doorlopen worden. Het Nederlandse begrip is afgeleid van het Engelse DTAP: Development, Testing, Acceptance and Production

		mobiel
Any Device	*<telewerken en toegang>*	*Receiver en token*
Monitor	*Fujitsu B24W5 Eco/-6 LED*	
Keyboard, Mouse	*Fujitsu KB400, M500T*	
Mobiele werkplek	*Surface Pro, Windows 10*	*Mobiele werkplek*

5.6.3 'Any Device'

- Persoonlijke mobiliteit wordt ondersteund met smartphones;
- De persoonlijke (Outlook) gegevens van de gebruiker op de smartphones worden gesynchroniseerd door gebruik te maken van Microsoft Outlook ActiveSync;
- Voor synchronisatie zijn diverse beveiligingspolicies van kracht.

5.6.4 Updates

Voor elk component in een infrastructuur komen updates beschikbaar. De oorzaak voor deze updates zijn zeer divers. Hotfixes, beveiligingslekken en nieuwe functionaliteit zijn hier voorbeelden van. Ook leveranciers komen met adviezen om bepaalde updates te implementeren. Dit omdat de support op een product anders verloopt, om functionaliteit toe te voegen of om fouten in software te repareren.
Vanuit de diverse disciplines wordt verschillend naar deze updates gekeken, zo zal de Security Officer een update die een beveiligingslek dicht zo snel mogelijk in productie willen zetten, terwijl een Service Manager dezelfde update ziet als een risico, omdat deze de beschikbaarheid van de infrastructuur in gevaar kan brengen.

Ook de snelheid waarmee updates geïnstalleerd worden gemaakt is van belang. Een security update moet zo snel mogelijk beschikbaar worden, terwijl minder belangrijke updates minder snel of helemaal niet beschikbaar hoeven te worden gemaakt.

Standaard 24.	Voor elk software component en of ICT dienst moet een updateplan beschikbaar zijn, dat voldoet aan de voorwaarden zoals beschreven in paragraaf 5.6.4.

5.7 Security services

De beveiligingsmaatregelen zijn gebaseerd op de BIG (Baseline Informatiebeveiliging Nederlandse Gemeenten) van de Informatiebeveiligingsdienst (IBD). De BIG is afgeleid uit de ISO normen 27001/27002. De IBD heeft 3 doelen:

1. Het preventief en structureel ondersteunen van gemeenten bij het opbouwen en onderhouden van bewustzijn als het gaat om informatiebeveiliging;
2. Het leveren van integrale coördinatie en concrete ondersteuning op gemeente specifieke aspecten in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging.
3. Het bieden van gerichte projectmatige ondersteuning op deelgebieden om informatiebeveiliging in de praktijk van alle dag naar een hoger plan te tillen.

Standaard 25.	Beveiligingsmaatregelen dienen te voldoen aan de in paragraaf 0 gestelde eisen.

Daar waar relevant zijn specifieke beveiligingsmaatregelen per onderdeel beschreven.

5.7.1 Logische beveiliging applicaties

- Elke gebruiker dient een toepassing onder een eigen gebruikersnaam te benaderen.
- Serviceaccounts krijgen de meest restrictieve rechten die nodig zijn voor de werkzaamheden die het moet verrichten en bijvoorbeeld geen volledige administrator rechten of console login rechten;
- Iedere gebruiker dient met een eigen login in te loggen op de database. Wanneer binnen een applicatie gebruik wordt gemaakt van een netwerk-login, dan dient er binnen de applicatie een autorisatiesysteem aanwezig te zijn en moet het mogelijk zijn een gebruiker te koppelen aan processen binnen de database;
- Als er een eigen autorisatiesysteem binnen de applicatie is en er gebruik wordt gemaakt van één gemeenschappelijke database gebruikersnaam, dan mag deze niet de eigenaar van het schema zijn en of DBA rechten hebben;
- Alle wachtwoorden die worden opgeslagen in de database dienen versleuteld te zijn. Wachtwoorden mogen niet leesbaar in bestanden, scripts of databases worden opgeslagen;
- In een toepassing dient een mogelijkheid opgenomen te zijn om het eigen wachtwoord te vernieuwen;
- In de documentatie dient duidelijk opgenomen te zijn hoe de verschillen in de autorisatie geregeld kunnen worden;
- Er worden geen wachtwoorden gebruikt in scripts e.d.;
- Er mag geen gebruik worden gemaakt van standaard door leveranciers aangeleverde wachtwoorden. Standaard wachtwoorden van leveranciers worden na installatie gewijzigd;
- Er mag alleen bij hoge uitzondering en na goedkeuring door de Service eenheid ICT gebruik worden gemaakt van speciale hardware zoals b.v. een dongle;
- In applicaties ingebouwde functionaliteit, of via een applicatie benaderbare functionaliteit, die potentiële beveiligingsrisico’s met zich mee brengt (bijvoorbeeld toegang tot een command-prompt) kan door de Service eenheid ICT worden geweigerd of uitgeschakeld. Het gebruik en het functioneel beheer van de applicatie moeten zodanig zijn ingericht, dat hiervoor geen bijzondere rechten (zoals SYS ADMIN) noodzakelijk zijn;
- Remote support is alleen toegestaan via een door het Servicepunt ter beschikking gestelde voorziening. De leverancier krijgt de beschikking over een account met de overeengekomen autorisaties. Dit account staat standaard ‘dicht’, maar wordt op verzoek en in overleg met de functioneel beheerder en ICT tijdelijk opengezet;
- Toepassingen die vanuit Internet benaderbaar zijn, worden ontsloten via de ESB Digikoppeling, of door middel van een (door de leverancier te leveren) DMZ koppelvlak. Rechtstreekse toegang vanaf het internet naar de infrastructuur wordt niet toegestaan.

5.7.2 Internettoegang

- Iedere medewerker heeft toegang tot het Internet;
- Het downloaden van uitvoerbare bestanden (exe, plug-ins, ActiveX etc.) is om beveiligingsredenen geblokkeerd;
- Het gebruik van Internet wordt mogelijk gemaakt en beveiligd met een Cloud based Web Filter en Proxy Services.
- De ICT infrastructuur is via een dataverbinding hoog beschikbaar gekoppeld aan Internet;
- Internetdiensten worden ten alle tijden ontsloten door o.m. gebruikmaking van een firewall;
- Er kan gebruik worden gemaakt van specifieke firewall poorten, echter het gebruik van zogenaamde firewall 'ranges' is niet toegestaan;
- Servicepunt 71 maakt gebruik van een beperkt aantal vaste IP adressen voor communicatie van en naar het internet. Een beperkt aantal hiervan zijn gereserveerd voor specifieke doeleinden welke niet kunnen worden gewijzigd.
- Toepassingen die verkeer tussen het Internet en de infrastructuur veroorzaken, bijvoorbeeld in het kader van e-dienstverlening, worden in het DMZ-deel van het netwerk ontsloten richting de infrastructuur via reverse proxy servers en access gateways;
- Directe bestandstoegang van af het internet of vanuit de DMZ zone met interne systemen is niet toegestaan.

In de infrastructuur worden de applicatie- en web diensten aangeboden

- Er mag onder geen beding vertrouwelijke of persoonsdata worden opgeslagen in de DMZ zone of andere opslaglocaties welke direct verbonden zijn met het internet en welke onder beheer van Servicepunt 71 vallen.
- Data uitwisseling van en naar het internet en of naar de DMZ dient bij voorkeur beveiligd te worden op basis van SSL encryptie. Bij het uitwisselen van vertrouwelijke (persoons)informatie is dit een eis.
- Voor koppelingen naar cloudservices als Azure ; AWS ; Office365 wordt gebruik gemaakt van de voor deze diensten als best practise gedefinieerde standaards.

5.7.3 Remote Access / externe gebruikers

- Voor thuiswerkers en gebruikers van andere (semi) overheidsorganisaties of leveranciers is de infrastructuur alleen toegankelijk als het organisatieonderdeel waarmee deze externe organisatie een overeenkomst heeft, instaat voor de integriteit van de betreffende gebruikers.
- Op locaties van andere (semi) overheidsorganisaties wordt de infrastructuur alleen toegankelijk gemaakt voor de door het verantwoordelijke organisatieonderdeel aangewezen personen. Hierbij wordt de verbinding alleen via de door remote access beschikbare beveiligingsmechanismen beschikbaar gesteld.
- Remote access wordt geboden via de Citrix Netscaler, hierbij worden 2-factor authenticatie tokens verstrekt;
- Andere vormen van remote access zijn afhankelijk van de gebruikte toepassing of applicatie. Mogelijke voorbeelden zijn mailsynchronisatie, webdiensten, BYOD en leverancier afhankelijke wensen.
- Koppelingen en of data uitwisseling met derde welke een (semi) permanent karakter hebben kunnen enkel tot stand worden gebracht op basis van een permanent aanwezige IPSec VPN koppeling tussen de infrastructuren van beide organisaties. Deze VPN koppelingen worden getermineerd op de firewall van Servicepunt 71.
- Anti-malware, Webfiltering en Virusscanning

- Voor anti-virus ; anti-malware op servers en FAT clients wordt gebruik gemaakt van McAfee Endpoint security, met als management de centraal opgestelde McAfee ePolicy Orchestrator server .De Anti-virus en anti-Malware modules maken deel uit van de op de clients en servers geplaatste Virusscan Enterprise versie.
- Voor anti-virus ; anti-malware ; en webfiltering op Surface tablets wordt gebruik gemaakt van Panda AD360
- E-mail security en spam filtering op basis van een cloud bassed hosted Email Security,
- Web filtering tevens op basis van een hosted cloud bassed security oplossing
- Centrale Firewall welke is voorzien van aanvullende scanning en security opties.

Bijlage 1 Datacenter services

Koelingsoptimalisatie is toegepast door het creëren van warme- en koude luchtstraten in de ruimte. Kabelgaten in de racks zijn afgedicht door middel van brandstopkussens met als doel het mengen van luchtstromen in de racks te voorkomen. Het servicepunt streeft naar een zo efficiënt mogelijk gebruik van energie. Uitgangspunt hierbij is het OpenDCME model, zie: http://www.opendcme.org.

1.1 Eisen MER ruimtes

Stroomvoorziening op een gescheiden groep met voldoende vermogen (hoofdvoeding). De ruimte is gevoed vanuit UPS via overnamepaneel gekoppeld aan noodstroomaggregaat met automatische inschakel / synchroniseer inrichting. De aggregaat dient minimaal de volgende meldingen te kunnen doorgeven via een GBS systeem of gescheiden telefoonkiezer (gesproken berichten):

- in bedrijf;
- uit bedrijf;
- brandstofpeil;
- storing.

Voor werkzaamheden (stofzuigen en dergelijke) zijn aparte 230V-16A groepen (non-UPS) aanwezig, voorzien van aardlekschakelaar, bedienbaar vanuit de ruimte zelf. Voor apparatuur groepen (UPS) in de ruimte geld minimaal 2 gescheiden groepen per patchkast. De groepverdeling en de hoofd / aardlekschakelaars zijn in aparte kast ondergebracht in de ruimte zelf (subverdeler). De ruimte is voorzien van eigen “schone” aardingsnet. Per kast is een aparte stroomverdeler opgenomen met aardlekschakelaars (automaat) voor de aansluitpunten met maximaal 2 aansluitpunten per schakelaar. Per kast zijn minimaal 4 spanningsverdelers (230V / 16A) aanwezig. De ruimte moet voorzien zijn van dubbele Airco, onderling gekoppeld, voorzien van SNMP/webmodule. Aircosysteem op gescheiden NON-UPS 400V-32A groep (per unit), via verdeler op noodstroomaggregaat gekoppeld. Verder moet de ruimte voorzien zijn van een true-online double conversion driefasen UPS systeem (enkele uitvoering is toegestaan als er een aggregaat aanwezig is), voorzien van SNMP/webmodule. Autonomie voor totale belasting ca. 30 minuten, rekening houdend met toekomstige uitbreiding. Wanden; ondervloer; plafond voorzien van stofbindende coating. De ruimte dient een brandvertraging te hebben van 60 minuten.
Ook is de ruimte voorzien van een gecertificeerde gasblusinstallatie. Het brand-detectiesysteem dient een aspiratietype te zijn.
Het brandmeldsysteem moet gekoppeld te zijn aan een in het gebouw aanwezige hoofd BMC.
De toegang tot de ruimte moet voorzien zijn van degelijk hang en sluitwerk conform BRL3104 of NEN5096 Klasse 2. De deur heeft een sleutelslot en een elektronisch toegangscontrolesysteem met contactloze uitlezer. De ruimte moet een gescheiden zone te zijn op een beveiligingsinstallatie, met een inlooproute van buitenaf.

Indien de ruimte een raampartij bevat, geld het volgende:

- Inbraak vertragende beglazing;
- Warmte werende en inbraak vertragende folie aan binnenzijde (BSS 6206 Klasse B 175 micron);
- Barrièrestangen aan binnenzijde;
- Zonwering, in overeenstemming met de rest van het pand voor het ontnemen aan zicht van buitenaf;
- IR PIR anti-masking detectors (minimaal 2) aangesloten op beveiligingsinstallatie Grade 2 of 3 / NCP 2 of 3;
- Een netwerk gekoppelde IP camera met autorisatie voor monitoring.

Ten aanzien van de patchkasten worden de volgende eisen gesteld:

- 46HE hoog, 800mm breed, en 1000mm diep;
- Moeten voor en achter benaderbaar zijn;
- Zijn voorzien van gaasdeuren;
- Rangeerogen tussen iedere twee switches;
- Rangeerogen tussen ieder paneel;
- Bekabeling minimaal Cat 6a.

Bij nieuwbouw wordt CAT 7 overwegen met inserts. Telefonie en Data wordt gescheiden aangebracht:

- De voorkant data
- De achterkant telefonie voor analoge lijnen.
- Indien VOIP, groene kabels gebruiken voor telefonie; blauw voor data; rood voor management.

1.2 Eisen SER ruimtes

- Ruimte moet voorzien zijn van Airco bij meer dan 5 switches of gekoppeld zijn aan een gebouw luchtbehandeling.
- Patchkasten moeten voor en achter benaderbaar zijn;
- Patchkasten zijn voorzien van gaasdeuren;
- Patchkasten zijn 46HE hoog, 800mm breed, en 1000mm diep;
- 19” frame voorzien van “U aanduiding”;
- 230 V voorziening op een schone aarde (bij nieuwbouw op gescheiden groep);
- Patchkasten zijn geaard, inclusief deuren (aardingseis zie boven);
- Rangeerogen tussen iedere twee switches;
- Rangeerogen tussen ieder paneel;
- Bekabeling minimaal Cat 6a bij nieuwe aanleg ;
- Bekabeling minimaal Cat 5e bij bestaande bekabeling;

Kabelkleuren en toegangseisen worden bepaald door de datacenterbeheerder.

1.3 Bekabeling

De infrastructuur is gebaseerd op het Ethernet protocol. Het is beschikbaar op de verschillende gemeentelijke locaties via 6 Cisco Nexus 5000 switches. WAN verbindingen maken gebruik van single mode glasvezel. Binnen de gebouwen worden SER ruimtes onderling (backbone) verbonden met Multi-mode glasvezel (OM3). De horizontale bekabeling is minimaal Cat-5 UTP bekabeling. Opmerking: bij vervanging en uitbreiding van bekabeling is de toegepaste norm altijd minimaal CAT 6.

De gemeentelijke locaties zijn aan het LAN gekoppeld met:

- Glasvezelverbindingen single mode (dubbel uitgevoerd via gescheiden ringen met standaard vezelverdeling 8 / 4);
- site to site VPN .

Bijlage 2 Platform services

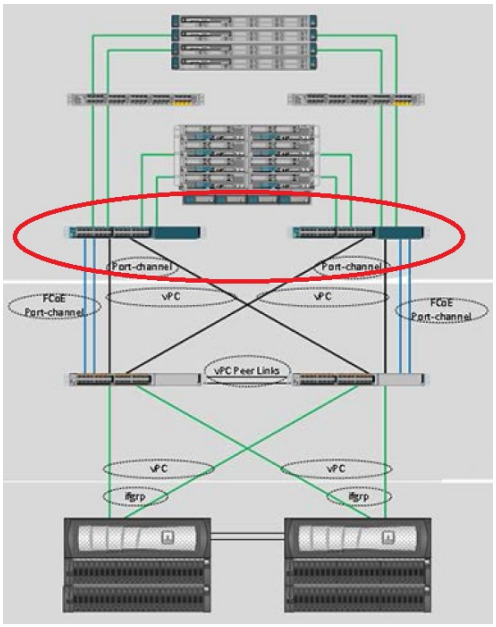
2.1 Network

Wi-Fi
Op een aantal locaties binnen het servicegebied van Servicepunt71 zijn Wi-Fi punten ingericht welke centraal worden beheerd. Deze punten bieden met een Guest signaal met encryptie uitsluitend verbinding met het internet en tot de Citrix Netscaler, via een apart Vlan Het synchroniseren van email via deze verbinding is eveneens mogelijk. Het wachtwoord van deze verbinding wordt maandelijks veranderd en gepubliceerd op het intranet. Op sommige locaties is tevens verbinding met het interne netwerk mogelijk, via een niet-openbaar signaal .

Firewalls en DMZ
In het DMZ tussen deze twee firewalls wordt er een Application Appliance ingezet in de vorm van een Citrix Netscaler[2]. Dit is de meest logische keus aangezien de Server Based Computing (SBC) omgeving van het Servicepunt71 is gebaseerd is op Citrix XenApp. Met de Netscaler kan deze omgeving veilig worden ontsloten naar de thuiswerkers op basis van two-factor authenticatie.

De centrale Firewall bestaat uit twee Palo Alto firewalls.

Fabric Interconnects
Om de huidige netwerkinfrastructuur te koppelen aan de UCS Bladecenters in een FlexPod oplossing zijn Cisco UCS Fabric Interconnect switches nodig. Deze verbinden de server access switches aan de UCS blades. Zie afbeelding.

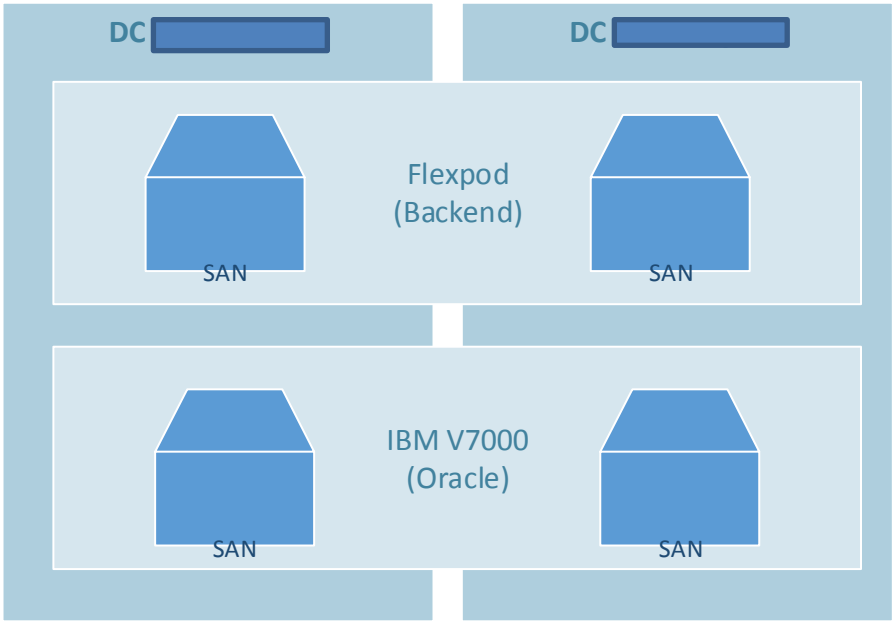


Figuur 3 Fabric Interconnects

2.2 Storage

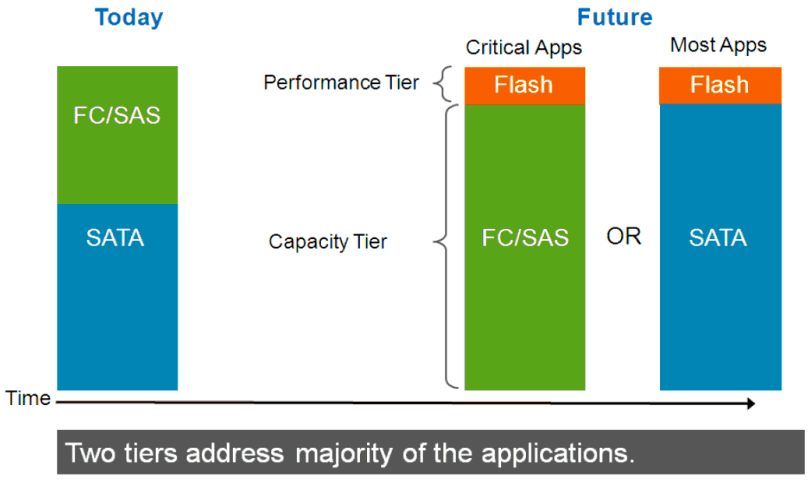
Van de huidige storageomgeving zijn de IBM V7000 systemen nog niet afgeschreven. Het zou een desinvestering zijn om deze bij de introductie van de nieuwe backend omgeving te vervangen. Dit resulteert echter wel in silovorming. Zie bijgaande afbeelding:

[2] Zie: http://www.citrix.com/products/netscaler-appfirewall/overview.html



Figuur 4 Storagesilo's

NetApp biedt tiering door middel van Virtual Storage tier. Hierbij wordt Flash technologie (SSD) ingezet om de performance van de onderliggende Flash, FC, SAS of SATA schijven te verbeteren. Zie bijgaande afbeelding.



Figuur 5 NetApp view op auto tiering

Er zijn drie oplossing beschikbaar[3]:

- Flash Accel (Server);
- Flash Cache (Controller);
- Flash Pool (Disk cabinet).

2.2.1 Werkplekprofielen

Om zoveel mogelijk tegemoet te kunnen komen aan de specifieke eisen en wensen van de gebruikers zijn er tot nu toe drie gebruikersprofielen gedefinieerd.

- Hybride Profiel - standaard SBC profiel inclusief RES WorkSpace Manager;
- Lokaal Server Profiel – uniek per server niet gemanaged.

[3] Zie: http://bitpushr.wordpress.com/2013/07/30/differences-between-netapp-flash-cache-and-flash-pool/

Het hybride profiel heeft de volgende eigenschappen:

- Gebruikers beschikken over een eenduidige interface waarmee ze doeltreffend hun applicaties kunnen starten en hun documenten kunnen beheren;
- Eenmaal door een gebruiker gemaakte instellingen in applicaties en werkomgeving worden automatisch meegenomen naar de virtuele "xenapp-server" desktop;
- Gebruikers beschikken alleen over de applicaties waarvoor ze geautoriseerd zijn;
- De gebruiker heeft een gestandaardiseerd bureaublad, uitsluitend de taal, toetsenbordinstellingen, achtergrondkleur, muis, desktop-snelkoppelingen en printerinstellingen kunnen gewijzigd worden;
- De definitie van een verplicht profiel in samenhang met "Zero Profile" technology van RES zorgt voor het snel laden van het gebruikersprofiel met behoud van specifieke tevoren gedefinieerde instellingen.

Voor het lokaal server profiel ten behoeve van Administrators en Beheer geldt het volgende:

- Serverbeheerders hebben waar mogelijk functionele beperkingen op de werkomgeving;
- Het voor de systeembeheerder geldende profiel zal dan ook alleen voor systeembeheer doeleinden worden ingezet;
- De basis beveiligingsopties (zoals bijv. het beveiligen van de screensaver met een wachtwoord) gelden ook voor de beheerders.
- Servicepunt 71 streeft ernaar om gebruik te maken van RBAC voor het uitvoeren en toekennen van beheerwerkzaamheden

Bijlage 3 Application services

3.1 SDL codes

Bijlage

Figuur 6

3.2 Algemene eisen

- Er moet gebruik gemaakt worden van binnen de gemeente gebruikte versies van besturingssystemen, database management systemen en middleware componenten;
- Voor alle software geldt dat deze moet voldoen aan de richtlijnen van de fabrikant van het besturingssysteem waarop de software wordt geïnstalleerd;
- Als gebruik wordt gemaakt van een applicatieserver, moet deze kunnen worden uitgevoerd als virtuele server onder Hyper-V
- Voor zover (nieuwe) applicaties geen server vereisen, maar alleen gebruik maken van file services, geldt dat programmatuur en data gescheiden moeten kunnen worden, waarbij de DFS share P:\ beschikbaar is voor programmatuur en de F:\share voor (applicatie)data;. Voor het overige mogen geen vaste driveletters worden gebruikt;
- Er mag geen gebruik gemaakt worden van vaste paden (hard coded). Path-instellingen (installatiemap, etc.) moeten met parameters gezet kunnen worden;
- De leverancier dient aan te geven wat de frequentie is van reguliere updates;
- Specificaties van hard- en software moeten aangeleverd worden als onderdeel van de wijzigingsaanvraag bij SE ICT;
- Ondersteuning door de leverancier dient gedurende de geplande gebruiksduur gewaarborgd te zijn;
- Bij oplevering van de toepassing dient er overdracht plaats te vinden aan de Service eenheid ICT van de handleidingen, installatiebeschrijving, licentiegegevens, etc.;
- Alle te installeren software wordt aangeleverd op dusdanige wijze, bijvoorbeeld op CD, dat deze binnen de gemeente gearchiveerd kan worden en gebruikt kan worden bij herinstallaties;
- De leverancier dient deel te nemen aan het intakeproces voor het (re) packagen van de client-software;
- Uitgangspunt is een “locked down environment” waarbij gewone gebruikers geen installatie- of schrijfbevoegdheid hebben op de lokale opslag.
- Autorisaties dienen met het package te worden geregeld, voor wat betreft de benodigde toegang tot programma- en dataschijven, databases etc.;
- Per applicatie is, in principe, een aparte server ingericht die, waar mogelijk, wordt aangeboden als gevirtualiseerde server op basis van Hyper-V 2012 R2.
- In de ontwikkeling en bouw van de applicatie is Security en Privacy by design het uitgangspunt
- De leverancier van; de locatie van ; de applicatie en diens dataopslag voldoet (voor zover van toepassing) aan de geldende wet- en regelgeving omtrent het gebruik en/of uitwisseling van persoonsgegevens

3.3 Resourcegebruik

- Na afsluiting van een applicatie moeten de gebruikte resources worden vrijgegeven en moeten tijdelijke bestanden worden opgeruimd;
- Een niet meer gebruikte applicatie moet gede-installeerd kunnen worden;
- De benodigde ruimte moet aangegeven door middel van een degelijke sizing als onderdeel van de wijzigingsaanvraag bij SE ICT. Hierin wordt rekening gehouden met datagroei voor de levensduur van de applicatie.

Bijlage 4 Presentation services

4.1 Type werkplekken

Werkplek type	Hardware	Opmerking
Thin Client	Igel, UD5, model 730	'Normale' gebruiker
Desktop	Dell Optiplex 790	Waar applicatie virtualisatie niet kan
Laptop	<selectie lopend>	Mobiele toepassingen
Workstation	<selectie lopend>	Zware toepassingen
Any Device	*<telewerken en toegang>*	*Receiver en token*
Surface tablet	*Microsoft Surface Pro*	*Flexwerken*
Monitor	*Fujitsu B24W5 Eco/-6 LED*	
Keyboard, Mouse	*Fujitsu KB400, M500T*	

4.1.1 Update policy

De update policy beschrijft hoe de diverse updates behandeld moeten worden. Aangezien er talloze updates per jaar uitkomen is het onbegonnen werk om deze allemaal door het release proces te halen. Het is van belang om op een efficiënte wijze het kaf van het koren te scheiden om op die manier het release management proces niet onnodig te belasten en toch een betrouwbare en beschikbare infrastructuur te houden. Hiervoor wordt de volgende policy gehanteerd.

Major updates

Het implementeren van major updates zijn dusdanig complex dat deze niet door de beheerorganisatie uitgevoerd worden. Het bepalen van de impact en de risico's van de update zal een te groot beslag leggen op de resources die de beheerorganisatie beschikbaar heeft. Het risico bestaat dan dat de primaire taak van de beheerorganisatie – het beheren van de bestaande omgeving – in gevaar komt.

Deze updates zullen via een project geïmplementeerd moeten worden. Uiteraard kunnen en moeten medewerkers van de beheerorganisatie onderdeel zijn van een dergelijk project. Het project bepaald de changes die nodig zijn om de major update te implementeren, en maakt afspraken met het release management proces omtrent de wijzigingen die nodig zijn door te voeren.

Minor updates

Minor updates zijn minder complex vergeleken met major updates, maar kunnen niet zonder meer worden uitgerold op de infrastructuur. Dit type updates moet het volledige release management proces door. Pas als er goedkeuring is kan de update in productie worden gezet.
De volgende policy wordt hierbij gehanteerd.

Beschikbaarheid
- Het uitgangspunt is dat de infrastructuur maximaal één minor update achterloopt;

Deze policy voorkomt dat men dusdanig achterloopt met updates dat er problemen ontstaan met support van de leverancier. Daarnaast voorkomt het problemen in de infrastructuur door nieuwe bugs die door de minor update geïntroduceerd worden op te lossen.

Bijvoorbeeld: Exchange 2013 SP3 is op 20 juni 2010 uitgekomen. Vanaf dat moment kan SP2 uitgerold worden. Uit verder onderzoek blijkt dat er met de introductie van SP2 nieuwe bugs zijn ontstaan. Door de implementatie van rollup 4 voor SP2 worden deze verholpen.
Er kan in uitzonderlijke situaties afgeweken worden van de procedure. Bij het uitkomen van een SP voor Microsoft Office bijvoorbeeld is de impact en het risico erg groot. Er kan dan bepaald worden om het SP niet uit te rollen, of uit te stellen. Ook als al bekend is dat er op korte termijn een uitrol van Office 2013 plaats zal vinden. Daarnaast kan er ook voor worden gekozen om een minor update eerder uit te rollen. Bijvoorbeeld om een bepaald probleem op te lossen.
De beslissing om een SP niet of juist eerder uit te rollen zal moeten worden onderbouwd en worden voorgelegd aan release management.

Impactanalyse
In de impactanalyse moet de scope van de minor update worden bepaald. Daarna kunnen de (kritieke) bedrijfsprocessen worden bepaald waar de update een impact op heeft. Als laatste kan het risico worden bepaald, alsmede de maatregelen om deze tot een minimum te te beperken. Onderdeel van de impactanalyse is een fallbackplan.

Updateplan
Het updateplan is een technisch draaiboek met daarin alle te nemen stappen die nodig zijn om de update uit te rollen. Bij elke stap wordt een uitvoeringstijd en tijdstip geplaatst evenals de uitvoerende partij. Ook het fallbackplan moet worden beschreven.

Communicatieplan
Het communicatieplan bestaat uit een plan van aanpak, wanneer wordt wie op welke manier benaderd.

Update procedure
De minor updates zijn groter in omvang en impact ten opzichte van patches. Daarom moet er meer aandacht worden besteed aan de impactanalyse voordat een dergelijke update uitgerold kan worden. Hiervoor moeten de release notes en de installatie-instructies goed worden vertaald naar de specifieke infrastructuur van Servicedesk71. Uit dit onderzoek volgt dan een updateplan. Dit plan beschrijft stap-voor-stap alle acties die genomen moeten worden om de update te installeren.

Activiteit	Vragen
Beschikbaarheid controleren	Is er al een nieuwere versie beschikbaar? Als men afwijkt van de regel om één versie achter te lopen, beschrijf dan waarom er afgeweken wordt.
Impactanalyse maken	Welke systemen worden geupdate? Hoe lang duurt de update? Is de beschikbaarheid voor de gebruikers gewaarborgd?
Updateplan maken	Welke acties moeten er genomen worden? Wat als het mislukt?
Communicatieplan opstellen	Mits noodzakelijk.

Patch updates

Omdat er talloze patches uitkomen voor de software die gebruikt wordt in de infrastructuur moet bepaald worden of de patch wel relevant is. Ook zullen leveranciers met updateverzoeken komen. Ook deze verzoeken moeten voldoen aan de update policy.

Critical patches
Omdat een leverancier het label “Critical” aan een patch heeft gegeven wil niet zeggen dat het voor de infrastructuur een critical patch is. Een geheugenlek in een Microsoft DHCP server is kritisch, maar niet als er gebruik wordt gemaakt van een Novell DHCP server.

Non-Critical patches
Non-Critical patches worden in principe niet in productie geplaatst, tenzij hier aanwijsbare argumenten voor zijn. In dat geval zal dit via een change gebeuren.

Bijlage 5 Security services

5.7.4 Werkplek beveiliging

Men krijgt toegang tot het werkstation en de functies in het netwerk met een persoonlijke gebruikersnaam en een wachtwoord. De gebruikersnaam wordt door de Service eenheid ICT verstrekt en is strikt persoonlijk. Het wachtwoord kan door de gebruiker zelf bepaald worden en moet aan de volgende regels voldoen:

Specifiek voor notebooks geldt:
- De inhoud van de bestanden op de notebook is versleuteld (encrypted)
- Bij het opstarten kan de gebruiker kiezen:
  - Als node in de infrastructuur
  - In stand alone mode

Notebook gebruikers kunnen op aanvraag beschikken over een beveiligde UMTS verbinding met het netwerk.

Bijlage 6 Management services

6.1 Installatie van de werkplek

De werkplekken worden door de Service eenheid ICT beheerd vanuit een centraal installatie- en beheerpunt. Werkplekken (FAT clients) worden geïnstalleerd met Windows Deployment Server MDT. Met RES Workspace en Automation Manager wordt de configuratie ingeregeld en worden applicaties op de werkplek van de geautoriseerde gebruiker geïnstalleerd. De thin clients (Igel) worden uitgerold met de UMS beheertool, embedded Windows is hier standaard op aanwezig.

Met Windows Server Update Services (WSUS) worden automatisch de (beveiligings-)patches voor het Windows besturingssysteem geïnstalleerd. Clients kunnen met behulp van Wake on LAN op afstand worden uitgezet c.q. aangezet. Voor de Surface Tablets is een combinatie van Intune en MDT in gebruik voor het beheer en onderhoud, waarbij updates via Windows Update online verlopen.

6.2 Config Management

Provisioning Services wordt ingezet voor het imagen van de SBC servers en de daarop aangeboden applicaties. PXE wordt gebruikt om de fat clients gecentraliseerd te beheren.

6.3 Monitoring

Standaard wordt bij Servicepunt71 gebruik gemaakt van SNMP voor monitoring van IT devices en of besturingssystemen.

Voor eisen ten aanzien van logging dienen de BIG richtlijnen (Handreiking Aufdit en Logging IBD) aangehouden te worden. Servicepunt71 voorziet standaard in Syslog en Windows Eventlog functionaliteit

6.4 Backup en restore

Voor het back-uppen en restoren van (applicatie)servers wordt gebruik gemaakt van IBM’s Tivoli Storage Manager (ITSM). Rman (recovery manager) wordt gebruikt voor de backup van Oracle Databases.