



Aanvullingen Programma van Eisen en Wensen

*Aanvulling op Programma van Eisen en Wensen
t.b.v. gemeente Midden-Groningen*



ICT-Algemeen

- Opdrachtnemer begeleidt kosteloos een eventuele datamigratie
- Opdrachtnemer gaat akkoord met Verwerkersovereenkomst van Opdrachtgever

Technische Architectuur

- De oplossing worden geleverd als Software as a Service (SaaS)
- Er wordt minimaal een test-, acceptatie- en productieomgeving beschikbaar gesteld
- Indien er sprake is van een Webbased userinterface kan deze zonder beperking ingezet worden door de laatste twee versies van de meest gangbare en ondersteunde browsers (Microsoft Edge, Google Chrome, Apple Safari en Mozilla Firefox) zonder gebruik te maken van plug-ins (zoals Flash, Silverlight, Active X, etc)
- De Oplossing ondersteunt authenticatie via de lokale Active Directory van de Opdrachtgever. Gebruikers die via deze route zijn geauthenticeerd, krijgen via Single Sign-On (SSO) toegang tot alle onderdelen van de Oplossing, binnen de grenzen van hun machtigingen.
- Daarnaast ondersteunt de Oplossing authenticatie via Microsoft Entra ID (voorheen Azure Active Directory), met ondersteuning voor SAML 2.0 en/of OpenID Connect (OIDC).
- Voor gebruikers die niet (meer) zijn opgenomen in de lokale Active Directory maar wel via Entra ID worden beheerd, moet de Oplossing Multi-Factor Authenticatie (MFA) via Entra ID worden ondersteund. Dit geldt bijvoorbeeld voor externe gebruikers of in het kader van een overgang naar cloudbaseerde identiteitsbeheer.
- Leverancier levert benodigheden aan voor algoritmeregister (invullen sjabloon van het algoritmeregister).

Eisen die moeten worden meegenomen in een op te stellen SLA

- Leverancier stelt voor ondersteuning op afstand een Nederlandstalige servicedesk beschikbaar.
- De helpdesk is het centrale punt (single point of contact) voor het melden van incidenten, het stellen van vragen, indienen van wijzigingsvoorstellen en geeft informatie/ inzicht in de afhandeling daarvan. De helpdesk van de Leverancier levert zowel telefonische ondersteuning als ondersteuning via e-mail en/of een web portaal. Meldingen betreffende een verstoring van de prioriteit 1 dienen altijd ook telefonisch gemeld te worden.
- Het aanmelden van een Melding gebeurt door contactpersonen, die Opdrachtgever bij aanvang van de overeenkomst doorgeeft aan de servicedesk van Leverancier.

Deze personen zijn voor Leverancier het eerste aanspreekpunt op het gebied van de Programmatuur. Deze personen krijgen toegang tot het klantportaal, waarbij ze alle Meldingen van Opdrachtgever kunnen inzien en muteren.

- Bij het aanmelden en afhandelen van een Melding ontvangt de melder per omgaande een mailbericht met ticketnummer op zijn of haar mailadres. Daarnaast wordt de benodigde metadata voor het opstellen van een Beschikbaarheids- en Servicelevel rapportage per Melding in de Melding vastgelegd. Meldingen worden gedurende de looptijd van de SLA niet verwijderd.
- Daarnaast stelt Leverancier 24/7 (met uitzondering van Onderhoudswerkzaamheden aan het servicedesk systeem welke vroegtijdig aan Opdrachtgever gecommuniceerd zijn) een online registratiesysteem beschikbaar voor het registreren van verstoringen, incidenten en vragen.
- Voor het reageren op en afhandelen van verstoringen geldt de volgende werkwijze.

Urgentie	Mate van Verstoring
Zeer hoog (prio 1)	• De Verstoring is dermate ingrijpend dat bedrijfskritische processen van Opdrachtgever moeten worden gestaakt, oplossing is noodzakelijk. • Security of privacy incident
Hoog (prio 2)	• Kan niet werken: bedrijfskritische processen van Opdrachtgever zijn verstoord en kunnen niet naar behoren worden uitgevoerd, oplossing is noodzakelijk.
Midden (prio 3)	• Kan deels werken: met behulp van workaround kunnen processen van Opdrachtgever (deels) worden uitgevoerd, oplossing is noodzakelijk
Laag (prio 4)	• Kan werken: uitvoeren of uitstel is (tijdelijk) mogelijk, oplossing is gewenst • Cosmetische Verstoring

- In eerste instantie vindt prioriteitsbepaling plaats door Leverancier aan de hand van bovenstaande tabel. Wanneer Opdrachtgever het niet eens is met de prioriteitsbepaling door Leverancier kan Opdrachtgever de Verstoring escaleren via de reguliere escalatieprocedure als beschreven in de SLA.
- De tabel voor het bepalen van de prioriteit is beschreven voor Incidenten van het type Verstoring in de SLA. Niet voor informatievragen, opdrachten, wensen, etc. standaard wordt bij niet-Verstoringen uitgegaan van prioriteit 3. Opdrachtgever en Leverancier kunnen gezamenlijk tot een andere prioriteit komen.

1.1 Reactie- en Functiehersteltijd

- Aan de hand van de prioriteit worden de volgende Reactie- en Functiehersteltijden gehanteerd.

Prio	Reactietijd	Functie-hersteltijd	Werkwijze afhandeling	Prestatie-norm op tijd
1	n.v.t.	0 - 4 uur (uiterlijk 12.00 uur de volgende Werkdag)	Opdrachtgever meldt het Incident telefonisch bij Leverancier. De contactpersonen als genoemd bij het 1e, 2e én 3e escalatieniveau van zowel Leverancier als Opdrachtgever worden direct geïnformeerd.	85% van de Incidenten binnen de Reactie- en functie-hersteltijd gemeten op basis van de rapportage-periode.
2	1 Werkuur	2 Werkdagen	Leverancier neemt binnen 1 werkuur contact op met Opdrachtgever. Tevens worden het 1e, 2e én 3e escalatieniveau van zowel Leverancier als Opdrachtgever geïnformeerd.	
3	4 Werkuren	5 Werkdagen	Leverancier registreert en handelt de Melding af. Er hoeven geen extra escalatieniveaus te worden geïnformeerd	
4	8 Werkuren	10 Werkdagen	Leverancier registreert en handelt de Melding af. Er hoeven geen extra escalatieniveaus te worden geïnformeerd	

Een Incident wordt gesloten als één van de volgende situaties is bereikt:

- Het Software Probleem is opgelost en de oplossing is geaccepteerd door Opdrachtgever;
- Als een workaround ter beschikking is gesteld die acceptabel is voor Opdrachtgever en er gecommuniceerd is of (en wanneer) het Incident definitief wordt opgelost in een Upgrade of Update
- Als een oplossing is aangeboden en na tien (10) Werkdagen geen reactie is ontvangen van Opdrachtgever;
- De Opdrachtgever om andere redenen akkoord is met het sluiten van het Incident.
- Voor de voorgestelde Reactie- en Functiehersteltijd gelden de volgende **randvoorwaarden**:
- De tijd gedurende welke het Incident in de toestand 'wachten op Informatie / wachten op Klant / wachten op Sluiten' ligt, telt niet mee in bovengenoemde oplostijden. Dit kan bijvoorbeeld zijn dat Opdrachtgever aanvullende informatie dient te verschaffen.

- De genoemde oplostijden zijn niet van toepassing op Testomgevingen. Voor Storingen in de testomgeving geldt altijd prioriteit vier (4).
- Indien sprake is van directe gevolgen voor de geplande productiegang op de Productieomgeving, kan Opdrachtgever verzoeken om een incident met prioriteit 1 en 2 versneld in behandeling te nemen.

1.2 Communicatieafspraken

1.3 Onderstaande communicatie afspraken worden gevolgd bij Incidenten.

Prio	Communicatie
1	• Prio 1 meldingen worden telefonisch gemeld aan de servicedesk van Opdrachtnemer door Opdrachtgever; • De Verstoring wordt tevens door Leverancier en Opdrachtgever gemeld bij escalatieniveau 2 & 3; • De Verstoring wordt door Leverancier geregistreerd in haar online registratiesysteem. Ieder werkuur stelt Leverancier Opdrachtgever op de hoogte van de voortgang van de oploswerkzaamheden.
2	• Prio 2 meldingen worden via het online registratiesysteem door Opdrachtgever gemeld aan de servicedesk van Opdrachtnemer • De Verstoring wordt tevens door Leverancier en Opdrachtgever gemeld bij escalatieniveau 2 & 3. Iedere 8 werkuren stelt Leverancier Opdrachtgever op de hoogte van de voortgang van de oploswerkzaamheden
3	Prio 3 meldingen worden via het online registratiesysteem door Opdrachtgever gemeld aan de servicedesk van Opdrachtnemer
4	Prio 4 meldingen worden via het online registratiesysteem door Opdrachtgever gemeld aan de servicedesk van Opdrachtnemer

1.4 Beschikbaarheid dienst

- De gehele oplossing is in beginsel 24 uur per dag/ 7 dagen per week toegankelijk, onafhankelijk van tijd, plaats en type device. De Beschikbaarheid van de gehele (incl. alle omgevingen van de) oplossing (functionaliteit en data), uitgaande van een Beschikbaarheid van de gemeentelijke ICT-infrastructuur van 100%, wordt dagelijks van 07:00 tot 23:00 uur voor ten minste 98,0% (per maand) gegarandeerd. Voor eventuele web portalen geldt eveneens: 07:00 tot 23:00 uur op alle dagen. Downtime vanwege installatie- en herstelverzoeken van de gemeente wordt niet meegerekend in het meten van deze Beschikbaarheid. Gepland beheer en Onderhoud, met risico op downtime, worden in beginsel buiten deze tijden uitgevoerd. Gedurende de Beschikbaarheid van alle omgevingen wordt een gelijke performance aangeboden, waarmee ten minste wordt voldaan aan de gestelde performancevereisten.
- Leverancier stelt Opdrachtgever direct proactief op de hoogte bij Verstoringen aan de geleverde SaaS-diensten. Verstoringsmeldingen van prio 1 & 2 zijn direct via de software zichtbaar bij inloggen of als pop-up als de Gebruiker is ingelogd.

1.5 Lijncommunicatie

- Communicatie tussen Opdrachtgever en Leverancier is een essentieel onderdeel van een goede samenwerking. Deze communicatie vindt plaats op diverse niveaus. Om het contract goed te kunnen beheren wijzen partijen per niveau een vast contactpersoon als aanspreekpunt.

1.6 Overlegvormen en frequentie

- Goede samenwerking tussen Leverancier en Opdrachtgever vereist elkaar goed 'kennen' en blijven kennen. Met andere woorden, partijen kennen elkaars ontwikkelingen en behoeften. Daarmee wordt geborgd dat het proces van Opdrachtgever en de Applicatie(ontwikkeling) van Leverancier op elkaar afgestemd blijven. Hiertoe vindt op regelmatige basis afstemming plaats op operationeel, tactisch en strategisch niveau.

Strategisch

Opdrachtgever	Leverancier	Frequentie	Onderwerpen
Directeur en/of contracteigenaar en/of contractmanager /I-adviseur	Directeur/accountmanager	1x per jaar	▪ Klanttevredenheid ▪ Evaluatie samenwerking/ contract ▪ Langetermijnvisie ▪ Evaluatie kengetallen ▪ Financieel resultaat ▪ Indien van toepassing, contract updating ▪ Facturering ▪ Relevante ontwikkelingen Leverancier en Opdrachtgever ▪ Ontwikkelingen in de markt ▪ Managementrapportage

Tactisch

Opdrachtgever	Leverancier	Frequentie	Onderwerpen
Contractmanager ICT en/of informatiemanager	Service Manager en/of Accountmanager	4x per jaar	▪ Relevante ontwikkelingen Leverancier en Opdrachtgever ▪ Evaluatie contract ▪ Beleid en doelstellingen ▪ Contractbeheer en mutatiebeheer ▪ Informatie/escalaties vanuit het operationeel overleg ▪ Kwaliteitsbeheersing ▪ Klantbeleving ▪ Facturatie ▪ Innovatie- en besparingsmogelijkheden ▪ Prijsindexering ▪ wenswijzigingen ▪ Service level agreement wijzigingen en KPI's

Operationeel

Opdrachtgever	Leverancier	Frequentie	Onderwerpen
Servicedeskmanager en/of functioneel beheerder(s)	Servicedeskmedewerker en/of servicedeskmanager	1x per zes weken	▪ algemeen (dagelijkse gang van zaken) ▪ kwaliteit Dienstverlening (rapportages, trends) ▪ klachten en reacties (Correctief en preventief) ▪ meldingen (opvolging, trendontwikkeling) ▪ Diverse ondersteuningsvragen

- Leverancier is verantwoordelijk voor de verslaglegging inclusief afsprakenlijst voor elk overleg. Het verslag wordt binnen vijf (5) Werkdagen na het overleg digitaal aangeleverd bij de Opdrachtgever (contractmanager).

1.7 Escalatiematrix

- Onderstaande personen hebben contact over uitvoering van de Overeenkomst en de SLA. Indien een Incident op het niveau van het operationele werkveld niet naar tevredenheid van Opdrachtgever of Leverancier wordt afgehandeld, kunnen beide partijen conform het onderstaande schema escaleren:

Niveau	Vertegenwoordiger Opdrachtgever	Vertegenwoordiger Leverancier
1 – Operationeel	Functioneel beheer Tel: e-mail:	Servicedesk(manager) Tel: e-mail:
2 – Tactisch	Informatieadviseur Tel: e-mail:	Accountmanager Tel: e-mail:
3 – Strategisch	Directeur /Teamleider/informatiemanager Tel: e-mail:	Directeur Tel: e-mail:

- Partijen houden dit overzicht in onderlinge afstemming actueel.

1.8 Rapportage en controle

- Er wordt per kwartaal in de maand na het sluiten van het kwartaal door Leverancier aan Opdrachtgever gerapporteerd over de Diensten en Dienstverlening ten opzichte van de afgesproken Servicelevels. Deze rapportage geeft inzicht in:
 - Beschikbaarheid: Overzicht van Beschikbaarheid van de Programmatuur over de afgelopen periode;
 - Performance: Rapportage over de prestatie van de Programmatuur over de afgelopen periode ten opzichte van de afgesproken prestatienormen;
 - Servicelevels: Rapportage over het aantal en soort Meldingen per prioriteit en verantwoording over het al dan niet behaald hebben van de Servicelevels rondom Reactie- en oplostijden;
 - Gebruikers: Overzicht van het aantal Gebruikers en rechten dat de afgelopen periode gebruikt heeft gemaakt van de Programmatuur, inclusief de eventuele gevolgen die dat heeft gehad;

Eisen vanuit Datateam

- De gevraagde oplossing dient te kunnen koppelen met de gemeentelijke Business Intelligence Systemen.
De gegevens moeten op één van de volgende manieren ontsloten worden:
 - Database benaderbaar via API vanuit MW Power BI of MS Azure
 - Database geautomatiseerd benaderbaar via een dump van de database / datakubus

- Data geautomatiseerd benaderbaar via een datafeed (mogen losse bestanden zijn, bijvoorbeeld CSV-bestanden)
 - Data niet geautomatiseerd benaderbaar via een (periodieke) dump van de database / datakubus
 - Data niet geautomatiseerd benaderbaar via een datafeed
- Bij de inschrijving / implementatie dient opdrachtnemer een actueel ERD (Entity Relationship Diagram) en/of IM (Informatiemodel), oftewel datamodel, op te leveren.
- Het datamodel dient bij voorkeur in opzet en terminologie te zijn afgestemd op het Gemeentelijk Gegevensmodel (GGM).
- De opgeslagen data wordt na een onderling af te stemmen periode uit de systemen verwijderd.

Eisen vanuit Communicatie

- De software moet voldoen aan de Web Content Accessibility Guidelines (WCAG) 2.1 op niveau AA. Dit geldt voor alle gebruikersinterfaces die via een browser of app beschikbaar zijn.
- De leverancier levert een toegankelijkheidsverklaring volgens het model van www.toegankelijkheidsverklaring.nl.
- Deze verklaring moet actueel, volledig en openbaar beschikbaar zijn.
- Leverancier voert een onafhankelijke toegankelijkheidsaudit uit (bijv. op basis van WCAG-EM) en levert het rapport aan Opdrachtgever.
- Eventuele gebreken worden opgenomen in een verbeterplan met planning en verantwoordelijke partij.
- De software is getest met eindgebruikers, inclusief mensen met een functiebeperking (visueel, motorisch, cognitief, auditief).
- Resultaten van deze tests worden bij oplevering gedeeld.

De software ondersteunt:

- Navigatie met toetsenbord (zonder muis)
- Schermlezers (bijv. NVDA, VoiceOver)
- Hoog contrast instellingen
- Verhoogde tekstgrootte tot 200% zonder verlies van functionaliteit
- Leverancier levert technische documentatie aan waarin wordt aangegeven hoe de toegankelijkheid is geborgd. Inclusief hoe aanpassingen/upgrades geen negatieve invloed hebben op toegankelijkheid.
- Leverancier verplicht zich om gedurende de looptijd van de wensOvereenkomst wijzigingen of uitbreidingen ook toegankelijk te ontwikkelen en testen.
- Bij updates moet een nieuwe audit/toetsing gedaan worden indien relevant
- Alle helpdocumentatie, onboardingmateriaal en klantenservicekanalen zijn ook digitaal toegankelijk. Denk aan: toegankelijke PDF's, video's met ondertiteling, telefonische ondersteuning als alternatief.

Eisen vanuit DIV en Archief

- De software voldoet aan de Archiefwet 1995, inclusief de zorgplicht voor duurzame toegankelijkheid.
- De software ondersteunt het handelen conform NEN-ISO 16175-1 & -2 (functionele eisen aan software voor informatie- en archiefbeheer).
- De software ondersteunt processen gericht op het bewaren, beheren en overdragen van informatieobjecten, inclusief metadata.
- De software moet in staat zijn om informatieobjecten te voorzien van metadata volgens TMLO of MDTO.
- Metadata moet automatisch of handmatig koppelbaar zijn aan documenten (zoals: titel, auteur, status, bewaartermijn, classificatiecode).
- De software ondersteunt het vormen van digitale dossiers en registraties van relaties tussen documenten en besluiten, processen of zaken.
- Documenten worden opgeslagen in een duurzaam toegankelijk formaat, zoals PDF/A, ODF of XML.
- De software ondersteunt migratie naar een eDepot of andere duurzame opslagomgeving.
- De software bewaart audittrails van bewerkingen, inclusief mutatiegegevens en gebruikerslog.
- De software ondersteunt het instellen van bewaar- en vernietigingstermijnen conform selectielijsten.
- Beheerder ontvangt notificaties wanneer bewaartermijnen verlopen.
- Er is een proces voorzien voor autorisatie en vastlegging van vernietiging (inclusief vernietigingsbewijs).
- Gebruikersrechten zijn op document- of dossierniveau instelbaar.

- Alle toegang wordt gelogd en is achteraf herleidbaar.
- Voldoet aan de eisen van de BIO (Baseline Informatiebeveiliging Overheid), waaronder logging, encryptie, en backup.
- De software ondersteunt koppelingen via open standaarden zoals API's of StUF-ZKN / RGBZ.
- Er is ondersteuning voor uitwisseling met DMS, zaakstelsel of e-Depot (zoals die van het Nationaal Archief of andere beheerders).
- Documenten zijn exporteerbaar inclusief metadata.
- Bij contractbeëindiging moet leverancier zorgen voor export van alle gegevens in open formaten, inclusief metadata.
- De software ondersteunt een retourbestandsformaat dat overdraagbaar is naar andere systemen.

Eisen vanuit Informatiebeveiliging

- De opslag van persoonsgegevens vindt encrypted en fysiek plaats binnen de Europese Economische Ruimte
- De Opdrachtnemer werkt volgens de normen die worden gesteld in ISO 27001 tbv Informatiebeveiliging en ISO 2000 t.b.v. Service management Opdrachtgever
- Er wordt binnen 14 dagen na gunning van de Opdracht een Data Protection Impact Assessment (DPIA) uitgevoerd. De Opdrachtnemer ondersteunt hier kosteloos bij.
- De in de DPIA voorgestelde maatregelen worden per direct doch niet later dan 14 kalenderdagen na uitvoering van de DPIA door Opdrachtnemer opgevolgd
- Eventuele wachtwoorden worden via een veilige, versleutelde verbinding verstuurd
- Toegang tot de applicatie gaat via HTTPS
- De Opdrachtnemer beschikt over een geldig ISO27001 certificaat en een jaarlijkse ISAE-verklaring van een EDP-Auditor
- De Opdrachtnemer voldoet aan de norm Baseline Informatiebeveiliging Overheid (BIO)
(checklist : <https://www.bio-overheid.nl/ico-wizard/>)
- De systemen zijn voldoende beveiligd, niet door middel van Software en zijn voorzien van een security suite (dus niet alleen een virusscanner)
- Informatie mag niet zonder uitdrukkelijke toestemming van de Eigenaar (Opdrachtgever) de gebouwen verlaten
- Opdrachtnemer laat periodiek een PEN-test uitvoeren door een onafhankelijke partij en geeft inzage in de uitkomsten van deze PEN-testen
- Hardening van HTTP-headers middels beveiligingsrichtlijnen wordt toegepast
- Ten behoeve van de loganalyse is op basis van een expliciete risico afweging de bewaarperiode van de logging bepaald op 10 jaar. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd
- Medewerkers van de Opdrachtnemer die betrokken zijn bij de implementatie en onderhoud van de geboden Oplossing hebben een geheimhoudingsverklaring ondertekend

- Medewerkers van de Opdrachtnemer die betrokken zijn bij de implementatie en onderhoud van de geboden Oplossing zijn in het bezit van een relevante Verklaring Omtrent Gedrag (VOG)
- De gebruikte firewalls maken gebruik van Unified Threat Management (UTM) en zijn Next Generation Firewalls (BGFW)
- De Oplossing is voldoende beveiligd tegen digitale dreigingen op basis van de methode Defense in depth (zie: [https://en.wikipedia.org/wiki/Defense_in_depth_\(computing\)](https://en.wikipedia.org/wiki/Defense_in_depth_(computing)))
- De gebruikte firewalls zijn voldoende beveiligd:
- De software is up-to-date (en beschikt over een geldige licentie)
- Gateway Antivirus
- Intrusion Prevention (IPS)
- Web Application Proxy
- Geo Location (blocking)
- Segmentatie Netwerk (eigen netwerk)
- Geen shared hosting
- Connecties van buitenaf via reverse proxy
- Gegevens uit de productie-omgeving worden niet gebruikt in ontwikkelomgeving, tenzij deze zijn geanonimiseerd en de proceseigenaar toestemming heeft gegeven
- De authenticatie (correct en foutief) en bijbehorend tijdstip worden vastgelegd.
- Gegevens worden niet buiten hun bron opgeslagen, behalve voor Continuïteitsdoeleinden.
- Gegevens uit de productie-omgeving worden niet gebruikt in test- en acceptatieomgevingen tenzij deze zijn geanonimiseerd en de proceseigenaar toestemming heeft gegeven
- E-mail uit naam van de gemeente Midden-Groningen wordt altijd beveiligd en geauthentiseerd via relay servers van de gemeente Midden-Groningen verstuurd
- Dataminimalisatie (beperken van verwerking van persoonsgegevens) wordt Toegepast
- Voor transportbeveiliging wordt gebruik gemaakt van VPN, of SSL over internet of KPN Lokale Overheid/GGI
- Zero footprint (geen data op endpoints) wordt toegepast
- in het geval dat de Oplossing direct benaderbaar is buiten het gemeentelijk netwerk wordt de identiteit geblokkeerd na 5 achtereenvolgende foutieve authenticatiepogingen. Deze blokkade blijft 15 minuten actief
- Self-signed certificaten zijn niet toegestaan. De certificaten worden uitgegeven door de gemeente Midden-Groningen
- De werking van de Oplossing kan getest worden zonder gebruik te maken van echte Persoonsgegevens
- Kopieën zijn niet toegestaan op systeemniveau
- Informatie mag niet zonder uitdrukkelijke toestemming van de Eigenaar de gebouwen verlaten.
- Bij het sturen en ontvangen van e-mails wordt gebruik gemaakt van alle hiervoor relevante, voor overheden verplichte, beveiligingsstandaarden. Op dit moment

betekent dat de correcte toepassing van SPF, DKIM, DMARC, DNSSEC, STARTTLS, DANE

- De Opdrachtnemer garandeert adequate backup- en restorevoorzieningen van de Oplossing waarbij in geval van een gebeurtenis buiten de invloedssfeer van de Opdrachtnemer (bijvoorbeeld een ramp of incident) de afgesproken dienstverlening binnen 48 uur kan worden gecontinueerd en waarbij het verlies van gegevens maximaal 0,5 werkdag kan bedragen
- De oplossing beschikt over een niet-muteerbare audit-trail met daarin minimaal de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis. Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.
- Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald op 10 jaar. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd
- In het kader van ENSIA moeten er rapportagemogelijkheden zijn over de verdeling van lees- en schrijfrechten onder gebruikers in de vorm van autorisatiematrix en kwartaalrapportages
- De opdrachtnemer gaat akkoord met het Informatiebeveiligingsbeleid van de De werkzaamheden met betrekking tot wijzigingen in de Oplossing wordt door de Opdrachtnemer/derden vastgelegd in rapportages
- “Security by Design”: Opdrachtnemer onderbouwt dat beveiligingsmaatregelen in de oplossing afdoende geregeld zijn. Dit betreft zowel maatregelen getroffen door Opdrachtnemer als door andere partijen die betrokken zijn bij het treffen en in stand houden van deze beveiligingsmaatregelen. De “security by design principes” kunnen daarbij als leidraad dienen (dit hoort bij Informatiebeveiliging)