Gemeente Bergen op Zoom

Beleid

Informatiserings- en automatiseringsmanagement

Programma | BoZ in Control

Beleidsdocument

Versie:	1.3	Datum	05-06-2024
Bestuurlijk opdrachtgever	Directeur Bedrijfsvoering – Jaap Perfors	Voor akkoord:	College
		Datum:	03-07-2024
Opdrachtnemer	Manager Informatisering & Automatisering – Elsemieke Viergever		
Auteur	Projectleider ICT – Lieve van Wijk - van Schelven		

Inhoudsopgave

1 INLEIDING 3

1.1 AANLEIDING 3
1.2 PROBLEEMSTELLING 4
1.3 OPDRACHTFORMULERING 6
1.4 DOELSTELLING BELEID 6
1.5 LEESWIJZER 6

2 INFORMATISERINGS- EN AUTOMATISERINGSMANAGEMENT 7

2.1 WAT IS INFORMATIEMANAGEMENT? 7
2.2 WAT IS AUTOMATISERINGSMANAGEMENT? 7
2.3 INFORMATISERING- EN AUTOMATISERINGSMANAGEMENT BINNEN DE ORGANISATIE 7
2.4 DOELEN INFORMATISERINGS- EN AUTOMATISERINGSMANAGEMENT 9

3 PROCESSEN, MIDDELEN EN MENSEN 11

3.1 PROCESSEN 11
3.1.1 Universeel Service Management 11
3.1.2 Bedrijfskritische processen en applicaties 12
3.2 MIDDELEN EN SYSTEMEN 13
3.2.1 Informatie 13
3.3 DIENSTVERLENING 17
3.3.1 Applicaties en architectuur 18
3.3.2 Portfolio I&A 21
3.4 MENSEN 24
3.4.1 Borging (3 Lines Model) 24
3.4.2 Eerste lijn 25
3.4.3 Tweede lijn 25
3.4.4 Derde lijn 26
3.4.5 Rol en positionering afdeling I&A 26

4 BIJLAGEN 28

4.1 ROLLEN, TAKEN EN VERANTWOORDELIJKHEDEN 28
4.1.1 User 28
4.1.2 Superuser 29
4.1.3 Configuratiebeheerder 30
4.1.4 Wijzigingsbeheerder 31
4.1.5 Incidentbeheerder (Information Security Officer) 33
4.1.6 Informatieadviseur 35
4.1.7 Adviseur Informatiehuishouding 36
4.1.8 Informatiebeheerder 37
4.1.9 Applicatie-eigenaar 38
4.1.10 Functioneel beheerder 39
4.1.11 Technisch IT-beheerder 41
4.2 ICT-PROCESSEN 43
4.2.1 Wijzigingsmanagement 43
4.2.2 Configuratiemanagement 43
4.2.3 Patchmanagement 44
4.2.4 Incidentmanagement 45
4.3 BELEID VOOR INRICHTINGSPRINCIPES 46
4.3.1 Beleid voor logische toegangsrechten (Roll Based Access Control) 46
4.3.2 Beleid voor geautoriseerde soft- en hardware en informatiedragers 46
4.3.3 Beleid voor (virtuele) servers 46
4.3.4 Beleid voor endpoints 47
4.3.5 Beleid voor software/applicaties 47
4.3.6 Beleid voor netwerkapparatuur en firewalls 47

4.3.7 SIEM/SOC beleid 47
4.3.8 Escrow regeling beleid 48
4.3.9 Wachtwoordbeleid 48
4.3.10 Back-up & Recovery beleid 48
4.3.11 Releasebeleid 49
4.3.12 Beleid voor aansluiten op gemeentelijk netwerk en gebouw gebonden installaties 50
4.3.13 E-mailbeleid 50
4.3.14 Websitebeleid 50
4.3.15 Beleid Business Intelligence 50
4.3.16 Mobile Device beleid 50

1 Inleiding

1.1 Aanleiding

Vanuit bestuurlijke, ambtelijke en wettelijke opgaven professionaliseert de afdeling I&A het informatiemanagement van de gemeente. Dit gebeurt onder andere met het vaststellen van verschillende beleidsdocumenten en de inrichting van processen en procedures.

Organisatieontwikkeling

Intern is de organisatieverandering vanuit het programma 'Bergen in Beweging: Organisatieontwikkelingsplan 2022 – 2024, 1.0 afgerond en wordt deze vervolgd in versie 2.0. Vanaf 1 mei 2023 zijn managers benoemd om de nodige slagen te maken naar een gezonde bedrijfsvoering zoals verwoord in het Organisatieontwikkelingsplan '*Bergen in Beweging'*. De doelstelling is om ***'de interne organisatie op orde te brengen én te verstevigen'.*** In 2023 is gestart met de implementatie van integraal management: de inrichting van de PIJOFACH-ondersteuning en het vormen van de nieuwe afdelingen. ***'Deze implementatie vraagt aanpassing op de harde kant (o.a. structuur, systemen, processen) én op de zachte kant (cultuur, ontwikkelen van competenties etc.)'.***

Met dit beleidsdocument geven we invulling aan de I (informatie: Informatiebeveiliging, Informatiemanagement) van 'PIJOFACH' en stellen we kaders voor de harde kant, waarmee we structuur, systemen en processen inrichten, voor onze informatievoorziening vast.

Bestuursakkoord

Naast bovengenoemde is er in het bestuursakkoord een paragraaf opgenomen, onder *programma 5: Bedrijfsvoering, financiën en dienstverlening*, waarbij twee onderdelen worden benoemd:

1. Om 'in control' te raken, optimaliseren we de informatievoorziening en
2. We maken afspraken over het niveau van digitale veiligheid en nemen de BIO in acht.

In dit beleidsvoorstel leggen we afspraken vast, waarmee we een niveaustandaard neerzetten voor onze digitale weerbaarheid Daarnaast zetten we de informatieorganisatie neer, waarmee we de integraliteit en samenhang van de informatievoorziening waarborgen en het mogelijk maken om de organisatie te begeleiden bij het regievoeren op de informatievoorziening. Tevens wordt de basis gelegd om de informatievoorziening zo optimaal mogelijk in te richten.

Begroting 2024

In de begroting van 2024 wordt binnen *Programma 1: Bestuur en Ondersteuning* gesproken over het belang van het verhogen van de digitale weerbaarheid:

1. A.1.3.2 'We verhogen de digitale weerbaarheid (informatieveiligheid Q1-Q4)

Voor de continuïteit in de dienstverlening en bedrijfsvoering is een solide niveau van informatieveiligheid nodig. Inwoners moeten ervanuit kunnen gaan dat hun persoonsgegevens veilig zijn bij de gemeente. We streven komende jaren naar een situatie waarin beheersmaatregelen op het vlak van informatieveiligheid gedocumenteerd zijn, op gestructureerde wijze worden uitgevoerd en dat de uitvoering van de maatregelen aantoonbaar is en wordt getoetst (PDCA). Ook hebben wij een applicatie in gebruik, waarin dit wordt vastgelegd. Om de ICT-omgeving beschikbaar, integer en vertrouwelijk te maken en houden, is het allereerst van belang om te weten wat er zich allemaal binnen die ICT-omgeving bevindt. Om deze reden starten we een inventarisatie en documentatie van alle ICT-onderdelen en hun onderlinge relaties. Hierbij brengen we onder andere alle applicaties, koppelingen, processen en data in beeld. Om deze basis in kaart te brengen en te documenteren wordt een externe IT-architect ingehuurd. Na de inventarisatie en documentatie van de ICT-omgeving richten wij ons op bedrijfscontinuïteit in relatie tot onze ICT-omgeving. In 2024 starten wij met het inrichten van een beheersproces waarbij de gemeente maatregelen treft om de continuïteit van de meest kritische bedrijfsprocessen te garanderen, bij een ICT-uitval of verstoring. De inrichting van dit beheersproces raakt de hele organisatie en medewerkers moeten hiervoor getraind worden.

Paragraaf 2 - Dienstverlening

2. A.12.1.2 We bewaken de voortgang van elke vraag of melding van onze inwoners

Doen wat je belooft: dat is de basis voor elke dienstverlening. We zorgen voor een voorspelbare afhandeling met een proactieve terugkoppeling op vragen en meldingen van onze inwoners. Daarvoor gaan we procesmanagement inrichten. De applicaties die we gebruiken voor de afhandeling van vragen en meldingen richten we zodanig in dat voortgang centraal inzichtelijk is, zodat gestuurd kan worden op een afgesproken kwaliteitsniveau. We starten een project, waarbij inwoners en ondernemers (ongeacht het communicatiekanaal dat ze kiezen) eenzelfde afhandeling krijgen en ook zelf de voortgang van hun melding kunnen inzien.

Het project Duurzame Digitale Dienstverlening is inmiddels van start met als doel om te kijken naar de inrichting van een document- en zaaksysteem in combinatie met een klantportaal, waarmee we de voortgang van elke vraag of melding van onze inwoners kunnen bewaken.

Paragraaf 5 – Weerstandsvermogen en risicobeheersing

3. Aantasting vertrouwelijkheid, integriteit of beschikbaarheid van informatiesystemen

Voor het functioneren en de dienstverlening aan de inwoners gebruikt de gemeente Bergen op Zoom steeds meer gegevens, die we steeds meer uitwisselen en bewerken. Mede als gevolg van de decentralisaties in het sociaal domein heeft de gemeente steeds meer (bijzondere) persoonsgegevens in beheer. Ook wordt steeds meer informatie digitaal opgeslagen en overgedragen en worden systemen en data steeds vaker aan elkaar gekoppeld. Een recente ontwikkeling is het toegenomen thuiswerken. Dit soort gebeurtenissen wordt steeds groter in aantal en vernuftiger. Niet alleen de kans op deze gebeurtenissen neemt toe, maar ook de impact waarbij gedacht kan worden aan het in geding komen van de bedrijfscontinuïteit, vertrouwelijke gegevens die in verkeerde handen komen, imagoschade, financiële schade (herstelkosten, boetes, claims etc.) en ontwrichting van processen met maatschappelijke, economische of sociale gevolgen. In 2022 zijn de volgende maatregelen genomen: het opstellen van een crisisplan cybersecurity-incidenten, het overstappen op de ICT-infrastructuur van Sogeti en het uitfaseren van de oude infrastructuur van ICT WBW en zijn de eerste stappen gezet voor het op orde brengen van de processen incidentmanagement en wijzigingsbeheer. Tevens is in 2022 goedkeuring gegeven op het nieuwe mobile device beleid. Dit legt een basis die nodig is om de nieuwe telefoons en laptops van de gemeente beter te beveiligen. In 2023 wordt het project 'Informatiebeveiliging' (o.a. het wachtwoordbeleid) verder uitgevoerd.

4. Niet volledig voldoen aan de NIS2 richtlijn

In 2025 zal de Nederlandse versie van de Europese Network and Information Security directive (NIS2) van kracht worden. De NIS2 is bedoeld om de cyberbeveiliging en de weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren. De exacte impact voor gemeenten is nog niet duidelijk maar toont nogmaals de noodzaak aan van het aantoonbaar voldoen aan de volledige Baseline Informatiebeveiliging Overheid (BIO) door gemeenten. Naast de BIO, eist de NIS2 ook beveiliging van operationele technologie (OT), een effectieve Information Security Management System (ISMS) en een Business Continuity Management System (BCMS) volgens de normen ISO 27001 (managementsysteem voor informatiebeveiliging) en ISO 22301 (managementsystemen voor bedrijfscontinuïteit).

Vier bovengenoemde punten geven het belang aan van een informatisering en automatisering die op orde is. Integriteit, betrouwbaarheid en beschikbaarheid van informatie is cruciaal in het kunnen leveren van dienstverlening van bepaald niveau.
Daarnaast moeten we kunnen voldoen aan onze verantwoording voor landelijke wet- en regelgeving, denk hierbij aan de AVG, Rechtmatigheidsverantwoording, de Baseline Informatiebeveiliging Overheid en vanaf eind 2024 de NIS2. We willen een actieve, betrouwbare en dienstverlenende organisatie zijn om op te bouwen. Door slagvaardig en wendbaar te zijn, kunnen we snel inspelen op ontwikkelingen en veranderopgaven die nodig zijn. Met dit beleid voldoen we aan de opzet van opzet, bestaan en effectieve werking binnen het programma *Verhoogde Digitale Weerbaarheid*, welke in 2023 is gestart.

Strategisch beleid op Informatievoorziening (iVisie) 2023-2027

De vastgestelde iVisie (2023-2027) zet voor afdeling I&A en de gemeente Bergen op Zoom de stip op de horizon. Het Informatiemanagementbeleid spitst meer toe op specifieke onderwerpen uit de iVisie en is daarmee een verlengde hiervan.

1.2 Probleemstelling

In control

In de huidige situatie zijn wij onvoldoende 'in control'. Onder andere zijn wij minder dan noodzakelijk ***effectief, doelmatig en efficiënt in het inzetten van onze (beperkte) middelen.*** Daarnaast raak je alleen in control met inzicht. Juist dit inzicht ontbreekt op dit moment.

A. **Juiste informatie voor het maken van beslissingen**: informatie van juiste kwaliteit en goede beschikbaarheid, komt beslissingen ten goede. Er is op dit moment minder grip op bedrijfsvoering, besluitvorming is daardoor niet altijd goed onderbouwd en hierdoor is er onvoldoende inzicht en overzicht.
B. **Ontdekken van nieuwe mogelijkheden**: Door het ordenen van data en deze te analyseren, ontstaan er allerlei nieuwe mogelijkheden, kun je kosten besparen en groei realiseren. Dit is op dit moment slechts in bepaalde mate.

C. **Wendbaarheid**: Indien de situatie erom vraagt, kun je sneller reageren, als informatie goed toegankelijk is. Op dit moment is dat onvoldoende mogelijk.
D. **Efficiëntie**: Bedrijfsprocessen worden efficiënter door het verkrijgen van relevante informatie, wanneer je dat nodig hebt. Op dit moment is onze informatie versnipperd verkrijgbaar, door verschillende automatiseringsoplossingen heen.
Betere samenwerking: Binnen bedrijfsprocessen leveren verschillende afdelingen hun bijdrage. Een goede informatievoorziening helpt de onderlinge samenwerking verder. De samenwerking binnen informatisering en automatisering dient verder te worden versterkt.

Dienstverlening

Op dit moment kunnen we inwoners niet te allen tijden voorzien van duurzame informatie en voortgangsbewaking. Onze informatievoorziening en automatisering is hier niet op toegespitst. Het toegankelijk maken van informatie (vindbaar, beschikbaar, leesbaar, interpreteerbaar en betrouwbaar) vraagt om bepaalde voorzieningen en automatisering, zodat de toegankelijkheid en daarmee de duurzaamheid van informatie, bestand is tegen veranderingen van elke aard. De kaderstellingen worden in dit beleid vastgelegd.

Informatiebeveiliging

De Informatiebeveiligingsdienst, onderdeel van de VNG, voert elk jaar onderzoek uit naar het onderwerp informatiebeveiliging en heeft voor 2024 de volgende risico's benoemt met betrekking tot het onderwerp, waarmee beschikbaarheid, integriteit en vertrouwelijkheid van informatie in het geding komt:

A. **Uitval**: er bestaat een kans van uitval van de dienstverlening en bedrijfsvoering. Digitale processen worden zo niet meer ondersteund en dienstverlening en bedrijfsvoering komen stil te liggen.
B. **Schade**: vertrouwelijke informatie kan in verkeerde handen terechtkomen. Zo kunnen mensen onterecht toegang krijgen tot vertrouwelijke informatie, wat nadelig kan uitvallen voor onze inwoners en ondernemers. Laten we ook niet vergeten dat dit hoge boetes en mogelijk imagoschade oplevert.
C. **Fouten**: er kunnen fouten in de dienstverlening ontstaan, waardoor informatie niet meer integer is. Dit kan leiden tot vertraagde of foute beslissingen, verkeerde handelingen en verspilling van tijd en menskracht.

Er is daarnaast ook een dreigingsbeeld geschetst door de VNG:

A. **Ransomware**: de aanvallen door cybercriminelen hebben tegenwoordig destructievere gevolgen;
B. **Kwetsbaarheden**: steeds meer en ernstigere kwetsbaarheden in software worden geconstateerd en
C. **Gevaren uit zicht**: het werken met verschillende partners, zorgt ervoor dat gevaren in de keten uit het zicht raken.

De gevolgen van bovengenoemde problemen zijn onder andere hoge herstelkosten, reputatieschade en minder vertrouwen in de gemeente.
Belangrijk om bij dit onderwerp te noemen, is dat technologie alleen niet onze veiligheidsproblemen zal oplossen. Het vraagt om een cultuurverandering en meer digitale vaardigheden, want vooralsnog ontstaan bijna alle fouten door menselijk handelen.

Data en systemen moeten **beschikbaar** zijn, dienen de juiste gegevens te bevatten (juist, volledig en actueel, dus **integer**) en hier dient **vertrouwelijk** mee om te worden gegaan.

Toezichthouders

Het West Brabants Archief (WBA) en Interbestuurlijk Toezicht Informatie- en Archiefbeheer namens Provincie Noord-Brabant houden toezicht over onze informatiehuishouding.
Het West Brabants Archief (WBA) en Interbestuurlijk Toezicht Informatie- en Archiefbeheer (IBT)
Dit beleidsdocument omschrijft de doelstellingen, middelen, wegen en prioriteiten voor de ontwikkeling en te beheren onderdelen van de gemeentelijke informatievoorziening, zoals voorgeschreven door het West Brabants Archief. Daarmee wordt voldaan aan eis 1 van het inspectierapport van het WBA: De gemeente beschikt over een actueel informatiebeleidsplan.
Samen met het Strategisch Beleid voor Informatievoorziening (de iVisie), geeft dit beleid de leidende principes:

- De **organisatie** rondom de informatievoorziening
- De **visie** rondom de informatievoorziening
- **Beschrijving van de huidige** informatievoorziening
- Toegepast **kwaliteitssysteem**

1.3 Opdrachtformulering

Gezien de probleemstelling hebben de directeur Bedrijfsvoering en wethouder Pals de opdracht gegeven aan de manager Informatisering & Automatisering om beleid te schrijven die enerzijds aansluit bij de inrichting en implementatie van de harde kant en anderzijds de zachte kant van de gemeentelijke informatievoorziening.

Bij deze opdrachtformulering komen bestaande beleidsdocumenten, zoals Gemeentelijke Informatiebeleid (ICT Basisinfrastructuur en werkplekvoorziening 2021), Wachtwoordbeleid en Mobile Device Beleid te vervallen. Deze worden in hernieuwde vorm opgenomen in dit document.
Met de opzet en inhoud van dit document is er voortgeborduurd op de inhoud van het Strategisch Beleid op Informatievoorziening (iVisie).

1.4 Doelstelling beleid

*Enerzijds het aantonen van de **opzet (ontwerp) van beheersmaatregelen** binnen opzet, bestaan en effectieve werking, zoals getoetst door auditors, ten behoeve van het programma Verhoogde Digitale Weerbaarheid van de Informatiebeveiligingsdienst en anderzijds het **in control** raken met onze informatisering en automatisering door het **stellen van kaders,** het **vastleggen van afspraken** en het **neerzetten van de informatieorganisatie,** om zo een optimale dienstverlening aan te kunnen bieden aan inwoners en organisaties binnen de gemeente (externe klanten), maar ook aan onze interne klanten (alle afdelingen en samenwerkingsverbanden die wij bedienen). Er wordt een **eenduidige werkwijze** neergezet: 'Dit is hoe we het doen in Bergen op Zoom'.*

1.5 Leeswijzer

Het eerste hoofdstuk gaat in op de managementvormen informatisering en automatisering en welke doelen deze vormen kennen. Hoofdstuk 3 gaat in op de processen, middelen en mensen. Er wordt ingegaan op universeel service management, welke middelen (architectuur, applicaties, functioneel beheer, informatiebeheer) we inzetten om de doelen te bereiken en met wat voor informatie-organisatie (3LM en de rol van afdeling Informatisering & Automatisering) we dat doen. Ook wordt er ingegaan op het portfolio.
In de bijlage worden rollen met bijbehorende taken en verantwoordelijkheden omschreven. Tevens wordt er ingegaan op de 4 ICT-processen en beleid voor inrichtingsprincipes.

2 Informatiserings- en automatiseringsmanagement

Informatie en informatievoorzieningen worden steeds belangrijker. Met de verregaande digitalisering van werkzaamheden en een groei van informatie-gedreven werken, is een goede informatievoorziening bepalender dan ooit om de strategie en werkprocessen van de gemeente tot uitvoering te brengen. Het gaat daarbij met name om de functionele kant (informatiekant van I&A) en anderzijds om het strategisch belang van de infrastructuur (de automatiseringskant van I&A). Dit vraagt om goed ingericht informatiserings- en automatiseringsmanagement.

2.1 Wat is informatiemanagement?

Informatiemanagement is te definiëren als het geheel van processen, structuren, mensen, middelen en procedures (afspraken), waarmee een organisatie zorgt voor continue afstemming tussen vraag naar en aanbod van informatievoorziening en IT, op zowel strategisch-, tactisch- als operationeel niveau.
Goed ingericht informatiemanagement zorgt voor een informatievoorziening die stabiel en betrouwbaar is, ondanks dat deze voortdurend wijzigt. Met andere woorden: informatiemanagement is het middel om evenwicht tussen beheren en ontwikkelen van de informatievoorziening aan te brengen.
Het gaat dus om de vertaling van de informatiebehoefte in de organisatie naar een goede informatievoorziening, die de processen optimaal ondersteunt.

2.2 Wat is automatiseringsmanagement?

Automatiseringsmanagement is het automatiseren van bedrijfsprocessen. Het kan helpen bij het vereenvoudigen van werkzaamheden, vergroten van digitale transformatie, verhogen van klanttevredenheid, verbeteren van serviceniveaus en/of reduceren van kosten.

2.3 Informatisering- en automatiseringsmanagement binnen de organisatie

Informatiserings- en automatiseringsmanagement komt terug in elke laag en op elk niveau binnen de organisatie. Het ‘richten’ op strategisch niveau, het ‘inrichten’ op tactisch niveau en het ‘verrichten’ op operationeel niveau is gebaseerd op beschikbare informatie en de analyse van data, plus de beschikbaarheid en mogelijke toepassingen van automatiseringsmiddelen. Alleen met de juiste middelen, die de juiste data leveren, is de juiste sturing mogelijk op elk specifiek niveau.

De domeinen bevatten de reguliere bedrijfsvoering, zoals mensen, middelen, processen, etc. Bij het domein Informatie wordt de vraag vanuit het domein bedrijfsvoering, of overige domeinen, omgezet naar een informatiserings- of automatiseringsoplossing. Bij het domein ICT gaat het om het ontwerpen en beheren van ICT-toepassingen (automatisering) en daarbij de vragen beantwoorden vanuit de andere twee domeinen (bedrijfsvoering en informatie).

Op strategisch niveau wordt de richting bepaald, aan de hand van organisatiestrategieën. Binnen domein Informatie en ICT dient dit strategische beleid als aansluiting op de organisatiestrategieën. Een niveau lager, gaat het over mensen, middelen en processen en hoe deze in te zetten om de strategieën te bepalen. Op operationeel niveau worden dan de daadwerkelijke werkzaamheden uitgevoerd.

Met het verder professionaliseren van informatiserings- en automatiseringsmanagement, geeft afdeling I&A gehoor aan ‘Dit is hoe we werken in BoZ’, volgens het Organisatieontwikkelingsplan. Daarbij is integratie tussen informatisering en automatisering en de domeinen benodigd. Via dit beleid worden daarvoor kaders en randvoorwaarden gesteld, zodat I&A, naast een ondersteuning aan de organisatie op een reactieve manier in positie wordt gesteld en expertise, dus toegevoegde waarde, kan leveren.

Aan de hand van dit beleid werken we naar een integrale aanpak, waarin informatisering en automatisering een plek krijgt binnen de organisatiestrategieën. Door het vroegtijdig betrekken van informatisering en automatisering op strategisch niveau, zal de informatievoorziening (het aanbod) beter aansluiten op de vraag.

Vanuit procesmatig werken op tactisch en operationeel niveau kan er verticaal gestuurd worden, zodat het mogelijk is beoogde resultaten te behalen. Alleen als er wordt gedacht vanuit resultaten, om de (interne) klant zo goed mogelijk te bedienen, lukt het om het denken vanuit organisatiestructuren los te laten en doelen te realiseren vanuit processen.

2.4 Doelen Informatiserings- en automatiseringsmanagement

Wat wil gemeente Bergen op Zoom eigenlijk bereiken met Informatisering- en Automatiseringsmanagement? In het kader hiervan kennen we acht doelstellingen.

1) Leveren van (meer)waarde voor de organisatie

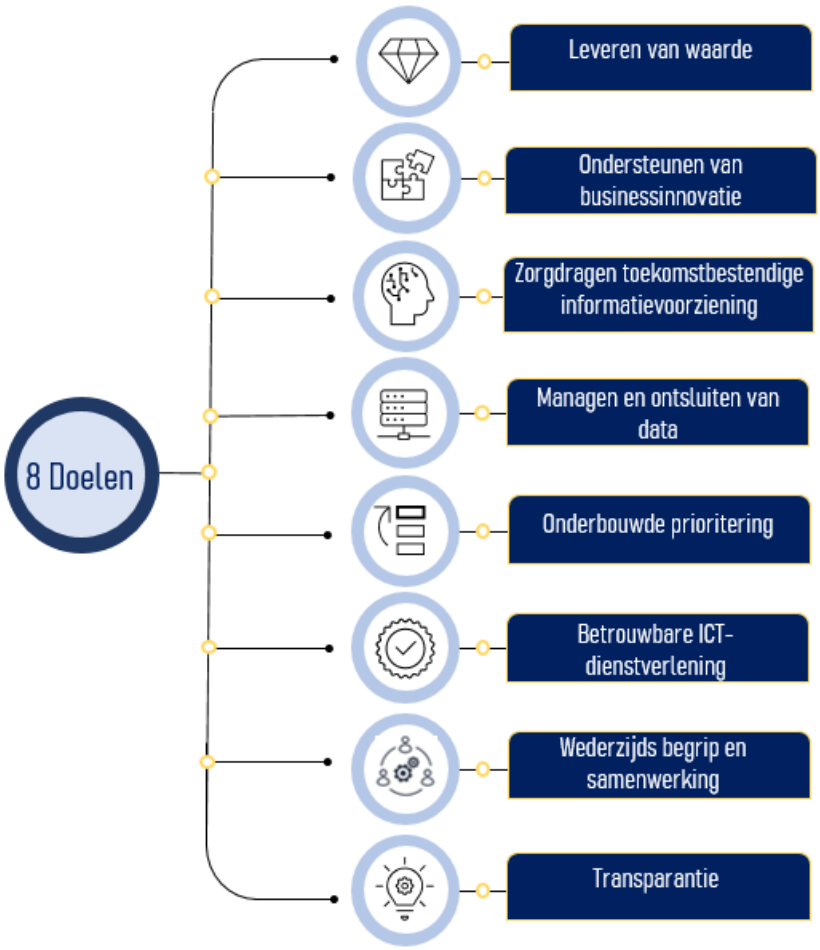
De ICT sluit aan op de organisatiestrategie en faciliteert daarmee de bedrijfsprocessen optimaal.

2) Faciliteren van business innovatie

Mogelijkheden in de ICT worden ingezet om vernieuwingen en verbeteringen in de organisatie te realiseren.

3) Zorgdragen toekomstbestendige informatievoorziening

Het is belangrijk om te sturen op een informatievoorziening die betrouwbaar, kostenefficiënt en onderhoudbaar is. Tevens is het belangrijk om relatief eenvoudig aanpassingen door te kunnen voeren bij veranderingen.



4) Managen en ontsluiten van data

Informatisering en Automatisering ondersteunt bij het beschikbaar stellen en omzetten van gegevens naar bruikbare informatie voor de organisatie. Hiermee is er meer inzicht, kunnen betere beslissingen worden genomen, is de organisatie meer in control en wordt er een hogere klanttevredenheid gecreëerd.

Data Management gaat over het veilig en kwalitatief beheer van data. Het managen van data omvat het onderhouden, actualiseren, beheren en beveiligen van data.
Binnen een specifiek domein is een toegewezen data-eigenaar hier verantwoordelijk voor. Wie data-eigenaar is van welk specifiek domein is vastgelegd in een Data Governance. BIC (Business Intelligence Centre) heeft in relatie tot Data Management een signalerende en ondersteunde rol. Denk hierbij aan het vervaardigen van datakwaliteit rapportages teneinde data-eigenaren in staat te stellen en de data-kwaliteit te verbeteren.

Het ontsluiten van data voor analyse en visualisatie valt onder verantwoordelijkheid van BIC.

5) Onderbouwde prioritering

Als doel heeft het inrichten van informatiserings- en automatiseringsmanagement dat processen, middelen en mensen zo optimaal mogelijk worden ingezet op de meest waardevolle initiatieven. Er wordt naar een ideale situatie toegewerkt.

6) Betrouwbare ICT-dienstverlening

Zorgen voor een effectieve inrichting van de ICT-diensten, zodat de organisatie goed ondersteund wordt.

7) Wederzijds begrip en samenwerking

Door te zorgen dat ICT de zorgen en wensen van de organisatie snapt en de organisatie de (on)mogelijkheden van ICT begrijpt, zal begrip voor elkaar groeiende samenwerking versterken.

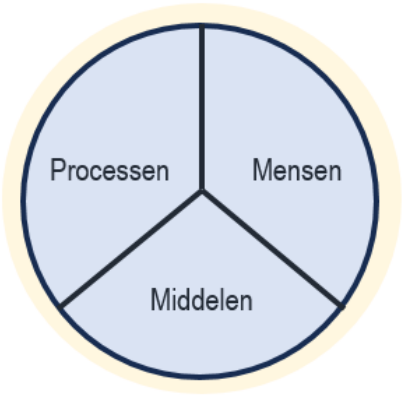
8) Transparantie

Het is belangrijk om prestaties inzichtelijk te maken van ICT-projecten en -processen, zodat de organisatie in control is en blijft.

De gemeente Bergen op Zoom wil aantoonbaar in control zijn om de doelstellingen van de gemeente effectief, efficiënt en transparant te kunnen behalen. Daarnaast heeft de gemeente als doelstelling om een actieve, betrouwbare en dienstverlenende gemeente zijn: 'een organisatie om op te bouwen'. Ook wenst de gemeente slagvaardig en wendbaar te zijn, dus snel in te kunnen spelen op ontwikkelingen en grote (verander)opgaven die zich voordoen.

Door het juist inzetten van informatiserings- en automatiseringsmanagement, is bovengenoemde mogelijk en heeft het allerlei positieve bijdragen:

- **Hogere klanttevredenheid**, het **in control** komen van de organisatie (de eerste en tweede lijn van control) en voldoen aan wet- en regelgeving aangaande **informatiebeveiliging**;
- **De continuïteit van de bedrijfsvoering** wordt geborgd en tegelijkertijd wordt er voldaan aan wet- en regelgeving, plus het behalen van programmadoelstellingen (de externe én interne wereld);
- **Borgen van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening** om zo een optimale dienstverlening aan burgers, bedrijven en samenwerkingspartners te kunnen leveren;
- **Betere beslissingen**: informatie van juiste kwaliteit en goede beschikbaarheid komt beslissingen ten goede. Er is grip op bedrijfsvoering. Besluitvorming is altijd goed onderbouwd en hierdoor is er voldoende inzicht en overzicht;
- **Ontdekken van nieuwe mogelijkheden**: Door het ordenen van data en deze te analyseren, ontstaan er allerlei nieuwe mogelijkheden, kunnen kosten bespaard worden en kunnen we groei realiseren. Hierbij wordt informatieveiligheid als voorwaarde gesteld voor een betrouwbare en veilige informatievoorziening;
- **Wendbaarheid**: Indien de situatie erom vraagt, kun je sneller reageren, als informatie goed toegankelijk (vindbaar) is.
- **Efficiëntie**: Bedrijfsprocessen worden efficiënter door het verkrijgen van relevante informatie, wanneer je dat nodig hebt;
- **Duurzame toegankelijkheid:** informatie is toegankelijk (vindbaar, beschikbaar, leesbaar, interpreteerbaar en betrouwbaar) op het juiste moment voor de juiste personen.
- **Betere samenwerking**: Binnen bedrijfsprocessen leveren verschillende afdelingen hun bijdrage. Een goede informatievoorziening helpt de onderlinge samenwerking verder.



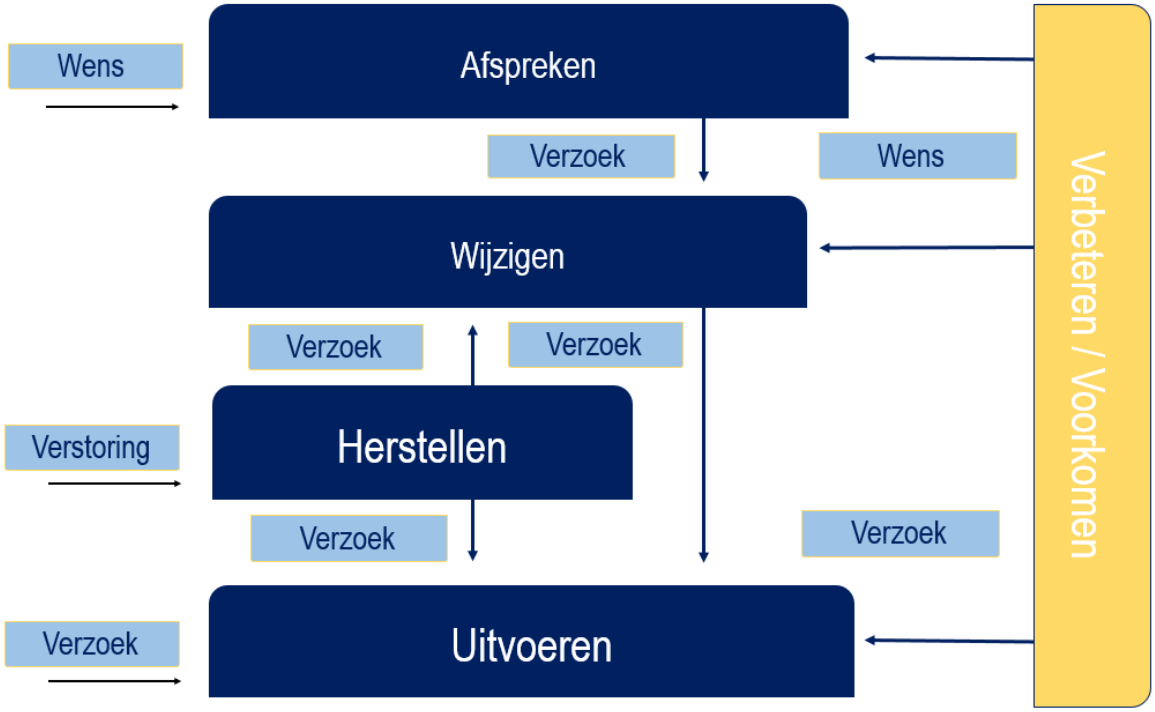
3 Processen, middelen en mensen

Bij informatiserings- en automatiseringsmanagement komen drie onderdelen samen: processen, middelen en mensen, waarbij het gaat om het vertalen van de informatiebehoefte in de organisatie naar een juiste aansluiting op de informatievoorziening, welke de processen optimaal ondersteunt.

3.1 Processen

3.1.1 Universeel Service Management

De processen van informatisering en automatisering zijn binnen de gemeente Bergen op Zoom ingeregeld via het Universeel Service Management (USM) systeem. Dit is een methodische werkwijze waar de dienstverlenende afdeling I&A mee werkt, om zo een gestandaardiseerde en gestructureerde service te kunnen leveren.



A) Afspreken

Binnen het afspreekproces wordt er samen met de klant gekeken naar de huidige dienstverlening en worden wensen voor aanpassingen besproken. Indien benodigd worden nieuwe afspraken gemaakt. Een voorbeeld hierbij is het aanschaffen van een nieuwe applicatie.

B) Wijzigen

Het wijzigingsproces is het meest centrale proces in het USM-model. Het kan worden getriggerd vanuit vier kanten: 1. Vanuit een wens voor het daadwerkelijk doorvoeren van nieuwe afspraken, 2. Vanuit een verstoring waarbij een wijziging moet worden doorgevoerd om de verstoring te herstellen of in de toekomst te voorkomen, 3. Vanuit een klantverzoek. 4. Vanuit een intern verbetervoorstel. Denk bij een wijziging aan het aanpassen van de inrichting van een applicatie.

C) Herstellen

In geval van een verstoring wordt een herstelproces opgestart. Verstoringen worden volgens prioritering afgehandeld. Denk hierbij aan het wegvallen van een het netwerk, of een account dat niet kan worden opgestart.

D) Uitvoeren

In het uitvoerproces gaan we uit van standaardwerkzaamheden: ‘going concern’.

E) Verbeteren / Voorkomen

Naast bovengenoemde processen is het ook wenselijk fouten, storingen, etc. te voorkomen en verbeteringen door te voeren. Afhankelijk van de aanlevering van deze verbetering, wordt of het afspraakproces, of uitvoeringsproces opgestart.

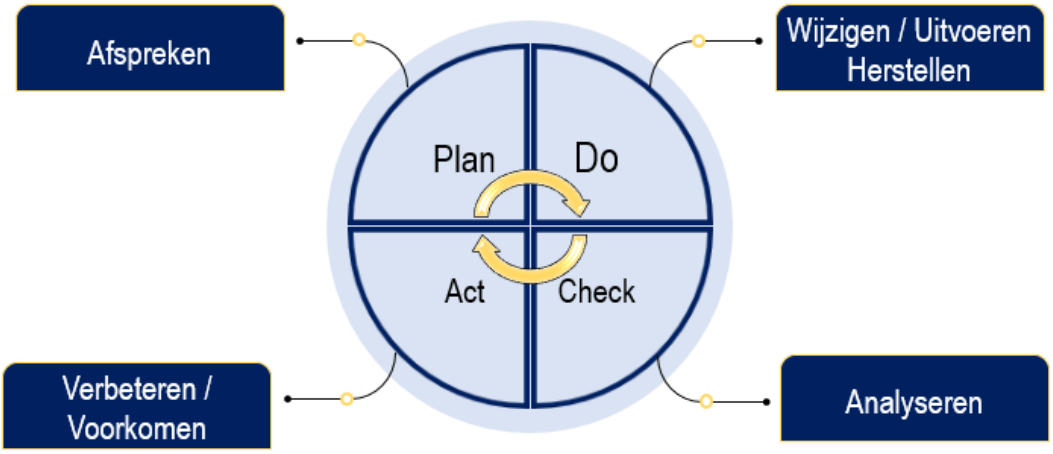
Bovengenoemde processen worden geactiveerd door drie triggers: Wensen, Verzoeken en Verstoringen.

Wensen, verzoeken en verstoringen

Een wens is een nieuwe vraag van de klant. Een wens kan zorgen voor een nieuwe afspraak tussen afdeling I&A en de klant, maar ook nieuwe afspraken met de leveranciers, of de invoering van wet- en regelgeving, als deze voldoet aan de opgestelde eisen. Een verzoek is een aanvraag, gebaseerd op bestaande afspraken. Een verstoring (incident) staat een bestaande afspraak in de weg: de dienstverlening kan niet volgens afspraak worden geleverd.

Deze methodiek volgt de PDCA-cyclus op volgende wijze:

1. **Plan**: in de planfase worden organisatiedoelen en eventueel de behoefte van de klant vertaald naar een informatie- en/of, automatiseringsstrategie. In deze fase worden met de klant nieuwe afspraken gemaakt, of bestaande afspraken gewijzigd,



2. **Do:** het 'doen' staat gelijk aan het beheren van de informatisering en automatisering: in deze fase wordt uitgevoerd, hersteld en gewijzigd volgens de bestaande of nieuw gemaakte afspraken.
3. **Check**: in de analysefase worden mogelijkheden om de organisatie effectiever en efficiënter te maken door informatie en/of automatie op een andere manier te gebruiken. Denk hierbij aan data-analyse en sturingsinformatie.
4. **Act:** in de verbeterfase worden analyses omgezet in nieuwe afspraken en deze doorgevoerd.

3.1.2 Bedrijfskritische processen en applicaties

Vanuit het perspectief van het 3LM model en de PIJOFACH-taken (met de I van Informatie), ligt de verantwoordelijkheid voor de informatievoorziening primair bij managers van de afdelingen, waarbij de I staat voor Informatievoorziening.

Dat betekent dat zij zelf verantwoordelijk zijn voor het in stand houden van hun processen, informatisering en automatisering in geval van nood. Zij dienen bedrijfscontinuïteitsplannen op te stellen en deze periodiek in de praktijk te testen. Afdeling Informatisering & Automatisering heeft hierin een faciliterende rol en ondersteunen daar waar nodig is en dienen hiervoor betrokken te worden in het kader van afspraken over back-up en recovery, hersteltijden, uitvaltijden, uitwijkmogelijkheden, SLA's met leveranciers, etc. Daarnaast biedt afdeling Informatisering & Automatisering kaders waarbinnen geopereerd dient te worden. Zo kan er eenduidigheid, optimalisatie van het applicatielandschap en integraliteit worden gewaarborgd. De tweedelijns functies hebben de signalerende rol hierin.

3.2 Middelen en systemen

'Zonder noodzakelijke middelen, geen business': de middelen en systemen ondersteunen de mensen en processen, waarbij er extra aandacht nodig is om te zorgen voor aansluiting van deze drie onderdelen. Zonder goed gereedschap ontstaat er frustratie en inefficiëntie. Zonder aandacht voor de mensen ontstaat er vervreemding, onverschilligheid en worden systemen niet goed gebruikt.
Gezien de gemeente een informatieorganisatie is, is informatie hét belangrijkste middel om onze zorgplicht uit te kunnen voeren. Daarnaast dienen we ook randvoorwaarden te stellen om de dienstverlening omtrent informatisering en automatisering uit te kunnen voeren. Tevens dient het applicatielandschap mensen en processen te ondersteunen, middels gestelde kaders binnen de ICT-architectuur.

3.2.1 Informatie

Voor het correct beheren van de gemeentelijke informatie is verschillende wet- en regelgeving relevant: de Archiefwet, Wet Open Overheid, Wet Elektronische Publicaties en de nog in werking te treden wet Modernisering Elektronisch Verkeer.

De belangrijkste bepaling van de archiefwet is dat overheden hun informatie in goede, geordende en toegankelijke staat moeten brengen en bewaren. De informatie moet dus makkelijk te vinden en te raadplegen zijn. Ook moeten overheden zorgen voor de vernietiging van informatie die daarvoor in aanmerking komt, omdat vernietiging van informatie de toegankelijkheid van de nog te bewaren informatie vergroot.
De belangrijkheid van toegankelijke informatie is ook belangrijk voor de uitvoering van de Woo en tevens één van de plichten. De Woo regelt namelijk de actieve en passieve openbaarheid van documenten. Dit kan alleen slagen als de informatie ook daadwerkelijk duurzaam toegankelijk is gemaakt. Duurzaam toegankelijke informatie is vindbaar, beschikbaar, leesbaar, interpreteerbaar, betrouwbaar en toekomstbestendig. In de Woo is ook bepaald dat overheidsorganisaties hun informatiehuishouding moeten verbeteren. Ook hierbij is duurzaam toegankelijke informatie het belangrijkste aspect.
De Wep introduceert een verplichting voor gemeenten om alle wettelijk voorgeschreven bekendmakingen, mededelingen en kennisgevingen van (voorgenomen) besluiten die niet tot één of meer belanghebbenden zijn gericht, in een officieel elektronisch publicatieblad te publiceren. Met de Wet modernisering elektronisch bestuurlijk verkeer (Wmebv) krijgen inwoners en ondernemers het recht om officiële berichten elektronisch aan gemeenten en andere overheidsorganisaties te versturen.

Om aan wet- en regelgeving omtrent onze informatiehuishouding te kunnen voldoen, is er een afhankelijkheid van onze middelen, mensen en processen. Uit een eerste onderzoek blijkt dat ons applicatielandschap niet is ingericht op geldende wet- en regelgeving. We weten ook al dat dit niet volledig naar wetgeving in te richten is. Ook zien we dat qua kennis omtrent onze informatiehuishouding nog een grote inhaalslag te behalen valt op dit vlak. Niet alleen voor informatiemedewerkers (informatiebeheer en -adviseurs), maar ook voor mensen die informatie produceren (op de afdeling).

Verbeterplan Informatiehuishouding

Een belangrijk onderdeel binnen 'Informatie' is het Verbeterplan Informatiehuishouding. Dit verbeterplan is gebaseerd op het Rapport Archiefinspectie gemeente Bergen op Zoom dat door de archivaris, in het kader van het wettelijk toezicht op het archiefbeheer van de gemeente Bergen op Zoom, is opgesteld. Ook het Interbestuurlijk Toezicht Informatie- en Archiefbeheer (IBT) - Toezichthouder van de provincie - toetst de kwalitatieve staat van de informatiehuishouding van een gemeente. In de beoordeling laat het zich leiden door de verslaglegging van de archivaris. De resultaten uit het Verbeterplan Informatiehuishouding zorgen voor verbetering van de informatiehuishouding van de gemeente, met overdracht naar beheer, zodat de huishouding toekomstbestendig wordt en blijft. In een cyclus van twee jaar worden we getoetst, waarbij het ene jaar een inspectie plaatsvindt en het andere jaar er wordt gekeken naar de tussenstand van de ontwikkelingen en het college dat hierover verantwoording aflegt.

Naar aanleiding van het inspectierapport in 2023 ligt de nadruk op het verbeteren van de informatiehuishouding van gemeente Bergen op Zoom. Zodoende dat er op verschillende belangrijke onderdelen binnen de archiefwet uitgangspunten worden opgesteld in dit beleid.

Uitgangspunten en eisen (archief)wet- en regelgeving

Hieronder volgt een globale omschrijving van de uitgangspunten omtrent de gemeentelijke informatiehuishouding:

- Focus bij het duurzaam beheren van informatie op 167 zaaktypen met procesgebonden informatie die bewaard moet blijven
- Te bewaren digitale informatie, moet overgebracht worden naar het e-depot van het WBA.

Blijvend te bewaren informatie, gaat naar het e-depot, als deze MDTO eisen hanteren. Dat gaat óf rechtstreeks, als een applicatie dat kan, óf via het DMS als een applicatie niet direct gekoppeld kan worden. In het geval van blijvend te bewaren informatie, zal er vernietigd moeten worden in de vakapplicaties en DMS, aangezien het overbrengen inhoudt dat het beheer van de informatie wordt overdragen en hier wordt ook een verklaring van ondertekend. Met vernietigen van informatie in de vakapplicaties wordt álle informatie bedoeld, dus ook metadata.

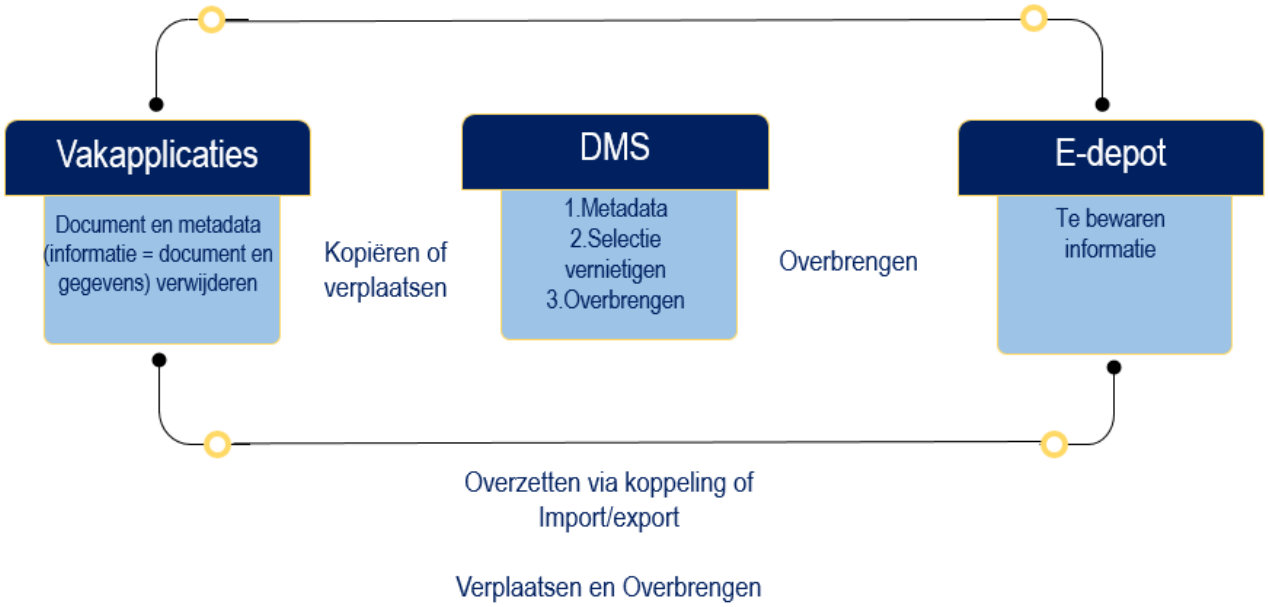
- Om de overige informatie conform de archiefwet te bewaren en vernietigen, moet onderzocht worden of er handmatig vernietigd kan worden, als dit niet geautomatiseerd kan worden opgelost.
- We zullen een stevige gesprekspartner moeten zijn richting onze leveranciers en bij nieuwe applicaties kijken naar het verschil tussen de GIBIT en de archiefwet, waarin we eisen tussentijds onze data te mogen vernietigen.
- Voor het koppelen met het e-depot kan gekeken worden naar directe koppelingen of een import/export optie.

E-depot

- Procesgebonden te bewaren informatie moet naar het e-depot worden overgebracht. Waarbij de archiefwet nu nog voorschrijft dat het informatie betreft wat ouder is dan 20 jaar, wordt dat in de nieuwe archiefwet veranderd naar 10 jaar. Met dit uitgangspunt anticiperen we op de nieuwe overbrengingstermijn.
- Procesgebonden te vernietigen informatie, mag in de applicatie blijven en mag in de applicatie worden vernietigd. Gegevens over te vernietigen informatie dienen geëxporteerd te kunnen worden voor het maken van een verklaring van vernietiging.

Nationaal archief geeft aan dat het een eis is om blijvend te bewaren informatieobjecten binnen twintig jaar over te brengen naar een archiefbewaarplaats, met als doel dat gebruikers erop kunnen vertrouwen dat blijvend te bewaren informatie, ook in de toekomst is en, op termijn, openbaar wordt. Met andere woorden: blijvend te bewaren informatie is ook in de toekomst nog duurzaam toegankelijk voor gebruikers.

Overbrengen is een juridisch begrip, waarmee wordt aangeduid dat het overgebrachte informatieobject aan bepaalde eisen van de Archiefwet, Archiefbesluit en Archiefregeling moet voldoen. Zo is overgebrachte informatie in principe openbaar en zijn er geen kosten verbonden aan raadpleging. Overbrengen naar een archiefbewaarplaats betekent dat de verantwoordelijkheid voor het beheer van blijvend te bewaren informatie wordt belegd bij een speciaal daarvoor ingerichte organisatie. Dit is noodzakelijk omdat niet alle overheidsorganisaties er op zijn ingesteld informatie voor eeuwig te bewaren.



Archiveren by Design

Om door te gaan op hetgeen hierboven genoemd, kunnen we stellen dat we archiveren by design (deels) toepassen. Bij de inrichting van een informatiesysteem, worden bovengenoemde uitgangspunten bekeken en aan de hand daarvan informatie duurzaam toegankelijk gemaakt. Met 'duurzaam toegankelijk' wordt bedoeld dat informatie gedurende de bewaartermijn:

- Vindbaar;
- Beschikbaar;
- Leesbaar;
- Interpreteerbaar;
- Betrouwbaar;
- Bestand tegen veranderingen, voor zo lang als nodig.

Archiveren gebeurt in de applicaties, indien dit mogelijk is volgens de wet- en regelgeving. Indien niet mogelijk, of wanneer de kosten en benodigde capaciteit niet opwegen tegen het voordeel, wordt er gearchiveerd in het documentmanagementsysteem. Hierbij wordt ook de gebruikerskant afgewogen.

Daarbij wordt tevens gekeken naar:

- Te bewaren informatie en overbrengen naar het e-depot
- Welke metagegevens minimaal nodig zijn
- Hoe vernietiging wordt ingericht
- Documentopslag: hoe richten we dat in?
- Welke mate van automatisering er wordt toegepast?

Vakapplicaties

Afhankelijk van het eindresultaat van een zaak, worden de juiste gegevens aan een zaak gekoppeld. Denk hierbij aan selectielijsten en metadata.

Vernietiging

Eisen voor vernietiging zijn opgenomen in de informatiearchitectuur van de gemeente. Ook tijdens de marktoriëntatie wordt er extra focus gelegd op onderdelen van de archiefwet, waaronder vernietiging. De GIBIT dekt helaas niet het geheel af, waardoor we apart contractueel zullen moeten vastleggen dat we tussentijds gegevens willen kunnen vernietigen uit (vak)applicaties en dienen de gegevens te kunnen worden geëxporteerd.

Informatieobjecten worden niet eerder en niet later vernietigd dan is aangeven in de selectielijst. Na vernietiging van een informatieobject is er een verklaring van vernietiging beschikbaar. Als informatieobjecten in aanmerking komen voor vernietiging na afloop van de bewaartermijn, dan moet dat volgens de wet ook gebeuren. Vernietigen is dus een verplichting. Waarbij de vernietiging wordt gedocumenteerd zodat de overheidsorganisatie zich hierover kan verantwoorden. Uit onderzoek blijkt dat veel applicaties hiertoe niet geschikt zijn. We zullen dus focus moeten aanbrengen, om stapsgewijs aan deze gestelde eisen te kunnen voldoen. Dit wordt ondergebracht in het Verbeterplan Informatiehuishouding, waarbij projectmatig gewerkt wordt richting de juiste implementatie en borging van dit vraagstuk.
Belangrijk om hieraan toe te voegen is dat het vernietigen van informatie, de toegankelijkheid van de te bewaren informatie verbeterd. Daarnaast is het ook zo dat deze informatie dus niet meer beveiligd hoeft te worden en tijdig vernietigen van gegevens de kans op datalekken (onbedoelde of ongeoorloofde toegang of verspreiding) aanzienlijk verkleint. Het is dus een belangrijke functie van informatiebeheer en versterkt, wanneer goed ingericht, informatiebeveiliging en privacy.

Metadatagegevensschema

Gemeente Bergen op Zoom hanteert een metadataschema, welke voldoet aan de MDTO-eisen. Het applicatielandschap kan hierop worden ingericht. Op dit moment is de inrichting van het e-depot van het West Brabants Archief ingericht op de verouderde TLMO-eisen. Dat betekent dat we in samenwerking met het Archief een nieuw schema opstellen. Voor reeds gestarte overbrengingswerkzaamheden blijven de huidige e-depot eisen gelden.

Duurzame Toegankelijkheid (DUTO raamwerk)

Het DUTO Raamwerk (vastgesteld in april 2024) is een instrument om stapsgewijs te werken naar informatie duurzaam toegankelijk maken. Het combineert architectuurprincipes met geldende wet- en regelgeving.

Waarom is Duurzame Toegankelijkheid van belang?
Er zijn drie perspectieven van waaruit duurzame toegankelijkheid belangrijk is.

- **Publieke waarde:** Vanuit het perspectief van de samenleving, kan overheidsinformatie bepaalde waarde vertegenwoordigen. Door deze informatie duurzaam toegankelijk te maken, stelt de overheid de maatschappij in staat om deze waarde te benutten.
- **Legitimiteit**: Welke producten en diensten de overheid levert en de voorwaarden waaraan deze moeten voldoen, is vastgelegd in wet- en regelgeving. De principes / uitgangspunten van duurzame toegankelijkheid van overheidsinformatie dragen eraan bij dat overheidsorganisaties rekening houdend met wet- en regelgeving, op een rechtmatige manier hun taken kunnen uitvoeren en verantwoording hierover kunnen afleggen.

- **Organisatie**: Duurzame toegankelijke informatie is een belangrijke grondstof voor de overheid. Het is de grondstof voor het leveren van producten en diensten, waarmee de overheid publieke waarde creëert binnen de geldende wettelijke kaders.

Het DUTO-raamwerk is van toepassing in alle gevallen waar een overheidsorganisatie omgaat met overheidsinformatie. Denk dan aan het registreren, vernietigen, migreren, bewaren of ter beschikking stellen van overheidsinformatie. Het DUTO-raamwerk is een instrument voor concrete, passende maatregelen voor het beheer van overheidsinformatie.
Om juist om te gaan met geldende wet- en regelgeving, zullen we dit instrument als hulpmiddel inzetten bij bestaande en nieuwe informatiserings- en automatiseringsvraagstukken.

Toegepast kwaliteitssysteem

Het wettelijk verplichte kwaliteitssysteem voor informatiehuishouding is opgenomen voor implementatie binnen het Verbeterplan Informatiehuishouding. Het kwaliteitssysteem van het West Brabants Archief wordt gehanteerd. De verantwoordelijkheid voor dit kwaliteitssysteem is belegd bij manager Informatisering & Automatisering.

3.3 Dienstverlening

De afdeling I&A stelt kaders, faciliteert de organisatie, bewaakt de integraliteit en samenhang van de totale informatievoorziening en begeleidt de organisatie om regie te voeren op informatievoorziening. De afdeling I&A is verantwoordelijk voor de adviserende, toetsende en uitvoerende activiteiten (hetgeen centraal is belegd) ten aanzien van de informatiserings- en automatiseringsfunctie.

Als primaire taak van I&A kan gezien worden: het beschikbaar stellen en houden van processen conform hetgeen afgesproken in de product- en dienstencatalogus, zodanig dat de organisatie haar werkzaamheden zonder belemmeringen kan uitvoeren. Om dit mogelijk te maken kent I&A een zogenaamde basisdienstverlening, waaronder alle generieke componenten van de informatievoorziening vallen om dit mogelijk te maken. Hieronder valt het beschikbaar stellen en houden van de (technische) infrastructuur (o.a. software, uitwijk, netwerk en dataverbindingen), maar ook het voldoen aan allerlei wettelijke verplichtingen en geadviseerde normen binnen het vakgebied.

I&A voert tevens regie; ze schept de voorwaarden voor de afdelingen om hun informatievoorziening te beheren en te ontwikkelen en begeleidt en adviseert de afdelingen bij realisatie van hun informatiekundige opgaven en digitale transformaties. Daarnaast voert ze regie op automatiseringstaken die zijn uitbesteed aan derde partijen.

Hiermee bewerkstelligt de gemeente dat er, bij de continue veranderingen in de procesinrichting, informatievoorziening, applicatielandschap en informatietechnologie, altijd sprake is van een stabiel en betrouwbaar werkend geheel en er een hoge mate van beschikbaarheid is op de beschikbaarheid van hoogwaardige informatie en informatievoorziening voor de organisatie.

Wat betreft wet- en regelgeving, denk hierbij aan informatiewetten, Europese Verordeningen, Informatiebeveiliging, Normenkaders (BIO), maar ook landelijke en maatschappelijke ontwikkelingen, trends, nieuwe ICT-ontwikkelingen, heeft I&A een signalerende en adviserende rol. De I binnen PIOFACH legt de verantwoording voor het opvolgen van wet- en regelgeving bij het lijnmanagement. Indien het benodigd is, kan er ondersteuning plaatsvinden vanuit I&A in de vorm van advies, projectleiding en beheer.

Randvoorwaarden

De dienstverlening kan alleen worden aangeboden als I&A vanuit de strategische doelstellingen proactief en reactief kan anticiperen op nieuwe en lopende vraagstukken. Via deze weg kunnen specialisten tijdig vraagstukken toetsen aan vastgestelde kaders en strategische doelstellingen.

Dit is ook van toepassing als ICT geen positie krijgt in de eigen infrastructuur, waardoor het beheer niet centraal in de organisatie wordt ingeregeld. Denk hierbij aan de aanschaf van camera's of ander gerelateerde ICT-technische, informatiserings- en automatiseringsvraagstukken. Ook deze vraagstukken dienen te worden getoetst en de ICT-processen dienen te worden gevolgd, zodat er wordt voldaan aan gestelde eisen en de juiste databases worden gevuld met de nieuwste informatie.

Reikwijdte dienstverlening I&A

I&A beheert het informatielandschap vanuit de producten- en dienstencatalogus, met eventueel bijbehorende addenda.

Reikwijdte dienstverlening ICT-leveranciers

De dienstverlening van de ICT-leveranciers zijn vastgelegd in een Service Level Agreement (SLA) en in de aanbesteding. Voor nieuwe dienstverlening zullen nieuwe afspraken worden gemaakt, welke weer worden opgenomen in de SLA. Gemeente Bergen op Zoom is eindverantwoordelijk en voert regie over de informatisering en automatisering.

Centraal en decentraal functioneel beheer

Applicaties gebruikt door meerdere afdelingen, complex qua beheer en belang van samenhang, worden centraal beheerd door afdeling Informatisering & Automatisering. Kleinere, specifiek toegespitst op bepaalde afdelingen, met simpele vorm van beheer, bijvoorbeeld ook extern beheer, kan decentraal worden belegd.
De keuze hiervoor zal in overeenstemming plaatsvinden tussen manager Informatisering & Automatisering en desbetreffende applicatie-eigenaar. De bijbehorende taken en verantwoordelijkheden, zijn in bijlage van dit document toegevoegd.

3.3.1 Applicaties en architectuur

Applicaties dienen het organisatiebelang en de architectuur van het applicatielandschap dient te voorkomen dat er kapitaalvernietiging plaatsvindt, of op een andere manier niet doelmatig te werk wordt gegaan.
De inzichtelijkheid van de architectuur van het applicatielandschap, maakt het mogelijk om tijdig te kunnen signaleren, sturen en rapporteren op wet- en regelgeving en informatievoorziening. Hiermee kan worden afgestemd op concrete beleidsmatige vraagstukken en wordt voorkomen dat er voornamelijk eenzijdig wordt geacteerd vanuit de wensen van de afdelingen ten behoeve van ICT-toepassingen.

Automatiseringsinrichting

Om voor de bedrijfsdoelstellingen en wet- en regelgeving de juiste informatie uit verschillende automatiseringstoepassingen te halen, maar ook om kostenefficiënt te zijn, processen en werkzaamheden te vereenvoudigen en serviceniveaus te verbeteren, is de inrichtingskeuze cruciaal. De keuzes bepalen de mate van slagen en succes.

De te bepalen richting is daarbij wel afhankelijk van de automatiseringsmogelijkheden en dat is waar het werken onder architectuur bij helpt. Zoals vastgesteld in het Strategisch Beleid op Informatievoorziening (iVisie) is het werken onder architectuur een succesfactor binnen informatiserings- en automatiseringsmanagement. Het draagt bij aan de uniformiteit, samenhang en bevordert een efficiënte en flexibele informatievoorziening.

Belang van architectuur

De gemeentelijke informatievoorziening groeit jaarlijks in omvang, samenhang en daarmee in complexiteit. De gemeente wil steeds verdergaande digitalisering en de technologische toepassingen maken dit mogelijk. Grip is hierbij belangrijk. Architectuur schept overzicht en stelt eisen, om complexiteit te reduceren en samenhang te bevorderen. Allerlei ontwikkelingen zorgen voor veranderingen; de architectuurprincipes geven aan op welke wijze we omgaan met deze veranderingen. Er ontstaat samenhang tussen de informatiebehoefte die voortkomt uit beleid, besturing en werkprocessen aan de ene kant, en de ICT-diensten, informatiesystemen en ICT-infrastructuur aan de andere kant. Hierbij wordt gewerkt vanuit de gedachtegang van de in- en externe klant. Om deze samenhang zo optimaal en inzichtelijk mogelijk te houden, moeten keuzes worden gemaakt en prioriteiten worden gesteld. Architectuur zorgt daarin voor kaders, zodat herkenbaarheid en herbruikbaarheid van oplossingen wordt toegepast.

Vooralsnog ligt de focus op informatiearchitectuur en technische architectuur. De aandachtsgebieden van Enterprise-architectuur en bedrijfsarchitectuur worden buiten beschouwing gelaten.

Vijf architectuurlagen

Door te werken onder architectuur is een organisatie onder te verdelen in vijf architectuurlagen: Grondslagen (beleid, besturing), Organisatie en processen; Informatie, Applicatie en Netwerk (ICT-Infrastructuur).
Omwille van uniformering en standaardisatie is er veel generiek aan de architectuur voor de overheid en zeker voor gemeenten. De Nederlandse Overheid Referentie Architectuur (NORA) bevat principes, beschrijvingen, modellen en standaarden voor het ontwerp en de inrichting van de digitale overheid. Het is een instrument dat door overheidsorganisaties kan worden benut in de verbetering van de dienstverlening aan burgers en bedrijven.
In 2009 is NORA door het kabinet vastgesteld als norm voor de overheid. GEMMA is een vertaling naar de gemeentelijke architectuur.

Onderstaande tabel geeft aan welke componenten er per laag van de architectuur zijn en wie verantwoordelijk is voor het actueel houden hiervan.

Architectuuraanpak

Laag	Component	Eigenaar	Vindplaats
Grondslagen	Visiedocumenten	Directie	BoZnet
	Sturingsfilosofie, organisatieontwikkeling, bestuursakkoord, begroting	Directie	BoZnet
	Informatiserings- en automatiseringsbeleid	Informatieadviseurs	BoZnet
	Informatiebeveiligingsbeleid	CISO	BoZnet
	Overzicht wetten en regels (landelijk)	Juristen	Wetten.nl
	Overzicht beleidsregels en verordeningen	Bestuurssecretariaat	Wetten.nl
Organisatie en processen	Overzicht processen en risico's	Managers	Applicatie Proces- en Risicomanagement (n.t.b.)
	Overzicht rollen, taken en verantwoordelijkheden	Managers	ADP
	Overzicht mandaten	Juristen	Mandaatregeling BoZnet
	Overzicht medewerkers en autorisaties	HRM	ADP (loopt een aanbesteding voor)
Informatie	Informatie-architectuur (GEMMA)	Informatieadviseurs en informatiehuishouding	iNavigator TopDesk
	Kaders en richtlijnen informatievoorziening	Manager I&A	BoZnet
	Metadatamodel	Informatieadviseurs en informatiehuishouding	iNavigator
	Informatiebehoefte	Managers	Domein en afdeling A3 Jaarplannen
	Overzicht DPIA's	Functionaris Gegevensbescherming	Register DPIA
Applicatie	Overzicht applicaties en applicatielandschap	Manager I&A	TopDesk
	Overzicht koppelingen en integraties	Manager I&A	TopDesk
	Overzicht leveranciers	Informatieadviseurs	TopDesk
Netwerk	Technische architectuur	ICT-dienstverlener	Juniper
Overall	Regie op architectuur	Manager I&A	CMDB's ▪ Applicatie proces- en risicomanagement ▪ TopDesk Netwerkscanning ▪ LANSweeper

Toepassen informatie-architectuur

Informatie-architectuur heeft een adviserend en ondersteunend karakter:

- Bij een informatiserings- en automatiseringsvraagstuk worden wijzigingen beoordeeld op o.a. de gevolgen voor de huidige ICT-infrastructuur en het applicatielandschap;
- Wanneer de intake resulteert in een project kan de informatieadviseur een projectstartarchitectuur (PSA) opstellen met de eisen waaraan het projectresultaat moet voldoen;
- Bij het aanbesteden van een ICT-gerelateerd project zal de informatieadviseur deze eisen vertalen naar het Programma van Eisen;
- De gevolgen van nieuwe wetten en richtlijnen worden vertaald naar de gewenste maatregelen voor de informatievoorzienig van de gemeente Bergen op Zoom;

- Rapportage over stand van zaken rond architectuur.

Actualiseren informatie-architectuur

- **Informatie-architectuur:** De GEMMA gebruikt een kader met referentiecomponenten. Elk component vertegenwoordigt een specifieke functie die met behulp van applicatie(service)s kan worden ingevuld. Ontbrekende functies tonen een hiaat, meerdere applicaties voor dezelfde functie bieden een mogelijkheid tot applicatierationalisatie. De applicaties van gemeente Bergen op Zoom zijn geplot op het GEMMA-model binnen een nog nader te bepalen applicatie. De rapportagemogelijkheden van deze tool worden in de praktijk gebruikt bij vraagstukken op het gebied van informatisering en automatisering.
- **Kaders en richtlijnen informatievoorziening:** Wetgeving en richtlijnen, normenkaders, beleidsuitgangspunten en doelstellingen worden omgezet in architectuurprincipes. Daarnaast biedt een standaard Programma van Eisen en vastgestelde onderdelen binnen de marktconsultatie ook duidelijke kaders en richtlijnen. Wijzigingsvoorstellen worden tijdens de intake beoordeeld op deze principes. De lijst met architectuurprincipes wordt regelmatig geactualiseerd en vastgesteld.
- **Gegevenslandschap:** Inzicht in het gegevenslandschap is belangrijk voor de kwaliteit van onze informatievoorziening. Welke gegevenssets zijn er, wie is daarvoor verantwoordelijk, welke applicaties maken er gebruik van, zijn enkele van de eigenschappen die moeten worden vastgelegd.
- **Applicatielandschap**: Van applicaties worden in TopDesk andere eigenschappen vastgelegd dan in het gegevenslandschap, zoals de namen van de leveranciers, functioneel beheerders en de eigenaar (manager). Daarnaast worden alle in gebruik zijnde applicatiemodules geadministreerd, alsmede de applicatietyperingen.
- **Architectuur koppelingen en integraties**: In TopDesk worden de applicaties in kaart gebracht tezamen met de koppelingen. Integraties worden weergegeven door samenwerkende applicatiefuncties in te kaderen.

Veranderingen in het landschap worden geadministreerd op het moment dat wijzigingen en projecten worden afgerond. De projectleider heeft dan de oplevering geaccordeerd en het resultaat in beheer gegeven aan de organisatie. Het team Informatieadvies wordt hiervan op de hoogte gebracht, zodat de administratie kan worden bijgewerkt.

Applicatielandschap

In het kader van applicatierationalisatie werken we met een standaard applicatielijst met bijbehorende functionaliteiten. Bij het onderzoeken van een wens, zal deze lijst worden geraadpleegd. Alleen bij het ontbreken van noodzakelijke functionaliteiten zal er overgegaan worden tot aanschaf van een nieuwe applicatie of module. Tevens wordt er kritisch gekeken naar het huidige applicatielandschap, waarbij als blijkt dat bepaalde functionaliteiten niet meer nodig zijn, er wordt overgegaan op het opzeggen van modules, dan wel applicaties.

3.3.2 Portfolio I&A

Het portfolio I&A is er om alle wensen te prioriteren en in te plannen. Deze wensen sluiten aan op datgeen is afgesproken in het bestuursakkoord, de begroting, de sturingsfilosofie en toekomstvisie in combinatie met wensen ontstaan vanuit de afdelingen. Zo wordt voorkomen dat er te veel initiatieven tegelijkertijd worden ondernomen, waardoor er ruimte ontstaat om structurele oplossingen te kunnen bieden. Het geeft dus focus en de juiste richting om de informatiebehoefte in beeld te krijgen en te vertalen naar geschikte oplossingen.

3.2.4.1 Strategische sturing

Proces

Tweemaal per jaar wordt gewerkt aan de strategische planning van I&A projecten (in het kort strategische planning). De eerste keer bij het vormen van het beleidskader en de tweede keer bij het opstellen van de begroting. De strategische planning beschrijft aan welke projecten wordt gewerkt voor het daaropvolgende jaar, met een doorkijk naar het tweede en derde jaar. Om een realistische planning af te geven, is het van belang om te weten wat de wens ongeveer inhoudt. Om die reden worden projecten alleen opgenomen op de strategische planning als hier een goedgekeurde projectstartnotitie aan ten grondslag ligt. Een voorwaarde voor het kunnen maken van deze strategische planning is dat afdeling I&A tijdig wordt betrokken bij het opstellen van jaarplannen en visies, zodat we aan kunnen sluiten met onze expertise.

Bij het opstellen van de strategische planning wordt input gebruikt vanuit:

- Het huidige portfolio
- Applicatielandschap (andere versies en end-of-life) en contracten (einde contractperiodes, voldoen aan standaarden)
- (Landelijke) wet- en regelgeving
- (Landelijke) ontwikkelingen
- Het bestuursakkoord
- Het strategisch beleid voor informatievoorziening
- De begrotingen van het huidige jaar
- De jaarplannen van het huidige jaar
- Ontwikkelingen, problemen en actualiteiten binnen de afdelingen
- Ontwikkelingen van (huidige) leveranciers op het gebied van informatiemanagement
- Etc.

De informatieadviseurs nemen bovengenoemde documenten door en zijn op de hoogte van nieuwe ontwikkelingen. Samen met de manager van de afdeling maakt de informatie-adviseur een voorstel voor de I&A projecten die op de strategische planning worden opgenomen. Indien gewenst benaderen zij ook medewerkers om de laatste ontwikkelingen in de afdelingen te bespreken.

De input wordt vervolgens verwerkt in een eerste versie van de strategische planning, waarbij de grote projecten ook opgenomen worden in het beleidskader. De tweede (definitieve) versie van de strategische planning wordt opgenomen in de definitieve versie van de begroting en jaarplannen.

Door middel van deze cyclus hanteert I&A een integrale benadering en afstemming voor ophalen van de voorlopige wensen en bijbehorende financiële dekking en capaciteit. De benodigde capaciteit heeft niet alleen betrekking op de capaciteit van de afdeling I&A, maar ook van de overige afdelingen in de organisatie, zoals van superusers of (decentrale) functioneel beheerders.

Het integrale voorstel wordt gedeeld met alle managers en de directieleden in het derde kwartaal van het jaar. Managers en directieleden kunnen tijdens deze bijeenkomst wijzigingsvoorstellen doen. De strategische planning wordt vervolgens vastgesteld door het Directieteam.

Randvoorwaarden

- **Financiering** voor projecten, dubbele licenties of structurele lastenverhoging worden ingedekt vanuit de afdelingen. Indien binnen de afdelingen of I&A geen beschikbaar budget is, wordt het project opgenomen in het bestuursakkoord en de begroting
- **Binnen de afdelingen en binnen I&A is capaciteit** beschikbaar om het project uit te voeren, inclusief de oriëntatiefase, maar ook capaciteit voor borging na oplevering van het project
- We plannen de capaciteit van I&A op basis van urenschema's, waarbij rekening wordt gehouden met onvoorziene en urgente werkzaamheden
- De eerste **prioritering** vindt plaats op basis van een prioriteitenmatrix, welke is opgenomen in het advies- en projectensjabloon

Planning

Twee keer per jaar wordt aan de strategische planning gewerkt (in het geel in de onderstaande planning). De eerste keer bij het opstellen van het beleidskader (in maart en april) en de tweede keer bij het opstellen van de begroting (in juli en augustus). De eerste keer wordt de strategische planning in concept gemaakt. Bij de tweede ronde is voor ieder project op de strategische planning een projectstartnotitie en wordt het eerste jaar in tertialen gepland (donkerblauw in de onderstaande planning). Nadat de begroting en de bijbehorende jaarplanning zijn goedgekeurd wordt de strategische planning niet meer aangepast, tenzij hier formele besluitvorming over plaatsvindt.

Strategische planning	Jaar 0			Jaar 1			Jaar 2			Jaar 3			Jaar 4		
	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
Maart – April															
Juli – Augustus															
Maart – April															
Juli - Augustus															

3.2.4.2 Tactische sturing

Proces

De tactische planning wordt drie keer per jaar opgesteld, met als basis de strategische planning. Op basis van de tactische planning wordt daadwerkelijk capaciteit ingepland voor de aankomende 17 weken (tertiaal) met een doorkijk naar de resterende tertialen van de strategische planning. De ingeplande capaciteit komt vanuit de afdeling I&A, maar ook vanuit de afdelingen. Het is dus van belang dat de manager commitment geeft op de tactische planning, omdat zijn of haar medewerkers ook ingepland dienen te worden in deze periode.

Bij het opstellen van de tactische planning worden nieuwe inzichten en bijstellingen verwerkt, denk hierbij aan:

- Langere of kortere doorlooptijden van lopende projecten
- Hernieuwde inzichten en bijstellingen in de projectopdracht ten opzichte van de projectstartnotitie
- Bijstelling van benodigde capaciteit

Randvoorwaarden

- Een project komt pas op de planning als voor het project een projectopdracht is goedgekeurd door de betreffende manager / opdrachtgever.
- Als een manager geen capaciteit vrij kan maken op zijn of haar afdeling wordt het project niet ingepland en kan het worden ingediend bij de volgende cyclus (een tertiaal later).
- Bij het plannen wordt rekening gehouden met een uitloop in doorlooptijd van 20%.
- Bij het plannen van capaciteit wordt rekening gehouden met een onvoorziene inzet van 10%.

Planning

Drie keer per jaar wordt aan de tactische planning gewerkt (per tertiaal). Voor het opstellen van de tactische planning is een doorlooptijd van één maand gereserveerd. De tactische planning is een maand voordat de betreffende periode ingaat

gereed. De basis voor de tactische planning is de strategische planning met bijstellingen. Waarbij het eerste tertiaal een planning per week bevat. De overige tertialen hebben een tertiaalplanning.

Tactische planning	Jaar 0			Jaar 1			Jaar 2		
	1	2	3	1	2	3	1	2	3
November				Week planning					
Maart					Week planning				
Juli						Week planning			
November							Week planning		
Maart								Week planning	
Juli									Week planning

3.2.4.3 Operationele sturing

Proces

De operationele planning wordt iedere maand opgesteld, met als basis de tactische planning. Op basis van de operationele planning wordt daadwerkelijk capaciteit ingepland voor de aankomende 4 weken met een doorkijk naar de komende maanden. De ingeplande capaciteit komt vanuit de afdeling I&A, maar ook vanuit de betrokken afdelingen zelf. Het is dus van belang dat de manager commitment geeft op de operationele planning, omdat zijn of haar medewerkers ook ingepland dienen te worden in deze periode.

Bij het opstellen van de operationele planning worden nieuwe inzichten en bijstellingen verwerkt, denk hierbij aan:

- Langere of kortere doorlooptijden van lopende projecten
- Hernieuwde inzichten en bijstellingen in de projectopdracht ten opzichte van de projectstartnotitie
- Bijstelling van benodigde capaciteit
- Het verwerken van spoedgevallen, waardoor er verschuiving in beschikbare capaciteit plaatsvindt

Randvoorwaarden

- Een spoedgeval komt pas op de planning als uit de startnotitie blijkt dat er capaciteit en (financiële) middelen beschikbaar zijn
- Een spoedgeval komt pas op de planning als blijkt dat er geen andere mogelijkheden zijn na het opstellen van een korte scenarioschets
- De projectplanning volgt verder de mijlpaalfasering van projecten en eventuele uitloop is in overleg met opdrachtgever afgestemd
- De adviesplanning wordt afgestemd op basis van de standaard doorlooptijden van de onderzoeks- en inkoopfase

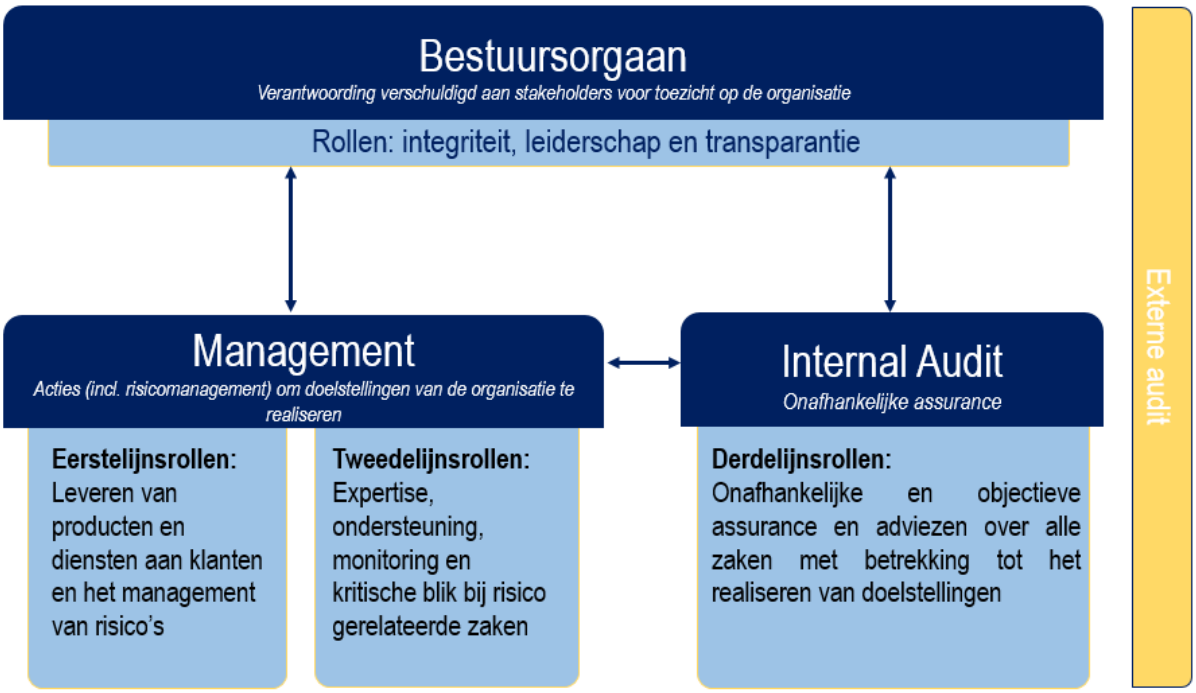
Planning

Een per maand wordt de maandplanning opgesteld. Voor het opstellen van de maandplanning is één week gereserveerd. De operationele planning is twee weken voordat de betreffende maand ingaat, gereed. De basis voor de operationele planning is de tactische planning met bijstellingen en incidenten.

Operationele Planning	Jaar 0		Jaar 1																										
	51	52	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Week 51																														
Week 1																														
Week 3																														
Week 5																														
Week 7																														
Week 9																														
Week 11																														
Week 13																														
Week 15																														
Week 17																														
Week 19																														

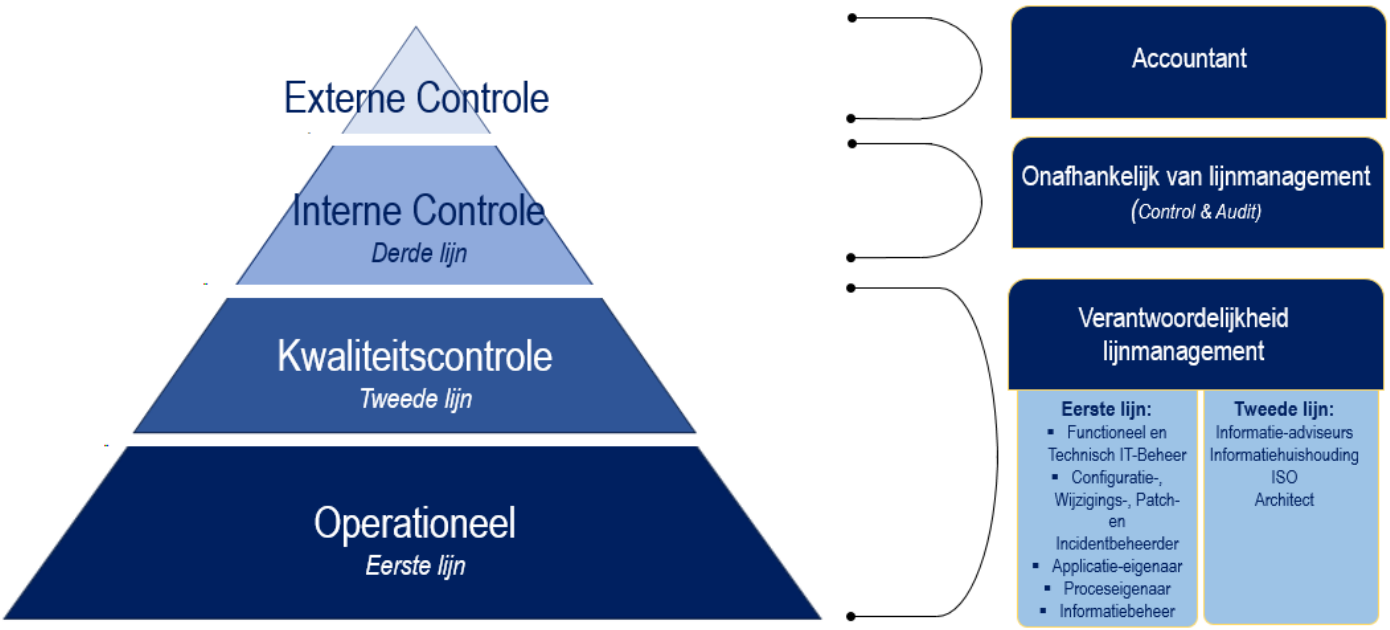
3.4 Mensen

3.4.1 Borging (3 Lines Model)



Het Directieteam heeft het 3 Lines Model (3LM) aangewezen als basis voor de inrichting van de interne beheersing en control-functie binnen onze organisatie. Het is een wezenlijk onderdeel van de sturingsfilosofie. Daarmee is het een solide uitgangspunt voor de inrichting van de informatiserings- en automatiseringsorganisatie, waarbij de taken worden verdeeld over de eerste, tweede en derde lijn en verantwoordelijkheden worden belegd op basis van PIJOFACH: de verantwoordelijkheid voor de informatievoorziening ligt primair bij managers van de afdelingen, waarbij de I staat voor Informatievoorziening.

Voor het optimaal kunnen laten functioneren van de gemeentelijke informatievoorziening zijn de rollen benodigd zoals opgenomen in de bijlage, die zowel door I&A, als medewerkers van afdelingen in de organisatie moeten worden ingevuld.



3.4.2 Eerste lijn

Afdeling I&A is niet (alleen) verantwoordelijk voor de informatievoorziening van de gemeente: vanuit het perspectief het 3LM model en de PIJOFACH taken (met de I van Informatie), ligt de verantwoordelijkheid voor de informatievoorziening primair bij managers van de afdelingen, waarbij de I staat voor Informatievoorziening.

Zowel centraal georganiseerd (binnen I&A), als decentraal gepositioneerd, zijn functioneel beheerders en superusers. Samen met informatiebeheerders, functioneel en technisch IT-beheer, configuratie-, wijzigings-, patch-, en incidentbeheer, applicatie-eigenaren en proceseigenaren vullen zij de informatiserings- en automatiseringsorganisatie van de eerste lijn en hebben daarmee de volgende verantwoordelijkheden:

A. Zijn primair verantwoordelijk voor het doorlopen van de fasen van informatisering en automatisering en daarmee een goede interne beheersing. De eerste lijn volgt de vastgestelde (ICT)processen en ziet toe op bewaking hierop.
B. Passen de door de 2e lijn ontwikkelde methoden en technieken toe. Voert periodieke controles uit en legt maandelijks verantwoording af op de (management)dashboards.

3.4.3 Tweede lijn

Informatie(huishouding)adviseurs en Information Security Officer zijn de tweede lijn en hebben daarmee de volgende verantwoordelijkheden:

A. Ondersteunen het verantwoordelijke management bij de PDCA van informatisering en automatisering.
B. Ontwikkelt systemen hiervoor met rapportages. Dit ter ondersteuning en advisering van de decentrale lijnmanager bij het bijsturen van de procesvoering en risicobeheersing, het uitvoeren van evaluaties en het afleggen van verantwoording.
C. Fungeert als een collectief van ‘architecten’ voor de vormgeving van de structuur, de systemen en de procedures die nodig zijn voor de inrichting en het doen functioneren van de strategische, tactische en operationele processen.

3.4.4 Derde lijn

De derde lijn is onafhankelijk gepositioneerd en voeren controle & audits over het opgezette systeem van de 2e lijn.

A. Voorziet de hoogste leiding van aanvullende zekerheid over de kwaliteit van sturing en beheersing van processen en risico's op het concernniveau.
B. Is niet verantwoordelijk voor de kwaliteit van het in control zijn van de organisatie, maar is wel verantwoordelijk om inconsistenties in de opzet en het bestaan van de control frameworks te analyseren en zichtbaar te maken. Dit framework hebben zij eerst opgezet, om vervolgens te toetsen en te analyseren.

3.4.5 Rol en positionering afdeling I&A

Informatisering & Automatisering heeft te maken met klanten op verschillende niveaus binnen de organisatie, maar opereert zelf binnen de eerste lijn.

A) Directieteam

Het Directieteam wordt door I&A geïnformeerd over compliancy ten behoeve van verschillende normenkaders. Denk hierbij aan de BIO, NIS2, ENSIA-verantwoording. Tevens leggen zij verantwoording af aan het DT ten behoeve van het uitvoeren van de vastgestelde beleidsstukken.

B) Managementteam

Het Managementteam wordt geïnformeerd over nieuwe ontwikkelingen, door te voeren maatregelen en zij worden gefaciliteerd door middel van verschillende toepassingen. Het gaat hierbij om advies, beheer en doorontwikkeling.

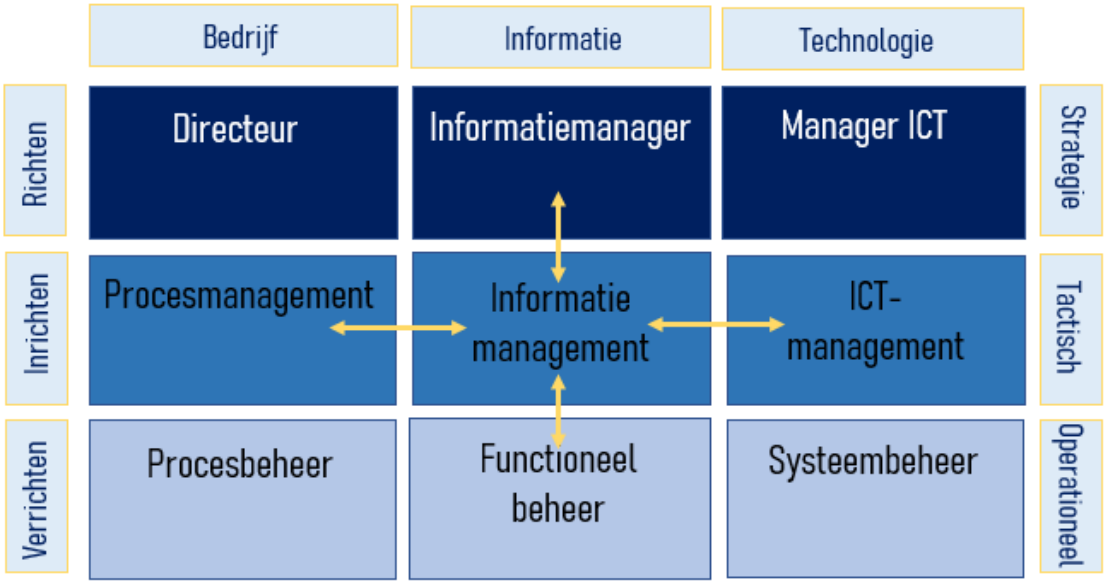
C) Medewerkers

Medewerkers worden gefaciliteerd door middel van een beveiligde werkplek (hard- en software).

D) Control en Audit

Derdelijns adviseurs worden voorzien van benodigde informatie ten behoeve van control en audits, maar ook van bewijslast ten aanzien van beheersmaatregelen.

Om de positionering van I&A vanuit taken en verantwoordelijkheden in de organisatie te kunnen duiden, maken we wederom gebruik van het negen-vlaksmodel van Maes; een veelvuldig gebruikt model op het gebied van informatiemanagement. Het model onderscheidt op de verticale as drie besturingsdomeinen:



Informatiemanagement is namens de gebruikersorganisatie verantwoordelijk voor de aanwezige informatievoorziening en daarbij ingezette informatiesystemen.

Op strategisch niveau is informatiemanagement verantwoordelijk voor het opstellen van de informatiestrategie, voor het opstellen van de strategie voor de informatievoorzieningsorganisatie en voor de informatiecoördinatie (het coördineren en

afstemmen tussen deze strategieën en andere beleidsplannen). Daarnaast is informatiemanagement verantwoordelijk voor een aantal sturende processen:

- **Financieel management**: Het bewaken van de kosten van de informatievoorziening
- **Planning & Control**: Aansturing van de tijds- en capaciteitsaspecten van de informatievoorziening
- **Behoefte management:** Bewaken van de kwaliteit van de informatievoorziening, en vertalen van ontwikkelingen in de behoeften vanuit werk- en bedrijfsprocessen in aanpassingen aan de informatievoorziening
- **Contractmanagement:** Het maken van goede afspraken met de ICT-leverancier en de opvolging hiervan

Ten slotte voert informatiemanagement vaak regie over projecten om te zorgen dat nieuwe ontwikkelingen aansluiten op doelstellingen voor de lange termijn.

Operationele taken als het ondersteunen van gebruikers, het specificeren van wijzigingen, het specificeren van nieuwe functionaliteiten, het testen van wijzigingen worden meestal uitgevoerd door functioneel beheerders of key-users.

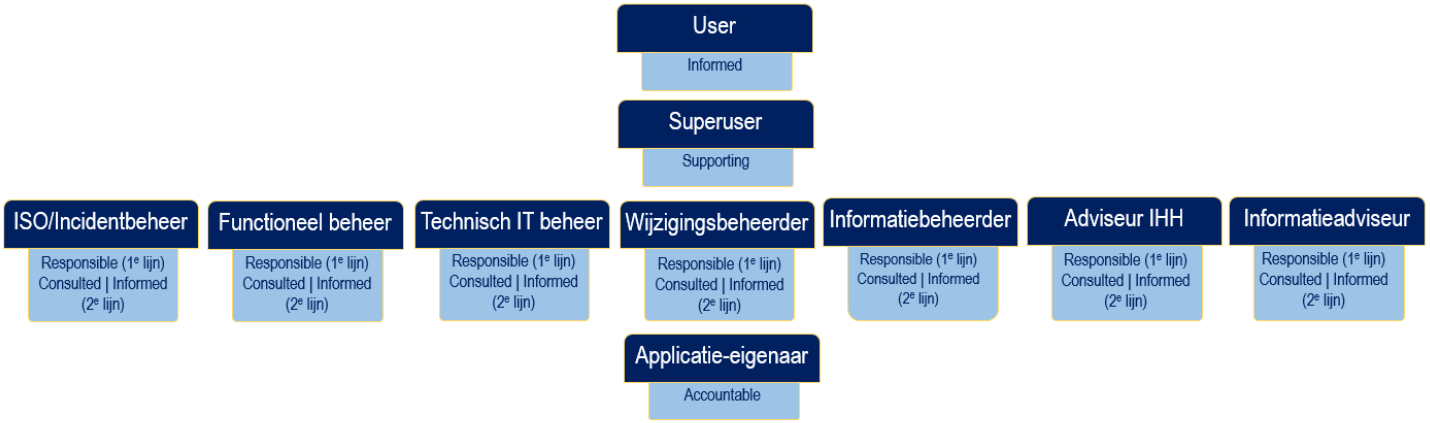
Technisch applicatiebeheer en andere ICT-processen vallen niet onder de gebruikersorganisatie maar onder de ICT-leverancier. Informatiemanagement en functioneel beheer verstrekken hieraan opdrachten, maar informatiemanagement is niet hiërarchisch verantwoordelijk voor dergelijke afdelingen.

4 Bijlagen

De bijlagen gaan in op tactische beleidskeuzes omtrent de informatieorganisatie (rollen, taken en verantwoordelijkheden), de inrichting van de 4 ICT-processen (wijzigen, patchen, configureren en incidenten) en inrichtingsprincipes omtrent automatisering.

4.1 Rollen, taken en verantwoordelijkheden

Ten behoeve van de informatieorganisatie zijn hier rollen uitgeschreven met bepaalde taken en verantwoordelijkheden.



4.1.1 User

Samenvatting van de rol

Een user is een medewerker uit de eerste lijn, die werkt met vakspecifieke tot organisatie brede (kantoor)applicaties en is bekend met de geautomatiseerde informatievoorziening *(informatie, applicaties, ICT-infrastructuur en dienstverleningsprocessen: informatievoorziening dat wordt uitgevoerd met behulp van programmatuur (software) en apparatuur (hardware).* Een user gebruikt de informatievoorziening zoals is voorgeschreven in beleid, processen en werkinstructies en zorgt ervoor dat zijn of haar kennis up-to-date is met betrekking tot (het gebruik van) de gemeentelijke en geautomatiseerde informatievoorziening.

Taken en verantwoordelijkheden

- In hoofdlijnen:
  - Verantwoordelijk voor het volgen van beleid, processen en werkinstructies met betrekking tot de gemeentelijke informatievoorziening
  - Verantwoordelijk voor het volgen van het Protocol Internet, E-mail en Social Media 2021 (binnenkort hernoemd naar Ambtelijke Gedragscode)
  - Verantwoordelijk voor het op peil houden van eigen kennis met betrekking tot applicaties, archiveren, informatiebeveiliging en privacy
  - Verantwoordelijk voor het op peil houden van eigen kennis met betrekking tot algemene digitale vaardigheden, gebruik en digitaal niveau, onder andere in het kader van integriteit
  - Behouden van beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens binnen de informatievoorziening

4.1.2 Superuser

Samenvatting van de rol

Een superuser is een medewerker uit de eerste lijn, die direct betrokken is en veel kennis heeft van de geautomatiseerde informatievoorziening *(informatie, applicaties, ICT-infrastructuur en dienstverleningsprocessen: informatievoorziening dat wordt uitgevoerd met behulp van programmatuur (software) en apparatuur (hardware).* De superuser vertegenwoordigt én ondersteunt de gebruikersorganisatie bij het gebruik van de geautomatiseerde informatievoorziening en zorgt voor actuele werkinstructies van de applicaties. De superuser fungeert als schakelpunt naar de (de)centraal georganiseerde functioneel beheerder. Elke applicatie heeft twee superusers en organisatie brede kernapplicaties, zoals een documentmanagementsysteem, zaaksysteem en financieel systeem, kent één superuser per afdeling.

Taken en Verantwoordelijkheden

- In hoofdlijnen:
  - Ondersteunen, instrueren en faciliteren gebruikers
  - Verzorgen van beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens
  - Het volgen van de 4 ICT-processen (wijzigen, patchen, incidenten en configureren), waaronder het functioneel testen van de applicatie(s) bij wijzigingen
  - Ophalen wensen, verzoeken en eisen vanuit de werkvloer en dient deze in bij de i-Adviseur of functioneel beheer.

- Borgen van benodigde kennis over geautomatiseerde informatievoorziening:
  - Beschrijven en onderhouden van applicatie gebonden werkinstructies
  - Ondersteunen van collega's met het werken binnen de geautomatiseerde informatievoorziening, aan de hand van werkinstructies en testscripts.
  - Signaleren van afwijkingen in de geautomatiseerde informatievoorziening aan de applicatie-eigenaar en (de/centraal georganiseerd) functioneel beheer.
  - Proactief verbeteracties signaleren in de geautomatiseerde informatievoorziening.

- Specificeren van gewenste veranderingen in de geautomatiseerde informatievoorziening:
  - Specificeren van de gewenste verandering in de geautomatiseerde informatievoorziening.
  - Specificeren van de functionele wens en de impact van de wijzigingen op het proces bepalen.
  - Schakelpunt tussen gebruikers en eventueel centraal georganiseerde functioneel beheerders en informatieadviseurs.

- Ondersteunen en faciliteren van gebruikers bij het correct en efficiënt gebruik van de bijbehorende geautomatiseerde informatievoorziening:
  - Geven workshops of trainingen aan gebruikers bij veranderingen.
  - Bij gebruikers meekijken bij de uitvoering van het werk en beantwoorden van vragen
  - Organiseren van gebruikers-overleggen
  - Signaleren en melden van onjuist gebruik
  - Informeren van de gebruikersorganisatie bij tekortkomingen in de geautomatiseerde informatievoorziening.
  - Informeren van de gebruikers over handige weetjes, nieuwe releases en ontwikkelingen
  - Evalueren van de ingebruikname en wijzigingen volgens PDCA

- Verzorgen van beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens in de geautomatiseerde informatievoorziening:
  - Toegang tot de geautomatiseerde informatievoorziening.
  - Autorisatiestructuren in de geautomatiseerde informatievoorziening.
  - Inhoudelijke controle op de gegevenskwaliteit.
  - Bewaken of het gebruik van de gegevens gebeurt binnen de vastgestelde kaders.
  - Bewaken van ongeoorloofd gebruik van gegevens.
  - Ondersteunen bij het beheren van data en informatie, conform de levenscyclus van informatie. Denk hierbij aan de archiefwet. Op het beheren van de data en informatie conform de levenscyclus van informatie

- Het functioneel testen van de geautomatiseerde informatievoorziening na het doorvoeren van veranderingen:
  - Maken en onderhouden van testscripts.
  - Uitvoeren van functionele testen.
  - Het accepteren van veranderingen in de geautomatiseerde informatievoorziening.

4.1.3 Configuratiebeheerder

Samenvatting van de rol

De Configuratiebeheerder is verantwoordelijk voor het proces om de configuratie-items actueel en volledig te houden. De configuratiebeheerder ondersteunt en adviseert hierin de superuser, functioneel en technisch beheerder en eigenaar van de configuratie-items.

Taken en Verantwoordelijkheden

- In hoofdlijnen:
  - Verantwoordelijk voor het bijhouden van configuratie-items van het IT-systeem.
  - Het toepassen van de PDCA-cyclus voor configuratiemanagement (plannen, doen, controleren, evalueren en aanpassen, daar waar nodig)
  - Schakelpunt tussen applicatie-eigenaar, wijzigingsbeheerder, incidentbeheerder, patchbeheerder, functioneel en technisch beheer en superusers wat betreft het up-to-date houden van het configuratiemanagementdatabase

- Verantwoordelijk voor beheer van de configuratiemanagementdatabase (CMDB):
  - Aanpassingen doorvoeren in het CMDB
  - Bewaken, analyseren en evalueren lopende zaken in CMDB.
  - Opstellen rapportages volgens de PDCA-cyclus

- Ondersteunen bij het inrichten van beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens in de configuratiemanagementdatabase:
  - CI's en specifieke kenmerken zijn up-to-date.
  - De gegevens zijn uniek, volledig en juist in de CMDB opgenomen.
  - Inhoudelijke controle op de gegevenskwaliteit.
  - Bewaken of het gebruik van de gegevens gebeurt binnen de vastgestelde kaders.
  - Bewaken van ongeoorloofd gebruik van gegevens.

- Regie, coördinatie, testen, evalueren en verbeteren van het configuratiemanagementproces:
  - Houdt ontwikkelingen rondom het proces in de gaten.
  - Adviseert, beoordeelt en controleert nieuwe toepassingen in het proces.
  - Coördineert grote veranderingen in het configuratiemanagementproces.

- Verantwoordelijk voor de benodigde werkinstructies, procedures en processen:
  - Verantwoordelijk voor beschikbaar stellen van actuele werkinstructies, procedures en processen ten behoeve van het gebruik van het configuratiemanagementproces.
  - Verantwoordelijk voor het gebruik van deze werkinstructies, procedures en processen binnen de gemeente.
  - Verantwoordelijk voor uitleg rondom het configuratiemanagementproces en het CMDB aan functioneel beheerders en superusers.

4.1.4 Wijzigingsbeheerder

Samenvatting van de rol

De Wijzigingsbeheerder is verantwoordelijk voor het beheer van de levenscyclus van alle (spoed)wijzigingen, met als primaire verantwoordelijkheid het mogelijk maken van gunstige (spoed)wijzigingen met minimale verstoring van het bedrijf.

Taken en Verantwoordelijkheden

- In hoofdlijnen:
  - Het beheren van organisatorische risico's, waarmee de impact van downtime op de organisatie is geminimaliseerd.
  - Is de spil voor goedkeuring en coördinatie van (spoed)wijzigingen en draagt daar verantwoordelijkheid voor, waardoor risico's, voordelen en afhankelijkheden voor elke (spoed)wijziging goed worden begrepen.
  - Het toepassen van de PDCA-cyclus voor wijzigingsmanagement (proces volgen, proces evalueren, rapporteren en aanpassen waar nodig).
  - Verantwoordelijk voor een verhoogde snelheid van het vrijgeven van (spoed)wijzigingen in de productie en zorgen dat deze veilig kunnen plaatsvinden.
  - Signaleren, en aandragen van verbeteringen voor het verminderen van problemen na een release.
  - Signaleren en aandragen van verbeteringen voor minder conflicten, fouten en rollbacks na wijzigingen.

- Verantwoordelijk voor bijeenroepen en voorzitten (Spoed) Wijzigingsadviescomité:
  - Signaleert tijdig (spoed)wijzigingen.
  - Roept vergaderingen bijeen en zit deze voor.
  - Zorgt ervoor dat informatie die besproken wordt in deze groepen volledig is, zodat weloverwogen beslissingen kunnen worden genomen op basis van deze gegevens.
  - Weet prioritering aan te brengen in de wijzigingen.
  - Keurt (spoed)wijzigingen goed of af.

- Verantwoordelijk voor beheer van (spoed)wijzigingsverzoeken:
  - Categoriseren van (spoed)wijzigingsverzoeken
  - Beoordelen en vastleggen van (spoed)wijzigingsverzoeken
  - Prioriteren van wijzigingen op basis van bedrijfsdoelen.
  - Beheren van de transitie van (spoed)wijzigingen van ontwikkelaars/leveranciers naar productie.
  - Accepteren of afwijzen van (spoed)wijzigingsverzoeken.

- Coördineren van het bouwen, testen en implementeren van (spoed)wijzigingen:
  - Stelt een wijzigingsplan op.
  - Coördineert en ondersteunt medewerkers bij het maken van testscripts.
  - Coördineert en ondersteunt medewerkers bij het doorlopen van testscripts.
  - Coördineert de implementatie van een (spoed)wijziging.
  - Maakt en verspreidt het (spoed)wijzigingsschema.

- Verantwoordelijk voor het bijhouden van benodigde documentatie:
  - Verantwoordelijk voor het bijhouden van alle documentatie over (spoed)wijzigingen (beleidsregels, procedures, sjablonen, enz.)
  - Produceren en beschikbaar stellen/verspreiden van managementrapporten in het kader van risicomanagement (ISMS)

- Regie, coördinatie, testen, evalueren en verbeteren van het patch- en wijzigingsmanagementproces:
  - Houdt ontwikkelingen rondom het proces in de gaten.
  - Beoordeelt en controleert nieuwe toepassingen in het proces.
  - Stemt met de verantwoordelijke en procesbeheerder het plan af.
  - Coördineert grote veranderingen in het wijzigingsmanagementproces.

- Communicatie beheerders IT-processen:
  - Wijzigingsbeheerder ontvangt patch- en wijzigingenverzoeken vanuit functioneel en technisch beheerders en (spoed)wijzigingen naar aanleiding van incidenten vanuit incidentenbeheerder en voert deze door volgens het patch- en wijzigingsmanagementproces.

- De wijzigingsbeheerder geeft de specifieke (spoed)wijzigingen door aan de configuratiebeheerder voor verwerking van het CMDB.

- Verantwoordelijk voor de benodigde werkinstructies, procedures en processen:
  - Verantwoordelijk voor beschikbaar stellen van actuele werkinstructies, procedures en processen ten behoeve van het gebruik van het proces en beoordeelt deze.
  - Verantwoordelijk voor het gebruik van deze werkinstructies, procedures en processen binnen de gemeente.

4.1.5 Incidentbeheerder (Information Security Officer)

Samenvatting van de rol

De rol van Incidentbeheerder is verantwoordelijk voor het beheer van incidenten en de organisatie na een incident zo snel mogelijk weer normaal te laten functioneren, met zo min mogelijk negatieve effecten op de core business van de organisatie.

Taken en Verantwoordelijkheden

- In hoofdlijnen:
  - Ontwikkelen en implementeren van specifiek informatiebeveiligingsbeleid.
  - Risicoanalyse- en beoordeling van technische systemen en infrastructuur.
  - Adviseren over informatiebeveiligingsvraagstukken.
  - Verantwoordelijk voor de overbrugging van de communicatiekloof tussen eindgebruikers, superusers en ICT-medewerkers.
  - Verantwoordelijk voor het definiëren en herkennen van een incident.
  - Verantwoordelijk voor de prioritering en doorzetten van een incident.
  - Het beheren van organisatorische risico's, waarmee de impact van downtime op de organisatie is geminimaliseerd.

- Verantwoordelijk voor risicoanalyse- en beoordeling van informatiebeveiliging op applicaties en infrastructuur:
  - Identificeren van potentiële kwetsbaarheden en bedreigingen in ICT-systemen.
  - Uitvoeren van penetratietests en vulnerability assessments om beveiligingsrisico's te identificeren.
  - Prioriteren van mitigerende maatregelen op basis van risicoanalyseresultaten en bedrijfsdoelstellingen.

- Verantwoordelijk voor het uitvoeringsplan en coördinatie van incidenten:
  - Incidenten vastleggen.
  - Incidenten classificeren.
  - Incidenten prioriteren.
  - Onderzoek en diagnose van incident uitvoeren.
  - Incidenten managen, oplossen (i.s.m. functioneel en technisch ICT beheer) en afsluiten.
  - Opzetten van een gestructureerd incidentresponsplan voor het omgaan met beveiligingsincidenten.
  - Coördineren van trainingen en oefeningen voor het incidentrespons- en informatiebeveiligingsteam.

- Coördineren van het incidentenproces:
  - Volgt het incidentenproces.
  - Coördineert medewerkers bij het vastleggen, classificeren, prioriteren, onderzoeken en oplossen van incidenten.

- Verantwoordelijk voor het bijhouden van benodigde documentatie:
  - Configureren van een realistische SLA-definitie, om aan de verplichtingen van (interne) klanten te voldoen.
  - Verantwoordelijk voor het bijhouden van alle documentatie over incidenten (beleidsregels, procedures, sjablonen, enz.)
  - Produceren en beschikbaar stellen/verspreiden van managementrapporten in het kader van risicomanagement in de daarvoor bestemde applicatie met betrekking tot informatiebeveiliging

- Regie, coördinatie, testen, evalueren en verbeteren van het incidentmanagementproces:
  - Houdt ontwikkelingen rondom het proces in de gaten.
  - Beoordeelt en controleert nieuwe toepassingen in het proces.
  - Stemt met de verantwoordelijke en procesbeheerder het plan af.
  - Coördineert grote veranderingen in het incidentmanagementproces.
  - Evalueert incidenten.

- Communicatie beheerders ICT-processen:
  - Incidentbeheerder ontvangt meldingen vanuit (super)users, functioneel en/of technisch beheerders, applicatie-eigenaren, wijzigingsbeheerder en vanuit de servicedesk en voert deze door volgens het incidentmanagementproces.
  - De incidentbeheerder geeft de specifiek benodigde wijzigingen door aan de wijzigingsbeheerder.

- Verantwoordelijk voor de benodigde werkinstructies, procedures en processen:
    - Verantwoordelijk voor beschikbaar stellen van actuele werkinstructies, procedures en processen ten behoeve van het gebruik van het proces en beoordeelt deze.
    - Verantwoordelijk voor het gebruik van deze werkinstructies, procedures en processen binnen de gemeente

4.1.6 Informatieadviseur

Samenvatting van de rol

De informatieadviseur is verantwoordelijk voor het analyseren en ontwerpen van de ICT-architectuur, met als doel hoogwaardige oplossingen voor het bedrijfsportfolio, applicaties, systemen, infrastructuur of gehele onderneming te kunnen bieden. De rol staat aan de basis van de realisatie van ICT-projecten. De informatieadviseur geeft (on)gevraagd advies en vertaald wensen naar werkbare oplossingen die bijdragen aan bedrijfsdoelstellingen en wet- en regelgeving. Overall dienen de rollen de volgende taken te bevatten:

Taken en Verantwoordelijkheden

- In hoofdlijnen:
  - Schakelpunt tussen de afdelingen en de ICT-dienstverlening
  - Gebruikersbehoeften analyseren en definiëren.
  - Productieselectiecriteria opstellen voor de inkoop van nieuwe software- en/of hardwarecomponenten.
  - Financiële en ICT-concepten beoordelen/controleren in het kader van nieuwe modules of applicaties, volgens vastgestelde standaarden.
  - Verantwoordelijk voor het stroomlijnen van bestaande architecturen.

- Proactief adviseren en ondersteunen in het architectenbeheer van het ICT-landschap:
  - Duidelijk krijgen van het precieze doel van een wens of verzoek.
  - Adviseren bij het selecteren van een oplossingsrichting van een wens.
  - Functioneel ontwerp maken van de oplossingsrichting.
  - Toetsen of de wens of het verzoek past binnen de applicatie en het applicatielandschap.
  - Bepalen van de impact van de oplossingsrichting op de geautomatiseerde informatievoorziening.

- Verantwoordelijk voor vertaling van trends en ontwikkelingen:
  - Vertalen van trends en ontwikkelingen binnen informatisering en automatisering.
  - Beoordelen trends en ontwikkelingen op relevantie.
  - Vertalen van trends en ontwikkelingen naar een visie, beleid en (verbeter)acties
  - Analyseren impact wetswijzigingen op gebied van beleid, systemen en processen en adviseert het management hierover.

- Verantwoordelijk voor het overzicht van het ICT-landschap, ontwikkeling en upgraden t.b.v. ICT-architectuur:
  - Alle in contract beheerde ICT-systemen zijn gemanaged en onderhouden om de bedrijfsdoelstellingen te behalen.
  - Bedrijfsdoelstellingen en potentieel in kaart gebracht door middel van ICT-infrastructuur.
  - Het aansluiten van de strategische bedrijfsdoelstellingen en tactische vraagstukken op de ICT.
  - Ontwerpen van systemen die in lijn zijn met operationele resources en de digitale infrastructuur van de organisatie.

- Verantwoordelijk voor het bijhouden van benodigde documentatie:
  - Verantwoordelijk voor het bijhouden van beleid(sregels) over informatisering en automatisering

4.1.7 Adviseur Informatiehuishouding

Samenvatting van de rol

De adviseur informatiehuishouding is verantwoordelijk voor een toekomstbestendige informatiehuishouding en doet dat door wet- en regelgeving te vertalen naar de praktijk. De adviseur informatiehuishouding geeft (on)gevraagd advies en vertaald wensen, bedrijfsdoelstellingen en wet- en regelgeving naar werkbare oplossingen die bijdragen aan een optimale informatiehuishouding. Overall dienen de rollen de volgende taken te bevatten:

Taken en Verantwoordelijkheden

- In hoofdlijnen:
  - Verantwoordelijk voor implementatie van (nieuwe) wet- en regelgeving en het in kaart brengen van de verschillen tussen de huidige en gewenste situatie en hoe daar gefaseerd te geraken.
  - Adviseert over en implementeert beleid omtrent informatiehuishouding.
  - Verantwoordelijk voor informatiebewustwording onder collega's en het kenbaar maken van de noodzaak van een goede informatiehuishouding.
  - Op strategisch en tactisch niveau hét aanspreekpunt voor omgaan met informatie conform wet- en regelgeving.

- Verantwoordelijk voor vertaling van trends en ontwikkelingen naar visie, beleid, procedures en advies:
  - Vertalen van trends en ontwikkelingen naar een visie, beleid en (verbeter)acties t.b.v. informatiehuishouding.
  - Analyseren impact wetswijzigingen op gebied van beleid, systemen en processen en adviseert het management hierover.

- Verantwoordelijk voor het centrale proces rondom Woo-verzoeken
  - Verantwoordelijk voor het inrichten en verbeteren van het centrale proces van Woo-verzoeken.
  - Coördineren van de afhandeling van binnenkomende Woo-verzoeken in de organisatie.
  - Fungeren als Woo-contactpersoon voor burgers en bedrijven bij het indienen van Woo-verzoeken.
  - Draagt zorgt voor centrale rapportage omtrent Woo-verzoeken inclusief analyse en verbetervoorstellen.

- Draagt zorg voor duurzaam toegankelijk maken en houden van informatie en adviseert hierover:
  - Brengt informatie binnen processen in kaart en adviseert over duurzaam toegankelijk maken van deze informatie.
  - Signaleren als er binnen afdelingen een archiveringsvraagstuk speelt.
  - Stel het informatiebeheerplan op inclusief advies over het duurzaam toegankelijk maken
  - Draagt zorg voor implementatie en borging van het advies voor het duurzaam toegankelijk maken van informatie
  - Stelt het metadatagegevensschema op, beheert deze en voert deze door
  - Onderzoekt de (on)mogelijkheden van het aansluiten op een e-depot per werkproces en voert de aanpassingen door

- Borgen kennis informatiehuishouding:
  - Ontwikkelen en verzorgen van trainingen op het gebied van informatiehuishouding.
  - Contactpersoon van West Brabants Archief en Interbestuurlijk Toezicht Informatie- en Archiefbeheer

4.1.8 Informatiebeheerder

Samenvatting van de rol

De informatiebeheerder is verantwoordelijk voor het beheren van documenten en informatie op een gestructureerde en overzichtelijke manier en dat deze op de juiste wijze worden opgeslagen en georganiseerd. Dossiers worden op de juiste manier beheerd en gearchiveerd en hierover worden rapportages opgesteld. Overall dient de rol de volgende taken te bevatten:

Taken en Verantwoordelijkheden

- In hoofdlijnen:
  - Verantwoordelijk voor het registreren en distribueren van (geautomatiseerde) documenten.
  - Verantwoordelijk voor het beheren van de selectielijst van alle archiefbescheiden in de organisatie.
  - Verantwoordelijk voor de overdracht van informatie naar de archiefbewaarplaats.
  - Verantwoordelijk voor inhoudelijke ondersteuning voor zaakgericht werken
  - Archiveren van informatie volgens vastgestelde procedures en richtlijnen.
  - Bijdragen aan continue verbeteren van het informatiebeheerproces.
  - Verantwoordelijk voor het beheer van de fysieke archiefruimte.

- Verantwoordelijk voor het registreren en distribueren van documenten waar dit niet geautomatiseerd is:
  - Digitaliseren en registreren van inkomende, uitgaande en interne documenten.
  - Het distribueren van (digitale) post.
  - Draagt zorg voor actief openbaar maken van informatie, volgens vastgestelde procedures en regelgeving.
  - Monitoren en sturen op tijdig en juiste afhandeling van de binnenkomende documenten.

- Verantwoordelijk voor het beheren van de selectielijst van alle archiefbescheiden in de organisatie:
  - Draagt zorg voor het actueel houden van de selectielijst van archiefbescheiden in de organisatie.
  - Fungeert als eerste aanspreekpunt voor medewerkers met vragen over informatiebeheer.
  - Voert de selectie op bewaren en vernietigingen en/of controleert de geautomatiseerde selectie.
  - Voert de vernietiging, digitale vervanging, bruikleen e.d. uit. eventueel in samenwerking met de afdelingen of de functioneel beheerders.

- Verantwoordelijk voor de overdracht van informatie naar de archiefbewaarplaats:
  - Overdragen van te bewaren informatie (digitaal en fysiek) naar het West Brabants Archief en e-depot
  - Produceren en naleven vernietigingslijsten

4.1.9 Applicatie-eigenaar

Samenvatting van de rol

De Applicatie-eigenaar, lijnmanager, is verantwoordelijk voor zowel de functionaliteit, alsmede de gegevens, als het gebruik van de applicatie en de gegevens die in de applicatie worden opgeslagen. De Applicatie-eigenaar is verantwoordelijk voor de wijzigingen in de functionaliteit van de applicatie, alsmede de vernieuwing van de applicatie. Elke applicatie heeft een eigenaar. Als Applicatie-eigenaar ben je ook verantwoordelijk voor contract- en leveranciersmanagement, tenzij deze taak gedelegeerd is aan afdeling Informatisering & Automatisering. Tevens is de eigenaar verantwoordelijk voor de eventuele kosten van een update, incident, vervanging, toevoeging of aanpassing van bestaande functionaliteiten.

Taken en Verantwoordelijkheden

- In hoofdlijnen:
  - Verantwoordelijk voor de applicatie en dat de gegevensverwerking de gehele levenscyclus wordt ondersteund, conform wensen en eisen van proceseigenaar.
  - Verantwoordelijk voor de naleving van wet- en regelgeving (aangevuld met relevante normenkaders).
  - Verantwoordelijk voor beschikbaarheid, beveiliging, naleving, onderhoud, back-up en ondersteuning van het geautomatiseerde en de bijbehorende kosten hiervoor.
  - Verantwoordelijk voor het gebruikersbeheer.
  - Het validatieplan, gebruikersvereisten, applicatieconformiteitsbeoordelingen, validatierapporten- en samenvattingen formeel goedkeuren.
  - Verantwoordelijk voor beheer op de softwaretoepassingen binnen de organisatie.
  - Verantwoordelijk voor beschikbaarheid en integriteit van de gegevens.
  - Verantwoordelijk voor toegang tot applicatie.

- Verantwoordelijk voor beheer en beveiligen van één of meerdere applicatie(s):
  - Is eindverantwoordelijk voor het in bedrijf houden van de applicatie(s).
  - Laat zich adviseren over applicatie(gebruik) en knelpunten.
  - Verantwoordelijk voor juiste beheer programmaversies, daarbij behorende documentatie en voor de installatie van nieuwe applicatiesoftware

- Verantwoordelijk voor het herstellen, aanpassen en verbeteren van de applicatie:
  - (Escalatie)contactpersoon voor IT-leveranciers.
  - Verantwoordelijk voor het laten uitwerken, vastleggen en documenteren van de wijzigingen in TopDesk en het CMDB.
  - Verantwoordelijk voor het laten uitvoeren van wijzigingen in functionaliteiten.
  - Verantwoordelijk voor het laten beschrijven en onderhouden van testscripts.
  - Verantwoordelijk voor het laten testen van de applicatie na doorvoeren van een aanpassing.

- Beoordelen en besluiten over advisering en ondersteuning in het functionaliteitenbeheer van een applicatie:
  - Beoordelen en besluiten over een oplossingsrichting van een wens.
  - Verantwoordelijk voor een functioneel ontwerp van een oplossingsrichting.
  - Verantwoordelijk voor het laten bepalen wat de impact is van de oplossingsrichting op de geautomatiseerde informatievoorziening.

- Verantwoordelijk voor de benodigde werkinstructies, procedures en processen:
  - Verantwoordelijk voor beschikbaar stellen van actuele werkinstructies, procedures en processen ten behoeve van het gebruik van de applicatie(s) en beoordeelt deze.
  - Verantwoordelijk voor het gebruik van deze werkinstructies, procedures en processen binnen de gemeente.

4.1.10 Functioneel beheerder

Samenvatting van de rol

De Functioneel Beheerder is een rol die zich met name richt op het adviseren, faciliteren en ondersteunen van de procesbeheerders en het doorvoeren van aanpassingen in een applicatie. Daarmee ontwerpt en ontwikkelt de functioneel beheerder de ICT-architectuur, met als doel hoogwaardige oplossingen voor het bedrijfsportfolio, applicaties, systemen of infrastructuur. Het niveau van de functie verschilt naar aanleiding van de complexiteit van de werkzaamheden. Afhankelijk van de applicatie en de complexiteit kan de rol centraal en decentraal georganiseerd worden. Alle applicaties hebben een functioneel beheerder.

Taken en Verantwoordelijkheden

- In hoofdlijnen:
  - Beheren, beveiligen en bedienen van één of meerdere applicaties.
  - Verhelpen van storingen en het bieden van gebruikersondersteuning.
  - Mede opzetten en beheren van werkinstructies.
  - Installeren en testen van applicatiesoftware.

- Beheren, beveiligen en bedienen van één of meerdere applicatie(s):
  - Is verantwoordelijk voor het in bedrijf houden van de applicatie(s) en daarmede ook om de juiste patches en/of software-updates door te voeren.
  - Bewaakt applicatie(gebruik) en signaleert vroegtijdig knelpunten.
  - Beheert programmaversies en daarbij behorende documentatie.
  - Installeert in samenwerking met de leverancier nieuwe applicatiesoftware.

- Het herstellen, aanpassen en verbeteren van de applicatie:
  - Contactpersoon voor IT-leveranciers.
  - Analyseren van trends in verstoringen en structurele oplossingsrichting voorstellen.
  - Uitwerken, vastleggen en documenteren van de wijziging in Topdesk en het CMDB.
  - Beschrijven en onderhouden testscripts.
  - Testen van de applicatie na doorvoeren van een aanpassing.
  - Ondersteunen van de procesbeheerder bij ingebruikname van de aanpassing in de applicatie.

- Regie, coördinatie, testen en installeren van applicatiesoftware:
  - Houdt ontwikkelingen rondom de applicatie in de gaten.
  - Beoordeelt en controleert de releasenotes
  - En het aanbevelen van nieuwe functionaliteiten.
  - Maakt een implementatie- of transitieplan bij grote veranderingen in de applicatie.
  - Stemt met de leverancier het transitieplan af.
  - Coördineert grote veranderingen in de applicatie.
  - Installeren en testen van applicatiewijzigingen. Dit gebeurt naar aanleiding van gebruikerswensen voor aanpassingen die niet in de standaardapplicaties voorkomen. Zowel voor toepassingen in de centrale computerapparatuur als voor toepassingen voor de persoonlijke devices.
  - Uitwerken, vastleggen en documenteren van wijzigingen in TopDesk en het CMDB.

- Proactief adviseren en ondersteunen in het functionaliteitenbeheer van een applicatie:
  - Duidelijk krijgen van het precieze doel van een wens of verzoek.
  - Adviseren bij het selecteren van een oplossingsrichting van een wens.
  - Functioneel ontwerp maken van de oplossingsrichting.
  - Toetsen of de wens of het verzoek past binnen de applicatie en het applicatielandschap.
  - Bepalen van de impact van de oplossingsrichting op de geautomatiseerde informatievoorziening.

- Interne en externe contacten:
  - Heeft contacten met leverancier(s) van de applicatie(s).
  - Heeft interne contacten met medewerkers via de superusers binnen de gemeente.

- Mede opzetten en beheren van de nodige werkinstructies, procedures en processen:
  - Stelt in overleg werkinstructies, procedures en processen op ten behoeve van gebruik en beheer van hard- en software en legt deze voor aan de leidinggevende.
  - Ziet toe op het gebruik van deze werkinstructies, procedures en processen binnen de gemeente en signaleert en adviseert aan de leidinggevende hieromtrent.

- Deelnemen in automatiseringsprojecten:
  - Neemt deel aan automatiseringsprojecten en doorloopt daarin het gehele traject van probleemanalyse, data-analyse, systeemanalyse, voorbereiding van de aankoop van de standaardapplicatie of aanpassen van standaardapplicaties en implementatie (o.a. door scholing).

- Communicatie beheerders ICT-processen:
  - Functioneel beheerders ontvangen signalen van benodigde wijzigingen vanuit, superusers, informatieadviseurs, technisch beheer en configuratiebeheerder.
  - Functioneel beheerders verwerken de benodigde wijzigingen in het daarvoor aangewezen systeem.

4.1.11 Technisch IT-beheerder

Samenvatting van de rol

De Technisch IT-beheerder is verantwoordelijk voor het dagelijks beheer en onderhoud van de ICT-omgeving binnen een organisatie. De Technische IT-beheerder is een centraal gepositioneerde rol binnen de afdeling Informatisering & Automatisering. Hij of zij zorgt ervoor dat de hard- en software up-to-date blijft en voldoende back-ups beschikbaar zijn. Daarnaast verhelpt de Technische IT-beheerder storingen of zet deze meldingen door naar externe leveranciers en ziet toe op de afhandeling hiervan. De beheerder adviseert en verricht uitvoerende en ondersteunende werkzaamheden op automatiseringsgebied ten behoeve van de gemeente.

Taken en Verantwoordelijkheden

- In hoofdlijnen:
  - Beheren, beveiligen en bedienen van de computersystemen.
  - Verhelpen van storingen en het bieden van gebruikersondersteuning.
  - Mede opzetten en beheren van werkinstructies
  - Installeren en testen van aanvullende computerprogrammatuur.

- Beheren, beveiligen en bedienen van het centrale computersysteem:
  - Is verantwoordelijk voor het in bedrijf houden van de computersystemen.
  - Bewaakt de computercapaciteit en signaleert vroegtijdig knelpunten.
  - Beheert programmaversies en daarbij behorende documentatie.
  - Installeert in samenwerking met de leverancier nieuwe systeemsoftware.
  - Ziet toe op de beveiliging van de centrale computerruimte.

- Beheren en uitgeven van ICT-hardware:
  - Uitgeven en beheren van computers, laptops, tablets, telefoons, beeldschermen, toetsenborden, muizen en overige apparatuur.
  - Inspoelen van laptops en computers.
  - Verantwoordelijk voor de werking van de werkplekken op de verschillende locaties van de gemeente.
  - Verantwoordelijk voor de werking randapparatuur.
  - Verantwoordelijk voor de werking netwerkaansluitingen en hardware binnen gemeentelijke locaties.

- Verhelpen van storingen en het bieden van gebruikersondersteuning:
  - Verhelpt storingen en lost probleemsituaties op met betrekking tot hard- en software en schakelt daarbij zo nodig technici van de leverancier in. Ziet toe op de uitvoering van werkzaamheden door derden.
  - Geeft richtlijnen aan en ondersteunt eindgebruikers zowel voor wat betreft systeembeheerszaken als voor vragen rondom het gebruik van de persoonlijke devices.

- Regie, coördinatie, testen en installeren van aanvullende computerprogrammatuur:
  - Houdt ontwikkelingen rondom de computerprogrammatuur in de gaten.
  - Installeren en testen van computerprogrammatuur. Dit gebeurt naar aanleiding van gebruikerswensen voor aanpassingen die niet in de standaardapplicaties voorkomen. Zowel voor toepassingen in de centrale computerapparatuur als voor toepassingen voor de persoonlijke devices.

- Proactief adviseren en ondersteunen in het technisch IT-beheer van computersystemen en (rand)apparatuur:
  - Duidelijk krijgen van het precieze doel van een wens of verzoek.
  - Adviseren bij het selecteren van een oplossingsrichting van een wens.
  - Technisch ontwerp maken van de oplossingsrichting.
  - Toetsen of de wens of het verzoek past binnen de bijbehorende (rand)apparatuur.
  - Bepalen van de impact van de oplossingsrichting op de geautomatiseerde informatievoorziening.

- Interne en externe contacten:
  - Heeft contacten met leveranciers van zowel hard- als software ten behoeve van pc's en servers.
  - Heeft interne contacten met medewerkers binnen de gemeente.

- Mede opzetten en beheren van de nodige werkinstructies, procedures en processen:
  - Stelt in overleg werkinstructies, procedures en processen op ten behoeve van gebruik en beheer van hard- en software en legt deze voor aan de leidinggevende.

- Ziet toe op het gebruik van deze werkinstructies, procedures en processen binnen de gemeente en signaleert en adviseert aan de leidinggevende hieromtrent.

- Deelnemen in automatiseringsprojecten:
  - Neemt deel aan automatiseringsprojecten en doorloopt daarin het gehele traject van probleemanalyse, data-analyse, systeemanalyse, voorbereiding van de aankoop van de standaardapplicatie of aanpassen van standaardapplicaties en implementatie (o.a. door scholing).

4.2 ICT-processen

4.2.1 Wijzigingsmanagement

Een wens, verzoek of verstoring kan aanleiding zijn voor een wijziging aan de informatievoorziening. Deze wijzigingen worden gecontroleerd doorgevoerd binnen het wijzigingsmanagementproces.

Wijzigingsmanagement draagt er zorg voor dat wijzigingen op de ICT-infrastructuur (ICT-middelen en -diensten) efficiënt en effectief worden doorgevoerd, met zo min mogelijk verstoring van de kwaliteit van de dienstverlening, zodat deze dienstverlening blijft voldoen aan de eisen die hieraan zijn gesteld. Daarbij kan het zowel gaan om processen als ook applicaties, netwerken of hardware. Daarnaast kan wijzigingsmanagement bruikbaar zijn voor het gecontroleerd uitvoeren van patchmanagement en daarmee de ICT-omgeving actueel houden en beschermen tegen kwetsbaarheden.

Wijzigingsmanagement wordt in gemeente Bergen op Zoom als essentieel proces ingezet voor het veilig houden van de ICT-omgeving onder invloed van veranderingen. Wijzigingsmanagement wordt gebruikt voor up-to-date houden en verbeteren van systemen, om schade en/of misbruik van ontstane kwetsbaarheden te mitigeren, voor het uitfaseren van oude soft- en/of hardware en het implementeren van verschillende beveiligingsmaatregelen.

Om dit proces nauwgezet toe te kunnen passen, worden de volgende randvoorwaarden vastgesteld:

Proces

- Er is een formeel, beschreven, geaccepteerd en werkend wijzigingsmanagementproces
- Spoedpatches volgen hetzelfde proces, maar de doorlooptijd is aanzienlijk korter
- Alle wijzigingen worden beoordeeld, geclassificeerd, ingepland, getest, geïmplementeerd, gedocumenteerd (incl. CMDB) en geëvalueerd
- Wijzigingen worden uitgevoerd op basis van SLA afspraken, bijvoorbeeld in een onderhoudsvenster. Afwijkingen hierop worden zorgvuldig afgestemd en gecommuniceerd. (Bijvoorbeeld spoedwijzigingen)
- Wijzigingen worden getest middels vooraf opgestelde testscripts, zodat er op uniforme wijze getest wordt
- Wijzigingen die binnenkomen via decentraal functioneel beheer bij afdeling I&A worden alleen behandeld, als deze tijdig zijn aangemeld en alle informatie compleet is
- Wijzigingen worden voor ingebruikname eerst getest in een TA (test/acceptatie) omgeving, daar waar deze aanwezig is
- Bedrijfskritische applicaties hebben een TA omgeving en periodiek wordt de TA omgeving geüpdatet
- Wijzigingen worden doorgegeven aan het configuratiemanagementproces, zodat de CMDB bijgewerkt kan worden
- Wijzigingen hebben altijd een impact en/of risicoanalyse en roll-back scenario
- Alle wijzigingen hebben een eigenaar

Wijzigingsadviescomité

- Er is een wijzigingsadviescomité (WAC) die de impact van changes onderzoekt en goedkeurt (met alle betrokken disciplines)
- Wijzigingen hebben goedkeuring nodig van de WAC, afhankelijk van of het een standaard of niet standaard wijziging is

Periodieke rapportage

- Er wordt gerapporteerd over geconstateerde afwijkingen in het wijzigingsmanagementproces.

4.2.2 Configuratiemanagement

Configuratiemanagement zorgt voor een actueel inzicht in alle hard- en software en onderlinge verbindingen binnen de organisatie. Om kwaadwillende en onbevoegden buiten de deur te houden moet allereerst bekend zijn welke hard- en software zich bevinden binnen het gemeentenetwerk of onder beheer van de gemeente vallen, zoals cloudoplossingen. Het is immers belangrijk dat zicht is op wat beschermd, beheerd en onderhouden dient te worden.
Configuratiemanagement is een randvoorwaarde om goed beheer uit te kunnen voeren. Zoals het gericht beheren van de omgeving en het opsporen van onbekende en ongeautoriseerde apparaten binnen het netwerk. Inzicht in hardware en software is de basis voor de ICT-foto die de gemeente aan de Informatiebeveiligingsdienst (IBD) levert, waardoor de IBD gericht advies kan leveren over kwetsbaarheden in de gemeentelijke hard- en software.

Om dit proces nauwgezet toe te kunnen passen, worden de volgende randvoorwaarden vastgesteld:

Proces

- Er is een formeel, beschreven en geaccepteerd configuratiemanagementproces

Configuratiemanagementdatabases (CMDB's)

Een Configuratie Management Database (CMDB) is een type database die wordt gebruikt voor het beheren, documenteren, koppelen en volgen van configuratie-items (CI's) gedurende de levenscyclus van bijvoorbeeld een product, computersysteem of software.

I&A legt de configuratie-items vast die benodigd zijn voor de uitvoering van haar primaire taak: het beschikbaar stellen en houden van processen, zodanig dat de organisatie haar werkzaamheden zonder belemmeringen kan uitvoeren, hetgeen binnen de producten- en dienstencatalogus is afgesproken. Deze configuratie-items worden in de daarvoor bestemde CMDB applicatie vastgelegd.

Periodieke rapportage

- Er wordt periodiek gerapporteerd, passend bij de Plan, Do, Check, Act cyclus, over de aanwezige hard- en software en geconstateerde afwijkingen in het configuratiemanagementproces.-
- Eens per jaar wordt de classificatie van bedrijfskritische systemen opnieuw getoetst door de eigenaar en indien nodig bijgesteld.

Configureren

- Alle configuratiewijzigingen worden gelogd
- Indien er wijzigingen in de ICT-infrastructuur plaatsvinden (via een wijzigingsverzoek), dienen de gegevens in de configuratiemanagementdatabase geüpdatet te worden

Configuratie-item

Een configuratie-item is een fysiek of virtueel middel, welke noodzakelijk is om een product/dienst in stand te houden, herstellen of te wijzigen. Voor I&A betekent dit alle ICT-gerelateerde componenten.

- I&A is verantwoordelijk voor een actueel, volledig overzicht van alle configuratie-items
- Randvoorwaarden is dat elk configuratie-item een eigenaar heeft
- De classificatie van het configuratie-item wordt vastgesteld door de eigenaar en wordt eenduidig vastgelegd

Netwerk scannen

- Het netwerk wordt gescand voor nieuwe hard- en software. De informatie uit deze scans wordt opgenomen in de daarvoor bestemde CMDB's

4.2.3 Patchmanagement

Het doel van Patchmanagement is tweeledig:

1. het is gericht op het inzichtelijk maken van de actuele stand van kwetsbaarheden en toegepaste patches binnen de beheerde infrastructuur,
2. op een zo efficiënt mogelijk wijze met zo min mogelijk verstoringen stabiele (veilige) systemen te creëren.

Patches komen uit om nieuwe functionaliteiten door te voeren en/of om beveiligingskwetsbaarheden te verhelpen. Er zijn standaard patches die gewoon het normale proces kunnen volgen en er zijn spoedpatches die snel doorgevoerd moeten worden en niet het gewone proces kunnen volgen. Organisaties zoals de IBD geven geregeld kwetsbaarheidswaarschuwingen, hier wordt ook een waarde aan gehangen hoe groot de kwetsbaarheid is.

Patchmanagementproces

- Er is een formeel, beschreven en geaccepteerd patchmanagementproces
- De uitrol van patches volgen het wijzigingsmanagementproces
- De toegepaste patches dienen in de CMDB toegevoegd te worden
- Er is een specifiek proces voor kritische/beveiligingspatches (spoedpatches)
- Hoog geclassificeerde patches dienen binnen één week geïnstalleerd te worden en volgen het spoedwijzigingsproces
- Er wordt regelmatig gecontroleerd of nieuwe relevante patches zijn uitgebracht

Patchen

- Alle uitrol van patches volgen het wijzigingsmanagementproces
- Onderhoudsvensters voor de installatie van patches zijn gedefinieerd in de SLA

- Patches worden beoordeeld op relevantie. De meest recente, relevante patches dienen binnen de gestelde termijn te zijn geïnstalleerd

Periodieke rapportages

- Er wordt gerapporteerd over de geconstateerde afwijkingen in het patchmanagementproces

4.2.4 Incidentmanagement

Er zijn verschillende soorten incidenten: van incidenten in de bedrijfsvoering tot fysieke gebeurtenissen, zoals bijvoorbeeld brand. Binnen dit genoemde proces wordt er alleen ingegaan op informatiebeveiligingsincidenten, met een variatie van kleine verstoringen, tot serieuze incidenten, zoals een ransomware aanval of datalek.
(Basis-)maatregelen kunnen risico's op informatiebeveiligingsincidenten sterk verminderen. Incidenten zijn echter nooit helemaal te voorkomen. Daarom is het van groot belang dat de gemeente is voorbereid, als er een incident plaatsvindt. De schade bij een incident kan met goede voorbereiding worden beperkt. Deze beperking wordt bepaald door het incidentmanagementproces, deze te oefenen en regelmatig te actualiseren.

Incidentmanagementproces

- Er is een formeel, beschreven en geaccepteerd incident- en responsmanagementproces
- Medewerkers weten wat informatiebeveiligingsincidenten zijn en waar ze deze kunnen melden
- Er is een duidelijk escalatie pad, voor het geval incidenten niet volgens de SLA opgelost kunnen worden

Incident- en responsmanagement

- Alle incidenten (en eventuele oplossingen) worden centraal geregistreerd
- Incidenten worden naar prioriteit ingedeeld en behandeld
- Incidenten worden afgehandeld volgens de oplostijden, zoals gedefinieerd in de SLA
- Er wordt een eigenaar aan elk incident toegewezen
- Informatiebeveiligingsincidenten zijn gemakkelijk te onderscheiden van overige incidenten
- De servicedesk is opgeleid om correct met informatiebeveiligingsincidenten om te gaan
- Incidenten kunnen ook buiten de kantooruren worden opgelost

Periodieke rapportage en evaluaties

- Er wordt periodiek gerapporteerd over de geconstateerde afwijkingen in het incidentmanagementproces
- Grote incidenten worden geëvalueerd
- Er wordt periodiek gekeken naar trends om verbeteringen te initiëren

4.3 Beleid voor inrichtingsprincipes

4.3.1 Beleid voor logische toegangsrechten (Roll Based Access Control)

De gemeente bergen op Zoom hanteert IAM en RBAC als concepten voor toegang tot informatievoorziening en ICT. Alleen geautoriseerd en getrainde personen worden toegelaten tot bepaalde soft- en hardware.
Dit houdt in:

- Dat er gewerkt wordt met een Active Directory
- Alleen geautoriseerde gebruikers, vastgesteld door manager, veranderingen aan kunnen brengen in de identity repositories
- Identiteiten gegroepeerd kunnen worden
- Gebruikers geauthentiseerd worden om diensten en informatie te gebruiken
- Accounts enkel de rechten krijgen die ze nodig hebben voor hun werk, per module tot op documentniveau bepaald
- Er een proces is voor nieuwe medewerkers, medewerkers die van functie wijzigen en medewerkers die de organisatie verlaten (ook wel het IDU-proces genoemd). Dit proces is gebaseerd op basis van rollen, die wijzigen wanneer een medewerker van functie wijzigt
- Lijnmanagement kent de toegangsrechten van de verschillende rollen binnen zijn/haar team en weet daarmee waar medewerkers toegang tot hebben. Periodiek wordt gecontroleerd of de juiste rechten nog aan de juiste medewerkers zijn toegekend
- Accounts zijn uniek en naar één persoon te herleiden
- Account die langdurig niet worden gebruikt worden vanwege veiligheidsoverwegingen geblokkeerd.
- Hiervan worden manager en HR business partner middels rapportage van op de hoogte gesteld. Zij bepalen of accounts worden geblokkeerd, bewaard of verwijderd
- Externe accounts voor leveranciers dienen te voldoen aan de volgende eisen: een account is te relateren aan een persoon, geen groepsnamen of applicatie/admin namen zijn toegestaan. Er worden zo min mogelijk rechten uitgedeeld (least-privelege). Indien mogelijk wordt er gewerkt via TeamViewer om controle te kunnen houden op de te maken werkzaamheden. MFA is geconfigureerd. Registratie van deze toegang is vastgelegd in TopDesk
- Toegang tot Teams/SharePoint gebeurd alleen op basis van beperkte toegang tot alleen de benodigde informatie. Registratie van deze toegang is vastgelegd in TopDesk
- Elke maand vindt er controle plaats op openstaande accounts voor externen en wordt nagegaan of dit nog actueel is, anders wordt toegang ontzegd.

Voor Admin accounts gelden nog aanvullende regels:

- Het gebruik van admin accounts is minimaal en het gebruik hiervan is minimaal
- Administrators gebruiken persoonlijke admin accounts en enkel om activiteiten uit te voeren waar deze rechten voor nodig zijn
- Accounts zijn uniek en naar één persoon te herleiden
- Admin accounts zijn ten alle tijden op basis van multifactor authentication. Voor de virtuele machines geldt dat deze alleen binnen de AVD te benaderen zijn

4.3.2 Beleid voor geautoriseerde soft- en hardware en informatiedragers

Alleen geautoriseerde soft- en hardware worden toegelaten. Informatiedragers zijn een fysiek medium waarop digitale gegevens kunnen worden opgeslagen. In gemeente Bergen op Zoom wordt er met geautoriseerde soft- en hardware en informatiedragers op de volgende manier omgegaan:
Dit houdt in:

- Elk apparaat heeft een unieke sleutel, waarmee aangemeld wordt op het netwerk (privé en gemeentelijk netwerk). Dit is een beveiligde verbinding met MFA. (Mobiele) informatiedragers zijn versleuteld. Bitlocker (versleuteling) is actief op alle managed laptops.
- Elke soft- en hardware voldoet aan de bedrijfsregels, zoals het gemeentelijk beleid (o.a. Informatiserings- en automatiseringsbeleid en Informatiebeveiligingsbeleid), maar ook landelijke wet- en regelgeving.
- Gebruik van harddisks en USB-stickers zijn niet toegestaan, op wettelijke uitzondering na zoals geldend in de samenwerking tussen politie en afdeling Openbare Orde en Veiligheid en bij het gebruik van rioleringsinspecties voor afdeling Beheer Openbare Ruimte.

4.3.3 Beleid voor (virtuele) servers

Met servers wordt bedoeld computers die diensten verlenen aan andere computers. De volgende eisen worden gesteld aan (het gebruik van) de gemeentelijke servers, ook wel hardeningseisen genoemd:

- Anti-malware software is op alle servers geïnstalleerd
- Webservers gebruiken HTTPS/HSTS

- De servers zijn voorzien van de juiste patches
- Het aantal accounts en beheerders is geminimaliseerd en de regels, zoals omschreven bij 4.2.1 gelden ook hier
- Er vindt logging plaats op alle servers
- Ongebruikte poorten zijn gedeactiveerd
- Er is een proces voor wijzigingen/updates op de server ingericht en wordt gevolgd
- Ongebruikte services zijn uitgeschakeld
- Alleen noodzakelijke componenten zijn geïnstalleerd
- Bij inrichting wordt de PTLU standaard toegepast
- Er wordt geen gebruik gemaakt van standaard wachtwoorden
- Back-up & restore is toegepast en wordt jaarlijks getest

4.3.4 Beleid voor endpoints

Met endpoints wordt bedoeld elk apparaat dat verbinding kan maken met het gemeentelijke netwerk. De volgende eisen worden gesteld aan (het gebruik van) endpoints:

- Anti-malware software is op alle endpoints geïnstalleerd
- Endpoints zijn voorzien van de juiste patches
- BYOD's worden in een apart VLAN ondergebracht, middels netwerksegmentering

4.3.5 Beleid voor software/applicaties

Software/applicaties is een verzamelnaam voor apps, besturingssystemen en(SaaS) programma's die op Imobile devices worden gebruikt. Het is een set instructies of programma's die een computer/laptop vertellen wat te doen. Er zijn twee componenten: systeemsoftware (besturingssystemen, apparatuur stuurprogramma's en hulpprogramma's) en applicatiesoftware (software om specifieke taken voor de gebruiker uit te voeren).
De volgende eisen worden er gesteld aan (het gebruik van) software, dan wel applicaties:

- Software/applicaties worden alleen op basis van het wensenproces I&A aangeschaft, waarbij de aanvraag wordt beoordeeld op eisen gesteld in: de GIBIT, de ICT Kwaliteitsnormen, ISO certificering, verwerkingsovereenkomst, gemeentelijk beleid en geldende wet- en regelgeving, onder andere in het kader van informatiebeveiliging en AVG. Dat betekent dat er buiten dit proces om géén aanschaf van ICT gerelateerde toepassingen plaatsvind, noch demo's zonder specialisten worden aangegaan.
- Bij aanschaf en vervanging van applicaties geldt: Cloud only en data mag niet uit de Europese Economische Ruimte
- Per bedrijfsfunctie kent gemeente Bergen op Zoom één applicatie
- Software/applicaties worden volgens het juiste proces opgenomen in de CMDB
- Software voldoet aan standaarden van de PTLU lijst
- Software/applicaties zijn voorzien van de juiste patches
- Er wordt geen gebruik gemaakt van standaard wachtwoorden
- Alleen noodzakelijke componenten zijn geïnstalleerd

4.3.6 Beleid voor netwerkapparatuur en firewalls

Met netwerkapparatuur worden type computers bedoeld die informatiestromen naar andere op het netwerk aangesloten apparaten ondersteund. Een firewall is een netwerkbeveiligingsapparaat of -programma dat inkomend en uitgaand netwerkverkeer bewaakt en bepaalt welk verkeer wordt toegestaan en wordt geblokkeerd op basis van ingestelde regels.
De volgende eisen worden er gesteld aan (het gebruik van) netwerkapparatuur en firewalls:

- Er zijn adequaat ingerichte up-to-date firewalls en netwerkcomponenten
- Het netwerk is juist gesegmenteerd
- Ongebruikte poorten zijn dichtgezet (door onder andere het toepassen van network access control)
- Toegang wordt enkel toegekend voor geautoriseerde beheerders

4.3.7 SIEM/SOC beleid

Een SIEM staat voor Security Information and Event Management. SOC staat voor Security Operations Center. SIEM is een oplossing die organisaties helpen bedreigingen te detecteren, te analyseren en erop te reageren vóór schade is berokkend. SOC bewaakt en verbetert de beveiliging van een organisatie.
Door de inzet van SIEM/SOC is de gemeente in staat om vroegtijdig, zeer proactief, de IT-omgeving te bewaken, waardoor kleine verdachte veranderingen, met mogelijk grote gevolgen, al vroeg zijn te herkennen en daardoor aan te pakken. Bij SIEM worden alle individuele logs samengebracht in één systeem. Dit systeem scant vervolgens op afwijkend gedrag. De SOC gaat reageren op dit afwijkende gedrag.

Het operationele beheer hiervan ligt bij de ICT-leverancier. Gemeente Bergen op Zoom voert regie, wat betekent dat zij eindverantwoordelijk zijn. De gemeente is dus in de lead om te bepalen hoe de meldingen af te handelen. Concrete afspraken zijn vastgelegd in de SLA met de ICT-leverancier.
Module 2 van het Verhoogde Digitale Weerbaarheidsprogramma van de Informatiebeveiligingsdienst (onderdeel VNG) staat in de planning voor 2025 om projectmatig op te pakken, waarin SIEM/SOC verder uitgewerkt zal worden.

4.3.8 Escrow regeling beleid

Bedrijfskritische applicaties worden voorzien van een escrow regeling ten behoeve van het veiligstellen van de data in de applicatie. De applicatie-eigenaar bepaalt of een applicatie bedrijfskritisch is en geeft daarmee opdracht tot het verstrekken van een escrow regeling.

4.3.9 Wachtwoordbeleid

Voor toegang worden er specifieke eisen gesteld aan wachtwoorden. Hierbij wordt de BIO opmaat 2.0 gehanteerd, samen met optionele aanbevelingen:

- Maximale foutieve inlogpogingen: 5
- Minimale wachtwoordlengte van 12 invoeren voor accounts die geen MFA gebruiken (denk hierbij aan service, admin- en systeemaccounts)
- Minimale wachtwoordleeftijd is één dag
- Tijd geblokkeerd account na foutief inloggen is ingesteld op 15 minuten
- Maximale foutieve inlogpogingen 3 keer

4.3.10 Back-up & Recovery beleid

Gemeenten hebben een grote verantwoordelijkheid voor het beveiligen en veilig houden van haar informatievoorziening en gegevens om optimale dienstverlening te kunnen leveren. Onze bedrijfsvoering en primaire processen zijn namelijk in grote mate afhankelijk van de beschikbaarheid, integriteit en vertrouwelijkheid van informatiesystemen. Een van de maatregelen om deze betrouwbaarheid te borgen is de back-up en recovery voorziening.

Een back-up en recovery voorziening voorziet in een set aan opslag- en herstelmaatregelen om na een incident of verstoring de juiste (gemeentelijke) informatie met minimaal verlies terug te plaatsen en de normale werkzaamheden (dienstverlening) te hervatten. Het wapent de gemeente tegen onvoorziene incidenten, menselijke fouten en fouten in de programma's waarmee we werken. Dat varieert van een verloren bedrijfsdocument tot een zogenaamde ransomware aanval (gijzelsoftware die data of systemen versleutelt in ruil voor losgeld).

Met dit back-up en recovery beleid wil de Gemeente Bergen op Zoom duidelijkheid en richting geven aan een van de maatregelen waarmee zij de continuïteit van haar bedrijfsvoering en dienstverlening wil waarborgen. Dit beleid beschrijft welke uitgangspunten binnen de gemeente gelden met betrekking tot de back-up en recovery voorziening. Dit beleid is van toepassing op de hele organisatie en de leveranciers die onderdelen van onze ICT-omgeving hosten en beheren.

Ten behoeve van de beveiliging van informatie is er back-up en recovery beleid voor alle gemeentelijke voorzieningen. Het doel van dit beleid is te voorkomen dat in geval van gedeeltelijk of geheel verlies of beschadiging van data en /of programmatuur de dienstverlening van de gemeente geen hinder ondervindt. De gemeente Bergen op Zoom hanteert de onderstaande richtlijnen welke zijn ontleend aan de BIO en handreikingen van de IBD en vormen een aanvulling op het Informatiebeveiligingsbeleid van de gemeente.

- De gemeente gebruikt back-up en recovery om de gevolgen van de uitval en/of het verlies van informatie te minimaliseren;
- De afdeling Informatisering & Automatisering is belast met het uitvoeren van dit beleid
- Dataverlies wordt beperkt tot maximaal 24 uur. De maximaal toelaatbare hoeveelheid gegevensverlies noemen we RPO (Recovery Point Objective);
- De hersteltijd in geval van incidenten bedraagt maximaal 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen. De maximaal toelaatbare hersteltijd noemen we RTO (Recovery Time Objective);
- De back-ups van alle gemeentelijke informatie, software en besturingssystemen (en instellingen) wordt bewaard, zodat de computerbesturingssystemen, applicaties en informatie volledig hersteld kunnen worden in geval van een calamiteit (zowel bij ICT-leverancier als niet ICT-leverancier). Dit wordt bereikt met behulp van een combinatie van kopieën, incrementele back-ups, differentiële back-ups en transactielogboeken en systeem baselines om te kunnen voldoen aan de maximale RPO en RTO.
- De frequentie van back-ups wordt bepaald door de volatiliteit van de gegevens. De bewaartermijn voor reservekopieën wordt bepaald door het kritieke karakter van de gegevens en wetgeving. De frequentie en bewaartermijnen dienen in overeenstemming met de proces- en applicatie eigenaar afgestemd te worden.

De afdeling I&A faciliteert dit op basis van hetgeen afdelingen in hun BCM hebben opgenomen en waar I&A bij betrokken is;

- We hanteren de 3-2-1 regel voor back-up en restore waarbij onderstaande geregeld is:
    - Minstens drie versies van een back-up moeten worden bewaard, op tenminste twee verschillende opslagmedium, waarvan er 1 op een andere fysieke plek bewaard moet worden;
    - Er dient minimaal één volledige back-up te worden opgeslagen in een veilige, off-site locatie. Een off-site locatie dient een veilige ruimte in een apart gebouw van de gemeente te zijn of een locatie van een off-site storage-leverancier;
    - Zorg dat tenminste één back-up niet online benaderbaar is en beschermd wordt tegen veranderingen (air-gapped);
    - Back-ups worden dagelijks gecontroleerd;
- Het back-up proces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere;
- Alle gemeentelijke informatie welke staat op werkstations, laptops of andere draagbare apparaten moeten worden opgeslagen op een afgeschermde beheerde omgeving om back-up mogelijk te maken;
- Documenteren en up2date houden van de volledige back-up voorziening en recovery procedures. Dit resulteert in plannen voor back-up, testen, recovery en registreren van loggegevens. Daarin komen alle essentiële gegevens, rollen en taken terug om een hersteloperatie uit te kunnen voeren conform de continuïteitsvereisten.
- Data in SaaS-applicaties dient ook te voldoen aan de BIO maatregelen en leverancier kan aantonen dat hieraan voldaan wordt;
- Er zijn geteste ICT-procedures voor back-up en recovery;
- De back-up en recovery procedures moet worden getest conform de documentatie en deze moet regelmatig worden bijgewerkt om rekening te houden met nieuwe technologie, veranderingen in het bedrijf, en de migratie van toepassingen naar alternatieve platforms;
- Recovery procedures moeten minimaal op jaarbasis worden getest;
- Van back-up en recovery activiteiten en de verblijfplaats van de media wordt een logboek bijgehouden;
- De back-up media worden vernietigd in overeenstemming met het beleid omtrent behandeling van digitale media van de gemeente;
- Voor de toegang tot back-ups wordt (onder regie van de afdeling I&A) versleutelingstechnologie toegepast. De gemeente ziet toe op de uitvoering van deze beveiligingsmaatregel in termen van autorisatie, toegangssleutels en sleutelbeheer;
- Back-up en recovery moet voldoen aan AVG-wetgeving;
  Met het back-uppen van gegevens kunnen ook persoonsgegevens worden geback-upt. Op het moment dat op de back-up media persoonsgegevens worden opgeslagen vallen deze back-up media ook onder de AVG-wetgeving. Dit houdt in dat we in bepaalde gevallen verplicht zijn om iemands gegevens te verwijderen als diegene hierom vraagt. Bijvoorbeeld als de gegevens niet meer nodig zijn of als iemand zijn toestemming intrekt of dat er geen wettelijke basis meer is om deze gegevens te bewaren. Verder, om persoonsgegevens te beschermen moeten deze worden versleuteld, dus ook op het back-up medium. Wanneer er een oudere back-up teruggeplaatst wordt dan dienen verwijderverzoeken van gegevens opnieuw uitgevoerd te worden.
- Back-up en recovery valt niet onder de archiefwet;
  Back-ups mogen volgens de archiefwet niet gebruikt worden als archief omdat deze niet bestaat uit de originele data maar uit kopieën. In de tweede plaats dienen back-ups als een middel om gegevens te herstellen in het geval van een storing of een ramp. Back-ups zijn niet bedoeld om permanent te bewaren of te dienen als het officiële archief van een gemeente. Archiefstukken daarentegen worden zorgvuldig beheerd en bewaard in overeenstemming met de Archiefwet. Archiefstukken bevatten belangrijke informatie die permanent bewaard moet blijven voor toekomstige generaties en voor het publiek. Archiefstukken moeten aan specifieke eisen voldoen, zoals het bewaren van de integriteit en authenticiteit van de documenten, zodat ze kunnen worden gebruikt als bewijsstukken en als historisch materiaal.

4.3.11 Releasebeleid

Omtrent releases hanteert de gemeente het volgende beleid:

- We hanteren maximaal -1
- Spoedreleases in verband met een hoge kwetsbaarheid dienen binnen één week geïnstalleerd te zijn

4.3.12 Beleid voor aansluiten op gemeentelijk netwerk en gebouw gebonden installaties

Omtrent het aansluiten op gemeentelijk netwerk en gebouw gebonden installaties hanteert de gemeente het volgende beleid:

- Aansluiten op gemeentelijk netwerk alleen mogelijk op basis van het wensenproces, waarbij de aanvraag wordt beoordeeld op eisen gesteld in: de GIBIT, de ICT Kwaliteitsnormen, ISO certificering (minimumvereiste ISO27001, eventueel aanvullend met een assurance-verklaring, zoals ISAE3000-SOC2 en voor IoT/OT/PA/SCADA aangevuld met IEC62443 wanneer uit risicoanalyse blijkt dat risico's significant groot zijn), verwerkingsovereenkomst, gemeentelijk beleid en geldende wet- en regelgeving in het kader van informatiebeveiliging en AVG
- Aansluitingen en gebouw gebonden installaties worden volgens het juiste proces opgenomen in de CMDB

4.3.13 E-mailbeleid

Omtrent e-mail hanteert de gemeente het volgende beleid:

- Algemene e-mailadressen voor projecten worden aangemaakt op basis van hun tijdelijke aard en worden gesloten en juist gearchiveerd volgens vooraf afgesproken tijdsduur. Aanvraag van deze mailboxen geschied op toestemming van opdrachtgever project
- Algemene e-mailadressen voor afdelingen worden aangemaakt voor langdurige aard, waarbij de regels voor archiveren juist worden gehanteerd: ontvangen mails worden gekoppeld aan het juiste dossier binnen de daarvoor bestemde applicatie. De mailbox wordt eens per jaar geheel vernietigd. Indien de mailbox een jaar geen activiteit heeft, wordt de gehele mailbox gesloten
- E-mails in persoonlijke en gedeelde mailboxen worden gearchiveerd, zoals omschreven in het 'Protocol Internet, E-mail en Social Media 2021', welke is opgenomen in het Personeelshandboek van de gemeente en binnenkort wordt hernoemd naar 'Ambtelijke Gedragscode'
- E-mailberichten uit functionele mailboxen hebben een bewaartermijn van één jaar. Voor e-mailberichten uit geautomatiseerde mailboxen geldt een bewaartermijn van 3 maanden (of zoveel langer als nodig is, voor de bedrijfscontinuïteit / het administratieve proces)

4.3.14 Websitebeleid

Omtrent websites hanteert de gemeente het volgende beleid:

- (Gemeentelijke) websites/(sub)domeinen voldoen aan wet- en regelgeving, waaronder Single Digital Gateway en zijn afgestemd en goedgekeurd met afdeling Communicatie voor advies omtrent passende communicatie-uiting en huisstijl en met afdeling Informatisering & Automatisering voor technische toepassingen
- Van (sub)domeinen is duidelijk dat deze onderdeel zijn van gemeente Bergen op Zoom
- Websites mogen alleen worden aangevraagd door lijnmanagement. Zij zijn tevens eigenaar van de website en verantwoordelijk voor de inhoud van de website
- Eigenaar is verantwoordelijk voor het toepassen van de Wet Digitale Toegankelijkheid
- Afdeling Informatisering & Automatisering beheert benodigde certificering
- Websites worden opgenomen in de CMDB van afdeling Informatisering & Automatisering

4.3.15 Beleid Business Intelligence

De gemeente Bergen op Zoom creëert waarde uit zijn data via professioneel gegevensmanagement.
Doelstellingen: Het doel van BI is om nauwkeurige en tijdige informatie te leveren die nodig is voor operationele, tactische en strategische besluitvorming.
Gegevensbeheer: Alle data moet worden verzameld, opgeslagen en beheerd in overeenstemming met de geldende wet- en regelgeving. Dit omvat ook de bescherming van gevoelige en persoonlijke informatie.
Kwaliteit van de gegevens: De kwaliteit van de gegevens moet worden gewaarborgd. Dit omvat de nauwkeurigheid, volledigheid, consistentie en tijdigheid van de gegevens.

- De gemeente blijft te allen tijde eigenaar van alle data en gegevens vastgelegd in een applicatie
- Data en gegevens mogen nooit zonder toestemmingen worden gebruikt door of gedeeld met derden. Ook niet indien de data en gegevens zijn geanonimiseerd

4.3.16 Mobile Device beleid

Vanuit het kader van goed werkgeverschap zien we dat immateriële arbeidsvoorwaarden steeds belangrijker zijn voor medewerkers (bijvoorbeeld de balans tussen werk en privé en flexibele werktijden). Hier hoort ook een flexibele werkplek op kantoor bij, zodat je met je laptop en smartphone overal kunt werken. Zo'n werkplek bestaat uit één of twee schermen, een toetsenbord en muis die allen aangesloten zijn op een dockingstation waarop je je laptop makkelijk kunt aansluiten.

De laptop is niet langer meer een aanvulling op de werkplek, maar de laptop is de werkplek. Daarnaast richten we ons op het faciliteren van Slim Samenwerken tussen medewerkers binnen en buiten de organisatie. Zo sluiten we aan bij de organisatieontwikkeling en ook bij de nieuwe vorm van werken.

Definities

Mobile device: alle draagbare en draadloze communicatie en/of computerapparatuur. Hierbij wordt onderscheid gemaakt tussen communicatiemiddelen en computers. Mobiele telefoons en smartphones worden tot de communicatiemiddelen gerekend, terwijl laptops en tablets als computers worden beschouwd. Hierbij wordt de richtlijn van de Belastingdienst gevolgd.
Abonnementen: onder abonnementen worden het spraak en/of data abonnement van de gemeente verstaan.

Mobile Device beleid

Het MD beleid is vormgegeven rondom leidende principes. Deze principes fungeren als de basis van het beleid en zullen we periodiek toetsen of evalueren aan de hand van interne en externe ontwikkelingen.

Scope

Iedereen: medewerkers in dienst van de Gemeente Bergen op Zoom met gebruikersprofiel kantoorgerichte gebruiker en flexibele / mobiele gebruiker. Tenzij: niet kantoor-gerichte gebruiker (bijv. hovenier, schoonmaker). Voor de bestuurders en raadsleden geldt dat zij vanuit de wetgeving, de regeling 'Rechtspositiebesluit decentrale politieke ambtsdragers', voor de uitvoering van hun werkzaamheden mobiele apparatuur beschikbaar krijgen als bedrijfsmiddel (artikel 3.3.2 Informatie- en communicatievoorzieningen). Bestuurders en raadsleden vallen onder het gebruikersprofiel flexibele / mobiele gebruiker. Externe medewerkers voorzien doorgaans zelf in hun mobiele devices of maken gebruik van een device van de gemeente; de gemeente Bergen op Zoom stelt hen licenties en informatie in overeenstemming met het mobile device beleid beschikbaar om de overeengekomen taken uit te voeren.

Mobile First

Iedereen: die hier vanuit zijn/haar functie in aanmerking komt wordt gefaciliteerd met de juiste mobile devices t.b.v. het flexibel kunnen werken en uitvoeren van zijn/haar functie (laptop, tablet, smartphone).
Maatwerk: voor de specialistische gebruiker of de medewerker met bijzondere functionaliteiten. Zij krijgen passende devices aangeboden. Maatwerk vindt plaats in overleg met de manager van de vak afdeling en afdeling Informatisering & Automatisering (Advies en ServiceDesk) en indien nodig wordt door directie besloten (zie ook 2. Uitgiftevariant).

De gebruikersprofielen zijn als volgt vastgesteld:

Gebruikersprofiel	Omschrijving	Soort device
Niet-kantoorgerichte gebruiker	Werkt veelal niet aan een bureau en maakt nagenoeg geen gebruik van een werkplek	Geen laptop en telefoon
Kantoorgerichte/bureau gebruiker	Werkt doorgaans tijdens kantooruren vanuit een vaste werkplek, taken gericht op productie	Laptop zonder specifieke eisen voor afmetingen of draagbaarheid; telefoon
Flexibele/mobiele gebruiker	Werkt gedurende de dag op verschillende plekken en vergaderruimtes (waar en wanneer hij wil/geacht wordt) en wil naadloos overstappen/aansluiten	Laptop moet draagbaar en robuust zijn. Afmetingen maximaal 15 inch
Specialistische gebruiker	Werkt met speciale hard- en software met specifieke eisen aan devices	Laptop met specifieke eisen per case te beoordelen; telefoon

Bruikleen

Je wordt vanuit de gemeente gefaciliteerd met de juiste apparatuur voor het uitvoeren van je werkzaamheden. De apparatuur wordt vanuit de gemeente beheerd. Zodra je een device in bruikleen krijgt ga je digitaal akkoord met de bruikleenovereenkomst Gemeente Bergen op Zoom. In de bruikleenovereenkomst staan de afspraken over de aansprakelijkheid (bij schade of diefstal) en het zorgvuldig gebruiken en omgaan met de devices. Thuis en op kantoor zorgen we voor de juiste randapparatuur (beeldscherm, toetsenbord, muis, dockingstation) zodat je flexibel kunt werken als je werk dit toelaat. De werkplek thuis wordt gefaciliteerd met één beeldscherm, op kantoor zullen werkplekken voorzien worden van één of twee beeldschermen waarop je je laptop kan aansluiten. Thin-clients en vaste telefoons zullen we geleidelijk uit faseren waar mogelijk. Flexwerken met dockingstations wordt de norm. De laptop is bedoeld voor gebruik van zakelijke doeleinden. Als werknemer kun je het apparaat incidenteel gebruiken voor persoonlijke activiteiten,

zoals toegang tot sociale sites, e-mail, oproepen, enz. Je kunt op de laptop geen applicaties installeren. Op de telefoon kun je wel persoonlijke apps installeren.

Veilig werken

Met je laptop en telefoon beschik je over de juiste devices om je werk te doen daar waar je werkzaamheden dit toelaten. Je bent je bewust dat je werkt met data en gegevens van de gemeente of waar de gemeente verantwoordelijk voor is. Met die gegevens ga je zorgvuldig om en pas je de principes van Informatiebeveiliging en Privacy toe ongeacht vanaf welke werklocatie je werkt (zie hiervoor ook Beleid rondom informatiebeveiliging en privacy bij het gebruik van mobile devices).
De ServiceDesk richt de devices voor je in en zorgt daarmee voor een technisch optimale beveiliging van onze data en infrastructuur door implementatie van beveiligingssoftware (verplichte update, virusscanner, wachtwoorden etc.). Uiteraard ben je als eindgebruiker wel verantwoordelijk voor het verwerken van data en gegevens van de gemeente. Zie ook de handreiking (veilig) thuiswerken.

Technische ondersteuning

Technische ondersteuning: heb je vragen over je device? De collega's van de ServiceDesk helpen je graag op weg. Je kunt je vraag het beste stellen via het Selfservice portaal van TopDesk of anders mailen (servicedesk@bergenopzoom.nl) of bellen ((0164-27)7352). Indien nodig wordt je device vervangen. Reparaties van devices worden binnen de gebruiksperiode (4 jaar voor de laptop en 3 jaar voor de telefoon) bij de leverancier uitgevoerd.

Fiscaal

Aan de verstrekking van mobile devices zijn fiscale gevolgen verbonden. Via de werkkostenregeling kan de werkgever onbelaste vergoedingen aan werknemers geven. Welke dit zijn kun je afleiden uit het meest recente WKR-overzicht vergoedingen & verstrekkingen (zie artikel 22.1.7 Handboek Loonheffingen 2022). Terbeschikkingstellingen van computers en mobiele communicatiemiddelen en dergelijke apparatuur zijn gericht vrijgesteld als deze voldoen aan het zogenoemde
noodzakelijkheidscriterium. Dat betekent dat de gemeente dit mag verstrekken omdat het nodig is voor het werk. De mobile devices zijn dus geen verworven recht

Juridisch

De gemeente is en blijft eigenaar van de mobile devices die verstrekt worden.

Financieel

In de begroting is budget opgenomen voor dit beleid. Om overschrijding van het budget te voorkomen, beheert het team Informatie en Processen de aanmeldingen.

1. Uitgiftevariant

Voor de verschillende varianten is een afweging gemaakt tussen individuele keuzevrijheid, beheer en ondersteuning, informatiebeveiliging, privacy, fiscale en juridische consequenties. Met de varianten vinden we de balans tussen passend beheer- en beveiligingsniveau en gebruiksgemak. Hiermee kiezen we voor een beperkte keuzevrijheid van devices ten behoeve van het verbeteren van de informatiebeveiliging, privacy, beheer en ondersteuning. We kiezen voor een uniform beleid met eenduidige richtlijnen voor het faciliteren van medewerkers en duidelijkheid in het proces van aanvragen, bestellen en leveren. De gemeente kiest voor een standaardassortiment van smartphones en laptops. Dit assortiment selecteren we op de voor Bergen op Zoom vastgestelde eisen voor beheer en ondersteuning, informatiebeveiliging en privacy. We bieden een smartphone en laptop aan binnen het budget. Het uitleverproces loopt via de ServiceDesk. Daar waar nodig bieden we maatwerk.

Maatwerk

De werkzaamheden van een medewerker vormen de basis voor de uitgifte van mobile devices. Om tijd- en plaats onafhankelijk te kunnen werken heeft een medewerker een laptop en een smartphone nodig. Echter dit past niet voor elke functie. Indien functioneel noodzakelijk kan de (direct) leidinggevende een gemotiveerd afwijkingsaanvraag doen van de gestelde richtlijnen van hardware. Hiermee blijft er, mits voldoende gemotiveerd, ruimte voor individuele behoeften.
Maatwerk vindt plaats in overleg met de manager of (direct) leidinggevende van de vak afdeling en afdeling I&A (Advies en ServiceDesk) en indien nodig wordt door directie1 besloten. Hierbij wordt ook gekeken naar eventuele ontwikkelingen op de markt. We houden hierbij vast aan de volgende randvoorwaarden:

- Bij maatwerk is de manager of (direct) leidinggevende verplicht de noodzaak toe te lichten en functioneel te onderbouwen
- Maximaal 2 mobile devices per persoon: één smartphone en één laptop of vergelijkbaar product;
- Het maatwerk moet leiden tot de leidende principes

2. Regeling overgangsrecht

Het nieuwe mobile device beleid treedt per 1 januari 2023 in werking en is van toepassing op de devices die onder dit beleid worden uitgegeven.De devices die zijn aangeschaft onder het BYOD-beleid blijven tot het einde van de looptijd van de devices onder voorwaarden van het BYOD-beleid vallen. Heeft je BYOD-device het eind van de looptijd bereikt dan kan je onder het nieuwe beleid een device in bruikleen aanvragen

Wat verandert er concreet?

- De werkgever blijft eigenaar van de devices en verstrekt deze in bruikleen
- De medewerker ondertekent bij het in gebruik nemen van de smartphone of laptop digitaal de bruikleenovereenkomst
- Bij in gebruik name van de smartphone wordt één simkaart verstrekt met bijbehorend zakelijk data- en telefoonabonnement. Privégebruik wordt gedoogd zonder eigen bijdrage. Hierbij wordt uitgegaan van de fair use policy, hetgeen betekent dat je device primair bestemd is voor het uitvoeren van je werkzaamheden. Het data- en telefoonverbruik kan worden gemonitord. Als de medewerker al beschikt over een simkaart met bijbehorend data- en telefoonabonnement van de gemeente wordt deze simkaart overgezet naar de smartphone in bruikleen.
- Als je privé gegevens plaatst op je device kunnen deze worden gewist omdat je laptop/telefoon beheerd wordt door gemeente. Uiteraard doen we dit niet zomaar, bij schade, wisselen, verlies of diefstal wordt je telefoon altijd (op afstand) gewist
- Wanneer een medewerker de organisatie verlaat (vrijwillig of op initiatief van de organisatie) levert hij/zij alle verstrekte apparatuur in bij de ServiceDesk. Ook de apparatuur van je thuiswerkplek

De volgende **extra uitgangspunten** worden gesteld aan de mobile devices in het kader van informatiebeveiliging:

- Patchen en updates worden tijdig uitgevoerd op mobiele telefoons
- Alle devices maken gebruik van het bedrijfsportal. Hiermee worden de bedrijf kritische applicaties en gegevens afgeschermd en zijn deze op afstand te wissen. Daarnaast dient inloggen te gebeuren met o.a. fingerprint, face ID, toegangscode en MFA. Naast versleuteling wordt ook zero footprint toegepast.
- Bij geen up-to-date virusscanner en firewall, kan de toegang tot de ICT-infrastructuur van de gemeente worden geweigerd
  Er wordt gewerkt naar een situatie waarbij telefoons in beheer van de gemeente volledig worden beheerd en alleen voorzien van zakelijke apps die voldoen aan wet- en regelgeving en daarmee dus vertrouwd kunnen worden (whitelisting).