

Informatie- management, beveiliging en ICT

Uitvoeringsplan 2021 - 2022

21 APRIL

Robert van der Poel
Chief Information Officer



**Leidschendam-
Voorburg**

Inhoud

Inleiding.....	3
Strategische acties	4
Informatiebeveiliging	4
Werkplek van de toekomst	4
ICT management van de toekomst (sourcing strategie)	5
Uitvoeringsplan.....	7
Doelstelling	7
Resultaat.....	7
Fasering	9
Fase Voorbereiding.....	9
Fase Implementatie	9
Fase Migratie.....	9
Fase Overdracht naar Beheer	10
Beheersing	11
Tijd/Planning.....	11
Geld	11
Kwaliteit.....	11
Informatie/Communicatie	11
Organisatie.....	11
Risicobeheersing	12

Inleiding

In februari 2020 is de Informatiemanagement en ICT Missie, Visie en Strategie 2020 – 2024 (hierna Missie, Visie en Strategie) behandeld in de Gie Samenleving¹. In de Missie, Visie en Strategie staan de strategische acties benoemd voor het tijdvak 2020-2024.

Dit uitvoeringsplan geeft invulling aan de volgende strategische acties in 2021-2022:

- Informatiebeveiliging
- Werkplek van de toekomst
- ICT management van de toekomst

De gemeente heeft nadrukkelijk prioriteit gegeven aan informatiebeveiliging. In oktober 2020 is dit onderwerp in de beeldvormende raadsvergadering behandeld². N.a.v. van deze presentatie is er door de raad verzocht om in het bijzonder over dit onderwerp te rapporteren. Middels dit uitvoeringsplan wordt hierin voorzien.

Projecten die bijdragen aan de overige strategische doelstellingen (De Moderne Overheid en Gegevensmanagement) vallen onder het programma De Moderne Overheid (hierna DMO).

¹ Zie bijlage 1 voor de Informatiemanagement en ICT Missie, Visie en Strategie 2020-2024

² Zie bijlage 2 voor de presentatie over informatiebeveiliging

Strategische acties

Informatiebeveiliging

Een van de doelen die de gemeente zich heeft gesteld betreft de ‘Veiligheid van Informatie’. In de toenemende digitalisering is het borgen van informatieveiligheid en privacy essentieel. Steeds meer systemen worden aan elkaar gekoppeld en steeds meer mensen moeten toegang krijgen tot dit netwerk van informatie. Daarbij dient de gemeente tevens als organisatie te voldoen (compliant te zijn) aan relevante normen, kwaliteitseisen en wet- en regelgeving. Dit veilig maken en houden heeft de hoogste prioriteit.

Vanuit het perspectief van ‘Informatiebeveiliging’ zijn een viertal acties uitgezet die ertoe bijdragen dat de veiligheid van informatie binnen de gemeente geborgd wordt.

- Bewustwording, houding en gedrag;
- Autorisatie en Toegang;
- Grip op datastromen;
- Logging en monitoring.

De kaders hiervoor zijn vastgelegd in de ‘Beveiligingsarchitectuur’³. Kaders die gebaseerd en gefundeerd zijn op voor de gemeente relevante normen, kwaliteitseisen en wet- en regelgeving:

- IM ICT Missie, Visie en strategie 2020 – 2024
- NORA-referentiearchitectuur
- GEMMA-referentiearchitectuur
- TOGAF Architectuur
- BIO-versie 1.04
- (Waar nog toegepast) BIG-versie 1.2

In 2020 is de ‘Beveiligingsarchitectuur’ nader geconcretiseerd in een ‘Technische Doelarchitectuur’. In deze ‘Technische Doelarchitectuur’ is een heldere baseline aan kwaliteitseisen vastgelegd waaraan de ICT Infrastructuur dient te voldoen, wil het doel van ‘Veiligheid van Informatie’ binnen de gemeente gerealiseerd en geborgd worden.

Werkplek van de toekomst

De veranderende digitale wereld heeft ook een impact op de digitale werkomgeving van de gemeente. Plaats- en tijdonafhankelijk digitaal samenwerken is de norm geworden. De coronacrisis heeft voor een enorme versnelling gezorgd in 2020. Er is vraag naar een ander en meer divers palet aan

³ Zie bijlage 3 voor de beveiligingsarchitectuur

functionaliteit. Het is belangrijk om als organisatie proactief te voorzien in deze wensen om te borgen dat er efficiënt, effectief en veilig (samen)gewerkt kan worden en informatie niet gaat zwerven buiten de organisatie. Hiervoor is in 2020 versneld gestart met de inrichting en implementatie van de nieuwe digitale werkplek, waarbij de volgende punten centraal staan:

- Moderne *flexibele* werkplek
- Het is mogelijk om *volwaardig* digitaal samen te werken, ook in de keten
- Het is mogelijk om *veilig* samen te werken aan en delen van informatie met externe partijen
- Er is een divers aanbod van *standaard* voorzieningen voor ondersteuning op maat

De digitale werkplekken worden ingericht binnen Microsoft 365 conform microsoft standaarden, de BIO en valt binnen het Framework-VNG model⁴. Er zijn diverse projecten opgestart om deze werkplek goed in te richten en uit te rollen. Deels valt dit onder de beveiligingsprojecten en deels onder het programma DMO. In het uitvoeringsplan worden de projecten die vallen onder informatiebeveiliging meegenomen. Er vindt continu afstemming plaats met het DMO om de aansluiting van deze trajecten te borgen.

ICT management van de toekomst (sourcing strategie)

We leven in een informatie- en netwerksamenleving die steeds complexer wordt. De overheid maakt de stap naar een digitaal georiënteerde dienstverlening en bedrijfsvoering. De gemeentelijke dienstverlening en informatievoorziening verandert continue. Dit heeft als gevolg dat er een herziening komt van de gemeentelijke ICT-infrastructuur en -beheer op basis van outsourcing.

De sourcing strategie van LV hanteert de volgende uitgangspunten:

- Breng de techniek van ICT naar de cloud.
- Maak het mogelijk om continue innovatie te ondersteunen.
- Standaardisatie is leidend. Maatwerk doormiddel van een divers aanbod van standaard voorzieningen.
- Duurzaamheid door multi-inzetbaarheid middels de eenmalige implementatie van flexibele technologie.
- Beheerorganisatie op basis van regievoering op strategisch, tactisch en operationeel niveau.

LV wil zich focussen op kernactiviteiten en niet op de “harde” ICT (is geen kerntaak). Marktpartijen die zich toeleggen op deze taken kunnen deze producten en diensten vele malen beter en betrouwbaarder organiseren dan een gemeente, zoals:

⁴ Alle Nederlandse gemeenten kunnen sinds 1 februari 2019 gebruikmaken van de gemeentelijke voorwaarden van Microsoft. Gemeenten bepalen zelf of ze er gebruik van maken. Microsoft heeft hiervoor samen met VNG het Framework-VNG model in het leven geroepen, dit model bestaat uit juridische en commerciële voorwaarden op basis van het M365 E3 licentie model van Microsoft.

-
- Aantrekken en vasthouden van kwalitatief goed personeel en deze redundant bezetten
 - Op niveau houden van actuele kennis en kunde
 - Organiseren van (technische) beheersprocessen
 - Voldoen aan relevante normen, kwaliteitseisen en wet- en regelgeving.

Deze strategische keuze is ook bepalend geweest voor de keuze om de samenwerking met de gemeente Westland op het gebied van het ICT beheer te beëindigen en deze onder te gaan brengen bij gespecialiseerde marktpartijen.

Uitvoeringsplan

Doelstelling

Het informatiebeveiligingsproject en haar deelprojecten zullen ervoor zorgen dat de huidige ICT-infrastructuur in lijn gebracht wordt met de eisen zoals beschreven in de 'Beveiligingsarchitectuur en de 'Technische Doelarchitectuur'. De uitvoering van deze (deel)projecten zullen in de volgende hoofdstukken nader toegelicht worden.

Door de realisatie van de deelprojecten die onder dit uitvoeringsplan vallen brengt de gemeente Leidschendam-Voorburg haar ICT-infrastructuur op gebied van informatiebeveiliging op orde, zodat

- Haar informatiepositie op orde is en blijft;
- De gemeente daardoor toegankelijke, veilige en betrouwbare dienstverlening biedt aan onze inwoners, bedrijven en ketenpartners;
- Voldoet (compliant is) aan voor de gemeente relevante normen, kwaliteitseisen en wet- en regelgeving.

En zijn bepaalde ICT-onderdelen uitbesteed aan marktpartijen die deze producten en diensten vele malen beter en betrouwbaarder organiseren dan een gemeente, zoals:

- Aantrekken en vasthouden van kwalitatief goed personeel en deze kwantitatief weten te bezetten;
- Op niveau houden van actuele kennis en kunde;
- Organiseren van (technische) beheerprocessen;
- Voldoen aan relevante normen, kwaliteitseisen en wet- en regelgeving;
Waardoor de gemeente zich kan focussen op haar kernactiviteiten.

Resultaat

Op basis van dit uitvoeringsplan worden de volgende deelproducten op gebied van Architectuur, Netwerk, Security en ICT Infrastructuur gerealiseerd:

Architectuur

- Uitgangspunten en doelarchitecturen uitwerken voor de diverse projecten.

Netwerk

- Aanpassen en uitbreiden van de Firewall functionaliteit
- Life Cycle Management (LCM) van diverse netwerk componenten
- Verbeteren van lokaal (draadloos) netwerk

Security

- Implementeren van identity en access management (verbeteren van beveiliging rondom accounts)
- Beter beveiligen van de (cloud) netwerk toegang
- Verbeteren van de beveiliging analyses

- Verbeteren Antivirus/-Malware (incl. Sandboxing)
- Additioneel beveiligen van mail
- Moderne flexibele werkplek

Infrastructuur

- Upgraden van servers & virtualisatie
- Citrix upgrade
- Upgrade en aanbesteding van storage (opslag)
- Transitie naar andere uitwijk oplossing

Binnen deze projecten worden de volgende aspecten opgeleverd:

- Modernisering en implementatie van (verbeterde) beveiligingstechnieken die een bijdrage leveren aan de gestelde strategische acties op gebied van 'Autorisatie en Toegang', 'Grip op datastromen' en 'Logging en monitoring':
 - Netwerk (o.a. firewalls, netwerk op locaties en netwerkbeveiliging) is gemoderniseerd conform de 'Technische Doelarchitectuur'. ICT-infrastructuur (w.o. fysieke en virtuele servers, backup-, opslag- en uitwijk oplossingen) is gemoderniseerd conform de 'Technische Doelarchitectuur'.
 - Achterstallig onderhoud op gebied van security is weggewerkt, dan wel aangescherpt;
 - Verouderde hardware/softwarecomponenten zijn vervangen door nieuwe- en/of door leverancier ondersteunde versies;
 - Technische ontvlechting met de huidige ICT dienstverlener (Gemeente Westland).
- Voor ICT-onderdelen die in aanmerking komen om uitbesteed te worden richting marktpartijen: Gewenste marktpartij is geselecteerd en voert operationeel beheer over het betreffende onderdeel. En voldoet aan de gestelde wet- en regelgeving geldend voor de gemeente.
- Regieprocessen en verantwoordelijkheden inrichten die direct voortvloeien uit de projecten in het uitvoeringsplan.
- Vanuit de gemeentelijke ICT Regie Organisatie is communicatie/bewustwording Informatiebeveiliging geborgd en ingebed.

De hierboven beschreven deelprojecten beperken zich tot de genoemde resultaten. De volgende zaken liggen buiten de scope van dit uitvoeringsplan:

- De organisatorische aspecten van de ontvlechting met de huidige ICT-dienstverlener (Gemeente Westland);
- Het opzetten van de bredere ICT regieorganisatie;
- Diverse reguliere software upgrade trajecten van bedrijfsapplicaties die nodig zijn t.b.v. de beveiligingsprojecten en de ontvlechting.

Voor deze onderdelen zijn separate projecten opgezet die deze producten moeten opleveren of vallen onder regulier ICT life-cycle management.

Fasering

Elk benoemd deelproject binnen het uitvoeringsplan kent dezelfde opbouw qua fasering. Deze bestaat uit een Fase Voorbereiding, - Implementatie, - Migratie en - Overdracht naar Beheer. Per Fase zijn per project gerelateerde activiteiten benoemd.

Fase Voorbereiding

Deze fase kenmerkt zich per deelproject met name door inventarisatie van de huidige situatie van de in scope zijnde ICT-componenten, waarbij een GAP-analyse wordt uitgevoerd tegen de gestelde kaders in de 'Beveiligingsarchitectuur' en 'Technische Doelarchitectuur'.

Tevens wordt een strategische keuze gemaakt om de betreffende ICT-componenten wel/niet uit te besteden aan een marktpartij voor wat betreft het beheer ervan. In geval van keuze voor uitbesteding worden de daarvoor geldende procedures opgestart.

Daarnaast wordt in deze fase het 'High Level Design' (HLD) opgesteld en vastgesteld voor de nieuwe situatie. En worden nadere voorbereidingen getroffen voor de fase Implementatie zoals bijvoorbeeld een offerte opgevraagd voor benodigde nieuwe hardware/software en/of licenties.

Fase Implementatie

De fase Implementatie kenmerkt zich per deelproject in het realiseren en vaststellen van het 'Low Level Design' (LLD) waarin de oplossingsrichting op basis van het HLD nader is uitgewerkt zodat het gebouwd, geactiveerd en beheerd kan worden.

Eventuele benodigde hardware/software en/of licenties zijn besteld en geleverd. Deze nieuwe componenten worden ingebouwd en geconfigureerd zoals beschreven in het LLD. Tenslotte wordt de nieuwe situatie van ICT-componenten getest. Dit gebeurt parallel aan de huidige ICT-infrastructuur. In geval van een uitbesteding van ICT-componenten die in scope zijn van het betreffende deelproject, wordt de marktpartij geselecteerd en de afspraken met betrekking tot de dienstverlening voor operationeel beheer definitief gemaakt.

Tot slot worden voorbereidingen getroffen voor de fase migratie zoals o.a. het informeren van diverse belanghebbenden.

Fase Migratie

In deze fase vindt de feitelijke migratie plaats van de functionaliteiten (informatie- en verkeersstromen) die gebruik maken van de ICT-componenten in de huidige infrastructuur naar de ICT-componenten in de nieuwe opstelling binnen de infrastructuur.

Na een succesvolle migratie worden in deze fase de 'oude' ICT-componenten in de infrastructuur opgeruimd conform de daarvoor geldende procedures. En starten de laatste voorbereidingen voor de fase Overdracht naar Beheer.

Fase Overdracht naar Beheer

In deze laatste fase wordt de formele overdracht naar beheer gerealiseerd zodat operationeel beheer van de dienstverlening is geborgd.

In geval dat de dienstverlening van de betreffende ICT-componenten door de huidige ICT-dienstverlener gecontinueerd wordt, zal dit worden afgehandeld conform de daarvoor geldende procedures.

In geval van een uitbesteding, worden de betreffende ICT-componenten door de geselecteerde marktpartij in operationeel beheer genomen. En waarbij de huidige ICT-dienstverlener stopt met dienstverlening van de betreffende ICT-componenten.

Beheersing

De projectbeheersing voor de deelprojecten die onder het uitvoeringsplan vallen wordt gedaan op basis van de projectmanagementaspecten tijd (T), geld (G), kwaliteit (K), informatie (I), organisatie (O), communicatie (C) en risicobeheersing (R); de zogenaamde GROTICK.

Tijd/Planning

De globale planning⁵ van de deelprojecten die onder het uitvoeringsplan vallen loopt vanaf 2021 tot 2023. Het overgrote deel van de projecten wordt in de komende 2 jaar gerealiseerd. Een tweetal projecten kennen een langere doorlooptijd die tot 2023 kan doorlopen.

Per deelproject wordt de globale planning in de fase Inventarisatie nader uitgewerkt.

Geld

De informatiebeveiligingsprojecten die zijn benoemd worden gedekt door het extra toegekende budget van € 940.000,- per jaar in 2021 en 2022. Eerder genoemde flankerende projecten die voortkomen uit reguliere vervangingen, DMO of n.a.v. ontvlechting met Gemeente Westland worden gedekt door de reguliere ICT kredieten en budgetten.

Kwaliteit

Het eindresultaat van ieder deelproject, dient te voldoen aan de eisen geformuleerd in de 'Beveiligingsarchitectuur' en de daarvan afgeleide 'Technische Doelarchitectuur'. In elke fase van elk van de deelprojecten vindt een toetsing en acceptatie plaats op de op te leveren resultaten.

Informatie/Communicatie

De Raad zal via het projectenboek geïnformeerd worden over de voortgang van de realisatie van het uitvoeringsplan.

Externe belanghebbenden, waaronder de gemeente Westland, worden per deelproject (en zo nodig per fase) geïnformeerd gehouden over de voortgang en realisatie.

Organisatie

De projectorganisatie wordt conform de best practice van Prince2 uitgevoerd. Prince2 is een methode om een project volgens gestructureerde aanpak en duidelijk omschreven kader(s) te beheren. Het

⁵ Zie bijlage 4 voor de planning van het uitvoeringsplan

beschrijft procedures voor het coördineren en begeleiden van mensen en activiteiten binnen een project, maar geeft ook handvatten voor aanpassingen voor een project, wanneer het niet verloopt zoals het gepland is.

Voor de uitvoering van de deelprojecten zijn diverse disciplines (zowel intern als extern) met verschillende expertises benodigd. Niet alle disciplines zijn per deelproject met dezelfde regelmaat en mate van inzet nodig.

Risicobeheersing

Per deelproject is in de fase Inventarisatie een risicosessie voorzien, waarbij projectrisico's en beheersmaatregelen geïnventariseerd worden. Gedurende het betreffende deelproject wordt op regelmatige wijze (minimaal 1x per fase) getoetst of de risico's nog van toepassing zijn en/of er zich nieuwe risico's hebben geopenbaard.