2022

Bredase ICT kwaliteitsnormen

ICO
9-6-2022

Gemeente Breda

Inhoud

37

Inleiding

De bedrijfsvoering van de Gemeente Breda wordt direct of indirect ondersteund door informatie- en communicatiestructuur. Om de organisatie zo optimaal mogelijk te kunnen ondersteunen in hun bedrijfsvoering, is het belangrijk dat dat de informatie- en communicatietechnologie (ICT) zo optimaal mogelijk is ingericht. Dit vraagt om structuur aan te brengen en inzicht te geven in de onderlinge relaties. Er wordt dan ook wel gesproken van 'werken onder architectuur'. Elk onderdeel dat wordt toegevoegd of vervangen in de informatiearchitectuur zal moeten voldoen aan een aantal voorwaarden.

Doel

Het doel van dit document is het scheppen van randvoorwaarden waaraan leveranciers van ICT-voorzieningen zich aan conformeren. De voorwaarden hebben betrekking op de architectuur van de Bredase ICT-omgeving, beveiliging van Bredase ICT-omgeving, documentmanagement, landelijke standaarden en privacy etc.

Doelgroep

Dit document geeft aan belanghebbenden inzicht in de opbouw van ICT Infrastructuur en Informatie Architectuur. Van de lezer wordt verwacht dat hij/zij voldoende kennis heeft van de terminologie, dan wel de (gedeeltelijke) inhoud voorlegt aan een persoon die de betreffende kennis bezit.

Reikwijdte

Dit document biedt, zoals al eerder in dit document aangegeven, een beschrijving van de architectuur van de Bredase ICT-omgeving, de beveiliging van de Bredase ICT-omgeving, documentmanagement, landelijke standaarden en privacy en daarmee van de gemeente Breda. Vanwege de complexiteit van de architectuur en zijn uitgangspunten, is deze niet uitputtend. Indien specifieke details van belang zijn, dient een bijeenkomst belegd te worden met de belanghebbende en de bij de gemeente verantwoordelijke personen om inzicht te krijgen in hoe een en ander ingericht dient te worden. Tevens heeft deze bijeenkomst tot doel, te inventariseren waar mogelijk eventuele knelpunten zich voordoen in relatie tot de gemeentelijke infrastructuur en – architectuur.

DEEL A: COMPLIANCE

1. Informatiebeveiliging (BIO)

Aanleiding / Achtergrond

Gemeente Breda hecht veel waarde aan informatiebeveiliging. De gemeente Breda hanteert daarom het Strategisch beleid voor Gegevensbescherming, dit is vastgesteld door het bestuur van de gemeente. Dit beleid is in overeenstemming met de Baseline Informatiebeveiliging Overheid (BIO), de internationale standaard voor informatiebeveiliging de ISO27001/2 en de tactische uitwerking van het beleid NEN7510:2017 (de Nederlandse norm voor informatiebeveiliging ontwikkeld voor de zorgsector). Meer informatie over de BIO kan gevonden worden via https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/

Dit zijn onze uitgangspunten en eisen:

- Assuranceverklaring en/of een certificering

Aangezien de gemeente Breda veel van haar dienstverlening met behulp van leveranciers uitvoert, verwachten wij dan ook dat de leverancier zich gedurende de looptijd van het contract aantoonbaar conformeert aan de meest recente versie van de BIO of gelijkwaardig normenkader naast de geldende wet- en regelgeving.

De gemeente Breda verwacht dat er minimaal eens per drie jaar een informatiebeveiliging audit wordt uitgevoerd op het systeem en achterliggende processen. De gemeente Breda ontvangt hiervoor bij voorkeur een Assuranceverklaring en/of een informatiebeveiligingscertificering waarbij een onafhankelijk auditor verklaart dat het systeem en de achterliggende processen voldoen.
Er bestaan veel verschillende soorten Assurance, afhankelijk van de mate van de zekerheid die gegeven wordt over informatiebeveiliging. De leverancier overlegt hiervoor één van de meest voorkomende Assurance verklaringen uit de onderstaande tabel, best passend bij de situatie.

- ISO27001:2013 of hoger
- ISO27002:2013 of hoger
- ISAE3000 SOC1
- ISAE3402
- SOC Type 2 of 3
- NEN 7510
- ISO 22301
- DigiD

- Recht op het laten uitvoeren van een audit

De gemeente Breda behoudt zich altijd het recht voor om het systeem en de achterliggende processen te laten toetsen door een onafhankelijk auditor.

- Locatie dataverwerking

Naast persoonsgegevens zijn er ook andere vertrouwelijke gegevens zoals bijvoorbeeld financieel of politiek vertrouwelijke gegevens. Het uitgangspunt is dan ook dat het verwerken van gemeentelijke data plaats dient te vinden binnen de Europese economische ruimte (EER). Het verwerken van gemeentelijke data daarbuiten mag alleen plaatsvinden na toestemming van de gemeente Breda en conform de richtlijnen van de European Data Protection Board (EDPB).

- Logging

Informatiesystemen en ICT-infrastructuur genereren loginformatie voor veel activiteiten. Vanuit de BIO worden eisen gesteld aan logbestanden die worden gegenereerd, wie daar toegang toe heeft en wanneer worden deze loggegevens worden vernietigd.
Voor meer informatie zie hoofdstuk 12.4 van de BIO :
https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/

Informatiesystemen en ICT-infrastructuur dienen de mogelijkheid te hebben om audit logging weg te schrijven naar een externe logserver van de gemeente Breda om zodoende de integriteit van log data na een security incident te waarborgen.

Dit zijn uitzonderingen of bijzonderheden:
In het geval de wens is om hiervan af te wijken dient contact te worden gezocht met de team Gegevensbescherming van de gemeente Breda om de risico's hiervan te bepalen en zo nodig vast te leggen in het risicoregister.
Voor leveranciers geldt dat afwijkingen altijd gemeld moet worden bij de contracthouder.

2. Richtlijnen voor Webapplicaties

Aanleiding / Achtergrond

Een webapplicatie is een applicatie die bereikbaar is met een webbrowser of een andere client, die ondersteuning biedt voor het Hypertext Transfer Protocol (http) of de met versleuteling beveiligde vorm hiervan: https (http secure).
Voorbeelden hiervan zijn internetsites, extranetten, intranetten, software as-a-service (SaaS)-applicaties, webservices en web-api's.
Kwaadwillende vinden deze platformen steeds aantrekkelijker om digitaal aan te vallen. Om die reden is het belangrijk dat deze webapplicaties veilig zijn.

Dit zijn onze uitgangspunten en eisen:

Voor de Gemeente Breda vormen de **ICT-beveiligingsrichtlijnen voor webapplicaties** van het NCSC de norm voor het veiliger ontwikkelen, beheren en aanbieden van webapps.
Deze richtlijnen geven een overzicht van beveiligingsmaatregelen die aanbieders van webapplicaties kunnen nemen om een bepaalde mate van veiligheid te bereiken. De beveiligingsmaatregelen hebben niet alleen betrekking op de webapplicatie, maar ook op de beheeromgeving en de omringende hard- en softwareomgeving die noodzakelijk is om de webapplicatie te laten functioneren.

De gemeente Breda verwacht dat in voldoende mate wordt voldaan aan de maatregelen die in deze beveiligingsrichtlijnen worden beschreven. Deze ICT-beveiligingsrichtlijnen zijn hier te vinden : https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties .

Dit zijn uitzonderingen of bijzonderheden:
In het geval de wens is om hiervan af te wijken dient contact te worden gezocht met de team Gegevensbescherming van de gemeente Breda om de risico's hiervan te bepalen en zo nodig vast te leggen in het risicoregister.
Voor leveranciers geldt dat afwijkingen altijd gemeld moet worden bij de contracthouder.

3. Richtlijnen voor Mobiele apps

Aanleiding / Achtergrond

Mobiele apps zijn de afgelopen jaren in aantal explosief gegroeid om dienstverlening voor klanten te vereenvoudigen, contact mogelijk te maken, en nog veel meer.
Dit betekent ook dat kwaadwillende deze platformen steeds aantrekkelijker vinden om digitaal aan te vallen. Om die reden is het belangrijk dat zowel de mobiele apparaten als de apps die daarop draaien veilig zijn.

Dit zijn onze uitgangspunten en eisen:

Voor de Gemeente Breda vormen de ICT-beveiligingsrichtlijnen voor mobiele apps van het NCSC de norm voor het veiliger ontwikkelen, beheren en aanbieden van apps voor mobiele apparaten. Deze richtlijnen richten zich op de beveiliging van mobiele apps, dat wil zeggen de overdraagbare programmatuur die op een mobiel apparaat wordt uitgevoerd. De richtlijnen richten zich *niet* op de backend aan de serverzijde van de app of op de configuratie van het mobiele apparaat zelf. Zie hiervoor de ICT beveiligingsrichtlijnen voor webapplicaties (par. Richtlijnen voor Webapplicaties)
De gemeente Breda verwacht dat in voldoende mate wordt voldaan aan de maatregelen die in deze beveiligingsrichtlijnen worden beschreven. Deze ICT-beveiligingsrichtlijnen zijn hier te vinden : https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-mobiele-apps.

Opm. Als de mobile app met de back-end communiceert over https, dan kan de serverzijde worden gezien als webapplicatie. Hiervoor kan worden uitgegaan van de ICT beveiligingsrichtlijnen voor webapplicaties. Mobiele apparaten vallen meestal buiten het beheer van de uitgevende organisatie en kunnen dan niet centraal worden beveiligd.

Dit zijn uitzonderingen of bijzonderheden:
In het geval de wens is om hiervan af te wijken dient contact te worden gezocht met de team Gegevensbescherming van de gemeente Breda om de risico's hiervan te bepalen en zo nodig vast te leggen in het risicoregister.
Voor leveranciers geldt dat afwijkingen altijd gemeld moet worden bij de contracthouder.

4. Privacy (AVG)

Aanleiding/ Achtergrond
De gemeente Breda heeft de eisen en verplichtingen die voortvloeien uit de
De Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) uitgewerkt in het Strategisch Beleid voor Gegevensbescherming Breda.

AVG moet gevolgd worden t.a.v. het delen en koppelen van gegevens. DWZ Grondslag, doelbinding, proportionaliteit, subsidiariteit moeten in orde zijn. Vaak is een DPIA nodig voor er data gekoppeld mogen worden of gedeeld met een andere partij (ook intern).

Dit zijn onze uitgangspunten en eisen:

- Leveranciers zijn aantoonbaar compliant met het Strategisch gegevensbeschermingsbeleid van de gemeente Breda conform hoofdstuk 1 compliance en voldoen aan de gegevensbeschermingseisen die aan de betreffende leveranciers, ketenpartners en andere samenwerkingspartijen worden gesteld vanuit Inkoop of een organisatieonderdeel.

- Leveranciers signaleren proactief risico's voor de beveiliging van informatie en de omgang met (persoons)gegevens
- Leveranciers melden datalekken en (mogelijke) informatiebeveiligingsincidenten, conform de contractuele afspraken, direct bij de gemeente Breda.

Als de leveranciers in opdracht van de gemeente Breda persoonsgegevens verwerken en er sprake is van een relatie van verwerker (leverancier) en verwerkingsverantwoordelijke (gemeente Breda) dan leggen de gemeente Breda en de leverancier(s) specifieke afspraken vast in een verwerkersovereenkomst. De gemeente Breda hanteert hiervoor de VNG-modelverwerkersovereenkomst.
Meer informatie: https://vng.nl/nieuws/standaard-verwerkersovereenkomst-gemeenten-wordt-verbindend

Dit zijn uitzonderingen of bijzonderheden:

In het geval de wens is om hiervan af te wijken dient contact te worden gezocht met het team Gegevensbescherming van de gemeente Breda om de risico's hiervan te bepalen en zo nodig vast te leggen in het risicoregister.

- Voor leveranciers geldt dat afwijkingen altijd gemeld moet worden bij de contracthouder.
- In het geval dat er sprake is van gezamenlijke verantwoordelijkheid (gemeente Breda en leverancier) of van een zelfstandige verantwoordelijkheid van de leverancier, dient contact gezocht te worden met het team Gegevensbescherming, om nadere afspraken hierover vast te leggen.

5. Authenticatie en Identificatie externe dienstverlening

Aanleiding/ Achtergrond

De Wet Digitale Overheid (WDO) regelt dat publieke dienstverleners verplicht zijn om identificatiemiddelen van het betrouwbaarheidsniveau 'substantieel' of 'hoog' te gebruiken om toegang te geven tot online-diensten waarbij de overheid deze betrouwbaarheidsniveaus nodig vindt.
Hiermee wordt bedoeld dat burgers elektronische identificatiemiddelen (eID) krijgen met een hogere mate van betrouwbaarheid dan het huidige DigiD. Deze identificatiemiddelen geven publieke dienstverleners meer zekerheid over iemands identiteit. De wet stelt daarnaast open standaarden verplicht.

Dit zijn onze uitgangspunten en eisen:

DigiD

De gemeente Breda is aangesloten bij DigiD waardoor het mogelijk is dat burgers zich identificeren met behulp van DigiD voor elektronische dienstverlening.
De gemeente Breda wordt hiervoor elk jaar door een onafhankelijke auditor geaudit zoals gepubliceerd op de Logius website onder 'Norm ICT-beveiligingsassessments DigiD'.
In het geval van SaaS-oplossingen kan het zijn dat de DigiD aansluiting bij de leverancier wordt gerealiseerd en is de leverancier en eventuele sub leveranciers daarmee ook onderdeel geworden van deze jaarlijkse DigiD audit.
De gemeente Breda verwacht van de leverancier dat hiervoor elk jaar tijdig een TPM-verklaring (in pdf/a formaat) wordt aangeleverd waaruit blijkt dat aan de op dat moment geldende DigiD normen wordt voldaan. De kosten voor deze TPM-verklaring en eventueel hieruit voorvloeiende wijzigingskosten dienen te worden ondergebracht in de aanbieding/ overeenkomst.

eHerkenning

De gemeente Breda ondersteunt online identificeren via eHerkenning voor bedrijven en organisaties. In het geval dat dienstverlening aan organisaties via een SaaS-oplossingen wordt aangeboden, verwacht de gemeente Breda dat de leverancier(s) deze vorm van identificatie ondersteunen op het niveau EH3.

eIDAS

Uit de eIDAS verordening volgt dat de gemeente Breda verplicht is om Europees erkende inlogmiddelen te accepteren voor haar digitale dienstverlening.
Dit houdt in dat, in het geval dat Nederlandse burgers en bedrijven op betrouwbaarheidsniveau substantieel of hoog worden geaccepteerd (via DigiD of eHerkennning), ook eIDAS moet worden ondersteunt.
De eIDAS dienstverlening komt naast de bestaande DigiD en eHerkenning middelen en om te voldoen aan de eIDAS-verplichting voor online toegang dient een aansluiting op een eherkenning makelaar met minimaal koppelvlak versie 1.11 te worden gerealiseerd om daarmee toegang te verkrijgen op de eIDAS-infrastructuur.

Dit zijn uitzonderingen of bijzonderheden:

In het geval de wens is om hiervan af te wijken dient een melding te worden gemaakt bij het team Gegevensbescherming.
Voor leveranciers geldt dat afwijkingen altijd gemeld moet worden bij de contracthouder welke contact dient op te nemen met het team Gegevensbescherming.

6. Authenticatie en Identificatie interne bedrijfsvoering

Aanleiding / Achtergrond
Voor medewerkers en derden welke voor de gemeente Breda werkzaamheden uitvoeren is het belangrijk dat toegang tot gegevens en systemen waarvoor zij gemachtigd zijn op de juiste manier wordt verleend. Hiervoor is het noodzakelijk dat we de identiteit van de medewerker en eventueel het apparaat vaststellen en de juiste rechten hieraan toekennen.

Dit zijn onze uitgangspunten en eisen:

Active Directory

Binnen de gemeente Breda maken we gebruik van Microsoft Active Directory (AD) als authenticatiebron.
De Active Directory is ingericht op basis van één domein (breda.nl) en alle medewerkers met een loginaccount op het netwerk zijn hierin aangemaakt.
Het domein maakt gebruik van het functionaliteitsniveau: Windows Server 2016.

Azure AD

Voor het authentiseren van gebruikers en het autoriseren en toekennen van een rol aan gebruikers in geval van SaaS-applicaties, wordt gebruik gemaakt van Microsoft Azure AD. Het beschikbaar stellen van rechten aan een rol gebeurt binnen de betreffende SaaS-applicatie zelf.

Multi Factor Authenticatie (MFA)

Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van multi factor authenticatie (MFA). Het gebruik van Microsoft Authenticator is daarbij leidend.

802.1x apparaat authenticatie

De toegang tot het bedrijfsnetwerk van de gemeente Breda voor draadloze WiFi en bekabelde ethernet netwerken wordt beheerd met behulp van het 802.1x protocol. Van de opdrachtgever wordt verwacht dat zij voor de geleverde producten en diensten deze standaard ook ondersteunen, mits van toepassing. De door de opdrachtgever ondersteunde authenticatie protocollen welke binnen het 802.1x protocol gebruikt worden zijn op zijn minst EAP-TLS en PEAP-MSCHAPv2. Door de gemeente Breda wordt per opdracht het daadwerkelijk gebruikte authenticatie protocol bepaald op basis van gewenste beveiliging en beheersbaarheid binnen het product.

Role Based Acces Control

Toegang tot data/informatie is ingericht met autorisaties die zijn gebaseerd op rollen en functiescheiding RBAC (Role Based Access Control). Individuen worden niet rechtstreeks geautoriseerd in informatiesystemen, maar krijgen uitsluitend rechten door een vorm van groepslidmaatschap, op basis van de rol die ze hebben binnen een organisatie of bedrijfsproces. Ook de permissies op objecten/functies in informatiesystemen worden gegroepeerd in rollen.

Dit zijn uitzonderingen of bijzonderheden:
Er dient rekening gehouden te worden met een (technische) implementatie op basis van *Security-by-design.* Concreet wordt dan ook alleen voor het te koppelen informatiesysteem en/of de toepassing relevante informatie blootgesteld om authenticatie en autorisatie te realiseren. Indien gewenst is een document met specifieke richtlijnen op te vragen.

In het geval de wens is om hiervan af te wijken dient een melding te worden gemaakt bij het Architectuurboard.
Voor leveranciers geldt dat afwijkingen altijd gemeld moet worden bij de contracthouder welke contact dient op te nemen met het Architectuurboard.

7. Toegang Leveranciers

Aanleiding / Achtergrond

Zoals in de BIO (https://bio-overheid.nl/) onder paragraaf 9.4 is beschreven behoren er met leveranciers afspraken te worden gemaakt op het gebied van informatiebeveiliging om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie.

Dit zijn onze uitgangspunten en eisen:

Remote toegang leveranciers in geval van 'on premises' oplossingen.
Indien de systemen/data worden gehost bij de gemeente Breda (on premises) kan de opdrachtnemer voor eventuele ondersteuning, een leverancier op afstand toegang geven middels de Teamviewer applicatie waarmee de werkplek van de applicatiebeheerder kan worden overgenomen. Onder diens account, actief toezicht en verantwoordelijkheid kunnen dan eventuele werkzaamheden vervolgens gedaan worden. Een aantal zaken waar rekening mee gehouden moet worden:

- De leverancier krijgt geen toegang tot de serverconsole van afstand,
- De leverancier krijgt alleen toegang tot de serverconsole met ondersteuning van een senior ICT-beheerder van het team ICT Services van de afdeling Servicecentrum op de locatie van de gemeente Breda.

Remote toegang leveranciers in geval van 'SAAS' oplossingen.
Indien de systemen/data die niet worden gehost bij de gemeente Breda (Cloud) kan de opdrachtnemer voor eventuele werkzaamheden zich toegang verschaffen tot de systemen en data welke zich bevinden bij opdrachtnemer om de beheertaken conform de overeenkomst uit te voeren, mits de Gibit en ICT-kwaliteitsnormen van de gemeente Breda zijn geaccepteerd.
Op aanvraag levert opdrachtnemer een overzicht aan welke medewerkers van opdrachtnemer op welke moment (datum, tijdstip) toegang tot de systemen en data van opdrachtgever heeft gehad.

Dit zijn uitzonderingen of bijzonderheden:

In het geval de wens is om hiervan af te wijken dient contact te worden gezocht met de team ICTS van de gemeente Breda om de risico's hiervan te bepalen en zo nodig vast te leggen in het risicoregister.
Voor leveranciers geldt dat afwijkingen altijd gemeld moet worden bij de contracthouder.

8. Toegankelijkheid (Webrichtlijnen)

Aanleiding / Achtergrond
Miljoenen Nederlanders hebben één of meerdere beperkingen. Denk daarbij aan mensen die blind of slechtziend zijn of kleurenblind; doof of slechthorend; motorisch beperkt of zwakbegaafd; autistisch; laaggeletterd. En deze groep groeit. Het aantal ouderen groeit, er komen meer migranten die de Nederlandse taal niet goed machtig zijn.

In Nederland willen we dat openbare voorzieningen toegankelijk zijn voor alle burgers. Want ieder mens heeft het recht om gewoon als ieder ander mee te doen in de maatschappij.

Voor digitale voorzieningen is het niet anders. In onze samenleving kun je bijna niet meer zonder het internet en computers. En veel mensen willen dat ook helemaal niet missen. Daarom is digitale toegankelijkheid belangrijk, én verplicht voor alle overheidsinstanties. Als websites en apps goed in elkaar zitten kunnen ze door iedereen worden gebruikt, ook door bezoekers met een beperking. En dan kan echt iedereen meedoen.

Dit zijn onze uitgangspunten en eisen:
Gemeente Breda moet voldoen aan de toegankelijkheidseisen. Zie www.digitoegankelijk.nl voor de meest actuele informatie.
Voor leveranciers geldt dat afwijkingen altijd gemeld moet worden bij de contracthouder.

9. Standaarden

Aanleiding / Achtergrond

Ter bevordering van veilige en eenvoudige informatie-uitwisseling conformeren wij ons aan het “Pas toe of leg uit” beleid van het Forum Standaardisatie, zoals ook bekrachtigd in de Wet Digitale Overheid.

Daarnaast conformeren we ons aan de standaarden die vallen onder de GEMMA architectuur (GEMeentelijke Model Architectuur). Met deze standaarden wordt uitwisseling van gegevens tussen organisaties en systemen makkelijker.

Dit zijn onze uitgangspunten en eisen:

- Bij aanschaf van een ICT-product of ICT-dienst verzekeren wij onszelf dat deze gebruikt maakt van de verplichte standaarden van het Forum Standaardisatie.
- Bij aanschaf van een ICT-product of ICT-dienst streven wij naar het gebruik van de aanbevolen standaarden van het Forum Standaardisatie.
- Om te bepalen welke standaarden relevant zijn maken we gebruik van de beslisboom beslisboom 'Pas toe of leg uit'-lijst.
- Indien het een website betreft, en er standaarden moeten worden gebruikt die in lijst van 41 verplichte standaarden staan (www.forumstandaardisatie.nl/open-standaarden/verplicht), dan dient de website aantoonbaar hiervan gebruik te maken en op de juiste manier te hebben ingesteld.
  Dit dient te worden aangetoond met de online testtool van het Platform Internetstandaarden, zie hiervoor: https://internet.nl/.
- Standaarden voor de lokale overheid staan op www.gemmaonline.nl. Deze standaarden hebben altijd de voorkeur boven leveranciersstandaarden of maatwerkoplossingen. Leveranciers dienen de lifecycle van de standaarden te volgen en binnen uiterlijk 1 jaar nieuwe versies van standaarden te ondersteunen, of sneller indien dit wettelijk of contractueel verplicht is.

Dit zijn uitzonderingen of bijzonderheden:

Hier wordt van af geweken indien er een zwaarwegend business belang is, en mits de risico’s acceptabel zijn. Er dient dan een transitieplan met tijdlijn opgesteld te worden. Indien leveranciers wensen af te wijken van standaarden dienen zij dit uitdrukkelijk te melden tijdens het inkooptraject. De architectuurboard en Team Gegevensbescherming dienen allebei goedkeuring te verlenen.

DEEL B: BASIS KWALITEITSNORMEN

10. Devices en Werkplekconcepten

Aanleiding / Achtergrond

Gemeente Breda hanteert een mobiel tenzij beleid. De medewerk heeft daarbij de beschikking over een Azure AD joined laptop (CYOD-werkplek) voor standaard Office werk en het benaderen van cloud toepassingen. On premises applicaties worden beschikbaar gesteld via een AD-domain joined virtuele werkplek (virtuele BWP).

Dit zijn onze uitgangspunten en eisen:

Configuratie

De basisconfiguratie van alle werkplekken ziet er als volgt uit: ·

- Windows 10 Enterprise 64 bits Nederlands (GA channel),
- Office 365 ProPlus (Semi-Anual Enterprise Channel),
- Microsoft Edge
- Microsoft EndPoint Manager
- Microsoft Defender for Endpoint

Voor de virtuele BWP (multi-session) zijn de volgende configuratieonderdelen additioneel aanwezig:

- Microsoft .Net Framework 3.5 met Service Pack 1 en de laatste versie van Microsoft .Net Framework 4.x horende bij Windows 10.
- Microsoft Visual C++ Redistributable (laatst ondersteunde versies)
- Adobe Acrobat Reader DC (meest recente Nederlandse versie),
- Oracle Client 19.x.

Verder geldt dat:

- Een gebruiker lid is van de lokale Users groep. Hierdoor heeft hij beperkte mogelijkheden om activiteiten uit te voeren,
- Rechten op het bestandssysteem zijn beperkt.

De CYOD-werkplek heeft minimaal de volgende systeemconfiguratie:

- Quad core processor,
- SSD van 128 Gb,
- 8 GB Memory.

Softwaredistributie

Er wordt gebruikt gemaakt van software distributie voor uitrol van applicaties. Ook eventuele updates van applicaties zullen op deze manier worden verspreid. Het proces

intake, scripting, test en *uitrol* kent een gemiddelde doorlooptijd van 3-4 weken, houd hier voldoende rekening mee met aanleveren van software dan wel updates.

Dit zijn uitzonderingen of bijzonderheden:

- In het geval de wens is om hiervan af te wijken dient contact te worden gezocht met de team ICTS van de gemeente Breda om de risico's en impact hiervan te bepalen.

- We hanteren een actief beleid op het tegengaan van Shadow IT. Daarom blokkeren wij sommige online toepassingen waarvoor wij als gemeente een standaardoplossing bieden.

11. Lifecycle & Release Management

Aanleiding/Achtergrond

Om een stabiele, veilige en beheersbare omgeving te kunnen garanderen vindt er actief Life Cycle Management plaats op ICT en informatiesystemen welke in gebruik zijn binnen onze organisatie. Hiermee blijven we qua technologie en functionaliteiten up-to-date, en voorkomen we veiligheidsrisico's.

Dit zijn onze uitgangspunten en eisen:

- Onze systemen zijn maximaal 1 major versie oud.
- Systemen die End-of-Life dan wel End-of-Support dreigen te raken worden voor het verlopen van de betreffende termijn vervangen door een nieuwe versie of andere oplossing.
- We laten ons door de leverancier actief informeren over nieuwe softwareversies en (beveiligings) updates.
- Er is een intern en extern proces aanwezig om kritieke updates binnen een acceptabele doorlooptijd te implementeren welke recht doet aan het risico dat gelopen wordt.

Dit zijn uitzonderingen of bijzonderheden:

Hier wordt van af geweken indien er een zwaarwegend business belang is, en mits de risico's acceptabel zijn. Er dient dan een transitieplan met tijdlijn opgesteld te worden. De architectuurboard en Team Gegevensbescherming dienen allebei goedkeuring te verlenen en bepalen de doorlooptijd welke recht doet aan het te lopen risico.

DEEL C: OVERIGE KWALITEITSNORMEN

12. Infrastructuur: Hosting

Aanleiding / Achtergrond

De Gemeente Breda maakt gebruik van server virtualisatie voor applicatie en informatiesystemen welke on premises ontsloten (dienen te) worden. De betreffende omgeving is gevirtualiseerd op basis van Microsoft Hyper-V.

Dit zijn onze uitgangspunten en eisen:

Het besturingssysteem dat gebruikt wordt voor de virtuele machines:

- Microsoft Windows Server 2022 64-bits (Engelse versie).

De overige standaard software die geïnstalleerd is op een server:

- Microsoft Endpoint Manager,
- Microsoft Defender for Endpoint,
- Microsoft System Center Operations Manager agent,
- Microsoft Edge.

Voor de applicaties aan de serverkant gelden de volgende specificaties:

- De applicatie moet draaien als Windows Service,
- De applicatie moet op de D: schijf geïnstalleerd worden,
- De installatiedirectory moet door Gemeente Breda bepaald kunnen worden,
- De serverinrichting vindt op een dusdanige manier plaats dat componenten binnen een applicatie (webserver, database, et cetera) op gescheiden servers zijn geïnstalleerd.

Verder geldt dat voor iedere productieomgeving een gescheiden en representatieve acceptatieomgeving aanwezig moet zijn waarop wijzigingen binnen de onderliggende ICT-infrastructuur, koppelingen en de applicatie componenten zelf getest kunnen worden.

Dit zijn uitzonderingen of bijzonderheden:

In 2020 is de Bredase Cloudstrategie vastgesteld waarin de beweging naar een hybride Cloud is bekrachtigd. Microsoft Azure maakt hier een wezenlijk onderdeel vanuit en gaat op termijn voor een groot gedeelte de on premises omgeving vervangen. Nieuwe implementaties binnen Azure tijdens deze overgang fase dienen situationeel gereviewd te worden door een ICT-architect.

13. Infrastructuur: Networking

Aanleiding / Achtergrond

Goede connectiviteit draagt bij aan een optimale informatievoorziening. Beschikbaarheid, integriteit en veiligheid zijn essentieel daarin en komen tot uiting bij specifiek te maken inrichtingskeuzes.
Of het nu gaat om het ontsluiten van webservices, het aanbieden van een WIFI-netwerk of het koppelen met leveranciers, deze 3 thema's zijn van belang.

Dit zijn onze uitgangspunten en eisen:

- Gegevensuitwisseling is versleuteld.
- Gegevensuitwisseling tussen netwerkzones verloopt via een firewall en is zo specifiek mogelijk gedefinieerd.
- Gegevensuitwisseling tussen vertrouwde en niet vertrouwde netwerkzones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.
- Netwerktoegang is alleen mogelijk na succesvolle authenticatie (Network Access Control/802.1x).
- Webservices worden altijd ontsloten via een reverse proxy.
- Kritieke netwerkcomponenten zijn redundant uitgevoerd.

Dit zijn uitzonderingen of bijzonderheden:

Meer informatie:

- Handreiking hardening beleid https://www.informatiebeveiligingsdienst.nl/product/hardening-beleid-voor-gemeenten/
- Voor VPN-verbinding hanteren we bepaalde beveiligingsrichtlijnen. We maken hierbij een onderscheid tussen standaard- en vertrouwelijke data betreft het beveiligingsniveau van de verbinding. Indien dit van toepassing is kunnen de richtlijnen opgevraagd worden.

Uitzonderingen dienen beoordeelt te worden door een ICT-architect.

14. Infrastructuur: Databases

Aanleiding / Achtergrond

Binnen de Gemeente Breda voeren we de volgende 3 database standaarden, in volgorde van voorkeur;

- Microsoft SQL Server;
- PostgreSQL;
- Oracle Database Server.

Dit zijn onze uitgangspunten en eisen:

Microsoft SQL Server
Onze standaard op MS SQL gebied is Microsoft SQL Server 2019 met de laatste Service Pack. De collation die gebruikt is voor de installatie van de SQL instances is SQL_Latin1_General_CP1_CI_AS.

PostgreSQL
Onze standaard op PostgreSQL gebied is 11 welke draait op een standaard Windows server. De collation die gebruikt is voor de installatie van de PostgreSQL instances is UTF-8. PostGIS Spatial data extender is als standaardcomponent nodig

Oracle
Onze standaard op Oracle gebied is Oracle Database Server 19c Enterprise Editie welke draait op een standaard Windows server.
De collation die gebruikt is voor de installatie van de Oracle instances is AL32UTF8.

Indien een leverancier een applicatie levert waar een Oracle, SQL Server dan wel andere database onderligt, dan dient deze volledig gedocumenteerd en toegankelijk te zijn. Dit is nodig om de data snel en juist te kunnen benaderen voor mogelijke opname in het gemeentelijk datawarehouse.

De documentatie moet aan de volgende eisen te voldoen:

- Het volledige datamodel dient gedocumenteerd te zijn. Dus ook objecten als:
    - Tabellen, alle velden inclusief joins, constraints en indexen,
    - Views,
    - Stored procedures,
    - Functions,
    - Schema's,
    - Authenticatie,
    - Etc.

- De leverancier zorgt ervoor dat de documentatie actueel is en dat deze actief wordt bijgehouden. De documentatie wordt bij voorkeur vastgelegd in de database zelf (door bijvoorbeeld gebruik te maken van de ‘extended properties’ van de objecten) in plaats van in losse documenten.
- Deze documentatieplicht beperkt zich tot de database laag die gebruikt wordt voor rapportage dan wel bevraagd zou kunnen worden indien de data geladen zou worden in het gemeentelijk datawarehouse.

Dit zijn uitzonderingen of bijzonderheden:

15. Infrastructuur: Communicatiediensten (Telefonie/Mail)

Aanleiding / Achtergrond

Binnen de gemeente Breda gebruiken wij Microsoft Teams om het (vaste) zakelijke telefonieverkeer te regelen. Door middel van Direct Routing-technologie zijn de nummerblokken gekoppeld aan Microsoft Teams.
Als KCC-oplossing gebruiken wij momenteel nog een oplossing van Mitel.

Exchange Online wordt gebruikt als standaard e-mailvoorziening. Alle inkomende en uitgaande mail worden met Microsoft Defender voor Office 365 gescand op malafide URL's en bijlage.

Dit zijn onze uitgangspunten en eisen:

Het toepassen van onderstaande standaarden zorgt ervoor, dat de e-mail vanuit een organisatie als legitiem herkenbaar is en er wordt voorkomen, dat criminelen uit naam van de organisatie e-mails kunnen versturen.

De betreffende standaarden staan ook op de "Pas-toe of Leg-uit-lijst" van het Forum Standaardisatie van de Nederlandse Overheid. Meer informatie : Hoofdstuk 9 Open Standaarden Gegevensuitwisseling.

- *Internet standaarden*
- *TLS (beveiligde verbindingen)*
- *DNSSEC (domeinnaambeveiliging)*
- *SPF, DKIM en DMARC (anti-phishing/-spoofing)*
- *STARTTLS en DANE*: standaarden voor de beveiliging van mailverkeer middels encryptie.
- Het instellen van 'strikte policies' voor SPF en DMARC.
  Zolang dat niet is ingesteld weet de ontvanger nog niet wat te doen met verdachte e-mail.
  (Opm: Actieve policies zijn ~all en –all voor SPF, en p=quarantine en p=reject voor DMARC).

Indien een applicatie vanuit een Cloud omgeving e-mails stuurt namens het breda.nl domein, (bijvoorbeeld no-reply@breda.nl) en hierbij gebruik maakt van de e-mailomgeving van de hostingpartij, dan is dit alleen mogelijk indien de bovenstaande internet standaarden worden toegepast.

bron: Forum standaardisatie – Bestrijding e-mail fraude
bron: NCSC – Factsheet 'bescherm domeinnamen tegen phishing'
bron: IBD – Factsheet 'E-mail authenticatie'

16. Architectuur: Digitaal Samenwerken (Office 365)

Aanleiding / Achtergrond

Gemeente Breda maakt gebruik van Microsoft Office 365 als generiek Digitaal Samenwerkingsplatform en voor generieke kantoorautomatiseringstoepassingen.

Hierbij wordt gebruik gemaakt van het Framework-VNG licentiemodel, dit model bestaat uit juridische en commerciële voorwaarden op basis van het M365 E3 licentie model van Microsoft, met Microsoft 365 E5 Security en Microsoft 365 E5 Compliance. Meer informatie staat hier: https://www.vngrealisatie.nl/producten/gt-microsoft

Dit zijn onze uitgangspunten en eisen:

- De tenant heeft als naam BredaseCloud en is gekoppeld aan onze on premises Active Directory. Authenticatie op deze omgeving vindt plaats via een Azure AD koppeling waarbij onze Basiswerkplekken een single sign-on functionaliteit hebben en vanaf een externe werkplek ingelogd moet worden met AD credentials.
- Voor persoonlijke opslag van documenten wordt Onedrive gebruikt. Op Onedrive is extern delen uitgeschakeld.
- Voor digitaal samenwerken en communiceren wordt Microsoft Teams gebruikt, op teams is externe toegang op aanvraag mogelijk.
- Voor interne publishing (intranet/extranet/themasites/subsites) toepassingen wordt Microsoft Sharepoint gebruikt, op teams is externe toegang op aanvraag mogelijk.
- Het gebruiken van “externe” apps in O365 is niet toegestaan.
- Voor het gebruik van Office 365 zijn interne kaders en richtlijnen van kracht, hier dienen leveranciers zich ook aan te houden.

- Bij vergelijkbare functionaliteit heeft het gebruik van Office 365 voorrang. Op deze manier werken we aan rationalisatie en blijven we “in control” en voorkomen Shadow IT.

Dit zijn uitzonderingen of bijzonderheden:

- Geef het nadrukkelijk aan in uw aanbieding als uw oplossing gebruik maakt of wenst te maken van functionaliteit van Office 365.
- Geef het nadrukkelijk aan als u afwijkingen ziet op bovenstaande, architecten van gemeente Breda zullen in deze gevallen besluiten over afwijkingen.

17. Architectuur: Datagedreven sturen

Aanleiding / Achtergrond

De gemeente Breda groeit naar een datagedreven organisatie. In toenemende mate worden data gebruikt als feiten-onderbouwing ten behoeve van beslissingen en (geautomatiseerde) proces-uitvoer. De principes waaronder dat gebeurt zijn verwoord in de Informatiestrategie 2018-2020. Ambities op het gebied van (stedelijke) digitalisering staan bij voorbeeld in het Masterplan Digitalisering.

Om een stevige basis te leggen voor het datagedreven sturen, bouwt de gemeente Breda hard aan haar data-fundament. Werken onder architectuur is daarbij een belangrijk uitgangspunt.

Dit zijn onze uitgangspunten en eisen:

- Conform de Cloudstrategie werken we met de Cloud als toekomst in ons achterhoofd. Concepten, ontwerpen en producten dienen zoveel mogelijk Cloud-based of Cloud-ready (makkelijk over te brengen naar de cloud) te zijn.
- Bij het ontwikkelen (zowel aan de ETL kant, in de datawarehouses als aan de visualisatiekant) wordt het hergebruiken van bestaande code en configuraties zo makkelijk mogelijk gemaakt. Documentatie is toegankelijk voor alle “data-betrokkenen” en up-to-date.
- Bij alle datavraagstukken kijken we eerst naar het inzetten van onze eigen bestaande kerncomponenten (o.a. Datawarehouses, ETL tooling, Visualisatietooling, API tooling) en uiteraard ook databronnen. We willen “wildgroei” voorkomen en focus aanbrengen op onze kennisgebieden en in te zetten techniek.
- Data heeft altijd een eigenaar, welke verantwoordelijk is voor de kwaliteit van de gegevens en het juiste gebruik en beheer daarvan.
- Proceseigenaars zien erop toe dat gegevens die binnen een proces worden ingewonnen of geactualiseerd, op een vastgelegde wijze (middels een gegevensleveringsovereenkomst) worden opgeslagen.

Dit zijn uitzonderingen of bijzonderheden:

18. Architectuur: Zaakgericht werken

Aanleiding / Achtergrond

Met Zaakgericht Werken streven we een gestructureerde manier van het afhandelen van klantvragen en klantprocessen voor burgers en bedrijven na. Zaken worden op een eenduidige wijze vastgelegd en afgehandeld, waardoor de kwaliteit van de dienstverlening stabiel is en wet- en regelgeving geborgd. Alle informatie en documenten die bij een zaak horen worden opgeslagen in een Zaakdossier. Informatie is makkelijk terug te vinden en de wijze waarop besluitvorming heeft plaatsgevonden is goed te herleiden. De gemeente heeft inzicht in wat er speelt of speelde rondom een burger of bedrijf en kan hierdoor slim schakelen. Ook de archivering en vernietiging van de Zaakdossiers is geborgd.

Dit zijn onze uitgangspunten en eisen:

- Klantprocessen en klantvragen worden zaakgericht afgehandeld. Het generieke Zaaksysteem Djuma (Circle software) is hierin leidend. Indien er een sluitende business case voor is zetten we zgn Taakspecifieke procesapplicaties in (bijvoorbeeld een Burgerzaken- of Vergunningenapplicatie).

- Indien Zaakafhandeling plaatsvindt in een andere applicatie dan het generieke Zaaksysteem, dienen zaakgegevens en zaakdossier via een standaard koppeling op basis van Zaak-DMS Services (https://www.gemmaonline.nl/index.php/Zaak-_en_Documentservices) overgezet te worden naar het Zaaksysteem, oplossingen dienen deze te ondersteunen. In de toekomst worden de Zaak-DMS Services vervangen door de API-standaarden: https://www.gemmaonline.nl/index.php/API-standaarden, oplossingen dienen ook deze standaarden te ondersteunen.

- Ook de processen rondom Bestuurlijke Besluitvorming, de afhandeling van klantcontacten en klantpost vinden plaats in het generieke zaaksysteem.

- Voor Zaaktypenregistratie, archivering en vernietiging van Zaakdossiers is het Document Structuur Plan (DSP) leidend. Overbrenging naar het E-Depot (met TMLO metadatering) verloopt zo veel mogelijk via het Zaaksysteem. Dit om te voorkomen dat iedere applicatie een aparte koppeling met het E-Depot moet realiseren.

Dit zijn uitzonderingen of bijzonderheden:

- Indien het niet lukt om een Taakspecifieke applicatie en het generieke Zaaksysteem te koppelen op basis van standaarden, is het bij uitzondering mogelijk om de taak specifieke applicatie als archiefsysteem te gebruiken. De randvoorwaarden rondom archivering dienen dan wel gewaarborgd te zijn. Team Documentmanagement verzorgt in dit geval de toetsing. Deze toetsing gebeurt op basis van een set eisen uit de NEN-ISO 16175-1. De gemeentearchivaris dient de uiteindelijke toestemming te verlenen of een taakspecifieke applicatie gebruikt kan worden als archiefsysteem.

19. Architectuur: Geografisch Informatiesysteem (GIS)

Aanleiding / Achtergrond

Gemeente Breda maakt gebruik van Esri ArcGIS als basis het generieke platform voor Geo-informatie en GIS-functionaliteiten. Hiervoor zijn beschikbaar

- On premises desktop en servercomponenten in de Bredase cloud
- WebGIS
- Online componenten (SaaS)
- Mobiele apps

Het platform ondersteund de volgende functies: Geo data creatie, analyse, visualisatie en distributie middels REST services.

Dit zijn onze uitgangspunten en eisen:

Gebruik maken van dit platform heeft de voorkeur boven het gebruik van eigen Geo of GIS oplossingen. Met dit platform kan Geo-informatie op een eenduidige manier aangeboden en beheerd worden en is hergebruik van Geo-informatie in andere processen mogelijk.

Dataopslag is in PostgreSQL inclusief PostGIS.
De dataset en kenmerken dienen gemetadateerd te worden.

Het on premises platform is beschikbaar via https://geo.breda.nl

Dit zijn uitzonderingen of bijzonderheden:

Indien gebruik gemaakt wordt van de GIS architectuur van Breda altijd de afzonderlijk te licentiëren componenten en functionaliteiten aangeven

20. Integratie

Aanleiding / Achtergrond

Dit hoofdstuk beschrijft hoe Gemeente Breda om wil gaan met berichtenverkeer tussen systemen. Hierbij is een gestandaardiseerde aanpak gewenst, die de stad het vermogen geeft om wendbaar te kunnen zijn en snel te kunnen anticiperen/adapteren op veranderende behoeften.

Hergebruik en rationalisatie zijn nodig om de complexiteit van het berichtenverkeer te reduceren, de kwaliteit van de gegevensuitwisseling te verbeteren en beheer en onderhoud meer beheersbaar te maken.
De voorkeursvolgorde bij een nieuwe berichtstroom is respectievelijk: hergebruik bestaande integratie, toepassen van overheidscomponenten, inzetten van (standaard-)producten, zelfbouw.

Gemeente Breda vindt het belangrijk dat leveranciers actief samen met en/of namens gemeenten meebewegen met landelijke door gemeenten opgezette initiatieven, zoals Common Ground en Haal Centraal.

Dataclassificatie, privacy risico's en de aard van gegevensverwerking zijn leidend voor de regiebehoefte van de gemeente en daarmee de gewenste samenstelling van integratie.

Voor gestandaardiseerde integraties worden de volgende tools ingezet:

- API Gateway: beveiligen en monitoren van berichtenverkeer via webservices/API's. De API gateway van de gemeente wordt verplicht als tussenlaag ingezet wanneer een on-premises applicatie koppelt met een cloud applicatie. Ook bij cloud-2-cloud koppelingen is deze verplicht, tenzij daar uitzonderingen gelden die verder in dit hoofdstuk zijn beschreven. Een API gateway heeft geen invloed op “API keys” en berichtinhoud, welke onder het functioneel beheer vallen.
- nterprise Service Bus (ESB): routeren, hergebruiken, ontkoppelen, transformeren van berichtenverkeer. De Enterprise Service Bus is bedoeld voor generieke processen. Applicaties hebben vaak ook een eigen Service Bus.
- DigiKoppeling adapter: voor asynchroon berichtenverkeer met landelijke voorzieningen dient verplicht gebruik gemaakt te worden van de DigiKoppeling Adapter en aanverwante standaarden. DigiKoppelingen m.b.t. basisgegevens verlopen via de DigiKoppeling Adapter van de gegevensmakelaar. Breda heeft tevens een generieke DigiKoppeling Adapter welke wordt ingezet voor organisatie-brede processen, zoals die voor de Berichtenbox..

Dit zijn onze uitgangspunten en eisen:

- Het inzetten van een API gateway (van of namens de gemeente) is verplicht bij het uitwisselen van persoonsgegevens via webservices / API's.
- Tussen het on-premises datawarehouse van Breda en SaaS applicaties worden geen rechtstreekse databasekoppelingen gelegd. Dit gebeurt enkel via door Breda gekozen middleware, zoals een sFTP client/server, een ESB of een data-gateway.
- Koppelvlakken zijn altijd goed beschreven.
- Integratie gebeurt gestandaardiseerd, tenzij kan worden onderbouwd dat dit niet mogelijk is.
- Ontkoppeling is een streven. Hiermee kan het gedrag van app(licatie)s en webportalen hetzelfde blijven, wanneer er aan de achterkant iets verandert. Ook is de beschikbaarheid dan niet afhankelijk van beschikbaarheid van de onderliggende systemen.
- Koppelingen zijn beveiligd met tweezijdig TLS (2-way SSL) en er wordt aan beide zijden IP whitelisting toegepast. Bij voorkeur integreren leveranciers via een besloten netwerk.
- Voor toegang tot het besloten Diginetwerk van Logius, is het GGI-netwerk van VNG-Realisatie het standaard koppelnetwerk.
- Breda streeft naar enkelvoudige opslag, meervoudig gebruik (Single Source of Truth). Waar mogelijk wordt brondata hergebruikt, zodat beheer en administratie van gegevens eenvoudiger wordt.
- Met het oog op dataminimalisatie dient niet meer data te worden uitgewisseld dan noodzakelijk. Bij voorkeur enkel mutaties en met minimale tussenopslag.
- Gestandaardiseerd uitwisselen van data (via API's) heeft expliciet de voorkeur boven uitwisseling via sFTP of robots.
- Conform de principes van Common Ground en in het kader van herleidbaarheid en kwaliteit, wordt data niet naar de omgeving van Breda gepusht/gekopieerd, maar wordt het door Breda zelf bij bronsystemen opgehaald (pull).
  Uitzonderingen daarbij zijn API's en DigiKoppeling voor asynchroon berichtenverkeer.

sFTP

- Dataclassificatie is bepalend voor de beveiligingsmaatregelen (SSH sleutelpaar in geval van persoonsgegevens).
- IP whitelisting wordt verplicht toegepast.
- Data op de sFTP server wordt *tijdelijk* opgeslagen, volgens een afgestemd bewaartermijn.
- Gemeente Breda zet enkel bij uitzonderingen een eigen sFTP server in.

Dit zijn uitzonderingen of bijzonderheden:

- Een integratie tussen twee leveranciers (cloud-2-cloud) kan ook zonder tussenkomst van Gemeente Breda verlopen. Voorwaarden daarvoor zijn:

  - Het berichtenverkeer bevat géén persoonsgegevens.

  OF

  - Eén van de applicaties is een generieke integratievoorziening, waarmee Gemeente Breda inzicht in het berichtenverkeer heeft en waarbij beveiliging met 2-weg TLS is toegepast.

- Uitzonderingen dienen altijd te worden beoordeeld door een architect van gemeente Breda.

21. Distributie basisgegevens

Aanleiding / Achtergrond

De gemeente Breda maakt bij de uitvoering van haar wettelijke publieke taken gebruik van basisgegevens (basisregistratie- en kernregistratie-gegevens).
Voor de verwerking van deze basisgegevens, sluit de gemeente Breda zowel in haar rol als bronhouder als in haar rol als afnemer, aan op het (landelijke) stelsel van basisregistraties.
De gemeente Breda maakt hiervoor gebruik van een gemeentelijk generiek data distributie- en ontsluitingssysteem: het platform iConnect (MKS, iNzicht en CLIQ) van de leverancier PinkRoccade Local Government.

In de loop van de komende jaren zijn diverse ontwikkelingen van invloed op een juiste werking van het Stelsel van Basisregistraties. Denk hierbij aan: cloudtransities, Common Ground, Haal Centraal, Samenhangende Objectenregistratie, wijzigende informatiemodellen van basisregistraties e.d.
Om in de behoefte aan tijdige, volledige en juiste (combinatie van) basisgegevens te kunnen blijven voorzien, streeft de gemeente Breda naar continuïteit en innovatie van het gemeentelijk generiek data distributie- en ontsluitingssysteem.
Breda staat hierbij aan het begin van een transitieperiode, waarbij een hybride situatie (huidige en nieuwe standaarden) ondersteund wordt.
Dit vereist mede een innoverende houding aan de zijde van de procesapplicaties die aansluiten op dit gemeentelijke generieke data distributie- en ontsluitingssysteem.

Dit zijn onze uitgangspunten en eisen:

- Eenmalige registratie, meervoudig gebruik is het uitgangspunt bij het verwerken van basisgegevens.
  Procesapplicaties sluiten derhalve aan op het gemeentelijke generieke data distributie- en ontsluitingssysteem voor de afname van (en/of levering van) basisgegevens.
- Uitwisseling van basisgegevens vindt tijdens de transitieperiode plaats conform bestaande dan wel nieuwe gegevens- en berichtenstandaarden (StUF, API).
  Hierbij gaat de voorkeur uit naar nieuwe standaarden.
- Autorisatie van de gewenste af te nemen gegevenssets vindt plaats op basis van doelbinding.
- Actualiseren van basisgegevens in afnemende procesapplicaties vindt plaats aan de hand van een abonnementenservice op basis van afnemersindicaties, verstrekkingsregels en/of gebeurtenissen/notificaties.

- Voorafgaand aan aansluiting op het gemeentelijke generieke data distributie- en ontsluitingssysteem vindt een intake plaats.

Dit zijn uitzonderingen of bijzonderheden:

Uitzonderingen worden tijdens een intake besproken en worden beoordeeld door betreffende specialisten van gemeente Breda.

22. RPA

Aanleiding / Achtergrond

Robotic Proces Automation (of RPA) is een vorm van business proces automatisering, gebaseerd op software robots (bots) en in mindere mate op kunstmatige intelligentie (AI).

Robotsoftware simuleert menselijk handelen in informatiesystemen: handmatige copy/paste, type- en muisklik- acties in de zichtbare gebruikersinterface worden geautomatiseerd.

Een robot acteert als een extra gebruiker van een informatiesysteem, een virtuele medewerker of virtuele assistent. Deze is met name interessant voor repetitief, voorspelbaar en gestandaardiseerd werk, waar de toegevoegde waarde/kennis van de medewerker minimaal is.

Dit zijn onze uitgangspunten en eisen:

Om wildgroei aan RPA-oplossingen te voorkomen wordt UiPath gebruikt als standaardoplossing voor RPA.

Gemeente Breda zet bij voorkeur géén RPA in, wanneer:

- met gestandaardiseerde generieke voorzieningen hetzelfde kan worden bereikt. Gestandaardiseerde automatisering en integratie is meer robuust, efficiënt en veiliger. De “voorkant” van applicaties waarop een robot de focus heeft, heeft vaak een veranderlijk karakter;
- het proces of de werkzaamheden niet of minder geschikt is/zijn voor RPA (te veel uitzonderingen, hoge complexiteit, te weinig volume, te veranderlijk);
- er geen positieve business case is; oftewel de ontwikkel en beheerkosten wegen niet op tegen de uiteindelijke baten.

RPA kan een goede oplossing bieden, wanneer:

- de (voor de gebruiker onzichtbare) achterkant van applicaties moeilijk te integreren of automatiseren is.
  Met name bij legacy/silo- applicaties kan het ontsluiten van data of het integreren met andere systemen een uitdaging vormen, door het ontbreken van moderne koppelvlakken (API’s). Automatisering op de grafische gebruikersinterface kan dan uitkomst bieden;
- er sprake is van een stabiele omgeving, met weinig veranderingen in het proces en onderliggende software;
- procesoptimalisaties een valide business case (wel periodiek evalueren) hebben (niet alleen geld, ook kwaliteit, veiligheid).

Dit zijn uitzonderingen of bijzonderheden:

Uitzonderingen dienen altijd te worden voorgelegd aan en beoordeeld door een architect van gemeente Breda.

23. Archivering

Kaders

Met betrekking tot Wet- en regelgeving (Archiefwet en Archiefbesluit) gelden er voor (digitale) archivering, de normen op basis van de Archiefregeling zoals o.a.: ISO 15489 (Internationale norm Wet- en regelgeving), NEN-ISO 23081 / MDTO (Metagegevens voor duurzaam toegankelijke overheidsinformatie), NEN-ISO 16175 (principes en functionele eisen voor software om digitale informatie te creëren en te beheren) en NEN 2084 (Document typen).

Informatiesystemen

Een informatiesysteem is een systeem waarmee informatie over objecten of personen beheerd, verzameld, bewerkt, geanalyseerd, geïntegreerd en gepresenteerd kan worden. Tot een informatiesysteem in ruime zin worden naast de data en de technieken en faciliteiten om data te ordenen en te interpreteren vaak ook de ermee verbonden organisatie, personen en procedures gerekend.
Voor het document management wordt er een globale indeling gebruikt voor verschillende informatiesystemen:

- Informatiestroom <8 jaar te bewaren
- Informatiestroom >8 jaar te bewaren (duurzame toegankelijkheidseisen, overbrenging naar DMS of E-depot

Taak specifieke of branche (<8 jaar) applicaties

Voor het opslaan van digitale dossiers of informatieobjecten gelden er de volgende (sub)functies (functionaliteiten) binnen de applicatie of in een daarvoor ingerichte mappenstructuur:

- Opslaan van de informatieobjecten.
- Opslaan en ontsluiten metadata (informatieobjecten).
- Converteren informatieobject naar duurzaam opslagformaten.
- Opslaan en ontsluiten metagegevens informatieobjecten.
- Bewaren/selectie van informatieobjecten.
- Valideren van informatieobjecten.
- Vernietigen van informatieobjecten
- Vernietigingslijsten kunnen worden gegenereerd
- Mogelijkheid tot exporteren van metadata en informatieobjecten uit de applicatie op basis van vooraf te definiëren XML.
- Mogelijkheid tot mapping met metadata (NEN-ISO 23081).
- Digitaal informatiebeheer binnen de applicatie.

Overig

DMS / taak specifieke of branche applicatie

Documenten (informatieobjecten) zijn altijd terug vindbaar en toegankelijk gedurende de tijd dat deze wettelijk beschikbaar moeten zijn. In een document management systeem (DMS) of functionele applicatie is in ieder geval de metadata van documenten opgeslagen. De documenten zelf kunnen in de database van het DMS worden opgeslagen.

Duurzame opslag van informatieobjecten

Gemeente Breda kent één Document Structuur Plan (DSP) en één Producten en Diensten Catalogus (PDC). Gemeente Breda kent meerdere vakdomeinen die gebruik maken van domein of taak specifieke systemen met eigen Zaak afhandelingsfuncties. Voorbeeld hiervan is de Suite voor het Sociaal Domein dat door het Sociaal Domein wordt gebruikt.

De taak of functionele applicatie bevat altijd alle relevante informatie met betrekking tot de Zaak. Alle documenten (bestanden met informatie) kunnen worden opgeslagen in een centraal DMS. Indien de opslag in een functionele applicatie geborgd (dus voldoende document management functionaliteiten) is kan opslag (< 10 jaar) ook hierin plaatsvinden.

Archivering

Archiefwaardige documenten en informatie met beperkte (vaak wettelijke) bewaartermijn zijn in een archiefsysteem (met bijbehorende functionaliteiten) gearchiveerd. Dat kan ook het domein systeem of functionele applicatie zijn. Na afloop van de wettelijke bewaartermijn dient er vernietigd te kunnen worden vanuit het desbetreffende systeem.
In het DSP zijn de voorwaarden rondom bewaar en vernietigingstermijnen opgenomen.

Exporteren documenten en metadata

Archiefwaardige documenten (incl. relevante metadata) die blijvend of zeer lang te bewaren zijn moeten geëxporteerd kunnen worden vanuit het domeinsysteem of functionele applicatie als voorbereiding op de digitale archivering in het e-depot en andersom. Bij voorkeur in een XML-schema dat voldoet aan de landelijke standaarden (XML-standaard nationaal archief of MDTO).

24. Smart City & Sensoriek

Aanleiding / Achtergrond

In een Smart City kunnen we ervoor zorgen dat de stad veel efficiënter, sneller, veiliger en goedkoper kan worden georganiseerd. Tegelijkertijd ontstaan er ook nieuwe uitdagingen doordat concepten zoals security by design, privacy by design, standaardisatie, etc. vaak geen gemeengoed zijn.

Dit zijn onze uitgangspunten en eisen:

- Vooraf dient gecontroleerd te worden of e.e.a. conform de AVG is. Dwz: grondslag, doelbinding, proportionaliteit, subsidiariteit. Vaak is bij Smart City oplossingen een DPIA nodig om dit te beoordelen. Wij conformeren ons hierbij aan de “principes van voor de digitale samenleving”. https://vng.nl/sites/default/files/2019-11/09a-bijlage-principes-voor-de-digitale-samenleving.pdf
- Data gegenereerd in de openbare ruimte is publiekelijk beschikbaar en Breda is als opdrachtgever te allen tijde de eigenaar van de data.
- Maak gebruik maken van open standaarden, voorkom dat dat opgesloten zit in systemen.
- Er wordt zo veel als mogelijk gebruik gemaakt van het bestaande Smart City eco systeem (data platformen, verbindingen, et cetera).
- Pas de basisbeveiligingsprincipes uit de IBD-handreiking IoT beveiliging toe.
- Inzet van sensoriek gebeurt op een transparante en ethisch verantwoorde manier.

Dit zijn uitzonderingen of bijzonderheden:

Meer informatie:
- https://smartcitybreda.com/
- https://www.informatiebeveiligingsdienst.nl/product/handreiking-iot-beveiliging/