Basisarchitectuur
Shared Service Centrum

1. Inhoudsopgave

Inhoud

2. Inleiding

Waarom een basisarchitectuur

Voorloper of een slimme volger? “Het braafste jongetje van de klas” of opzoeken van randen? Gedegen en betrouwbaar of meer aan toeval overlaten? In de afgelopen jaren zien we een verschuiving van de focus van traditioneel beheersmatig naar meer vernieuwend, al blijft betrouwbaarheid en voorspelbaarheid vanzelfsprekend hierbij van groot belang. Er zijn ambities om te innoveren en om meer de randen op te zoeken door te experimenteren; natuurlijk enkel wanneer dit bijdraagt aan de organisatiedoelen. Het innoveren en experimenteren is geen doel op zich. Dit onderschrijft de noodzaak van een heldere basisarchitectuur dat als referentie inzicht, duidelijkheid en richting geeft. Met dit in het achterhoofd is de ‘Basisarchitectuur’, in het vervolg genaamd ‘BAS’ opgezet.

Hoe gaan we om met gegevens? Wat past er wel en niet binnen onze informatievoorziening? Wanneer voldoen we aan wet- en regelgeving? Zijn we toekomstbestendig? Allemaal voorbeelden van vragen die gesteld worden binnen de wereld van de informatievoorziening. Binnen onze organisaties zijn er op dit gebied verschillende beleidsuitgangspunten en afspraken bedacht, beschreven en uitgewerkt om richting te geven. Maar waar is dit eenvoudig (terug) te vinden, wat is leidend en hoe is het toe te passen?

Met deze BAS is vanuit informatiebeleid een document gemaakt waarin een bundeling is gemaakt van het aanwezige beleid en de beschreven afspraken van de samenwerkende organisaties. Voor het belangrijkste deel zijn dit beleid en afspraken overeenkomstig. Wel is het mogelijk dat er op elementen verschillen bestaan. In dit document wordt de basisarchitectuur beschreven die voor alle deelnemers geldt. Daarbij is er gepoogd om dit te beschrijven op een manier die ook goed toe te passen is in de praktijk. Hiermee is de BAS, de opvolger en verdere doorontwikkeling van de PSA die tot nu in gebruik was.

De BAS is leidend voor de Informatievoorziening van de onder het Shared Service Centrum samenwerkende organisaties (Noardeast-Fryslân, Dantumadiel, De Friese Waddeneilanden, Leeuwarden, Waadhoeke en de Dienst Sociale Zaken en Werkgelegenheid Noardwest Fryslân).

Dit document beschrijft de huidige (grotere) componenten van de informatievoorziening en geeft inzicht in de beleidskaders op het gebied van informatiearchitectuur, Gegevensmanagement, Informatiebeveiliging, Privacy, ICT-architectuur en Recordmanagement. Deze beleidskaders zijn zo ver als mogelijk overgenomen of afgeleid van landelijke wetgeving (wo. AVG en de Archiefwet) en overheidsstandaarden (wo. GEMMA). Gezamenlijk vormt dit de ‘Basisarchitectuur’ van onze organisaties.

Hoe is het document opgebouwd?

De eerste hoofdstukken (hoofdstuk 4 t/m 6), geven de context van dit document weer, geven inzicht in wat de basisarchitectuur inhoudt, op welk speelveld we ons begeven en hoe we omgaan met aanpassingen en uitbreidingen van de informatievoorziening . Hierna volgt er een hoofdstuk dat per beleidsterrein laat zien welke principes ten grondslag liggen aan beleidskeuzes, gevolgd door een aantal hoofdstukken waarin per beleidsonderdeel uitgelegd wordt waar welk vakgebied over gaat (hoofdstuk 8 t/m 12).

Het doel van het document is tweeledig. Het geeft inzicht in de achterliggende principes en context waar het informatiebeheer aan moet voldoen en levert tegelijkertijd een handvat voor de praktische uitwerking.

Voor wie en wanneer te gebruiken?

De BAS is primair bestemd voor de volgende doelgroepen:

- (potentiële) leveranciers
- (potentiële) SSC klanten / afnemers
- Opdrachtgevers (lijnmanagement)

- Functioneel ontwerpers
- Functioneel beheerders / Applicatiebeheerders
- Technisch beheerders
- Projectleiders
- Functionarissen in het i-domein: Recordmanagers, i-Architecten, Informatie-adviseurs, functionarissen security en Privacy (FG's en CISO's)
- Service Managers

3. Basisarchitectuur

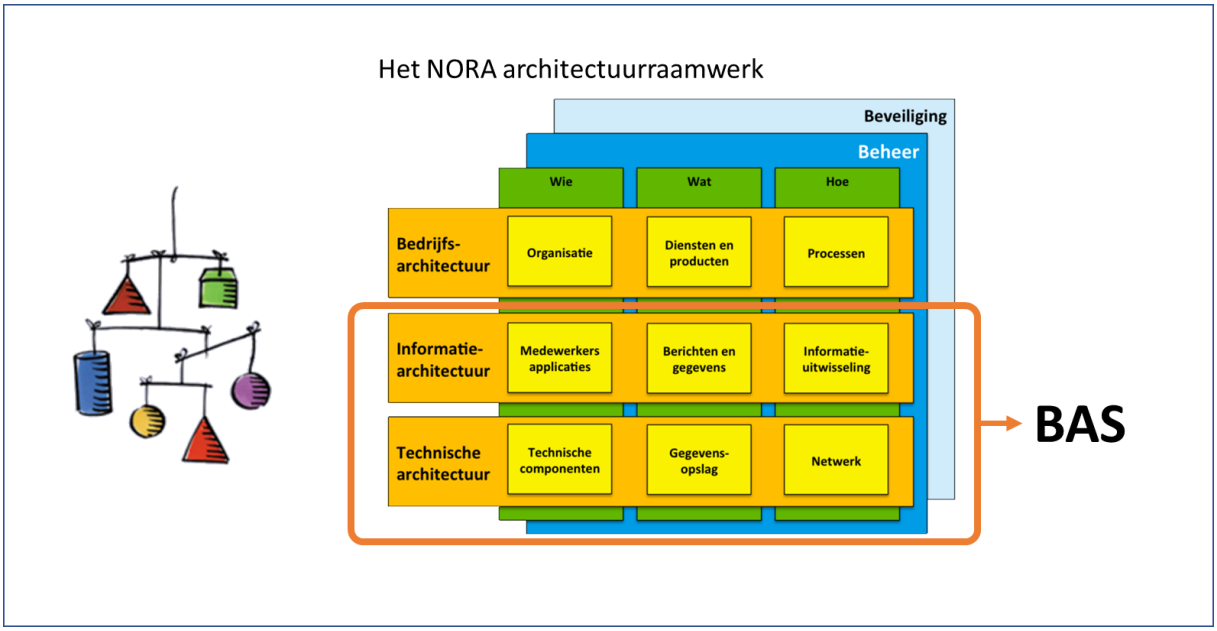
Gemeenschappelijke basisarchitectuur

De BAS is een uitwerking van een gemeenschappelijke basisarchitectuur, maar wat is een basisarchitectuur?

In een basisarchitectuur wordt vastgelegd welke principes gehanteerd worden en daarnaast worden richtinggevende uitspraken gedaan om tot een wenselijke situatie te komen. Hiermee zorgt het voor inzicht, duidelijkheid en richting. Een basisarchitectuur helpt om ontwikkelingen in samenhang en gestandaardiseerd aan te sturen. Ontwikkelen, bouwen, aanschaffen en implementeren onder architectuur zorgt ervoor dat de oplossingen onderling goed samenwerken en elkaar aanvullen. Een basisarchitectuur kan dan ook gezien worden als richtinggevend en sturend instrument. Dit geldt zowel in de bouwsector als op het gebied van informatievoorziening.

In de NORA- en GEMMA-referentiearchitecturen wordt uitgegaan van 3 architecturen of architectuurlagen. De Bedrijfsarchitectuur, de Informatiearchitectuur en de Technische architectuur. Deze architectuurlagen worden soms afgebeeld als onderdelen in een mobile. Elke aanpassing op een bepaald niveau heeft gevolgen voor de andere niveaus: de hele mobile raakt in beweging. Als je beleidsdoelstellingen of wettelijke taken veranderen, heeft dat gevolgen voor de eisen aan de informatievoorziening. En de technische architectuur is voorwaardelijk voor de uitvoering van het geheel.

In de BAS ligt de nadruk op de Informatiearchitectuur. De Technische Architectuurprincipes, kern en architectuurkeuzes komen aan de orde bij het onderdeel ICT-Architectuur en in bijlage ICT standaarden. De Bedrijfsarchitecturen van de deelnemende organisaties verschillen en zijn niet in samenhang vastgelegd. Dit onderdeel komt in de BAS niet aan de orde.



In de BAS zijn de relevante aspecten uit de beleidsterreinen informatiearchitectuur, gegevensmanagement, records management, informatiebeveiliging, privacy en ICT architectuur verwerkt. Voor deze BAS hebben alle beleidsverantwoordelijken van de genoemde beleidsterreinen vanuit hun perspectief input geleverd. Onderdelen die op vrijwel alle terreinen van toepassing zijn, zijn als basisprincipes opgenomen. Hier doorheen loopt de basis die voor ieder terrein van toepassing is. Dit is ook duidelijk zichtbaar in de hoofdstukken 7 tot en met 12 waarin begonnen wordt met informatievoorziening in algemene zin waarna de verschillende disciplines aan de orde komen.

Principes

Maar wat zijn nou die principes en waarom zijn deze benoemd? De principes kunnen gezien worden als de fundamentele uitgangspunten die er zijn om te komen tot een betrouwbare, gedegen en inzichtelijke informatievoorziening. Denk hierbij bijvoorbeeld aan de afspraak om 'onder architectuur' te werken, of de afspraak om te gaan voor reductie van complexiteit, dus voor eenvoud. Dit zijn afspraken die bijdragen aan het behoud van samenhang en inzichtelijkheid in de informatievoorziening. Maar ook meer specifieke principes zijn benoemd, bijvoorbeeld: "We streven naar eenmalig opslag, meervoudig gebruik" of "we hebben in de basis-infrastructuur geen single point of failures". Bij de eerste is het doel om te komen tot een gecontroleerde gegevenshuishouding waarbij er één "waarheid" bestaat. Dit draagt ook weer bij aan een het hoofdprincipe: "We voldoen aan wet- en regelgeving" en zorgt hiermee voor betrouwbaarheid, gedegenheid en duidelijkheid. Hetzelfde geldt voor "we hebben in de basisinfrastructuur geen single point of failures". Dit principe volgt uit "we ondersteunen maximaal de processen in onze organisaties" en dit draagt bij aan een betrouwbare informatievoorziening.

Als context voor de verschillende principes wordt in de hoofdstukken 8 tot en met 12 het domein en de kern van elk beleidsterrein geschetst. Daarmee wordt ook de samenhang tussen de disciplines duidelijk. Deze context kan gebruikt worden om bij vraagstukken na te gaan met welke vakgebieden afstemming te zoeken is.

Hoe toe te passen?

Door het document heen worden er uitstappen gemaakt naar de toepassing in de praktijk. Hier is bewust voor gekozen omdat dit juist een leidraad moet zijn voor de dagelijkse operatie. In hoofdstuk 6 is een richtlijn beschreven waar ingegaan wordt op de vraag "Hoe werken we?". Beheersbaarheid en inzicht zijn belangrijk, daarom is ten behoeve van het "aanschaffen en vervangen van toepassingen" een beschrijving opgenomen voor een eenduidige manier van werken. Omdat deze basisarchitectuur niet gezien moet worden als een set harde spelregels en een meetlat om te toetsen, maar juist meer als een handvat om vooraf te kunnen kijken wat passend is, wordt er groot belang gehecht aan die manier van werken. De basisarchitectuur en ook de functionarissen van de verschillende beleidsterreinen kunnen in het beginstadium worden gezien als referentie en denkkracht om met elkaar te bekijken hoe een ontwikkeling past binnen het grote geheel. Waarmee we er gezamenlijk voor zorgen dat we blijven voldoen aan wet- en regelgeving, dat we blijven voldoen aan architectuurprincipes en dat we handelen binnen de privacynormen en -waarden die we als organisatie hebben omarmd.

4. Samenwerkingsverband Noord Friesland

Sinds meerdere jaren werken de 4 Friese Waddeneilanden, De Dienst Sociale Zaken Noardwest-Fryslân, gemeente Noardeast Fryslân, gemeente Leeuwarden en gemeente Waadhoeke samen op het gebied van Informatievoorziening.

Het doel van de samenwerking is het verbeteren van de kwaliteit en efficiëntie van de informatievoorziening in de hele regio. Door te streven naar een gezamenlijk informatiebeleid van alle deelnemers, kunnen schaalvoordelen worden behaald, kan kennis worden gedeeld en kunnen de beschikbare middelen optimaal worden ingezet.

De samenwerking is vormgegeven in de volgende activiteiten:

1. Het beheren, ontwikkelen en vernieuwen van de functionele standaarden van de regionale samenwerking;

2. Het harmoniseren van (de ontwikkeling van) het informatiebeleid van de deelnemers, waaronder informatiebeveiliging, gegevensmanagement, records management en de informatiearchitectuur;

3. Het bevorderen van de standaardisatie van de inrichting van applicaties van de deelnemers;

4. Het afstemmen en waar mogelijk of gewenst integreren van de applicatieportfolio's van de deelnemers;

5. Het afstemmen en waar mogelijk of gewenst integreren van de projectportfolio's van de deelnemers;

6. Het afstemmen van de gewenste aanpassingen in de ICT-dienstverlening van de gemeente Leeuwarden (servicecatalogus en dienstverleningsovereenkomst).

7. Het uitwisselen van kennis en van elkaar leren op het gebied van informatiemanagement en ICT.

De samenwerking is contractueel vastgelegd in de diverse overeenkomsten: een centrumregeling, de servicelevel agreement (SLA), de productendienstencatalogus (PDC) en uitvoeringsafspraken (DAP). Naast deze formeel vastgelegde vormen van samenwerking, worden er specifieke afspraken gemaakt over de samenwerking. Dit kan per gremium, type dienstverlening en project/programma verschillen. Hoe de samenwerking wordt ingericht hangt af van de behoefte en kan verlopen van klant-leverancier-relatie tot een relatie van gelijkwaardige partners.

We zien dat de samenwerking op het gebied van ICT en dat van Informatiemanagement (IM) verschilt. Globaal opereert het SSC Leeuwarden als Centrumgemeente voor de levering, dan wel uitbesteding, van *ICT-faciliteiten* (infra-omgeving, werkplekken, telefonie e.d.). Deze faciliteiten worden door SSC-ICT ingekocht en uitgerold ten behoeve van de samenwerkende organisaties. De organisaties leveren daarbij regulier wensen aan met betrekking tot deze voorzieningen. Deze samenwerkingsvorm kan als klant-leverancier-model worden gezien.

Op het gebied van Informatiemanagement (applicaties, gegevens, koppelingen e.d.) is er vooral een samenwerkingsvorm. De organisaties trekken zoveel mogelijk gezamenlijk op bij besluitvorming over, het beheer van en de (door)ontwikkeling van één regionale informatievoorziening.

Voor de samenwerking zoals deze wordt beoogd binnen het SSC, hanteren we het volgende Governancemodel, bestaande uit de volgende overlegvormen:

1. Ontwikkeltafel: vertegenwoordigd door één i-manager/manager dienstverlening per organisatie. Besluit over regionale ontwikkelingen met betrekking tot de gezamenlijke i-voorziening.
2. SSC Tafel: vertegenwoordigd door één 'bedrijfsvoeringsmanager per organisatie. Evalueert het lokaal en regionaal functioneren van met name de door het SSC geleverde dienstverlening.
3. RIA: vertegenwoordigd door alle i-adviseurs van de organisaties. Adviseert aan Ontwikkel- en Experttafel en is bedoeld voor kennisdelen en standpunt bepalen bij ontwikkelingen met betrekking tot regionale en lokale informatievoorziening. Neemt initiatief voor jaarlijkse regionale en lokale ICT-behoeftemanagementcyclus.
4. Experttafel: vertegenwoordigd door één regionale specialist per domein (ICT Architectuur, IM Architectuur, RIA, Records Management, Gegevensmanagement, Informatiebeveiliging en Gegevensbescherming (Privacy)). Afstemming met lokale specialisten wordt door de vertegenwoordigend specialist georganiseerd. Toetst: voorgenomen ontwikkelingen m.b.t. de Informatievoorziening aan BAS principes en uitvoerbaarheid. Adviseert aan de Ontwikkeltafel.
5. Change Advisory Board (CAB): vertegenwoordigd door één Leeuwarder specialist per domein (ICT Architectuur, IM Architectuur, Records Management, Gegevensmanagement, Informatiebeveiliging en Gegevensbescherming (Privacy)). Regio-collega's kunnen op eigen initiatief bij ieder CAB aansluiten. Toetst: ingebrachte wijzigingen m.b.t. de Informatievoorziening aan BAS principes en uitvoerbaarheid.
6. Security Overleg Noord Friesland: vertegenwoordigd door Chief Information Security Officers van de deelnemende organisaties. Houdt toezicht op informatieveiligheid van de deelnemende organisaties.
7. Privacy Overleg Noord: vertegenwoordigd door de Functionarissen Gegevensbescherming van gemeente Noardeast-Fryslân, Waadhoeke, Dienst Sociale Zaken en Werkgelegenheid Noardwest Fryslân, de Friese Waddeneilanden en de gemeente Leeuwarden.

8. Regionaal Functioneel Applicatiebeheer: voor enkele applicaties wordt regionaal samengewerkt op het gebied van Functioneel Applicatiebeheer.

Naast de genoemde samenwerkingspartners levert het SSC Leeuwarden ook informatievoorzieningsdiensten aan het Regionaal Informatie- en Expertise Centrum Noord-Nederland (RIEC-Noord), Het Veiligheidshuis Fryslân, Hûs en Hiem en, bv SPORT. De inhoud van dit document is ook op deze partners van toepassing.

Deze 'Basisarchitectuur' is een gezamenlijk product; de 'spelregels' worden regiobreed toegepast.

In de samenwerking worden ook veel diensten, bijvoorbeeld voor ICT- infrastructuur en informatiesystemen, van verschillende leveranciers afgenomen. Afspraken worden vastgelegd in overeenkomsten. Gemeente Leeuwarden hanteert hiervoor standaardovereenkomsten, die landelijk beschikbaar gesteld worden, zoals de GIBIT-inkoopvoorwaarden en de standaard verwerkersovereenkomsten, die is afgeleid is van de VNG-standaard.

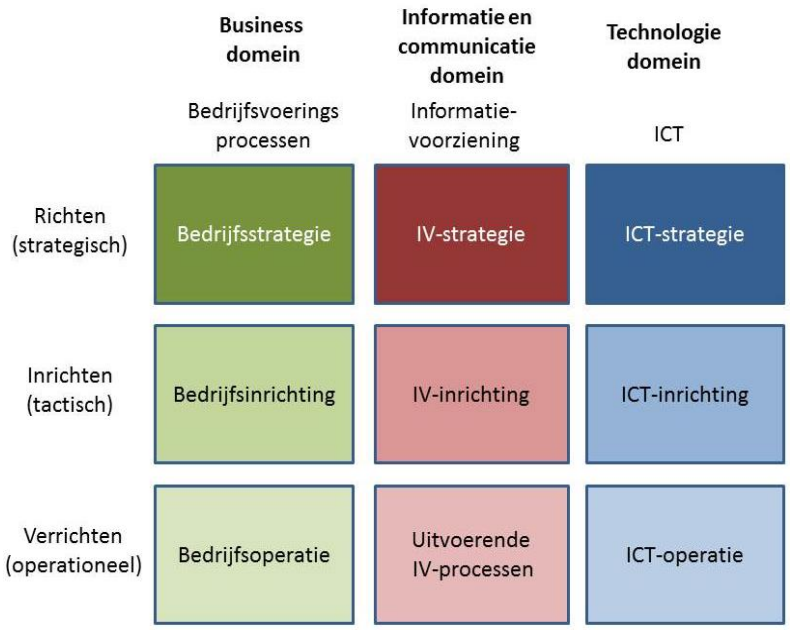
5. Aanpak bij aanschaf en vervanging van toepassingen

Voor iedere nieuwe of te vervangen toepassing volgen we een uniforme aanpak. Belangrijk hierbij is dat de behoefte vanuit de organisatie leidend is, maar ook dat de gekozen oplossing aansluit bij de in dit document vastgelegde architectuurkeuzes en - beleid. Dit laatste om ervoor te zorgen dat de oplossing kan functioneren binnen de al bestaande informatievoorziening en voldoet aan geldende wetten en richtlijnen.

Vanuit het RIA hebben we afgesproken alle nieuwe ontwikkelingen in gezamenlijkheid op te pakken. Natuurlijk kan het voorkomen dat een behoefte aan een nieuwe oplossing of een vervanging maar in één organisatie speelt. Dan nog zijn dezelfde 'spelregels' uit dit document van toepassing. Er bestaan immers geen op zichzelf staande oplossingen meer, er is altijd een relatie met de bestaande/gezamenlijke infrastructuur, architectuur en applicaties.

Het onderstaande '9-vlaks model van Maes' [1] wordt veel gebruikt om de informatievoorziening binnen een organisatie schematisch weergegeven. De domeinen bedrijfsvoering, informatievoorziening en ICT-technologie (kolommen) zijn hier afgezet tegen de niveaus van operatie (strategisch, tactisch en operationeel). In dit document hebben we de IV- en ICT-strategie vertaald naar concrete richtlijnen voor de IV- en ICT-inrichting. Hierbij is ook rekening gehouden met de belangen die spelen op de operationele laag, de oplossing moet tenslotte wel beheerbaar zijn.

[1] Ook bekend als het Amsterdams Informatiemodel (AIM); R. Maes, 2003, Informatiemanagement in kaart gebracht



De uniforme aanpak bij aanschaf en vervanging van toepassingen bestaat uit de inventarisatiefase, de inkoopfase en de realisatiefase. Tijdens de verschillende fases kan de Experttafel worden geconsulteerd bij issues, knelpunten en complexe vraagstukken, zowel binnen een project als in het overlappende deel over projecten heen. Ieder project wordt afgesloten met een evaluatiefase.

De nadere uitwerking van de aanpak bij aanschaf en vervanging valt onder de opdracht, vanuit de ontwikkeltafel, tot het komen van regionale governance. Deze wordt aan de volgende versie van de BAS toegevoegd.

6. Architectuurprincipes

Basisprincipes

1. We digitaliseren diensten en processen
2. We gaan zoveel mogelijk uit van generieke processen.
3. We beperken zoveel mogelijk het aantal gebruikte applicaties, oplossingen en producten.
4. We werken binnen onze organisatie onder deze (BaS)architectuur.
5. We omarmen de NORA- en GEMMA-architecturen.
6. We omarmen het gedachtengoed van Common Ground
7. We voldoen aan geldende wet- en regelgeving.
8. We ondersteunen optimaal en kostenefficiënt de processen in onze organisaties.
9. We gebruiken alleen producten waarop ondersteuning, bv. door leverancier, wordt geleverd
10. We voldoen aan de standaarden van Forum Standaardisatie.
11. We gaan uit van toekomstbestendige oplossingen.
12. We hebben geen voorkeur voor cloud of on-premise oplossingen.
13. We nemen ‘Open Source’-oplossingen mee in het keuzeproces van nieuwe ICT-oplossingen.
14. We borgen beschikbaarheid, integriteit, vertrouwelijkheid, bruikbaarheid, voortbestaan en aantoonbaarheid.

Principes recordmanagement

De onderstaande principes zijn gebaseerd op artikel 3 van de Archiefwet waar gesproken wordt over de verplichting voor overheden hun informatie in goede, geordende en toegankelijke staat te brengen en te houden en tevens de verplichting om te kunnen vernietigen. Daarbij geldt dat de informatie in ons beheer openbaar is tenzij op grond van bepalingen in wetgeving restricties op deze openbaarheid wordt gesteld

1. Wij zorgen dat *alle informatie in ons beheer* in een goede, geordende en toegankelijk staat is of wordt gebracht. Ongeacht of het gaat om blijvend te bewaren of op termijn te vernietigen informatie.
2. We beschikken over een overzicht van onze processen, projecten en andere activiteiten met de daarbij behorende
    a. informatie,
    b. informatieobjecten,
    c. de wettelijke bewaartermijnen,
    d. beheerprocessen,
    e. functionaliteiten voor het beheer en
    f. toe te passen of toegepaste technieken.
3. We houden de informatie en haar context gedurende de wettelijke bewaartermijn beschikbaar en toegankelijk.
4. We houden de integriteit en verschijningsvorm van onze informatieobjecten gedurende de wettelijke bewaartermijn in stand.
5. We kunnen informatie inclusief haar ontstaanscontext vinden en gebruiken.
6. Wij verrijken onze informatie met administratieve, beschrijvende en technische metagegevens, om de vindbaarheid, raadpleegbaarheid en interpreteerbaarheid van deze informatie nu en in de toekomst te waarborgen.
7. We vernietigen informatie waarvan de wettelijke bewaartermijn is verstreken.
8. We kunnen informatie inclusief haar context met behoud van integriteit uitwisselen met andere systemen en/of andere organisaties.

Principes gegevensmanagement

1. We streven naar eenmalig opslag, meervoudig gebruik.
2. We beheren de kwaliteit van gegevens actief en zorgen voor de beschikbaarheid van juiste gegevens.
3. We hanteren uniforme definities voor gegevens.
4. We stellen openbare gegevens actief en conform de eisen aan ‘open data’ beschikbaar voor hergebruik door derden.

Principes informatiebeveiliging

1. We hebben een actueel informatiebeveiligingsbeleid. Dit beleid is gebaseerd op de standaard voor overheden: de Baseline Informatiebeveiliging Overheid (BIO)
2. We hebben onze informatiebeveiliging ingericht op basis van inzicht in bestaande dreigingen en risico’s, de potentiële impact hiervan en onze risicobereidheid. Dit bepaalt de maatregelen die we nemen. We beseffen ons dat het realiseren van een 100% veiligheid onmogelijk is.
3. We leggen het gewenste informatiebeveiligingsniveau vast in de vorm van minimumeisen. Op basis van wet- en regelgeving, overeenkomsten met andere overheden en derden, of bij bijzonder kwetsbare en vitale componenten van de informatievoorziening, kan op onderdelen een hoger niveau van informatiebeveiliging gelden. Daarnaast wordt het voldoen aan relevante normenkaders van diverse audits op het gebied van informatieveiligheid als minimumeis gezien.
4. We hebben een governancestructuur ingericht die effectieve informatiebeveiliging mogelijk maakt. We wijzen per informatiesystemen een systeemeigenaar aan, en voor elk proces wijzen we een proceseigenaar aan.
5. We onderkennen het risico van menselijk handelen voor informatiebeveiliging. Daarom ondersteunen we een cultuur waarin medewerkers zich bewust zijn risico’s. We moedigen open communicatie hierover aan.
6. We voeren voor bestaande en nieuwe informatiesystemen een Basis-Beveiligings-Niveau (BBN-) toets uit, op basis van de BIO, om vast te stellen welke maatregelen op grond van de BIO verplicht gelden

ten aanzien van deze systemen. Voor nieuwe systeem wordt het uitgangspunt van ‘security by design’ toegepast.
7. We classificeren informatiesystemen, en de output van deze systemen volgens de Handreiking ‘Dataclassificatietoets BIO gemeenten’ (VNG, 2021) en zorgen dat deze minimaal beveiligd zijn volgens het bepaalde classificatieniveau. Aanvullend wordt voor de informatiesystemen met classificatie vertrouwelijk en hoger een risicoanalyse uitgevoerd.
8. We nemen die maatregelen die relevant zijn voor de beveiliging van informatie op verschillende momenten in de levenscyclus van informatie .
9. We bereiden ons voor op informatiebeveiligingsincidenten om de impact op de dienstverlening en bedrijfsvoering te beperken.
10. We onderkennen onze verantwoordelijkheid voor informatiebeveiliging bij uitbestede systemen en processen. We kiezen voor een integrale ketenbenadering voor het bepalen van risico’s en maatregelen.

Principes privacy

We voldoen aan de Algemene Verordening Gegevensbescherming (AVG) en (inter)nationale wet- en regelgeving met betrekking tot gegevensbescherming. Dit komt tot onder meer tot uitdrukking in de hierna genoemde principes:

1. We zijn transparant.
2. We zorgen voor minimale gegevensverwerking.
3. We zijn zorgvuldig.
4. We kunnen aan inzage-, correctie-, en verwijderingsverzoeken voldoen.
5. We maken afspraken met andere partijen, zoals leveranciers van applicaties en hostingbedrijven, die voor of namens ons de persoonsgegevens van onze betrokkenen verwerken.

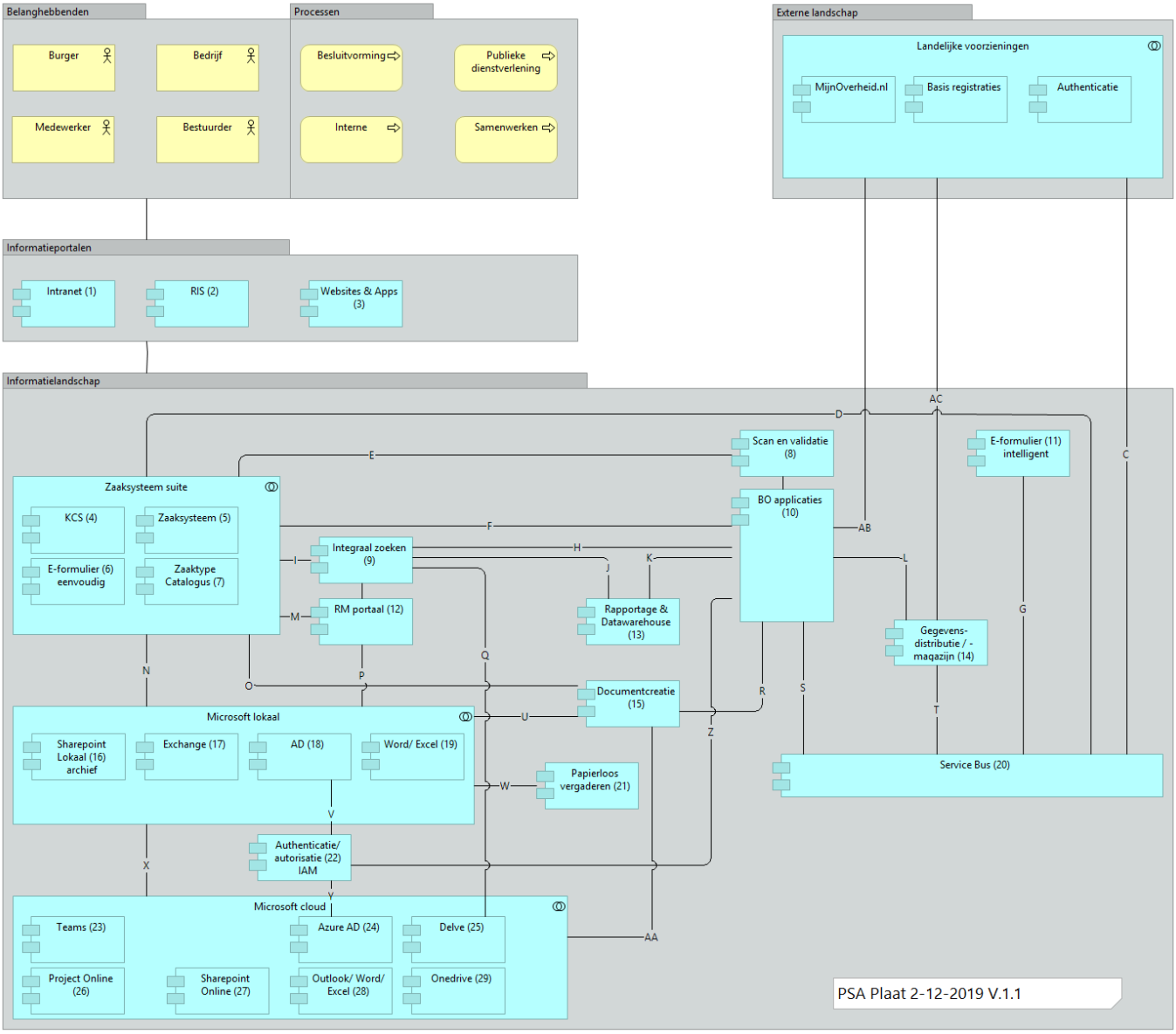
Principes ICT-architectuur

1. We hebben in de basisinfrastructuur geen ‘single point of failures’.
2. We beperken het aantal en soorten hardware, OS en software.
3. We streven naar flexibiliteit in schaalbaarheid en kunnen daarmee krimp, groei en ambities van de organisatie volgen.
4. We gaan uit van uniformiteit en standaardproducten.
5. We leveren een werkplek volgens “elke plaats en elk device”.
6. We geven de voorkeur aan marktconforme oplossingen, met een voldoende marktaandeel.

7. Kern informatievoorziening

Onderstaande afbeelding visualiseert de nieuwe (doel)architectuur van de samenwerkende organisaties in Noord Friesland. In bijlage Toelichting componenten worden de verschillende componenten per corresponderend nummer toegelicht.

Nieuwe toepassingen moeten maximaal van deze (generieke) componenten gebruik maken. Waar dat echt niet mogelijk is, is een onderbouwing voor de afwijking en beschrijving van de alternatieve oplossing benodigd. Iedere afwijking wordt beoordeeld door de Experttafel.



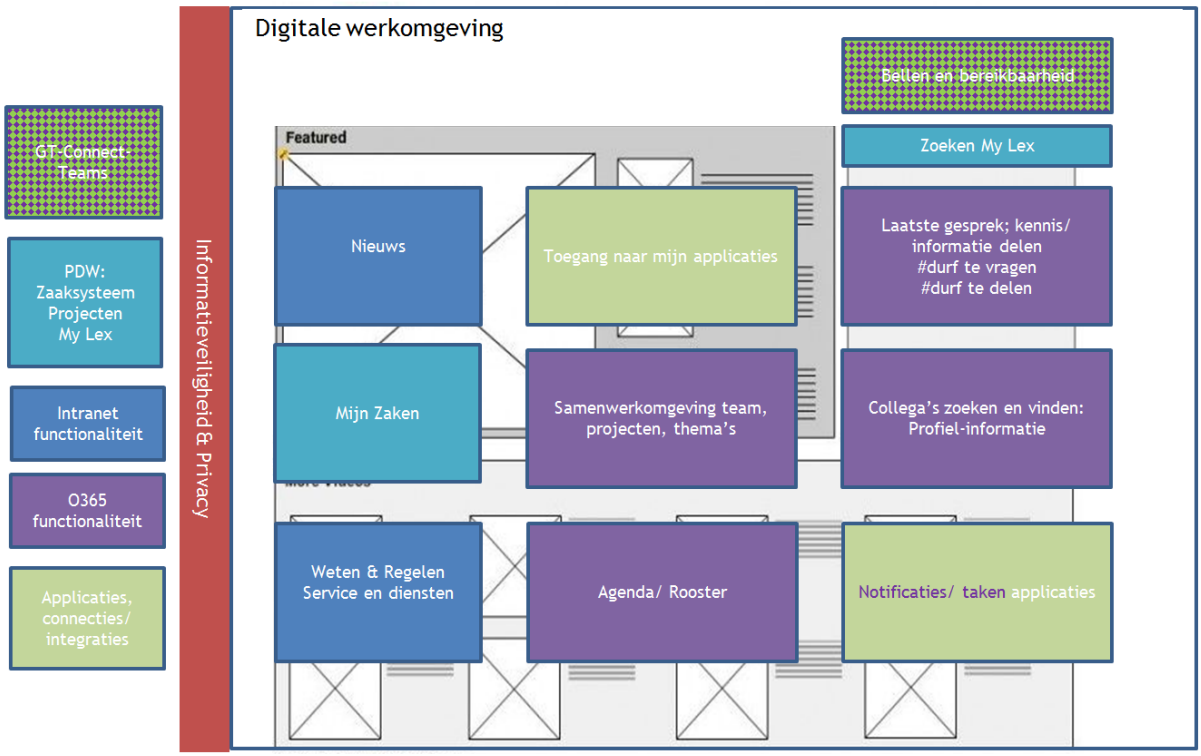
Portaal als centrale toegangspagina voor medewerkers

'Gebruiksvriendelijkheid' is cruciaal voor wat betreft toepassingen in het informatielandschap. Het werken met verschillende leveranciers zorgt voor verschillend werkende- en ogende oplossingen. Dit is onvermijdelijk. De integrale zoekfunctionaliteit maakt het mogelijk om door de verschillende toepassingen (en door het digitale archief) heen te zoeken. Er wordt een portaalpagina gecreëerd waarop de verschillende oplossingen naast elkaar gepresenteerd worden en opgeroepen kunnen worden. Ook de centrale zoekingang wordt op deze pagina beschikbaar gesteld en is dus altijd snel oproepbaar. Intranetfuncties zijn hier ook aan toegevoegd.

Gaandeweg zal het aantal toepassingen op deze pagina steeds verder groeien. De portaalpagina zal steeds meer de logische en eenvoudige toegang zijn tot een groot deel van de gemeentelijke informatie en informatiesystemen en zal onderdeel worden van het intranet.

De portaalpagina kan als volgt functioneel worden gevisualiseerd:

Digitale Werkomgeving



8. Kern Records management

Records management is dat deel van het informatiebeheer waarmee conform wettelijke vereisten op aantoonbare manier gedurende de (wettelijke) bewaartermijnen vorm wordt gegeven aan (1) de integriteit, betrouwbaarheid, vindbaarheid en bruikbaarheid van informatie die een functie heeft in een proces, project of andere activiteit, (2) het voortbestaan, beschikbaarheid en toegankelijkheid van die informatie en (3) het vernietigen, vervangen of overdragen van die informatie.

Het is van groot belang dat de overheid haar informatie op orde heeft, daarom is deze verplichting in wettelijke taken vastgelegd in de Archiefwet 1995 en onderliggende regelgeving.[2]

Op basis van juiste en volledige informatie kunnen correcte besluiten worden genomen. Wanneer de betrouwbaarheid en volledigheid van informatie aangetoond kan worden is controleerbaarheid, toetsing, reconstructie en verantwoording van handelen zeer goed mogelijk. Dit biedt een stabiele basis voor de dienstverlening, het concept van de iOverheid en de e-gemeente. Op deze manier kunnen bijvoorbeeld bezwaarschriften, schadeclaims en onnodige (financiële) risico's tot een minimum beperkt blijven. Ook worden de bestuurlijke integriteit en het imago van de gemeente hierdoor versterkt.

Er is een aantal argumenten om gegevens te verwerken, te genereren, op te nemen, te bewaren, toegankelijk te maken, beschikbaar te stellen, maar ook om gegevens na het verstrijken van de bewaartermijn zo snel mogelijk te vernietigen. Deze argumenten of beter belangen en het daarvan afgeleide goede informatiebeheer overstijgen het belang van alleen de bedrijfsvoering.

[2] En straks ook de Wet open overheid (WOO)

Wij zorgen daarom dat de gemeentelijke informatiehuishouding om de volgende redenen op orde is:

1. ***Democratisch belang*** - Zonder een goede en betrouwbare informatiehuishouding kan de gemeente aan belanghebbenden geen verantwoording afleggen of inzicht geven in haar handelen. Dit belang omvat elementen als openbaarheid, formele besluitvorming, rechtmatigheidstoetsing, controle door de Raad en de gemeentelijke rekenkamercommissie, 'good governance' en in relatie daarmee de algemene beginselen voor behoorlijk bestuur (ABBB). Deze zijn essentieel voor onze democratie en het vertrouwen van de burger in de overheid.
2. ***Administratief belang*** **-** Betrouwbare en snel vindbare informatie is een productiemiddel en is nodig voor de dagelijkse gang van zaken. Op basis van de beschikbare informatie neemt de gemeente besluiten die direct van invloed zijn op inwoners, bedrijven en de eigen organisatie.
3. ***Juridisch belang –*** Aan overheidsinformatie kunnen naast de gemeente zelf, inwoners en bedrijven, rechten ontlenen. Ook kan overheidsinformatie voor inwoners en bedrijven belangrijke bewijswaarde bevatten.
4. ***Economisch belang*** – Veel van de diensten, goederen, producten en activiteiten van de overheid zijn op geld te waarderen. Een voorbeeld daarvan is het beschikbaar stellen van overheidsinformatie in de vorm van open data. Een ander voorbeeld zijn het openbaar beschikbaar stellen van ruimtelijke plannen of materiaal waar de gemeente het intellectueel eigendom van heeft zoals foto's en andere werken. Zelf kan de gemeente een efficiency winst behalen en dus ook een economisch voordeel uit een informatiehuishouding die op orde is en het gebruik maken van betrouwbare data bij het datagedreven werken. Een wanprestatie van de kant van de gemeente kan leiden tot een financiële claim.
5. ***Cultureel-historisch belang –*** *Een deel van de (digitale) overheidsinformatie* van nu heeft een cultureel-historische waarde. Een informatiehuishouding van nu die niet op orde is, is een bedreiging voor de historische bronnen en het cultureel erfgoed van morgen.

Records management is breder dan alleen dan het beheer van het RM- of archiefsysteem. Om informatie duurzaam toegankelijk te maken en te houden, moet de organisatie op elk moment van de levenscyclus van informatie maatregelen nemen. Dit is wanneer er sprake is van

- Creëren en opnemen van informatie;
- Classificeren en Registreren;
- Kwaliteitscontroles;
- Opslag;
- Gebruik en hergebruik;
- Migratie en conversie (vervanging);
- Verwijderen van informatie (vernietigen of verplaatsen) of:
- Overbrengen van blijvend te bewaren informatie naar een archiefbewaarplaats.

9. Kern gegevensmanagement

Gegevens zijn het vierde bedrijfsmiddel binnen organisaties. Wanneer een organisatie een gedegen en transparante gegevenshuishouding heeft, kunnen gegevens op diverse manieren benut worden het realiseren van doelstellingen van de organisatie.

Binnen gemeenten zijn er veel gegevens in omloop, en wordt er op grote schaal data geproduceerd en verrijkt; het is als het ware een datafabriek. Maar hoe zorgen we er nou voor dat deze rijkdom aan gegevens ook optimaal benut kan worden en omgezet kan worden om informatie en inzicht te krijgen? Het antwoord hierop is door grip te hebben op gegevens. Dit wordt gerealiseerd door het maken van afspraken, inzicht hebben in de datahuishouding en voorzieningen te realiseren die deze grip faciliteren.

Daarnaast is het van groot belang om mensen bewust te maken van de rijke mogelijkheden van gegevens en wat daarvoor georganiseerd moet worden. Ook de onmogelijkheden ervan wanneer er geen grip is, moet hierbij aandacht krijgen. Dit alles is het blikveld van gegevensmanagement. Gegevensmanagement is daarmee

samen te vatten als het geheel van activiteiten om in een organisatie op het juiste moment over de juiste gegevens van de juiste kwaliteit te beschikken.

10. Kern informatiebeveiliging

Burgers, bedrijven en medewerkers mogen erop vertrouwen dat informatie en (persoons-)gegevens bij de gemeente in goede handen zijn. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren en vormt de basis voor het beschermen van rechten van burgers en bedrijven. Betrouwbare informatievoorziening houdt in dat informatie niet in handen van onbevoegden komt (‘vertrouwelijkheid’), beschikbaar is wanneer nodig (‘beschikbaarheid’) en inhoudelijk correct is (‘integriteit’). Het is van belang dat we dit ook na enige tijd nog kunnen verifiëren (‘aantoonbaarheid’). Dit vereist een integrale aanpak, duidelijke verantwoordelijkheden, de juiste maatregelen en risicobewustzijn.

Het proces van informatiebeveiliging is primair gericht op bescherming van informatie, maar is tegelijkertijd een 'vliegwiel'. Dit bewerkstellingen wij door vroegtijdig in te spelen op privacy en security gerelateerde vraagstukken door aan de voorkant mee te denken. Wij benaderen informatiebeveiliging niet normatief maar zoeken een goede balans tussen risico, beleid en informatieveiligheid. Het maakt verdergaande elektronische dienstverlening op verantwoorde wijze mogelijk, evenals nieuwe, innovatieve manieren van werken.

De scope van informatiebeveiliging omvat alle gemeentelijke processen, informatiesystemen, informatie en gegevens van de gemeente en externe partijen en omvat het gebruik en het beheer door medewerkers en externe partijen, ongeacht locatie, tijdstip en gebruikte systemen en applicaties.

Informatiebeveiliging is meer dan alleen de geautomatiseerde informatiesystemen en ICT-infrastructuur. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, beeldscherm et cetera) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen) maar ook mensen en processen.

11. Kern privacy

In 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Deze Europese verordening beschermt persoonsgegevens binnen de EER op hetzelfde niveau. De AVG stelt de kaders voor de verwerking van persoonsgegevens. Het bestuursorgaan (verwerkingsverantwoordelijke) moet kunnen aantonen dat zij aan de AVG-vereisten voldoet (‘aantoonbaarheid’).

In Nederland is de verordening uitgewerkt in de Uitvoeringswet AVG (UAVG) en diverse nationale sectorale wetgeving, bijvoorbeeld binnen het sociaal domein en de BRP. De gemeente en zijn medewerkers moeten zich houden aan een aantal wettelijke verplichtingen. Voor de gemeente maakt het de werkzaamheden, hoe gek het ook klinkt, niet wezenlijk anders dan voordat de AVG in werking is getreden. De gemeente kan gewoon haar wettelijke taken uitvoeren en moet zich daarbij houden aan de regels die in sectorale wetgeving zijn omschreven.

12. Kern ICT-infrastructuur

De kernbeschrijving ICT-infrastructuur is opgenomen in de betreffende bijlage.

13. Bijlagen

Begrippenlijst
Toelichting componenten
Relevante wetgeving
ICT-Standaarden 2024
Kernbeschrijving ICT infrastructuur
Ondersteunde bestandsformaten
Metagegevensschema
Samenwerkingsstructuur

14. Architectuurkeuzes

In dit hoofdstuk worden de hiervoor beschreven principes en uitgangspunten vertaald naar concrete architectuurkeuzes. De architectuurkeuzen zijn op de volgende wijze uitgewerkt:

Koptekst (bondig het onderwerp benoemen)
Uitgangspunt: *Beschrijf het architectuur uitgangspunt - **wat** streven we na.*
Toelichting: *Beschrijf **waarom** we dit willen.*
Uitwerking: *Geef aan **hoe** we dat denken te bereiken. Eventueel kunnen hier meerdere mogelijkheden worden benoemd (bijvoorbeeld bij verschillende invulling voor cloud/on-premise).*
Toepasbaarheid: *Geef aan wanneer de architectuurkeuzes wel of niet van toepassing zijn.*

14.1 Algemeen informatievoorziening

14.1.1 Hergebruik applicaties en componenten
Uitgangspunt: We beperken het aantal informatiesystemen zowel intern als binnen de regiosamenwerking. Nieuwe toepassingen moeten maximaal van generieke componenten gebruik maken.
Toelichting: Vanuit de gedachte een goed onderhoudbaar informatielandschap te hebben waarbij er gestreefd wordt om kosten en beheers inspanning zo laag als mogelijk te houden, beperken we het aantal te gebruiken informatiesystemen. Waar dat echt niet mogelijk is, is een onderbouwing voor de afwijking en beschrijving van de alternatieve oplossing benodigd.
Uitwerking: - Hergebruik van bestaande informatiesystemen. - Samenvoegen van informatiesystemen t.b.v. gelijke functionaliteit / GEMMA referentiecomponenten. - Kiezen van oplossingen die passen binnen het actuele landschap (zie hoofdstuk 7 - landschapsplaat) waarbij aangesloten wordt op generieke componenten (portaal/zoeken/zaaksysteem/formulieren/datadistributie/ESB)
Toepasbaarheid: Altijd (standaardset) Per traject specifiek maken (lijst van toepassingen zijnde generieke voorzieningen o.b.v. de plaat). Wanneer er geen voorzieningen hergebruikt hoeven te worden, dan kan deze eis vervallen.

14.1.2 Multitenancy
Uitgangspunt: We zetten zoveel als mogelijk in op multitenancy
Toelichting: Vanuit de gedachte dat het SSC een shared servicecenter is waarin we met meerdere samenwerkingspartners faciliteiten zo efficiënt als mogelijk inzetten, zetten we in op multitenancy. Hierbij kan multitenancy, zorgen voor lagere beheerinspanning , kosten reduceren en het informatielandschap minder complex maken.
Uitwerking: - Multitenancy is vooral relevant bij lokale installaties (on-premise). Bij cloudoplossingen kan multitenancy belangrijk zijn, voor het beperkt houden van het aantal koppelingen en gegevensbevragingen. - Afspraken maken over eventuele uitbreiding van multitenant-omgevingen voor toekomstige nieuwe partners.
Toepasbaarheid: Uit marktverkenning moet blijken of multitenancy geëist kan worden dan wel relevant is of in het geheel niet van toepassing. Dit betreft derhalve geen standaardeis of –wens.

14.1.3 Common Ground
Uitgangspunt: Bij elke aanschaf/vervanging kijken we of de gevraagde oplossing geheel of gedeeltelijk door Common Ground componenten ingevuld kan worden. We hergebruiken daartoe reeds ontwikkelde componenten uit de Common Ground componentencatalogus, dan wel ontwikkelen we in samenwerking met ander gemeenten en marktpartijen nieuwe componenten
Toelichting: Binnen het SSC streven we naar modernisering van de gemeentelijk IV-huishouding omdat we zien dat de huidige situatie op termijn niet houdbaar is. Door in te zetten op Common Ground, kunnen we de gegevens sneller en veiliger uitwisselen, worden we minder afhankelijk van leveranciers en krijgen burgers en bedrijven meer inzicht in wat er met hun gegevens gebeurt en kunnen we sneller inspelen op nieuwe ontwikkelingen. Hiermee gaat Common Ground bijdragen aan een open en transparante overheid.
Uitwerking: - Bij elke aanschaf/vervanging hebben (beschikbare) Common Ground componenten de voorkeur. - Bij (grote) vernieuwingstrajecten, worden aanbestedingen opgedeeld in kleinere uitvragen van functionaliteiten in plaats van grote alles omvattende systemen. - Bij vernieuwingstrajecten vragen we leverancier per keer wat hun Common Ground-bijdrage is in die situatie. - We zoeken leveranciers die een visie hebben over Common Ground en een actieve rol (willen) spelen bij deze beweging en in staat zijn deze samen met ons vorm te geven.
Toepasbaarheid: Altijd (standaardset) We bepalen zelf vooraf voor welke aanbestedingen een Common Ground-oplossing gebruikt, toegepast dan wel ontwikkeld dient te worden. We beseffen dat dit niet voor elke aanbesteding reëel is, cq dat de markt hiervoor nog niet klaar is. Wanneer we ervoor kiezen dat een CG-component vereist is, worden daartoe specifieke eisen en wensen opgesteld (bijv. ten aanzien van deelbaarheid, open-source en API's) Wel willen we in elke aanbesteding een duidelijk signaal afgeven aan de markt. Derhalve worden bovenstaande uitgangspunt standaard opgenomen.

14.1.4 Open Standaarden
Uitgangspunt: We voldoen aan de open standaarden, voorgeschreven in het beleid “open standaarden” van de Nederlandse overheid (zie: Forum Standaardisatie)
Toelichting: Vanuit de gedachte dat uitwisselen van digitale gegevens tussen overheden onderling en tussen de overheid, bedrijven en burgers van groot belang ís, willen we voldoen aan het gebruik van open standaarden. Hiermee verbetert de onderlinge verbinding omdat de ICT-systemen elkaar begrijpen en daarnaast zorgen we hiermee voor meer keuzevrijheid in ICT-leveranciers.
Uitwerking: - Oplossingen kiezen die voldoen aan de “verplichte” standaarden indien mogelijk. Sommige standaarden worden nog onvoldoende gebruikt binnen de publieke sector en zijn daarom verplicht (pas toe of leg uit). - Waar mogelijk en wanneer relevant proberen om oplossingen te kiezen die voldoen aan aanbevolen standaarden. Deze open standaarden zijn aanbevolen, omdat ze gangbaar zijn of in opkomst en veelbelovend.
Toepasbaarheid: Altijd (standaardset) – per keer bepalen welke standaarden van toepassing zijn en uitgevraagd kunnen worden tijdens de verificatie.

14.1.5 Inrichting is gedocumenteerd
Uitgangspunt: We zetten in op een gedocumenteerde inrichting van het informatielandschap.
Toelichting: Vanuit het oogpunt van transparantie en beheerbaarheid is het van belang dat inrichtingskeuzes worden gedocumenteerd. Hiermee ontstaat inzicht in de functionele en technische werking van het informatielandschap. Daarnaast wordt hiermee geborgd dat een informatielandschap beheersbaar blijft.
Uitwerking: - Functioneel ontwerp - Technisch ontwerp - Architectuurplaten - Installatiehandleiding - Gebruikershandleidingen
Toepasbaarheid: Altijd (standaardset) - check per aanbesteding welke documentatie van toepassing is.

14.2 Records Management

14.2.1 Compliancy
Uitgangspunt: We zijn compliant aan de NEN-ISO 15489, NEN-ISO 16175 en de NEN-ISO 23081
Toelichting: Dit is een wettelijke verplichting op basis van Artikel 2a van de Archiefregeling . De NEN-ISO 15489 beschrijft de records management activiteiten, de NEN-ISO 16175 de functionaliteiten waarover systemen moeten beschikken. De NEN-ISO 23081 is de basis voor de vast te leggen metadata.
Uitwerking: Bij de betrokken gemeenten ligt hier als basis een Verordening- en Besluit informatiebeheer. Bij de gemeente Leeuwarden zijn verder de Regeling Historisch Centrum Leeuwarden en het door het College in 2015 vastgestelde document *Informatiebeheer – Belang en uitgangspunten* beschikbaar. Tevens is bij die gemeente een op grond van de Archiefregeling voorgeschreven metagegevensschema beschikbaar.
Toepasbaarheid Indien in de uitvraag een koppeling met het Zaaksysteem/Zaaktypecatalogus/RM-portaal gevraagd is dan is deze niet van toepassing.

14.2.2 Archiefsysteem
Uitgangspunt: We beschouwen in onze architecturen het archiefsysteem niet als een object of zelfstandig digitaal systeem maar als een generieke functie die op alle processen van toepassing is.
Toelichting: Een archiefsysteem is een Informatiesysteem in de zin van geheel van normen, plannen, procedures en activiteiten waarmee een verwerkingsverantwoordelijke zijn archieffunctie vorm geeft. De archieffunctie omvat activiteiten en functionaliteiten die ook wel archiveren wordt genoemd. Archiveren is het geheel van nemen of uitvoeren van maatregelen waardoor zowel (1) integriteit, context en kwaliteit van gegevens met functionaliteiten behouden blijven en het voortbestaan van die gegevens en functionaliteiten wordt gegarandeerd als(2) het gecontroleerd vernietigen van gegevens mogelijk is. Met kwaliteiten worden (impliciet) aspecten bedoeld als: beschikbaarheid, betrouwbaarheid, bruikbaarheid, interpreteerbaarheid, raadpleegbaarheid, leesbaarheid, toegankelijkheid, vernietigbaarheid, vindbaarheid, uitwisselbaarheid, uniciteit en dergelijke. Binnen de archieffunctie zijn de volgende activiteiten te onderkennen: - Ontstaan van informatie - Opnemen van informatie; - Classificeren en registreren; - Toegangscontrole (autorisaties); - Opslag; - Gebruik en hergebruik; - Migratie en conversie; - Verwijderen van informatie (vernietigen of verplaatsen) Op technisch niveau zullen in een digitaal ecosysteem ten behoeve van deze activiteiten de benodigde functionaliteiten ter beschikking moeten zijn. Dit zijn te groeperen onder (1) opnemen, (2) ordenen, klasseren,

beschrijven, (3) beheren, onderhouden en volgen, (4) beschikbaar stellen, (5) selecteren en verwijderen (vernietigen), (6) documenteren en (7) autoriseren en waarmerken

Uitwerking: Dit gegeven zal zich uiten in de proces- informatie en ict architectuur. Op procesniveau wordt dit verder vorm gegeven door interne beleidsregels. Binnen de gemeentelijke organisatie zijn er diverse gespecialiseerde organisatieonderdelen en functionarissen die zich met deze activiteiten bezig houden. Door aan te sluiten op landelijke ontwikkelingen rond bijvoorbeeld Common Ground en GGL zal de benadering van de informatievoorziening verschuiven van een geautomatiseerde procesondersteuning naar echt digitaal werken. Deze benadering heeft ook gevolgen voor de manier waarop wij aankijken tegen bewaarstrategieën die langdurige bewaring, toegankelijkheid en beschikbaarheid van informatie met behoud van context mogelijk maakt. Het idee is dat daarmee ook de continuïteit en integriteit van de informatie met context gegarandeerd is, ongeacht het digitale systeem of systemen waarin zij beheerd worden.

Toepasbaarheid
Afhankelijk van data/proces wat de oplossing omvat. Bespreek met recordmanagement.

14.2.3 Metadata en zaaktypecatalogus

Uitgangspunt: We beschikken over een overzicht van onze processen, projecten en andere activiteiten met de daarbij behorende

1. informatie,
2. informatieobjecten,
3. de wettelijke bewaartermijnen,
4. beheerprocessen,
5. functionaliteiten voor het beheer en
6. toe te passen of toegepaste technieken.

Toelichting: Het doel is in control te zijn over het geheel van onze informatiehuishouding dat wij als ons kapitaalgoed beschouwen.

Een belangrijk middel daarvoor is het vastleggen van metadata. Dit is informatie over informatie. Metadata is een ruim begrip en betreft de volgende aspecten:
Metadata die informatie identificeren:
o.a. uniek registratienummer, datum opmaak, verzending of ontvangst, verwijzing naar een dossier of andere aggregatievorm, titel, auteur;
Metadata die juiste interpretatie van informatie mogelijk maken:
o.a. classificatienummer, verwijzing naar dossier, verwijzing naar proces en procedure;
Metadata die de authenticiteit van informatie aantonen:
o.a. datum opmaak, datum verzending of ontvangst, auteur, relatie met andere documenten, wijze van verzending; wijze van authenticatie (elektronische handtekening);
Metadata die het vinden van informatie vergemakkelijken:
onderwerp, auteur, titel, datum, classificatiecode;
Metadata die de beschikbaarheid en openbaarheid van de informatie ondersteunen:
o.a. rubricering, openbaarheid, uitzonderingscriteria, intellectueel eigendom, autorisatie
Metadata die correcte (re)presentatie mogelijk maken:
o.a. software en hardware omgeving, fysieke opslaggegevens, compressiegegevens;
Metadata die beheershandelingen cq verwerkingen sturen of mogelijk maken:
o.a. toegangsautorisatie, datum vernietiging of overdracht, datum conversie of migratie; hiertoe kunnen ook logistieke data gerekend worden (verblijfplaats);
Metadata die uitgevoerde beheershandelingen / verwerkingen vastleggen (aantoonbaarheid):
o.a. wanneer door wie gebruikt, datum conversie, vernietiging
Metadata noodzakelijk voor beheer en behoud (preservering) -
o.a. informatie over applicaties, datamodellen, metadatamodellen, bestandsformaten etc.

Metadata is op diverse plekken aan te treffen. Voorbeelden zijn niet alleen registraties van zaken en documenten of informatie opgenomen in documenten (eigenschappen van een document, header van een e-mailbericht en dergelijke) maar ook documentatie in de vorm van bijvoorbeeld procesbeschrijvingen, gebruikershandleidingen, release notes, de resultaten van toetsingen (intern en extern) waarmee de integriteit kan worden aangetoond, informatie over verwerkingen die leiden of kunnen leiden tot onherroepelijke aantasting van de integriteit van originele gegevens op het niveau van dataobject,

presentatie, verwerking, gedrag, functionaliteit of opslag en informatie over architectuur en systemen die werden gebruikt om de informatie te kunnen verwerken.

Voor de vastlegging van metadata kennen we een drietal niveaus te weten een definiërend, een uitvoerend en technisch niveau. Op definiërend niveau wordt metadata vastgelegd over type processen, projecten en zaken en over het type informatieobjecten (documenttypen). Op uitvoerend niveau, het niveau waar een proces, project of zaak wordt uitgevoerd, wordt metadata vastgelegd over dat proces, project of zaak met de daarbij behorende informatieobjecten. Op technisch niveau, het instrumentarium dat het werken mogelijk maakt, wordt het nodige vastgelegd over applicaties, digitale bestanden, bestandsformaten en opslag[4] Metadata die geautomatiseerd vastgelegd kan worden is geautomatiseerd vast te leggen.

Wij beschouwen de metadata als onlosmakelijk onderdeel van de objecten en gegevens die daarmee worden beschreven. Als gevolg daarvan is de bewaartermijn tenminste even lang als de bewaartermijn van de objecten en gegevens.

Voor een deel van het digitaal werken wordt gebruik gemaakt van een zaaktypecatalogus (ZTC) waarin op type niveau een deel van het verplichte overzicht in is verwerkt. Deze ZTC is de basis voor het zaakgericht werken en tevens een van bijlagen bij de respectievelijke handboeken substitutie.[5] Ook is het bedoeld als een van de instrumenten voor het latere beheer van naar de archiefbewaarplaats overgebrachte digitale informatie. Uitgangspunt is dat een zaak alleen digitaal kan starten wanneer de generieke kenmerken daarvan zijn vastgelegd als zaaktype in de ZTC.

Uitwerking: Dit wordt onder meer gerealiseerd middels het door de Archiefregeling verplicht gestelde overzicht dat tevens bruikbaar is als het door de AVG verplicht gestelde register van verwerkingen. Dit overzicht is tevens basis voor de zaaktypecatalogus (ZTC). Wij beschikken over een op grond van de Archiefregeling verplicht metagegevensschema waarin verwezen wordt naar het TMLO en een overzicht van toe te passen metadata, zie bijlage 6. Hierin staan ook uitgangspunten rond digitaal werken beschreven. Een deel van de documentatie is het resultaat van processen rond business cases, wijzigingen, aanbestedingen en toetsingen.

Toepasbaarheid:
Afhankelijk van data/proces wat de oplossing omvat. Bespreek met recordmanagement.

14.2.4 Vindbaarheid en bruikbaarheid

Uitgangspunt: We kunnen altijd de informatie inclusief haar context vinden en gebruiken.

Toelichting: Om taken en opdrachten op de juiste manier uit kunnen voeren is correcte en relevante informatie onontbeerlijk. Ter ondersteuning van de mogelijkheid tot correct gebruik en interpretatie van gevonden informatie is context bijvoorbeeld over het proces waarin de informatie is opgenomen noodzakelijk. Een gebruiker moet ervan uit kunnen gaan dat een zoekresultaat alles weergeeft waar hij of zij recht op heeft. In het geval dat de gebruiker niet over de juiste autorisatie beschikt zal hij of zij geattendeerd moeten worden dat niet alles getoond mag worden. (dat-informatie).[6] In de andere gevallen wordt ook de wat-informatie verstrekt.[7]
Zoeken en vinden maakt gebruik van de feitelijke inhoud van de informatie en/of op basis van metadata.
Op basis hiervan kunnen afgewogen standpunten ingenomen conclusies getrokken worden. Een correct zoekresultaat is een van grondslagen voor betrouwbare besluitvorming.

Uitwerking: Een individuele toepassing moet zelf beschikken over een goede zoek/vind functionaliteit. Tevens zal elke toepassing middels de eigen zoekmachine (MyLex) doorzoekbaar moeten zijn. In beide gevallen is de context van de informatie-onderdeel van het zoekresultaat.

Toepasbaarheid
Afhankelijk van data/proces wat de oplossing omvat. Bespreek met recordmanagement.

14.2.5 Voortbestaan
Uitgangspunt: We houden de integriteit en verschijningsvorm van onze informatieobjecten gedurende de wettelijke bewaartermijn in stand.
Toelichting: We kunnen ervan uitgaan dat het belang van gegevens altijd het belang van de techniek overstijgt en dat de bewaartermijn van de gegeven s in de meeste gevallen langer is dan de (economische) levensduur van technische oplossing. Daarom moeten er preserverende maatregelen genomen worden om het voortbestaan van de informatieobjecten (gegevens met context) integraal te kunnen garanderen. Een informatieobject bestaat uit een vijftal kenmerken te weten de inhoud, een structuur, een eigen context, gedrag (functionaliteit) en techniek die ervoor zorgt dat het in stand blijft en zich als een geheel toont. Zijn deze kenmerken ongeschonden dan kan ervan uit gegaan worden dat de integriteit en verschijningsvorm gegarandeerd zijn.
Uitwerking: Technisch gezien kunnen we dit bereiken door bijvoorbeeld het toepassen van (open) technische standaarden en open software zowel op het niveau van toepassingen als (open) bestandsformaten. Voor het laatste beschikken we over een overzicht van toegelaten bestandsformaten. Procedureel regelen we dit via het records management, functioneel applicatiebeheer en technisch beheer. Onderdeel van preservering zijn ook verwerkingen als transformeren, converteren en migreren. Ook het adapteren van de resultaten van oplossingen die ontstaan onder de vleugels van de Common Ground levert een bijdrage.
Toepasbaarheid: Altijd (standaardset) Wel bespreken met recordmanagement om de uitvraag specifiek te maken.

14.2.6 Vernietigen
Uitgangspunt: We kunnen altijd de informatie waarvan de wettelijke bewaartermijnen zijn verstreken vernietigen
Toelichting: Vernietigen is het proces waarbij ooit vastgelegde gegevens op geen enkele manier te achterhalen of te reconstrueren zijn. Zowel de Archiefwet als de AVG kennen een vernietigingsplicht. Voor persoonsgegevens geldt de regel dat deze te vernietigen zijn zodra de doelbinding is verstreken. Om te kunnen bepalen wat voor vernietiging in aanmerking komt moet eerst de informatie op basis van bewaar- en vernietigingsbelangen worden gewaardeerd. Het resultaat van deze waardering is opgenomen in de zaaktypecatalogus of een RM-Checklist. Geldende selectielijsten zijn de formele basis voor vernietiging bij overheden. Deze lijsten geven een bewaartermijn aan waarna vernietigd moet worden. Deze lijsten bevatten direct ook uitzonderingscriteria, De termijn van de doelbinding van de AVG is gelijk aan bewaartermijn van de selectielijst, De selectielijst bevat uitzonderingscriteria op basis waarvan in principe te vernietigen informatie alsnog voor blijvende bewaring kan worden aangewezen. Dit kan onder andere op basis van een hotspotmonitor. Een hotspot is een onderwerp/thema/item dat op een bepaald moment centraal in de aandacht staat en aantoonbaar invloed heeft gehad op de (lokale) samenleving. Wat niet te vernietigen is wordt na verloop van tijd formeel overgebracht naar de archiefbewaarplaats. In het geval van de gemeente Leeuwarden is dat het Historisch Centrum Leeuwarden.
Uitwerking: Beleidsmatige, procedurele en specifieke afspraken over vernietiging zijn vastgelegd. (Voor de gemeente Leeuwarden is dat in het document Spelregels vernietiging.) Dit document is onder meer gebaseerd op het Besluit informatiebeheer Leeuwarden 2018. De digitale systemen, of het nu in de cloud of on premise is, moeten beschikken over de benodigde vernietigingsfunctionaliteiten conform de NEN-ISO 16175. Vanwege allerlei mogelijke uitzonderingen, bijvoorbeeld hotspots, is geautomatiseerde vernietiging, te weten vernietiging zonder menselijke tussenkomst niet toegestaan. Er wordt alleen vernietigd op proces, project of zaakniveau. Van elke vernietiging is een verklaring op te stellen met een overzicht van wat vernietigd is.
Toepasbaarheid: Altijd Verschillende oplossingen mogelijk. Stem af met Recordmanagement voor de juiste invulling.

14.2.7 Migratie/Conversie
Uitgangspunt: Gemigreerde en/of geconverteerde data kan als nieuw origineel worden gebruikt.
Toelichting: Wanneer Migratie en/of conversie van data uitgevoerd wordt conform de regels van de Archiefwet krijgt de gemigreerde en/of geconverteerde set data de juridische status van nieuwe origineel. Na accordering is het bronsysteem met de oorspronkelijke data na een afgesproken periode te vernietigen.
Uitwerking: – Stel een conversie/migratieplan op ○ Bepaal de te converteren/migreren set data ○ Bepaal een oplossing voor niet te converteren/migreren data ○ Bepaal onder welk regiem de conversie/migratie is uit te voeren – Stel een testplan op ○ Bepaal in overleg met verantwoordelijken de criteria om het proces en de kwaliteit van de gemigreerde en/of geconverteerde data te testen ○ Bepaal wie de migratie/conversie test. – Test uitvoeren – Laat de uitgevoerde test door verantwoordelijken accorderen – Zorg voor de formele afwikkelingen ○ Verklaring/ Besluit met conversieplan, geaccordeerde test – Geef de data vrij voor productie – Zorg voor de vernietiging volgens procedure
Toepasbaarheid Afhankelijk van data/proces wat de oplossing omvat. Bespreek met recordmanagement.

14.3 Gegevensmanagement

14.3.1 Hergebruik van gegevens
Uitgangspunt: We streven naar hergebruik van authentieke gegevens door eenmalig inwinnen, meervoudig gebruik te hanteren. We bevragen basisregistraties en kernregistraties zoveel als mogelijk bij de bron. Dit kan zowel een interne of een landelijke voorziening zijn. Alleen voor persoonsgegevens van inwoners van de eigen gemeente is dit altijd eerst de interne BRP. Voor de basisregistraties waarvan we als gemeente geen bronhouder zijn, bevragen we te allen tijde de landelijke voorzieningen. Bij afwijken van dit uitgangspunt dient de specifieke situatie overlegd te worden.
Toelichting: Door eenmalig inwinnen en meervoudig gebruik te hanteren, hoeven burgers en bedrijven maar 1x gegevens te delen met de gemeente. Hiermee wordt voorkomen dat er verschillende gegevens binnen de gemeente gebruikt worden en is het actief beheren/bewaken van de datakwaliteit mogelijk.
Uitwerking: - Halen gegevens vanuit basisregistraties en Landelijke voorzieningen. - Gegevens, waarvan we bronhouder zijn, leveren aan basisregistraties. - Bijhouden van kernregistraties en hieruit gegevens laten ophalen door informatiesystemen. - Aansluiten op een LV via Integrale Zoekvraag binnen de gegevensmakelaar
Toepasbaarheid: Per aanbesteding bekijken of er gebruik gemaakt wordt van gegevens uit een basisregistratie of uit een kernregistratie.
Lijst met kernregistraties: • BAG+ • Bestemmingsplannen • BGT+ • BOR+ • BRP+ • Financien • Foto’s • Historische kaarten • Kunstwerken

- Meetbouten
- Monumenten
- Omgevingsplannen
- Ondergrond, verontreiniging
- Territoriale indeling
- Wegenlegger
- WIBON
- WKpB
- Zaken
- Personeel

14.3.2 Inzicht in gegevens
Uitgangspunt: We streven naar maximaal inzicht in onze gegevens huishouding.
Toelichting: Door inzicht te hebben in de datahuishouding, kunnen de mogelijkheden van de data maximaal benut worden in diverse vraagstukken van de organisatie. Het is duidelijk welke gegevens aanwezig zijn, wat er vastgelegd is, welke definities gehanteerd zijn wat de samenhang is en wat de kwaliteit is
Uitwerking: - Datamodellen/ Entiteitenmodellen beschikbaar stellen. - Definitiewoordenboek vastleggen. - Registratie opnemen in datacatalogus.
Toepasbaarheid: Van toepassing bij oplossingen waarbij data wordt opgeslagen.

14.3.3 Gegevenskwaliteit
Uitgangspunt: We streven naar actief beheer op gegevenskwaliteit
Toelichting: Door inregelen van signalerende monitoring, gegevenskwaliteits- rapportages/hulpmiddelen en door het maken van afspraken mbt verantwoordelijkheden binnen het datakwaliteitsproces wordt actief beheer op gegevenskwaliteit mogelijk.
Uitwerking: - Inrichten monitoring op gegevenskwaliteit door aan te sluiten op bestaande voorziening kwaliteitsmonitor gegevens. - Beschikbaar stellen rapportages mbt gegevenskwaliteit. - Inregelen en/of faciliteren via applicatie van een terugmeldvoorziening. - Afspraken maken rondom data-eigenaarschap.
Toepasbaarheid: Dit is geen standaardeis. Deze eis wordt opgenomen wanneer de aanbestede oplossing: - koppelingen heeft, waarbij oplossing als bron dient voor andere systemen. - gebruikt wordt bij financiële verantwoording, verrekening, doorbelasting dan wel P&C-cyclus - een bron is voor open data - onderworpen is aan een auditplicht

14.3.4 Verantwoordelijkheid en eigenaarschap
Uitgangspunt: De gemeente/uitvoeringsdienst/SSC (de 'gegevens producerende organisatie') wil zelf eigenaar zijn van de gegevens die geregistreerd worden. Daarnaast willen we transparantie in de rollen en verantwoordelijkheden rondom gegevens.
Toelichting: Door vast te leggen dat de gemeente/uitvoeringsdienst/SSC (de 'gegevens producerende organisatie') eigenaar is van gegevens en wie daarbij welke rol heeft op het gebied van gegevens, heeft deze zelf grip op de gegevens. Het is daarmee transparant wat erdoor wie met welke gegevens gebeurt. Hierdoor kan gegarandeerd worden dat gegevens alleen gebruikt worden voor doeleinden waar de aanbestedende dienst achter staat en dat het beleid geldt voor de gegevens waarvoor deze afspraken zijn gemaakt.
Uitwerking: - Verwerkersovereenkomst (in geval van persoonsgegevens). - Afspraken maken rondom beschikbaarheid en verwerken van gegevens. - Vastleggen eigenaarschap gegevens.

- Geheimhoudingsverklaring.
Toepasbaarheid:
Wanneer er data opgeslagen wordt in de oplossing. Niet van toepassing voor tooling.

14.3.5 Beschikking over gegevens
Uitgangspunt: We streven ernaar om op elk moment actuele gegevens toegankelijk te hebben.
Toelichting: Voor het SSC is het van belang om op elk moment toegang te hebben tot actuele gegevens. Hiermee wordt het mogelijk om gegevens opgeslagen in uw oplossing in te zetten voor meerdere doeleinden, denk hierbij aan bijvoorbeeld testen of data-analyse.
Uitwerking: - Beschikbaar stellen API - Beschikbaar stellen on-premise dataset (van toepassing bij cloud) - Export/ Import functionaliteit
Toepasbaarheid: Wanneer er data opgeslagen wordt in de oplossing. Niet van toepassing voor tooling.

14.3.6 Koppelen volgens standaarden
Uitgangspunt: Het koppelen van informatiesystemen gebeurt op een eenduidige manier, op basis van standaarden.
Toelichting: Er zijn veel verschillende manieren om verbindingen te maken waar de koppelingen hun gegevens over kunnen uitwisselen. Om een wildgroei aan verschillende soorten te voorkomen hebben we een beperkt aantal afgesproken. Door informatiesystemen te koppelen volgens standaarden, zorgen we voor een onderhoudbaar landschap waarin we niet afhankelijk zijn van inrichtingskeuzes van leveranciers en zorgen we voor transparante en veilige uitwisseling van gegevens.
Uitwerking: Voor koppelingen van cloud applicaties naar landelijke voorzieningen, of van cloud applicaties onderling zijn de cloud leveranciers verantwoordelijk. Voor koppelingen van en naar onze on-premise omgeving hanteren we de volgende normen: - Koppelingen worden gemaakt op basis van de VNG-standaarden. - Aansluiting op een landelijke voorziening verloopt via Haal Centraal. Wanneer de LV nog niet via Haal Centraal beschikbaar is wordt er gekoppeld volgens de Digikoppeling standaarden. - Gestructureerde berichten via Stuf/XML of API-koppelingen verlopen via de ESB/ Broker voorziening (JNET). Deze is via internet, Gemnet en Diginetwerk bereikbaar. - Berichten- en API-koppelingen tussen interne voorzieningen die herbruikbaar zijn verlopen ook via de ESB/ Broker voorziening (JNET). - Koppelingen tussen externe en interne systemen die niet via de ESB/ Broker voorziening afgehandeld kunnen worden, worden via een reverseproxy oplossing afgehandeld. - Alleen voor verkeer dat niet via de ESB/Broker voorziening of een reverseproxy oplossing kan verlopen, wordt een site-2-site VPN-verbinding aangemaakt.
Toepasbaarheid: Inventariseer welke koppelingen (zowel intern als extern) mogelijk nodig zijn. Indien er geen koppelingen nodig zijn, hoeven er op dit vlak geen inkoopeisen opgenomen te worden. Bespreek de te realiseren koppelingen met de informatiearchitect om te bepalen welke inkoopeisen van toepassing zijn.

14.4Informatiebeveiliging

14.4.1 Aantoonbaarheid
Uitgangspunt: We zijn compliant aan de Baseline Informatiebeveiliging Overheid BIO – ISO27001/27002
Toelichting: De aanbestedende dienst hanteert de Baseline Informatiebeveiliging Overheid (BIO) als leidraad voor de informatiebeveiliging, de BIO is gebaseerd op ISO 27002:2017. Van leveranciers wordt verwacht om te voldoen aan de gestelde normen die conform de BIO worden geëist en dit aantoonbaar kunnen maken.
Uitwerking: Als een leverancier producten en/of diensten levert aan de gemeente, dan dient de leverancier uit te gaan van het basisbeveiligingsniveau van de gemeente, dat gebaseerd is op de BIO. Door te voldoen aan de gestelde normen kan er zekerheid afgegeven worden over de genomen maatregelen bij het aanbieden van uw product. Voor het aantonen van de veiligheid van uw webapplicatie of website hanteren wij de relevante normen uit het normenkader ICT-Beveiligingsrichtlijnen voor webapplicaties van het NCSC. Een oplossing/product/dienst is aantoonbaar compliant aan de BIO waarin tenminste de onderstaande onderdelen in zijn opgenomen. (eis) • ISO 27001 certificering • Logging • Logische scheiding omgevingen • Meldplicht informatiebeveiligingsincidenten • Hardening serveromgeving en systemen • Toepassing Security by design • Toepassing van encryptie • Toegangsbeveiliging • Toepassing van Advanced Threat Protection • Uitvoeren van Security assessments • Zero footprint op mobiele apparatuur • Beveiliging van fysieke omgevingen • Centraal gebruikers- en rechten beheer • Single Sign On (SSO) • Multifactor authenticatie • Persoonsgebonden accounts
Toepasbaarheid: Altijd (standaardset) Afhankelijk van de werking van het aangeboden product of dienst. Overleggen met de Information Security Officer.

14.5 Privacy

14.5.1 Screening voor wettelijke vereisten AVG
Uitgangspunt: Voldoen aan wettelijke vereisten
Toelichting: De AVG schrijft voor dat de gemeente alleen een beroep hoort te doen op verwerkers als die afdoende garanties kunnen geven over het bieden van passende technische en organisatorische maatregelen zodanig dat de verwerking aan de vereisten van de AVG voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.
Uitwerking: Om te kunnen inschatten of hiervan sprake is, dient een potentiële verwerker desgevraagd het volgende aan de gemeente te overleggen of aan te tonen, alvorens wordt besloten met deze partij te gaan werken: - De aanwezigheid van een FG, indien dit wettelijk vereist is. - De aanwezigheid van protocollen over datalekken en de omgang met verzoeken van betrokkenen. - De aanwezigheid van een up-to-date privacy statement. - De aanwezigheid van een verwerkingsregister. - Certificering ten behoeve van beveiligingsmaatregelen zoals ISO of NEN. Indien de organisatie daarover niet beschikt zal op andere wijze aantoonbaar moeten maken of het voldoende maatregelen heeft getroffen ter beveiliging. Dit is ter beoordeling van de Security Officer.
Toepasbaarheid: Altijd (standaardset)

14.5.2 Afspraken over de verwerking van persoonsgegevens
Uitgangspunt: We maken afspraken met andere partijen die voor ons als verwerker van gegevens optreden.
Toelichting: Gemeenten mogen afwijken van de VNG verwerkersovereenkomst als daar een opmerking over wordt gemaakt in het jaar verslag. Daarvan is sprake bij de gemeente Leeuwarden. Zie voor toelichting en afwijking van het VNG model de overeenkomst van de gemeente Leeuwarden voor nadere uitleg.
Uitwerking: Zowel de verwerkingsverantwoordelijke, als de verwerker zijn verplicht om de volgende onderwerpen in de schriftelijke overeenkomst vast te leggen: **Algemene beschrijving** Een omschrijving van het onderwerp, de duur, de aard en het doel van de verwerking, het soort persoonsgegevens, de categorieën van betrokkenen en de rechten en verplichtingen als verwerkingsverantwoordelijke. **Instructies verwerking** De verwerking vindt in principe uitsluitend plaats op basis van schriftelijke instructies van de verwerkingsverantwoordelijke. De verwerker mag de persoonsgegevens niet voor eigen doeleinden gebruiken. **Geheimhoudingsplicht** Personen in dienst van of werkzaam voor de verwerker hebben een geheimhoudingsplicht. **Beveiliging** De verwerker treft passende technische en organisatorische maatregelen om de verwerking te beveiligen. Bijvoorbeeld pseudonimisering en versleuteling van persoonsgegevens, permanente informatiebeveiliging, herstel van beschikbaarheid en toegang tot gegevens bij incidenten, regelmatige beveiligingstesten. **Subverwerkers** De verwerker schakelt geen subverwerker(s) in zonder voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke. De verwerker legt aan een subverwerker in een subverwerkersovereenkomst dezelfde verplichtingen op als de verwerker richting de verwerkingsverantwoordelijke heeft. In de overeenkomst kan daarnaast ook afgesproken worden óf, en onder welke voorwaarden, de verwerker subverwerkers mag inschakelen. **Privacyrechten**

De verwerker helpt de verwerkingsverantwoordelijke om te voldoen aan zijn plichten als betrokkenen hun privacyrechten uitoefenen (zoals het recht op inzage, correctie, vergetelheid en dataportabiliteit).

Andere verplichtingen
De verwerker helpt de verwerkingsverantwoordelijke ook om andere verplichtingen na te komen. Zoals bij het melden van datalekken, het uitvoeren van een data protection impact assessment (DPIA) en bij een voorafgaande raadpleging.

Gegevens verwijderen
Na afloop van de verwerkingsdiensten verwijdert de verwerker de gegevens. Of bezorgt hij deze aan de verwerkingsverantwoordelijke terug, als dit gewenst is. Ook verwijdert hij kopieën. Tenzij de verwerker wettelijk verplicht is de gegevens te bewaren.

Audits
De verwerker werkt mee aan audits van de verwerkingsverantwoordelijke of die van een derde partij. En stelt alle relevante informatie beschikbaar om te kunnen controleren of hij zich als verwerker houdt aan de hierboven genoemde verplichtingen (uit artikel 28 AVG).

Toepasbaarheid: Altijd (standaardset)

14.6 ICT-infrastructuur

14.6.1 ICT-standaarden

Uitgangspunt: Om wildgroei aan allerlei verschillende producten en technieken te voorkomen hebben we ICT-standaarden afgesproken voor de ICT-componenten die wij zelf beheren.

Toelichting: Om onze ICT-omgeving beheersbaar te houden kiezen we voor bepaalde technieken en producten. We streven naar zoveel mogelijk gebruik van deze standaard componenten. Dit zorgt ervoor dat we minder kennis hoeven te hebben over allerlei producten in de breedte. We kunnen daardoor op de producten die we wel gebruiken diepgaande kennis opbouwen. Dit zorgt voor een verhoogde kwaliteit van onze dienstverlening.

Bij cloudapplicaties wordt het technisch beheer in het algemeen door de leverancier gedaan. Wanneer er vanuit cloudapplicaties geïntegreerd wordt met producten/applicaties die wij beheren, blijven onze ICT-standaarden ook gelden. Denk hierbij bijvoorbeeld aan benodigde client software, office plug-ins of koppelingen met andere (door ons beheerde) systemen.

Uitwerking: De ICT-standaarden worden vastgelegd in een apart document. Dit document wordt jaarlijks geactualiseerd en samen met onze samenwerkingspartners vastgesteld. Dit document is bijgevoegd in bijlage 7.

Oplossingen passen binnen de genoemde producten en technieken uit de bijlage ICT Standaarden. Dit geldt ook voor cloudapplicaties als deze interactie hebben met in de bijlage genoemde en door opdrachtgever beheerde producten.
Oplossingen passen binnen de ICT-omgeving zoals beschreven in de bijlage Kern beschrijving ICT-infrastructuur. Dit geldt ook voor cloudapplicaties als deze interactie hebben met in de bijlage beschreven door opdrachtgever beheerde omgevingen.

Toepasbaarheid: Altijd (standaardset)

14.6.2 Performance
Uitgangspunt: We willen dat applicaties en werkplek een acceptabele performance leveren.
Toelichting: Medewerkers maken veelvuldig gebruik van de diverse applicaties. Om prettig te kunnen werken is het van belang dat een applicatie en werkplek niet te traag reageert.
Uitwerking: e denken na over eisen aan de performance van applicaties en werkplek. Hier zijn geen harde richtlijnen voor te geven, wat acceptabel is verschilt per situatie. Wel hanteren we een aantal uitgangspunten om met performance om te gaan: - Bij nieuw aan te schaffen applicaties is het raadzaam eisen/wensen mee te gegeven over de reactietijden van een applicatie. Of er kunnen vragen worden gesteld over de performance van de geleverde toepassing, en hoe deze worden geborgd. Vooral bij cloudoplossingen is dit relevant omdat we daar afhankelijk zijn van de geleverde diensten door de cloudleverancier. Indien er geen afspraken gemaakt worden bij het afnemen van de dienstverlening kunnen er vervelende discussies ontstaan wanneer de performance niet naar wens is. - Voor de werkplek meten we continue een groot aantal verschillende reactietijden op de Citrix-omgeving. Hierdoor krijgen we inzicht in wat normaal is, en of/wanneer de performance verbetert of verslechtert. - In onze eigen SSC-basis infrastructuur (serverplatform, storage, netwerk en verbindingen) meten we continue de belasting. Drukte en overbelasting in de basis infra leidt al snel tot performance problemen. We stellen drempelwaarden op waar de belasting onder moet blijven, en stellen meldingen in indien de belasting boven de drempelwaarde uitkomt
Toepasbaarheid : Neem altijd een eis of wens op ten aanzien van performance.

14.6.3 Beschikbaarheid
Uitgangspunt: We streven ernaar om beschikbaarheid te borgen zodat we ten alle tijden toegang hebben tot data en functionaliteit.
Toelichting: Voor het leveren van de dienstverlening is het beschikbaar zijn van gegevens en functionaliteiten cruciaal. Zowel voor onze eigen systemen als voor systemen die via cloudoplossingen door derden geleverd worden, moet er aandacht zijn voor beschikbaarheid. Afhankelijk van de toepassing kunnen de daadwerkelijke eisen aan de beschikbaarheid verschillen. Beschikbaar is de situatie waarin een toepassing normaal functioneert en de beoogde werkzaamheden met de toepassing op acceptabele wijze kunnen worden uitgevoerd. De beschikbaarheid wordt veelal weergegeven in een percentage van de tijd, zoals 99,9% beschikbaarheid per maand. Een toepassing bestaat meestal uit een keten van meerdere componenten. De individuele componenten moeten daarbij altijd een hogere beschikbaarheid hebben, om gezamenlijk de gevraagde beschikbaarheid van de toepassing te kunnen leveren. Door bepaalde onderdelen dubbel (parallel) uit te voeren kan de beschikbaarheid verder verhoogd worden.
Uitwerking: We hebben binnen onze organisatie en met onze samenwerkingspartners afspraken gemaakt over de beschikbaarheid van onze informatiesystemen. Deze afspraken zijn vastgelegd in onze eigen SLA. Op basis daarvan worden voor onze infrastructuur keuzes gemaakt en maatregelen genomen om te voldoen aan die beschikbaarheidseisen. Denk hierbij aan het dubbel (redundant) uitvoeren van bepaalde componenten, en het kiezen voor bewezen producten en technieken. Beschikbaarheid wordt in het algemeen uitgedrukt in een percentage van de tijd waarin de dienst naar behoren functioneert. Het is hierbij van belang om vast te leggen over welke periode er gemeten wordt. Een applicatie met een beschikbaarheid van 99,8% per maand mag maximaal 87 minuten per maand niet beschikbaar zijn. Dat kan 1 storing zijn van bijna 1,5 uur, of een aantal kortere storingen verdeeld over een maand. Een beschikbaarheid van dezelfde 99,8% maar dan gemeten per jaar, leidt tot een maximale verstoring van 1044 minuten. Ook dit kan beperkt zijn tot 1 storing, die mag dan wel ruim 17 uur duren.

Gepland onderhoud wordt vaak uitgesloten van de beschikbaarheidsmeting. Het is daarom ook van belang afspraken te maken over de tijden waarop onderhoud uitgevoerd mag worden. Voor de onderdelen die we zelf beheren kunnen we daar flexibele afspraken over maken. Ook deze afspraken over onderhoudstijden zijn vastgelegd in onze SLA. Cloudleveranciers willen vaak geen maatwerk afspraken maken over onderhoudstijden. Hun applicaties worden meestal gedeeld gebruikt door alle klanten. Afstemmen van onderhoud leidt daardoor vaak tot tegenstrijdige belangen.

Inkoop: De te stellen inkoopeisen/wensen aan beschikbaarheid kunnen per situatie verschillend zijn. Ze dienen daarom per inkooptraject apart opgesteld te worden. Hieronder geven we enige begeleidende informatie die kan helpen bij het opstellen van de inkoopeisen/wensen.

Algemeen: Het is van belang dat de bereikbaarheid van de supportorganisatie van de leverancier past bij de eisen die we zelf aan de beschikbaarheid stellen. Zie hiervoor ook onderdeel 14.6.5 - Hersteltijden bij verstoringen.

On-premise: Wanneer de oplossing een on-premise product betreft zijn we zelf (grotendeels) verantwoordelijk voor de beschikbaarheid. Hoe vaak een apparaat defect raakt, of hoe vaak software door een programmeerfout vastloopt is echter iets wat buiten onze macht ligt. Op dat vlak kan een leverancier soms toch beschikbaarheidscijfers afgeven. Zeker bij professionele hardware zijn er vaak cijfers bekend over de gemiddelde tijd tussen defecten (MTBF = ‘mean time between failures’). Deze kunnen uitgevraagd worden bij een inkooptraject.

Cloud: Bij cloudoplossingen blijven we zelf verantwoordelijk voor een werkende kantoorwerkplek en is meestal een internetverbinding randvoorwaardelijk. Verder is de beschikbaarheid van een clouddienst grotendeels de verantwoordelijkheid van de leverancier. Het is daarom van belang helder te krijgen welke beschikbaarheidsgaranties een leverancier geeft. Dit kan via inkoopeisen afgedwongen worden, of de door de leverancier afgegeven beschikbaarheid kan via open vragen meegewogen worden in de beoordeling. In dat laatste geval kan een dienst met een slechte beschikbaarheid, maar een gunstige prijs/rijke functionaliteit toch als beste oplossing uit de bus komen. Het is daarom aan te bevelen om de minimale beschikbaarheidseisen als inkoopeis op te nemen.

- Uw clouddienst heeft een minimale beschikbaarheid van 99,8% per maand, gemeten over 24 uur per dag en 7 dagen per week.
- U meet de beschikbaarheid van uw dienst zelf, en rapport hierover maandelijks aan opdrachtgever

Toepasbaarheid

Altijd (standaardset), per aanbesteding formulering bepalen.

14.6.4 Toekomstbestendige werkplek

Uitgangspunt: We geven de voorkeur aan webbased applicaties voor onze gebruikers.

Toelichting: We zien dat steeds meer medewerkers mobiel werken, en daar moeten we de aangeboden applicaties op aanpassen.

Uitwerking: Door te kiezen voor webbased applicaties kunnen we deze eenvoudig aanbieden op laptops en in het thuiswerkportaal. Indien een applicatie niet webbased is bieden we deze aan via de Citrix werkplek. In dat geval moet de applicatie gedistribueerd kunnen worden middels Microsoft App-V.

Toepasbaarheid: Altijd (standaardset)

14.6.5 Hersteltijden bij verstoringen
Uitgangspunt: We maken afspraken over hersteltijden bij verstoringen
Toelichting: Verstoringen kunnen optreden. Uitsluiten daarvan zou de informatievoorziening onbetaalbaar maken. Er kunnen wel maatregelen genomen worden om eventuele verstoringen zo snel mogelijk te verhelpen. Het is van belang om heldere afspraken te maken over het herstellen van verstoringen. Dan weten we waar we aan toe zijn, en waar we recht op hebben mocht er een verstoring voorkomen.
- Vanuit het SSC maken we afspraken met onze partners over de geleverde diensten. Hierin zijn ook reactietijden afgesproken bij het melden van verstoringen, en we hebben afgesproken dat we een verwachte hersteltijd aangeven. De hersteltijd hangt af van de impact die de verstoring heeft en het aantal mensen dat er last van heeft. De afgesproken tijden zijn te vinden in de SLA. - Met (cloud)leveranciers dienen we ook dergelijke afspraken te maken. Het is vaak nodig om leveranciers in te schakelen om verstoringen aan applicaties en technische infrastructuur op te lossen. In de afspraken moet aandacht zijn voor: • Servicewindow waarin de leverancier bereikbaar is (kantoortijden/24x7) • Een reactietijd waarin de leverancier de melding gaat oppakken. • Vaak blijft het bij een best effort inzet om het probleem op te lossen. In sommige gevallen worden er harde afspraken gemaakt over hersteltijden. Of er wordt een percentage afgesproken van meldingen die binnen een bepaalde tijd wordt opgelost.
Toepasbaarheid: Altijd (standaardset) bepaal per aanbesteding de formulering, maak gebruik van genoemde voorbeelden.

14.6.6 Hersteltijden bij calamiteiten
Uitgangspunt: We maken afspraken over hersteltijden bij calamiteiten
Toelichting: Een calamiteit is een plotselinge gebeurtenis die veel schade kan veroorzaken. De impact is zo groot dat een herstel via de normale procedures voor verstoringen niet meer mogelijk is. De hersteltijd is daardoor vaak moeilijk vooraf te bepalen. Er worden echter wel wettelijke eisen gesteld aan de beschikbaarheid van bepaalde informatie (zoals bijvoorbeeld de bevolkingsadministratie). Er moeten daarom voor bepaalde belangrijke informatiesystemen procedures uitgewerkt zijn om te herstellen van een calamiteit. Deze moeten ook periodiek getest worden.
Uitwerking: - Het SSC heeft een calamiteitenplan. Hierin is de organisatiestructuur en de te volgen aanpak in het geval van calamiteiten vastgelegd. - Van vastgestelde cruciale informatiesystemen zijn herstelplannen uitgewerkt. - Periodiek (minimaal 1x per jaar) testen we de herstelplannen in een gesimuleerde praktijktest. - Contracten met leveranciers die een rol hebben in het herstelplan moeten hierop ingericht zijn. - (Cloud)leveranciers die (onderdelen van) informatiesystemen verzorgen die van cruciaal belang zijn moeten ook een calamiteitenprocedure hebben, en dienen dit periodiek te testen. Resultaten hiervan moeten voor ons inzichtelijk zijn. Deze verplichting dient ook onderdeel te zijn van de overeenkomst die met de leverancier wordt aangegaan.
Toepasbaarheid: Alleen bij cloud applicaties die zo belangrijk zijn dat er bij afwijking van de beschikbaarheidsnorm maatregelen genomen moeten worden. Denk bijvoorbeeld aan de wettelijke verplichting voor de bevolkingsadministratie.

14.6.7 Back-up
Uitgangspunt: We maken back-ups van onze gegevens.
Toelichting: Het kan gebeuren dat opgeslagen gegevens verminkt raken of verloren gaan. In dergelijke gevallen moeten we een back-up beschikbaar hebben van waaruit de gegevens herstelt kunnen worden. Hierbij dient aandacht te zijn voor: - de hersteltijd (hoe lang duurt het voordat de gegevens zijn teruggezet) - het moment van de laatste back-up (hoeveel gegevens gaan er mogelijk verloren door verwerkingen die zijn gedaan tussen de laatste back-up en het moment waarop de gegevens verloren zijn gegaan). - Back-ups worden in een ander systeem ondergebracht dan waar de gegevens zich normaal bevinden. De gegevens moeten ook hersteld kunnen worden naar een totaal andere omgeving dan die waarvan de back-up is gemaakt.
Uitwerking: - Het SSC heeft een back-upbeleid voor alle on-premise systemen die ze beheert. Hierin staat hoe vaak we back-ups maken, en hoelang we deze bewaren. - De hersteltijd van een systeem is maximaal 24 uur. - Met leveranciers die gegevens voor ons verwerken maken we afspraken over back-ups, hersteltijden, bewaartermijnen en maximaal gegevensverlies. Deze afspraken zijn schriftelijk vastgelegd in een overeenkomst. Wat acceptabele afspraken zijn hangt af van het belang van die gegevens en dient per geval beoordeeld te worden.

14.7Contractueel en ondersteuning

14.7.1 Ondersteuning gebruikers
Uitgangspunt: We ondersteunen onze eindgebruikers maximaal bij het in gebruik nemen van nieuwe applicaties of updates daarvan.
Toelichting: Applicaties worden in de regel centraal uniform (door)ontwikkeld voor alle klanten. De snelheid van beschikbaarheid van nieuwe functionaliteiten is, vooral bij Cloudtoepassingen, vaak hoog. Ook het moment van daadwerkelijk 'releasen' van deze nieuwe functionaliteit wordt vaak door de aanbiedende leverancier bepaald. Hoewel snelle doorontwikkeling prettig is, zorgt het bij wat minder digitaal vaardige collega's ook voor onrust. 'De applicatie werkt niet meer zoals ik gewend was, wat moet ik doen?' Functioneel Beheerders van de samenwerkende partijen hebben hierin een begeleidende taak. Toch worden ook zij soms verrast door (te) snelle ontwikkelingen. Wij zoeken ondersteuning vanuit onze leveranciers om alle gebruikers op een goede wijze te kunnen begeleiden in hun gebruik van uw oplossing, ook als deze niet in Cloud-vorm wordt aangeboden.
Uitwerking: Per update of nieuwe applicatie bepalen we met de leverancier welke ondersteuningsvorm(en) onze eindgebruikers nodig hebben. Mogelijke vormen zijn: handleidingen, instructievideo's, e-learning, traditioneel leer'klas'. Met de leverancier ontwikkelen we vervolgens ook deze ondersteuning.
Toepasbaarheid: Afhankelijk van de behoefte van de business. Moet bepaald worden samen met de informatieadviseur.

14.7.2 Ondersteuning beheerders incl. SLA
Uitgangspunt: We beschikken over een optimale ondersteuning vanuit de leverancier.
Toelichting: Het beheer van lokale- en Cloudtoepassingen vraagt ondersteuning vanuit de leverancier. Met name de rol van Helpdesk, Technisch Beheer en in mindere mate Functioneel Beheer zijn hierbij van toepassing. Ook het releasebeleid van (cloud)applicaties speelt hierbij een rol. Het is voor het SSC van belang dit releasebeleid te kennen en te weten welke invloed zij hier wel en niet op kan hebben.

14.7.2 Ondersteuning beheerders incl. SLA
Het testen van updates is belangrijk. Enerzijds aan de kant van de leverancier, maar ook voor de beheerders aan SSC-zijde. Wij gaan ervanuit dat altijd een eigen test/acceptatie-omgeving voor het SSC beschikbaar wordt gesteld voor het functioneel testen en daarbij bewerken van eigen data. Wilt u beschrijven hoe u de volgende 4 punten kunt invullen voor het SSC: - Helpdesk (hoe is deze georganiseerd en beschikbaar), - Beheer (welke taken voert u uit en wat verwacht u van het SSC), - Releasebeleid (hoe en wanneer releast u nieuwe functionaliteit) en Testomgeving (hoe kan het SSC beschikken over een dedicated test/acceptatieomgeving).
Uitwerking: Het geheel aan (beheer)afspraken leggen we samen met de leverancier vast. Vaste onderdelen hierbij zijn: inrichting Helpdesk, taakverdeling Functioneel- en Technisch beheer tussen leverancier en afnemende gemeenten en diensten, Releasebeleid, 'Up'-time garantie, Escalatieprocedure.
Toepasbaarheid: Altijd (standaardset)

14.7.3 Licentiebeleid
Uitgangspunt: We betalen voor daadwerkelijk gebruik van applicaties.
Toelichting: Het SSC hecht waarde aan een transparant licentiebeleid. Betalen per gebruiker, flexibel op- en afschalen van gebruikers vinden wij daarbij belangrijk. We kopen ook geregeld samen met de SSC partners applicaties in. In die gevallen is het ook van belang om afspraken te maken met de leverancier dat toekomstige nieuwe SSC-partners ook gebruik kunnen maken van bestaande contracten.
Uitwerking: Dit bereiken we door samen een contract op te stellen waarmee, in redelijkheid, aantallen gebruikers per maand op- en afgeschaald kunnen worden inclusief de daarbij horende kostenverhogingen – en verlagingen.
Toepasbaarheid: Altijd (standaardset)

14.7.4 Exitstrategie
Uitgangspunt: We kunnen snel en volledig migreren naar een andere oplossing
Toelichting: Voor het SSC is continuïteit cruciaal. Mocht uw organisatie onverhoopt in een situatie raken waarbij de aangeboden oplossing niet meer door u kan worden geleverd (bijv. bij een faillissement), dan is het zeer gewenst vooraf afspraken te maken, zodat het gebruik van de oplossing op een andere wijze kan worden voortgezet. Bijvoorbeeld middels een Escrowregeling. Daarnaast kan door diverse omstandigheden besloten worden de samenwerking niet voort te zetten. In een dergelijk geval zullen de gegevens overgezet moeten worden naar een andere oplossing. Het SSC wil daarover vooraf afspraken maken, zodat helder is hoe we de gegevens in een open format aangeleverd krijgen. Deze afspraken leggen we vast in een exitstrategie.
Uitwerking: Dit bereiken we door samen een exitstrategie op te stellen en deze onderdeel te maken van het contract.
Toepasbaarheid: Altijd (standaardset)