



gemeente **Roermond**



Dienstverleningsovereenkomst (DVO)

TUSSEN ICT NML EN DE GEMEENTEN NEDERWEERT, ROERMOND, VENLO EN WEERT



Colofon

Titel *Dienstverleningsovereenkomst (DVO)*

Ondertitel *tussen de gemeenten Roermond, Nederweert, Venlo en Weert*

Versie, datum *Versie 1.34, 8 september 2017*

Referentie -

Samengesteld door *R. Meerts*

Bestandsnaam *DVO ICT NML v1.34*

Inhoudsopgave

1	Partijen, Looptijd en akkoord	1
2	Begrippen en uitgangspunten.....	3
2.1	Begripsbepalingen	3
2.2	Uitgangspunten	5
3	Overzicht diensten.....	8
4	Beheer	9
4.1	Apparatuur	9
4.1.1	Algemeen.....	9
4.1.2	Standaardisatie	9
4.1.3	Datacenters.....	10
4.1.4	Uitwijk	10
4.1.5	Externe beveiligings diensten.....	10
4.2	Applicaties.....	10
4.2.1	Applicatievirtualisatie.....	10
4.3	Administratieve taken	11
4.3.1	Registratie van hard- en software.....	11
4.3.2	Licentiebeheer.....	11
4.3.3	Documentatie	11
4.4	Storingsafhandeling	12
4.5	Backup en restore	12
4.6	Netwerk.....	12
4.7	Beveiliging.....	13
4.7.1	Virusprotectie	13
4.7.2	Spamfiltering	13
4.7.3	Firewalls.....	13
4.7.4	Certificaten.....	13
4.7.5	Authenticatie en autorisatie	14
4.8	Dataopslag	14
4.9	Telefonie	15
4.10	Uitgesloten producten en diensten	15
4.10.1	RAAS	15
4.10.2	Websites	15
4.10.3	Licentiebeheer applicaties.....	15

4.10.4	Audiovisuele middelen	15
4.10.5	Toegangsbeveiliging	15
5	Helpdesk	17
5.1	Escalatieprocedure	17
5.2	Calamiteitenprocedure	17
6	Kosten en financiering	18
6.1	Bepaling bijdrage per deelnemer	18
6.2	Kosten voortvloeiend uit datalek	18
7	Algemene bepalingen	18
7.1	Wijziging van de DVO	18
7.2	Rapportage en communicatiecatiestructuur	19
Bijlage 1.	Calamiteitenprocedure	22
Bijlage 2.	Sjabloon voortgangsrapportage	23
Bijlage 3.	Standaarden / Infrastructuur	25

1 Partijen, Looptijd en akkoord

<i>Doel</i>	Het doel van deze dienstverleningsovereenkomst (DVO) is het eenduidig vastleggen van afspraken over de dienstverlening ICT NML aangaande beheer, onderhoud, beveiliging en beschikbaarheid van de geautomatiseerde systemen van de deelnemende gemeenten.
<i>Looptijd</i>	De DVO geeft een nadere uitwerking van de taken die in het kader van de BVO bij ICT NML zijn overgedragen. De looptijd van de DVO is gelijk aan de looptijd van de gemeenschappelijke regeling. Tussentijds kan de DVO op basis van substantiële wijzigingen in de behoefte worden aangepast zoals in het juridische document is vastgelegd.

<i>Akkoord</i>	Met de ondertekening gaan de partijen akkoord met de afspraken in deze DVO
<i>Vertegenwoordiger</i>	<p style="text-align: center;">Gemeente Nederweert Vertegenwoordiging Datum Handtekening</p> <p style="text-align: center;">Gemeente Venlo Vertegenwoordiging Datum Handtekening</p> <p style="text-align: center;">Gemeente Weert Vertegenwoordiging Datum Handtekening</p> <p style="text-align: center;">Gemeente Roermond Vertegenwoordiging Datum Handtekening</p>

2 Begrippen en uitgangspunten

2.1 Begripsbepalingen

Onderstaand overzicht bevat de omschrijving van enkele in deze DVO gebruikte begrippen.

Afhandelingstermijn

De maximale termijn waarbinnen de regeling een gemelde storing, probleem of vraag dient af te handelen. De regeling hanteert hierbij vaste afhandelingstermijnen, welke toegelicht worden in het service level agreement (SLA). Onder het afhandelen van een storing, probleem of vraag wordt normaal gesproken oplossen bedoeld, tenzij hier andere afspraken over gemaakt zijn.

Applicatie

Programma op de server of werkplek voor algemene, beheersmatige, bedrijfsmatige of administratieve doeleinden.

Backup

Het maken van een reservekopie van programmatuur en data op een aparte locatie. Hiermee worden de gegevens op de server veiliggesteld voor calamiteiten. Ook het teruglezen van de gegevens naar de server is mogelijk. Dit wordt aangeduid met de term 'restore'.

BAG

basis registratie adressen en gebouwen

Beheer(der)

Het team ICT beheerders van ICT NML. Daarmee worden de betrokken beheerders van de deelnemende gemeenten bedoeld.

BIG

Baseline Informatiebeveiliging Nederlandse Gemeenten.

Breedband

Netwerk van (glasvezel)verbindingen tussen de locaties van de deelnemende gemeenten. Via deze breedbandverbinding zullen de locaties hun Gemnet en Internetverbinding gaan afnemen en gebruik gaan maken van centrale servervoorzieningen.

BRP

basis registratie personen

Data

Elektronische gegevens.

DVO

Dienstverleningsovereenkomst waarin de afspraken zijn vastgelegd over het beheer, onderhoud, beveiliging en beschikbaarheid van de ICT-omgeving van de deelnemende gemeenten.

Helpdesk

Afdeling binnen de gemeente die centraal aanspreekpunt is voor de melding van vragen, storingen/problemen, incidenten en wijzigingsverzoeken met betrekking tot het gebruik van de ICT-voorzieningen. Iedere deelnemende partij komt terecht bij een gezamenlijk gedeelde

helpdesk 1^{ste} lijn. De toegang kan verschillen door het gebruik van een eigen al bestaande ingang, of het gebruik maken van de ingang bij ICT NML.

(ICT) Infrastructuur

Het geheel van werkstations, servers, dataopslag, netwerkapparatuur en netwerkverbindingen.

ITIL

Information Technology Infrastructure Library. Een internationaal referentiekader voor het inrichten van de beheerprocessen binnen een ICT-organisatie.

Mobiele apparaten / Mobile devices

Hiermee worden apparaten bedoeld die niet direct aan een werkplek of netwerk gekoppeld zijn en vooral bedoeld zijn om locatieafhankelijk te kunnen werken, bijvoorbeeld tablets, laptops en smartphones.

Netwerk

Alle componenten die datacommunicatie tussen de netwerkapparatuur mogelijk maakt.

PDC

Producten Diensten Catalogus

Randapparatuur

Apparatuur die gekoppeld wordt aan een workstation of server, zoals printers, scanners en kaartlezers.

Remote

Beheer op afstand.

Router

Netwerkcomponent die een verbinding realiseert tussen twee of meer netwerken, bijvoorbeeld een gemeentelijk netwerk. De router wordt geleverd en beheerd door de regeling.

RSA SecurID Token

Dit is een hardware- en softwarematige sleutel waarmee je in combinatie met een PIN code op een veilige manier toegang kunt krijgen tot het netwerk.

Regeling

De organisatie ICT NML die gevormd wordt door de ICT medewerkers uit de deelnemende gemeenten samen te voegen.

Server

Computersysteem voor centrale beschikbaarheid van data en applicaties alsmede het printen naar op het netwerk aangesloten printers.

SLA

Service Level Agreement, een overeenkomst met smart geformuleerde doelen ten aanzien van de dienstverlening.

Stand-alone PC

Computersysteem welke niet is aangesloten op het interne computernetwerk van de gemeente.

Software

Verzamelnaam voor besturingssystemen en applicaties.

Switch

Netwerkapparaat waarmee computers onderling verbonden worden en daarmee een netwerk vormen.

Wide Area Network (WAN)

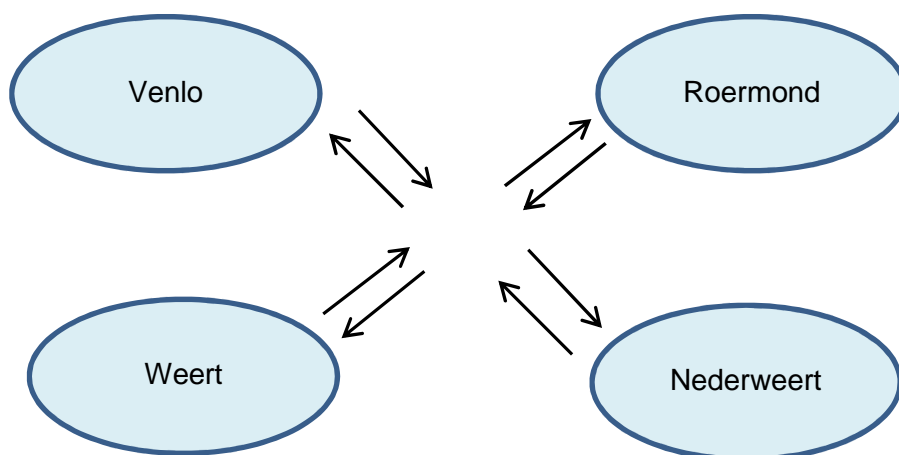
Eigenlijk worden hiermee de buitenpandige verbindingen bedoeld, het intergemeentelijk netwerk en de verbindingen met Internet en Gemnet. Hiermee worden alle locaties, de lokale netwerken en de daarin opgenomen netwerkcomponenten met elkaar verbonden.

WIKI

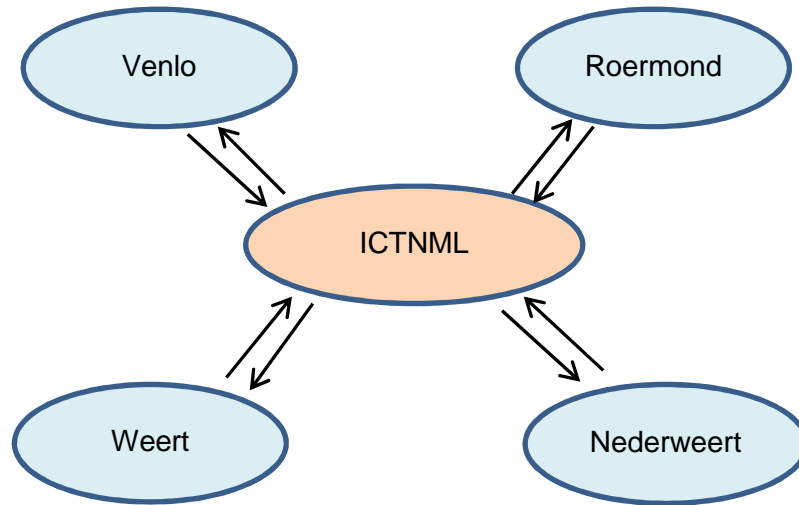
Een wiki is een [applicatie](#) of (web)toepassing, waarmee webdocumenten gezamenlijk kunnen worden bewerkt en ontsloten. Bekend voorbeeld van een wiki is [Wikipedia](#).

2.2 Uitgangspunten

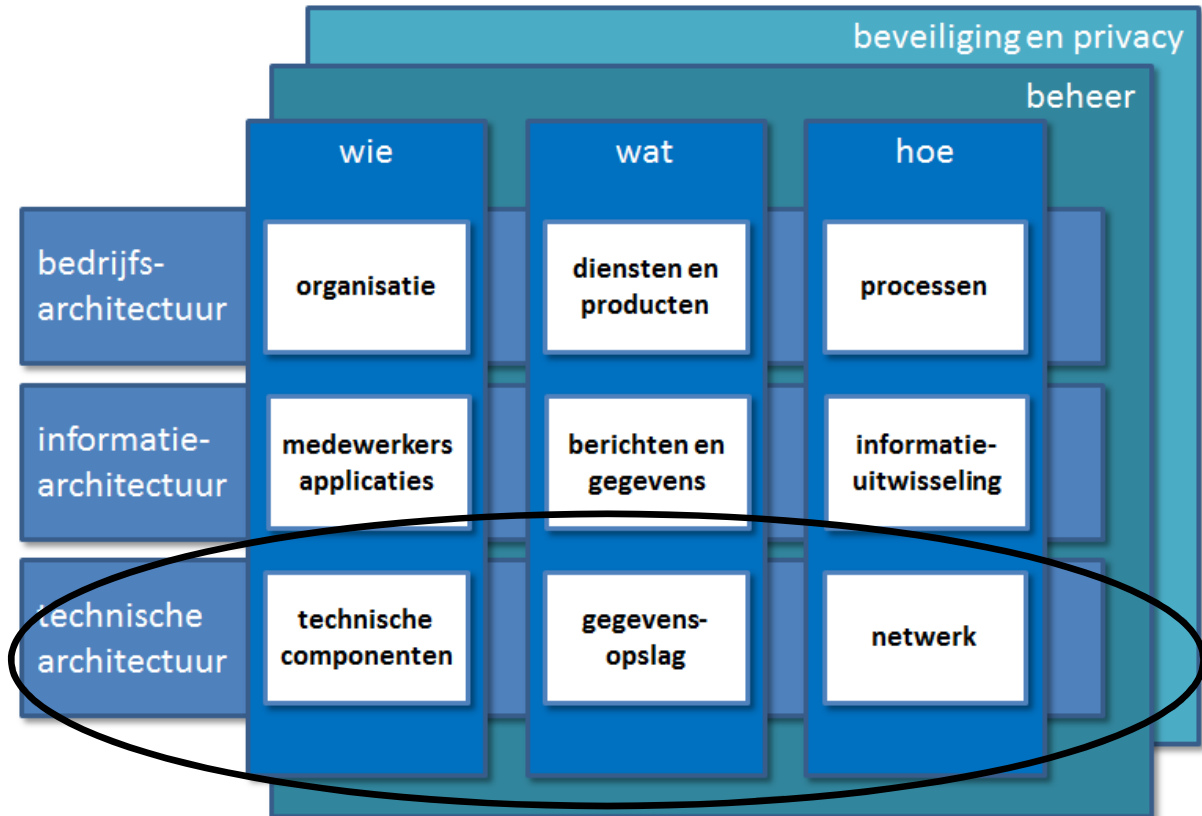
ICT NML is een zelfstandige organisatie met een eigen entiteit. Het is een zware gemeenschappelijke regeling, in de vorm van een publiekrechtelijke organisatie in een bedrijfsvoeringsvariant (BVO). De ICT infrastructuur van de deelnemende gemeenten zijn gecentraliseerd en er wordt onderling gewerkt op een gedeeld platform. De verantwoordelijkheid voor de ICT infrastructuur en het beheer ervan is de verantwoordelijkheid van ICT NML.



De betrokken ICT medewerkers van de deelnemende gemeenten gaan over naar de organisatie ICT NML en worden functioneel en operationeel aangestuurd door de teamleiders van ICT NML onder regie van de manager. Om naar de deelnemende gemeenten een eenduidige dienstverlening te verzorgen en de verantwoordelijkheid eenduidig te beleggen, wordt in deze DVO de regeling gezien als de leverende partij en als een aparte organisatie beschouwd. Schematisch ziet het er dan als volgt uit:



ICT NML zal het totale beheer van de ICT infrastructuur voor de deelnemende gemeenten op zich nemen. In deze DVO zijn afspraken gemaakt welke werkzaamheden daarvoor worden uitgevoerd. Kortweg komt het erop neer dat het beheer gevoerd wordt op de onderste (technische) laag van het NORA 9-vlaksmodel. Het betreft feitelijk de reeds bij de gemeenten aanwezige apparatuur zoals die aanwezig was bij de aanvang van de regeling of zoals die daarna door ICT NML is aangeschaft.



Afbeelding 1: NORA 9-vlaksmodel

De inrichting van de infrastructuur, servers, standaardinrichting van werkstations en beveiliging is voor alle gemeenten gestandaardiseerd. Deze standaards zijn vastgesteld door het bestuur en te vinden in de WIKI van ICT NML. Afwijkende wensen worden in overleg met de Manager ICT en de directieraad besproken en hiervoor kunnen meerkosten in rekening worden gebracht. Verderop in deze DVO is uitgewerkt wat er precies onder het beheer valt.

Advieswerkzaamheden vallen binnen bestek van deze DVO, indien het advies betrekking heeft op (verbeteren van) het beheer zoals beschreven in deze DVO of in de WIKI. Voor advies dat buiten het bestek van DVO en WIKI valt zullen in voorkomende gevallen afspraken gemaakt worden en kunnen meerkosten in rekening gebracht worden. Hiervoor zal een addendum op het DVO opgesteld worden.

3 Overzicht diensten

De regeling levert aan de gemeenten de volgende diensten:

1. Diensten / Systeeminrichting: betreft de helpdesk diensten, de technische service, inclusief inkoop op het gebied van accounts & rechten, backup & restore, certificaten, email, beveiliging & spam, netwerktoegangen en connectiviteit.
2. Hardware / Gebruikersapparatuur: betreft de technische service inclusief inkoop op het gebied van werkplek ICT apparatuur, mobiele apparatuur en de multifunctionals, printers en scanapparatuur.
3. Applicaties / Software: hierbij gaat het om het beschikbaar stellen en het waarborgen van de technische werking ofwel de service tot aan het opstartscherm, vanaf dat punt nemen de applicatiebeheerders van de gemeenten zelf het over.
4. Advies en Projecten: advies- en projectmanagement dat door ICT NML aan partners ter beschikking wordt gesteld waarbij de desbetreffende capaciteit op basis van uren verrekend wordt.

4 Beheer

Het in goede staat brengen en houden van de apparatuur, het lokale en wide area netwerk, de backup/restore, de uitwijk en de beveiliging van data en de geautomatiseerde gegevensverwerkende systemen. In dit hoofdstuk staat beschreven welke producten en diensten er door de regeling wordt geleverd.

4.1 Apparatuur

4.1.1 Algemeen

Het beheer beperkt zich tot de apparatuur en infrastructuur zoals die tijdens te start van de regeling bij de deelnemende gemeenten aanwezig was of die later via ICT NML is aangeschaft en opgenomen in het netwerk.

ICT NML verzorgt het beheer van telefonie. Dat betekent dat de reguliere beheer werkzaamheden voor het standaard functionere van telefonie deel uit maken van de basisdienstverlening.

Eventueel is maatwerk in overleg mogelijk welke tegen meerkosten uitgevoerd kunnen worden.

Om een goede, efficiënte, veilige en stabiele ICT omgeving te verkrijgen en te behouden dienen de deelnemende gemeenten zich te conformeren aan de standaarden en werkwijze die gezamenlijk in de regeling wordt afgesproken en gehanteerd.

Het is de gemeenten niet toegestaan op eigen initiatief en op een afwijkende manier (netwerk)apparatuur aan te sluiten op de netwerkomgeving of software te installeren op de apparatuur die onder het beheer van de regeling valt.

Storingen aan genoemde apparatuur kunnen gemeld worden via de Helpdesk van ICT NML. De Helpdesk draagt zorg voor registratie. Als zij de melding en als zij na een korte analyse niet zelfstandig kunnen afhandelen zetten zij deze door naar de beheerders van de regeling. Deze kunnen de storing ter afhandeling melden bij de leverancier(s). De leverancier zal (conform garantie- en/of onderhoudsvoorwaarden) hardwarestoringen oplossen.

Het beheer van de ICT infrastructuur kan (gedeeltelijk) op afstand worden uitgevoerd. Ten behoeve van de continuïteit wordt de technische infrastructuur continue bewaakt met behulp van software die gebreken signaleert en rapporteert aan de beheerders van de regeling. Storingen buiten werktijden komen terecht bij de dienstdoende beheerder.

4.1.2 Standaardisatie

Om de kosten van het beheer op een aanvaardbaar niveau te houden, zijn er binnen de regeling afspraken gemaakt over standaardisatie van de werkstations, netwerk- en randapparatuur .

Bij de start van de regeling is gekozen voor standaard hardware en een eenduidige technische ICT architectuur die voor alle gemeenten richtinggevend is.

Voor de aanschaf van de apparatuur zal conform de geldende aanbestedingsregels raamcontracten worden afgesloten met leveranciers. De leverancier zal geselecteerd worden via een aanbesteding, waarna ICT NML zelf een contract afsluit met de geselecteerde partij zodat de deelnemers dit niet meer zelf hoeven te doen. Nieuwe apparatuur zal altijd binnen deze raamcontracten worden aangeschaft.

In Bijlage 3 is een overzicht van de ICT architectuur en de gekozen standaarden opgenomen.

Om de standaardisatie te bewaken en zo de kosten van het beheer op een aanvaardbaar niveau te houden, is het opnemen cq. aanschaffen van nieuwe apparatuur in de netwerk omgeving ter beoordeling van de regeling. Aanschaf verloopt altijd via de regeling, maar zal wel invulling moeten geven aan de functionele behoefte van de deelnemende gemeenten.

4.1.3 Datacenters

In de regeling zullen de datacenters geconsolideerd worden tot twee datacenters. De locaties hiervan zijn bepaald in de gemeente Roermond en in de gemeente Venlo.

Het datacenter In Venlo en in Roermond zullen zodanig worden ingericht dat bij uitval van één van de twee locaties uitgeweken kan worden op de systemen in de andere locatie. Zie hiervoor paragraaf 4.1.4

4.1.4 Uitwijk

In de regeling zullen de datacenters zodanig worden ingericht dat ze kunnen dienen als elkaars uitwijk. Hierbij wordt zodanig ingezet dat bij uitval van een enkel systeem de functionaliteit binnen 4 uur kan worden overgenomen door de andere locatie.

Uitwijk is in ieder geval geregeld voor:

- BRP (basis registratie personen) BAG (basis registratie adressen en gebouwen) (wettelijke verplichting)
- Datastorage
- Authenticatieservers
- Domain servers
- Mailservers

Jaarlijks zal de uitwijk van het BRP en BAG worden getest. De resultaten van deze test zullen worden vastgelegd in een verslag die desgewenst t.b.v. de (BRP)audit kan worden overhandigd

4.1.5 Externe beveiligings diensten

Er wordt maandelijks een vulnerability scan uitgevoerd op alle publiek toegankelijke diensten. Deze scan toetst de buiten kant van het netwerk tegen alle bekende kwetsbaarheden, zodat hier door ICT-nml passende maatregelen voor genomen kunnen worden.

Tevens wordt al het in en uit gaand verkeer tussen het interne en externe netwerk gelogd. Deze log gegevens worden conform de BIG (Baseline Informatiebeveiliging Nederlandse Gemeenten) ten minsten 3 maanden bewaard. Op dit koppelvlak wordt ook gebruik gemaakt van een Intrusion Prevention System (IPS). Dit systeem analyseert het netwerk verkeer om patronen van malafide bronnen te herkennen en hier automatisch op te reageren. Op verzoek kan dat ook tussentijds, intensiever of specifiek uitgevoerd worden.

4.2 Applicaties

4.2.1 Applicatievirtualisatie

Applicaties zullen naar de werkplek worden “gedistribueerd”. Het betreft geen daadwerkelijke installatie, maar door middel van softwarevirtualisatie het streamen van de applicatie. De applicatie moet dus wel geschikt zijn voor deze wijze van distributie. Het geldt daarom ook als één van de criteria voor de aanschaf van nieuwe applicaties. De aanschaf van applicaties moet daarom in overleg met de i-adviseur van de gemeente en met ICT-nml gebeuren.

4.3 Administratieve taken

4.3.1 Registratie van hard- en software

Vanuit de regeling zal een uitvoerige registratie worden bijgehouden van de apparatuur en van de licenties die deel uitmaken van de regeling. Ook de registratie van beveiligingscertificaten wordt bijgehouden, zoals beschreven in paragraaf 4.7.4. Deze gegevens worden vastgelegd in een Configuration Management DataBase (CMDB) conform de Information Technology Infrastructure Library (ITIL) beheermethodiek.

Tenminste de volgende gegevens worden vastgelegd:

- Naam apparaat
- Merk en Type
- Leverancier
- Datum aanschaf
- Eigendom
- Locatie

4.3.2 Licentiebeheer

In de regeling wordt beheer over de licenties van het operating systeem, de databases en MS office gedaan. Andere applicatielicenties vallen er buiten. Zie hiervoor paragraaf 4.10.3.

Licentiebeheer wordt in ieder geval wel uitgevoerd voor de volgende software:

- Windows server
- Windows werkstations
- SQL server
- Exchange server
- VMWare
- AppV
- Client Access Licenties voor bovenstaande items.
- Backup software
- Oracle databases
- Anti-virus software
- Anti-spam software
- Microsoft Office
- Netwerk monitoring

4.3.3 Documentatie

De architectuur van de technische infrastructuur en de relatie / samenhang met de informatie-laag wordt tevens gedocumenteerd in een wiki. Bij ieder nieuw te starten project wordt de ICT architectuur beoordeeld en de gewenste nieuwe architectuur vastgelegd in een PSA (Project Start Architectuur).

Nadat de PSA tot stand is gekomen zal voor of tijdens de implementatie de uitwerking ervan worden beschreven in een technisch ontwerp. Hiermee samenhangend worden alle gegevens m.b.t. installatie en configuratie vastgelegd. Het technisch ontwerp wordt op een centrale plaats opgeslagen en zo mogelijk ook opgenomen in de wiki. De informatie is

beschikbaar voor alle medewerkers van de regeling en waar van toepassing ook voor de 1^{ste} lijn helpdesk , advies of andere organisatieonderdelen.

4.4 Storingsafhandeling

Gebruikers dienen storingen en vragen via de Helpdesk te melden. De 1^{ste} lijn helpdeskmedewerker zorgt voor een adequate registratie van de melding. Indien de melding niet door de 1^{ste} lijn kan worden opgelost, wordt deze door de 1^{ste} lijn medewerker doorgezet naar de 2^{de} lijn. Dit volgens de afspraken in het PDC en SLA.

4.5 Backup en restore

Dagelijks wordt er een backup gemaakt van de systemen en data (disc to disc). Dit verloopt door middel van een reversed incremental backup, waarbij een retentie tijd van 60 dagen wordt gehanteerd. Na 60 dagen wordt de backup overschreven. Er kunnen dus restore acties worden uitgevoerd tot maximaal 60 dagen terug.

Het monitoren van de status van een backup taak vindt dagelijks plaats. Het resultaat daarvan wordt in een logboek vastgelegd en kan desgewenst voor een interne controle of accountantscontrole worden overhandigd.

4.6 Netwerk

De volgende netwerken of netwerk-gerelateerde zaken (waaronder netwerkapparatuur) worden door de regeling geleverd en beheerd:

1. Intergemeentelijk netwerk:
Deze bestaat uit een hoogwaardige glasvezel-, of koperverbinding tussen de datacenters in Roermond en Venlo. Verder omvat dit ook de (gehuurde) verbindingen tussen alle deelnemende partijen en de datacenters in Roermond en Venlo.
2. Binnengemeentelijk interlokaal netwerk:
Het betreft de verbindingen tussen de verschillende gemeentelijke vestigingen. Het kan hier gaan om een eigen of gehuurde glasvezelverbinding, maar ook door derden geleverde "huurlijnen" of breedband verbindingen.
3. Lokaal netwerk:
Het betreft hier het LAN binnen de gemeentelijke gebouwen. Het kan hier om zowel een bedraad netwerk als WiFi netwerk gaan.
4. Gemnet:
Het betreft hier de Gemnet verbinding naar het private overheids-cloudnetwerk. Deze verbinding is dubbel uitgevoerd door vanuit ieder datacenter een verbinding naar het Gemnet te realiseren
5. Internet:
Het betreft de verbinding naar het Internet. Deze verbinding is dubbel uitgevoerd door vanuit ieder datacenter een verbinding naar het Gemnet te realiseren.

4.7 Beveiliging

4.7.1 Virusprotectie

Er wordt op verschillende niveaus door middel van anti-virus software van verschillende fabrikanten gecontroleerd op virussen.

Deze niveaus zijn:

- VDI werkplek
- Email
- Internetverkeer
- Servers

Indien er een virus wordt gevonden wordt deze door de anti-virus software verwijderd of indien dat niet mogelijk is wordt het geïnfecteerde bestand in quarantaine geplaatst.

Bij uitbraak van een zogenaamd zero-day virus (een tot dan toe onbekend virus) zal door specialisten vanuit de regeling op gecoördineerde wijze het virus worden bestreden met de volgende aanpak:

- Identificeren
- Isoleren
- Verwijderen
- Repareren

Bij uitbraak van een zich snel verspreidend virus kan door de regeling (delen) van de infrastructuur worden uitgeschakeld. Hierbij wordt gebruik gemaakt van een calamiteitenprocedure, waarin de besluitvorming en communicatie is vastgelegd (zie Bijlage 1)

4.7.2 Spamfiltering

Alle email wordt gescand door een anti-spam filter. Het gebruik van een anti-spam filter garandeert echter niet dat er geen spam doorgelaten wordt. Een juiste afstelling is daarin essentieel, waarbij vooral voorkomen wordt dat er vals positieve berichten (ten onrechte als spam aangeduide email) worden geblokkeerd. In praktijk kunnen ook normale berichten ten onrechte als spam worden aangeduid en tegengehouden. Dit kan nooit geheel worden voorkomen.

4.7.3 Firewalls

Firewalls worden ingezet om een goed beveiligde verbinding tussen het lokale netwerk en het Internet te realiseren. Het beheer van deze firewalls en DMZ (DeMilitarized Zone) maakt deel uit van de regeling. Hierbij zullen de componenten zoveel mogelijk worden gedeeld. Er worden geen firewalls tussen de gemeentelijke netwerken onderling geplaatst. Scheiden van de gemeentelijke netwerken gebeurt door middel van VLAN technieken.

4.7.4 Certificaten

Het aanvragen van beveiligingscertificaten ligt bij de gemeente zelf. De regeling zal de certificaten wel installeren en ook registreren. De regeling zal ook tijdig signaleren als een certificaat gaat verlopen en opnieuw moet worden aangevraagd. Hiervoor zal de regeling een registratie bijhouden van alle aangevraagde en geïnstalleerde certificaten.

4.7.5 Authenticatie en autorisatie

De regeling verzorgt alleen de autorisatie op netwerk-, systeem- en database niveau. Ook de mogelijkheid om applicaties te starten wordt verzorgd. De gemeente (applicatiebeheer) verzorgt echter zelf de autorisatie binnen de applicatie.

Applicaties en data op de server worden geplaatst op een systeem dat het mogelijk maakt om rechten toe te kennen aan bestanden en programma's. Het toekennen van rechten zal op groepsniveau plaatsvinden.

Concreet betekent dit dat de regeling autorisaties verleent op:

- Active Directory
- Oracle
- SQL
- Applicatietoegang vanuit het startmenu
- Email
- Netwerkschijven

Daar waar mogelijk zal het uitdelen van autorisaties bij de gebruiker zelf worden belegd. Een voorbeeld hierbij is het machtigen van gebruikers in outlook agenda en mail. Dit kan de eigenaar van de mailbox zelf uitvoeren.

Behalve autorisatie neemt de regeling ook het beheer van de authenticatie van personen op zich. Het betreft dan de authenticatie voor remote toegang met behulp van een RSA SecurID token. Dit omvat dan:

- De installatie en het beheer van de authenticatieserver(s)
- De inkoop, registratie en verstrekking van RSA tokens
- Het oplossen van storingen

4.8 Dataopslag

Voor de opslag van data wordt gebruik gemaakt van centrale opslagsystemen. De medewerker krijgt de beschikking over een eigen persoonlijke map en krijgt tevens toegang tot gedeelde mappen, zoals afdelingsschijven.

De opslag op de schijven is gelimiteerd. Indien extra capaciteit nodig is dient hiervoor een aanvraag bij de Helpdesk te worden ingediend, vergezeld van de goedkeuring van de leidinggevende.

Autorisaties op schijven, gebeurt altijd op groepsniveau. Er worden geen rechten uitgedeeld aan individuele gebruikersaccounts. Een groep kan wel bestaan uit slechts één gebruikersaccount.

Autorisaties worden altijd bepaald voor een complete map. Er worden geen autorisaties aan separate bestanden toegekend.

4.9 Telefontie

Het beheer op de vaste telefonie maakt formeel deel uit van de regeling. De taken welke ICT NML wel uitvoeren voor vaste telefonie staan beschreven in het PDC

4.10 Uitgesloten producten en diensten

4.10.1 RAAS

Het betreft hier het door Binnenlandse Zaken geleverd systeem voor afgifte van reisdocumenten dat fysiek bij iedere afzonderlijke gemeente in een beveiligde ruimte wordt geplaatst. Er wordt door de regeling geen actief beheer gepleegd op dit systeem. De beheerders van de regeling kunnen wel als contactpersoon fungeren voor het melden van storingen en de regeling zorgt voor het wisselen en opslag van backup / restore tapes. Deze taken kunnen desgewenst ook door een applicatiebeheerder van de gemeente worden uitgevoerd.

4.10.2 Websites

Het beheer van de Internet en Intranet sites van de deelnemende gemeenten valt buiten de regeling. Dit geldt voor zowel het functioneel als het contentbeheer. De regeling maakt het hosten van websites wel mogelijk door de technische infrastructuur te leveren. De installatie en registratie van certificaten valt dan onder de beheerswerkzaamheden van de regeling. Een gemeente kan er ook voor kiezen om de hosting van websites bij derden onder te brengen.

4.10.3 Licentiebeheer applicaties

In de regeling worden de licenties beheerd van Operating systemen, beheertools, databases en MS Office. Zie hiervoor paragraaf 4.3.2.

Het beheer van de licenties voor alle andere applicaties maakt geen deel uit van de regeling. Dit moet door de gemeente zelf (applicatiebeheer) worden uitgevoerd. Hierbij kan gedacht worden aan:

- Kleine kantoorautomatisering applicaties, zoals adobe, Visio, MS project, AutoCad
- Kernapplicaties, zoals GBA, Belastingen, onderwijs
- Geoapplicaties, zoals Nedbrowser en Grondmij applicaties
- Bedrijfsvoeringsapplicaties, zoals financiële pakketten, personeel registratie en DMS
- Midoffice applicaties

4.10.4 Audiovisuele middelen

Vanuit de regeling worden geen diensten geleverd voor audiovisuele middelen, zoals beamers, videoconferencing apparatuur, smartboards en geluidsinstallaties. Wel bieden we ondersteuning op de koppelvlakken (onze kant om te kunnen koppelen). Dit doen we samen met facilitaire afdeling van de deelnemende gemeente of met de leverancier van de audiovisuele middelen.

4.10.5 Toegangsbeveiliging

De toegangsbeveiliging tot de gemeentelijke gebouwen door middel van pasjessystemen worden niet beheerd vanuit de regeling.

Uitgesloten is van beheer:

- Het aansluiten en beheren van de badge-lezers en bekabeling.
- Het technisch en functioneel beheer van de applicatie
- De registratie van medewerkers in het systeem.

De regeling beheert wel:

- De infrastructuur waarop de applicatie met betrekking tot de toegangsbeveiliging is geïnstalleerd
- Het maken van backups en het uitvoeren van restore activiteiten

5 Helpdesk

De 1^{ste} lijn helpdesk maakt deel uit van de regeling. Deze helpdesk is gecentraliseerd en werkt voor iedere aangesloten gemeente. De ingangen en openingstijden zijn vastgelegd in het PDC en SLA.

5.1 Escalatieprocedure

Voor alle bij de Helpdesk binnengekomen meldingen wordt een afhandelingstermijn bepaald in het SLA. De Helpdesk bewaakt deze afhandelingstermijnen en zal in overleg treden met de gebruiker wanneer deze afhandelingstermijn niet gehaald wordt. Als een gebruiker er met de Helpdesk niet uitkomt, dan kunnen de volgende stappen worden ondernomen:

Stap 1: De gebruiker kan via zijn leidinggevende contact opnemen met de incidentmanager van ICT NML. De incidentmanager zal de nodige stappen ondernemen die moeten leiden tot het oplossen van de melding.

Stap 2: In geval van discussie of verschil van inzicht tussen aanmelder en incidentmanager wordt geëscaleerd naar de teamleider helpdesk en servicemanagement die de melding en de te nemen acties beoordeelt.

Stap 3: Indien dat voor de gebruiker ook niet tot het gewenste resultaat leidt, kan de teamleider via de Manager ICT of de leidinggevende van de gebruiker escaleren naar de vertegenwoordiger van zijn gemeente in het directieberaad.

5.2 Calamiteitenprocedure

In geval van ernstige verstoringen die langere tijd duren of een grote impact hebben treedt de calamiteitenprocedure in werking. Zie voor de uitwerking van deze calamiteitenprocedure in Bijlage 1.

6 Kosten en financiering

6.1 Bepaling bijdrage per deelnemer

Voor 2018 zijn de bijdragen reeds vastgesteld in de begroting 2018. Met ingang van begrotingsjaar 2019 wordt toegewerkt naar de volgende financieringsstructuur:

Er wordt onderscheid gemaakt tussen de volgende kostensoorten:

1. Gemeentespecifieke lasten;
2. Centrale lasten.

Ad. 1) de gemeentespecifieke lasten zijn kosten die specifiek zijn voor de individuele deelnemers en vaak ook locatiegebonden zijn, zoals:

- ✓ de individuele werkplekken (PC's, monitoren, laptops, tablets, etc.);
- ✓ de werkplek gebonden (kantoorautomatisering)software (Windows-licenties, Microsoft-Office, Antivirus, etc.);
- ✓ specifieke servers inclusief hun besturingssoftware.

Deze kosten worden één op één doorberekend aan de betreffende gemeente.

Ad. 2) de centrale lasten betreft alle personele lasten en de kosten van de inrichting, het onderhoud en het beheer van de gezamenlijke rekencentra, storage, servers, netwerk en overige kosten. Voor de financiering zijn er 2 tarieven berekend, namelijk:

1. Tarief voor een virtuele werkplek;
2. Tarief voor storage gebruik.

Bij de begroting wordt er bepaald hoeveel virtuele werkplekken er per deelnemer in gebruik zijn, alsmede het aandeel in het storage gebruik. Dit bepaald de bijdrage van de deelnemer.

6.2 Kosten voortvloeiend uit datalek

De kosten welke voortvloeien uit een opgelegde boete dan wel een aansprakelijkstelling als gevolg van een beveiligings- of datalek, worden door de deelnemers gezamenlijk gedragen naar rato van het aantal werkplekken, tenzij de aansprakelijkheid is ontstaan door grove opzet of nalatigheid van één der partijen. De aansprakelijkheid voor de geleden schade door grove opzet of nalatigheid van één der partijen, wordt door deze partij gedragen.

7 Algemene bepalingen

7.1 Wijziging van de DVO

Als een der partijen een wijziging van de afspraken in de DVO wenst op basis van substantiële wijzigingen in de behoefte van de dienstverlening door de regeling, dan zal dit aan de andere partij kenbaar worden gemaakt via het bestuur.

De manager ICT zal, na overeenstemming in het bestuur, er voor zorgen dat de gewijzigde situatie wordt beschreven in de DVO. De aanpassingen in het DVO zullen door alle deelnemende partijen moeten worden aangegaan en zal het daarvoor geldende besluitvormingstraject bij de deelnemers moeten doorlopen. De voorbereiding doet ICT NML,

het op route zetten binnen de eigen organisatie is belegd bij de accountmanagersrol van de deelnemende partij.

7.2 Rapportage en communicatiestructuur

Over de voortgang en de kwaliteit van de dienstverlening zal de manager ICT rapporteren aan:

- de accountmanagers van de deelnemers
- het bestuur

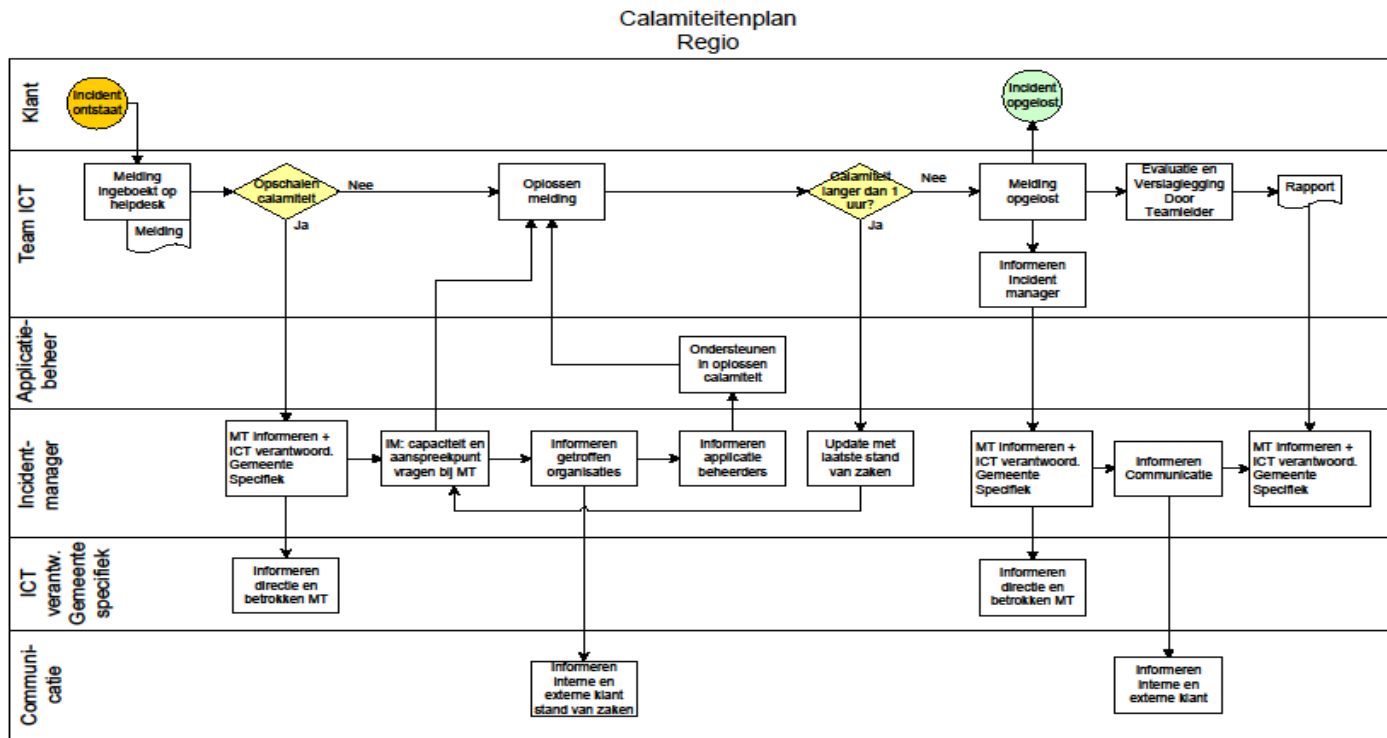
De rapportage zal gebeuren op basis van het format opgenomen in Bijlage 2. De frequentie van de rapportage is maandelijks, waarbij deze in de eerste week van de maand wordt verstuurd.

Over de afhandeling van meldingen (calls) en hun doorlooptijden zal worden gerapporteerd. Dit zal bij een verdere realisatie van de regeling verder worden ingericht.

De voortgang en resultaten vanuit ICT projecten zal door de projectleider van het desbetreffende project aan de bestuurlijk en / of ambtelijk opdrachtgever van dat project worden gerapporteerd. Door de manager ICT zal niet apart gerapporteerd worden over de ICT projecten.

Bijlage 1. Calamiteitenprocedure

Een melding van een incident of calamiteit wordt conform de regulier geldende processen gemeld bij de Helpdesk. Hier wordt een eerste beoordeling van de melding gedaan en wordt bepaald of het een incident of een calamiteit betreft. Op basis daarvan treedt onderstaande beslisboom in werking.



Bijlage 2. Sjabloon voortgangsrapportage

Regionale ICT samenwerking			
Steller:		Rapportageperiode:	
Ambtelijk opdrachtgever		Bestuurlijk Opdrachtgever:	Portefeuillehouders:

In dit rapport wordt maandelijks de belangrijkste gebeurtenissen m.b.t. de regionale ICT regeling gerapporteerd.

Belangrijkste gebeurtenissen deze periode (mijlpalen, gereed product)

Aandachtspunten en mogelijke problemen

-

Vooruitblik naar komende periode

(Gevraagde) besluiten

Planning

Status op te leveren resultaten




Realisatie Uren en Begroting




	Aantal Werkplekken	Factor
Roermond		
Venlo		
Weert		
Nederweert		

JANUARI

	Uren Bijgedragen	Uren Afgenomen	% Afgenomen	%Cumulatief
Roermond				
Venlo				
Weert				
Nederweert				

Toelichting sturingsparameters

Organisatie & Communicatie				
Kwaliteit (scope)				
(doorloop) Tijd				

-  Conform plan, geen maatregelen noodzakelijk
-  Dreigt af te wijken van het plan, maatregelen zijn gewenst cq genomen.
-  Wijkt af van het plan, maatregelen zijn noodzakelijk.

Bijlage 3. Standaarden / Infrastructuur

