

Programma van Eisen - Algemeen

ten behoeve van de
Europese openbare aanbesteding

met betrekking tot

**Regionale hoofdpst en levering betrouwbare
niveaumetingen**

1899714



Versie : 1.0
Datum : 22-09-2026

© Gehele of gedeeltelijke overneming, reproductie of openbaarmaking van de stukken, op welke wijze dan ook, zonder voorafgaan de schriftelijke toestemming van Waterschap Vallei en Veluwe is verboden, behoudens de beperkingen bij de wet gesteld. Het verbod betreft ook gehele of gedeeltelijke bewerking.

INHOUDSOPGAVE

DEFINITIES	3
1. DE AANBESTEDING IN VOGELVLUCHT	5
1.1. Inleiding	5
2. ALGEMENE EISEN	6
2.1. Projectmanagement	6
2.1.1. Startoverleg en planning	6
2.1.2. Plan van aanpak	6
2.1.3. Voortgang overleggen	7
2.1.4. Afwijkingen t.o.v. bestek	7
2.2. Opleverfase	7
2.2.1. Garantie Opdrachtnemer	7
2.2.2. Oplevering en Restpunten	7
2.2.3. Opleveren documentatie	8
3. ICT-EISEN	9
3.1. Applicatie	9
3.1.1. Plugin's en webbrowsers	9
3.1.2. App en responsive gebaseerd systeem	9
3.2. Veiligheidseisen	9
3.2.1. Beveiligingsstandaarden	10
3.2.2. Systeemprogrammatuur	10
3.3. Auditing	10
3.3.1. Algemeen	10
3.3.2. Audit-logbestanden	10
3.3.3. Inhoud logbestanden	10
3.3.4. ISO27001	11
3.4. Autorisatie	11
3.5. Gegevensbescherming	11
3.5.1. Algemeen	11
3.5.2. Multi-tenancy	11
3.5.3. Versleutelde verbinding	12
3.5.4. Verzenden emails	12
3.5.5. Eigendom gegevens/veilig stellen data	12
3.6. Identificatie & Authenticatie	12
3.6.1. Authenticatiedienst	12
3.6.2. 2-factor authenticatie	12
3.6.3. Wachtwoord eisen	12
3.6.4. Versleuteling wachtwoord	12
3.6.5. Single Sign On	12
3.6.6. Administratie accounts	13
3.7. Informatieveiligheid	13
3.7.1. Vulnerability scan	13
3.7.2. Pentest	13
3.7.3. Oplossen beveiligingsincidenten	14
3.8. Meldplicht datalekken	14
3.8.1. Melden beveiligingsincidenten	14
3.8.2. Kwalificatie datalek	14
3.9. Privacy	14
3.10. Servicevoorwaarden	14
3.10.1. Patch- en Vulnerability Management	14
3.10.2. DDoS maatregelen	15
3.10.3. Informatievoorziening	15
3.10.4. Testen	15
3.10.5. Back-up en recovery	15
3.10.6. Cyber Resilience Act (CRA)	15

Definities

In dit programma van eisen wordt een aantal begrippen met een beginhoofdletter gebruikt. Ook worden afkortingen gebruikt. Aan deze begrippen en afkortingen komt onderstaande betekenis toe.

Aanbestedende dienst

Waterschap Vallei en Veluwe is de Aanbestedende Dienst. Deze Aanbestedende dienst besteedt mede aan namens de volgende gemeenten, zijnde:

- Gemeente Amersfoort
- Gemeente Baarn
- Gemeente Barneveld
- Gemeente Blaricum
- Gemeente Brummen
- Gemeente Bunschoten
- Gemeente Eemnes
- Gemeente Ede
- Gemeente Elburg
- Gemeente Epe
- Gemeente Ermelo
- Gemeente Harderwijk
- Gemeente Hattem
- Gemeente Laren
- Gemeente Leusden
- Gemeente Nijkerk
- Gemeente Nunspeet
- Gemeente Oldebroek
- Gemeente Putten
- Gemeente Renkum
- Gemeente Renswoude
- Gemeente Rhenen
- Gemeente Scherpenzeel
- Gemeente Soest
- Gemeente Veenendaal
- Gemeente Wageningen
- Gemeente Woudenberg

Aanbestedingsleidraad

Procesbeschrijving van de aanbesteding met kenmerk 1899714.

Bemalingsgebied

Een geografisch afgebakend gebied waarin meerdere Objecten en onderdelen in de waterketen (afvalwater, grondwater en oppervlaktewater) met elkaar verbonden zijn.

Controller/Router/Modem

Een hulpmiddel om contact te maken tussen hoofdpst en PLC. Echter kan deze ook worden benut als opslag voor trendinggegevens en voor de controller geldt voor het omzetten van een protocol.

Devices

Alle apparatuur die een persoon kan toepassen om het web gebaseerde systeem en/of app op toe te passen, zijnde o.a. tablet en smartphone met Android/iOS van Apple operating system en personal computer en laptop met Windows of iOS als operating system en alle toekomstige gelijkwaardige apparatuur.

Dynamische gegevens/ Trendgegevens

Gegevens die op basis van een tijdseenheid worden vastgelegd en waarmee het gedrag van het object verklaart kan worden.

Hoofdpst/Telemetriesysteem

Het centrale punt waarin alle gegevens afkomstig uit een PLC of logger worden verkregen uit de objecten en waarmee de data o.a. kan worden opgeslagen, gevalideerd, bewerkt en geanalyseerd. Daarnaast kunnen alarmen worden uitgemeld en acties worden ondernomen. Ook is het mogelijk om op basis van beslisregelen, alarmering, data en/of formules objecten op afstand aan te sturen. Een hoofdpst kan ook gegevens bevatten die afkomstig zijn uit andere systemen, zoals neerslaggegevens of gegevens uit een andere hoofdpst.

Koppelvlak

Een blauwdruk van het object in het veld waarmee het object in een hoofdpst kan worden geconfigureerd. Hierin staat onder andere de adresseringslijst van de setpoints, trends, alarmen.

Lokale Hoofdpst

Een Hoofdpst die door een bepaalde gemeente wordt gebruikt en eventueel data levert aan de Regionale hoofdpst.

Monitoren

Het inzichtelijk maken hoe een object functioneert.

PLC

Een Programmable Logic Controller is een industriële computer die pompen en automatische processen aanstuurt.

Project

Een plan en aanpak om samenhangende en afgebakende werkzaamheden die nodig zijn om de Hoofdpst of levering van betrouwbare niveaumetingen succesvol te implementeren en op te leveren binnen een vastgestelde termijn.

(Communicatie) Protocol

Een vaste set afspraken en regels waarmee apparaten, software of systemen met elkaar kunnen praten en gegevens kunnen uitwisselen.

Statische gegevens

Gegevens die de werking van het object niet kunnen beïnvloeden bij eventuele wijzigingen. Voorbeelden hiervan zijn maatvoeringen van de put, hoog/laagwaterniveau, etc.

Systeemkoppeling

Koppelingen om systemen aan elkaar te verbinden. Zoals bijvoorbeeld een hoofdpst met een extern onderhoudsmanagementsysteem.

Telemetriegegevens

Alle meetgegevens, instellingen en alarmgegevens die een object beschikbaar heeft of toepast.

Opdrachtgever

Waterschap Vallei en Veluwe te Apeldoorn namens alle deelnemende gemeenten.

Opdrachtnemer

Inschrijver met wie Opdrachtgever de Overeenkomst heeft gesloten.

Regionale Hoofdpst

Een hoofdpst welke door meerdere gemeenten, waterschap en het UVT wordt gebruikt voor monitoring, sturing en beheer van watergerelateerde objecten.

Regionaal samenwerkingsverband

Alle genoemde gemeenten en waterschap Vallei en Veluwe onder 'Aanbestedende Dienst en teven Opdrachtgever' vormen samen het regionaal samenwerkingsverband. Het regionaal samenwerkingsverband heeft de samenwerking schriftelijk vastgelegd in een samenwerkingsovereenkomst (Centrumregeling).

UVT

Het uitvoeringsteam dat voor het waterschap en vrijwel alle inliggende gemeenten in het waterschapsgebied werkzaamheden uitvoert ten aanzien van meten, monitoring en beheer.

(Water gerelateerde) objecten

Objecten die ervoor zorgen dat water wordt afgevoerd of tijdelijk opgeslagen en objecten waar wordt overgestort. Putten waar alleen wordt gemeten vallen ook onder watergerelateerde objecten. Voorbeelden van watergerelateerde objecten zijn: (druk)rioolgemalen, bergbezinkvoorzieningen, overstorten, tunnelgemalen, drainagegemalen, regenmeter, etc.

Webgebaseerd

Een systeem waarin alle geëiste functies via internet als een service worden aangeboden, waar alleen een webbrowser benodigd is en waar geen software op de computer, tablet of smartphone geïnstalleerd hoeft te worden.

Werkend

Dit betekent dat alle gevraagde eisen correct functioneren en beschikbaar zijn voor eindgebruikers.

1. De aanbesteding in vogelvlucht

1.1. Inleiding

Voor u ligt het programma van eisen algemeen (hierna PvE algemeen) behorende bij de Europese openbare aanbesteding voor het sluiten van een Overeenkomst met één Opdrachtnemer per perceel voor het implementeren en onderhouden van een regionale hoofdpst en/of het leveren van betrouwbare (meet)gegevens voor overstortmonitoring.

Dit document is onlosmakelijk verbonden met de Aanbestedingsleidraad en bijbehorende bijlagen.

Dit document beschrijft de algemene eisen die gelden voor alle percelen of, indien specifiek aangegeven, voor bepaalde percelen.

De overige specifieke eisen per perceel zijn beschreven in de volgende documenten:

- Deel A: Programma van eisen hoofdpst
- Deel B: Programma van eisen levering betrouwbare niveaumetingen

2. Algemene Eisen

In dit hoofdstuk worden de eisen beschreven die aan de Opdrachtnemer en de Opdracht worden gesteld voor alle percelen.

2.1. Projectmanagement

De Opdrachtnemer neemt de volledige projectleiding op zich. Dit houdt in dat de Opdrachtnemer de verantwoordelijkheid draagt voor alle benodigde stappen om het project succesvol te laten verlopen, waarbij ten minste de onderdelen zoals beschreven in de onderstaande paragrafen wordt beschreven worden uitgevoerd.

2.1.1. Startoverleg en planning

De Opdrachtnemer organiseert een startoverleg waarin de details van de werkzaamheden worden besproken en de door de Opdrachtnemer opgestelde planning aan de te vormen projectgroep van de Opdrachtgever worden toegelicht. Het is van essentieel belang dat de projectleider van de Opdrachtgever volledig op de hoogte wordt gehouden van welke onderdelen door de Opdrachtnemer op welke momenten zullen worden uitgevoerd, zoals gedetailleerd staat beschreven in de aangeleverde planning welke door Opdrachtnemer is vervaardigd. Deze planning dient realistisch te zijn en ruimte te bieden voor mogelijke uitloop, calamiteiten en andere onvoorziene omstandigheden.

Het startoverleg, dat uiterlijk twee weken na de definitieve gunning plaatsvindt, wordt voorafgegaan door het versturen van een agenda door de Opdrachtnemer naar het projectteam van de Opdrachtgever. Hierbij wordt ook contact opgenomen om de aanwezigheid van de benodigde personen vanuit de Opdrachtgever te bevestigen.

De planning heeft als uitgangspunt dat de werkzaamheden aaneengesloten per gemeente of waterschap binnen de gestelde termijn worden uitgevoerd om het proces transparant te houden voor de projectleider van de Opdrachtgever. Ten minste één kalenderweek voor aanvang van de werkzaamheden wordt de Projectleider van de Opdrachtgever geïnformeerd over de uit te voeren werkzaamheden aan een Object in het veld, inclusief de verwachte duur van de onbereikbaarheid van het betreffende Object.

Voorafgaand aan de werkzaamheden wordt de projectleider van de Opdrachtgever ingelicht over de stappen die worden genomen om Objecten aan te sluiten op de te leveren Regionale Hoofdpost onder perceel A. Dit omvat tevens een risico-inventarisatie en bijbehorende maatregelen. Alle te nemen stappen worden schriftelijk vastgelegd in een definitief plan van aanpak, dat een kalenderweek voor aanvang van de werkzaamheden aan de projectleider van de Opdrachtgever wordt verstrekt.

Eventuele wijzigingen in de planning, aangebracht door de Opdrachtnemer, worden minimaal 5 werkdagen voor aanvang van de werkzaamheden met de projectleider van de Opdrachtgever besproken en schriftelijk doorgegeven. Alleen schriftelijke goedkeuring van de projectleider van de Opdrachtgever mogen de wijzigingen worden doorgevoerd. Bij geen akkoord blijft de planning dus zoals deze was. Open communicatie en duidelijke documentatie staan centraal bij het waarborgen van een succesvolle uitvoering van het Project.

De Opdrachtnemer benoemt gedurende het Project één contactpersoon (tevens projectleider), waarmee de projectleider van de Opdrachtgever communiceert. Deze persoon beheerst de Nederlandse taal zowel mondeling als schriftelijk en beschikt over voldoende inhoudelijke kennis met betrekking tot afvalwatergemalen en telemetrie. Het is verplicht dat deze contactpersoon bij alle overleggen aanwezig is, om een consistente en effectieve communicatiestroom te waarborgen. Het is toegestaan om een volwaardige vervanger vanuit de opdrachtnemer aan te wijzen en aanwezig te laten zijn bij één of meerdere overleggen.

2.1.2. Plan van aanpak

Het plan van aanpak, dat bij inschrijving is aangeleverd, wordt meer gedetailleerd beschreven en aangevuld op basis van hetgeen is afgestemd in het startoverleg en voldoet aan het programma van eisen. Hierin wordt ook een gedetailleerde planning opgenomen waarin geheel duidelijk is wat de Opdrachtnemer uitvoert en wat de Opdrachtgever dient uit te voeren en wanneer.

Het plan van aanpak wordt binnen 10 werkdagen aangeleverd aan de Opdrachtgever ter beoordeling. De Opdrachtnemer blijft echter verantwoordelijk voor de planning en een succesvolle uitvoering van het plan van aanpak.

Bij wijzigingen wordt een herziene versie van het plan van aanpak aangeleverd binnen 5 werkdagen na de wijziging.

2.1.3. Voortgang overleggen

Voortgang overleggen worden eens in de 4 weken gehouden, tenzij er problemen ontstaan in de planning als gevolg van acties van de Opdrachtgever, Opdrachtnemer, of indien de werkzaamheden niet conform het Programma van Eisen (PvE) worden uitgevoerd. In dergelijke situaties heeft de Opdrachtgever het recht om binnen 5 werkdagen na het verzoek van de Opdrachtgever een extra voortgangsoverleg te eisen.

De Opdrachtnemer is niet gerechtigd om meerwerk in te dienen voor de voortgang overleggen, tenzij de Opdrachtgever de enige geldige en reële oorzaak is van het ingelaste voortgangsoverleg.

De projectleider van de Opdrachtnemer fungeert als voorzitter van het voortgangsoverleg en is verantwoordelijk voor het opstellen van de verslagen (notulen) en de agenda. De agenda wordt uiterlijk twee dagen vóór het overleg aan de Opdrachtgever verzonden. Binnen één werkdag na ontvangst van de agenda geeft de Opdrachtgever goedkeuring en heeft Opdrachtgever tevens de mogelijkheid om aanvullende punten toe te voegen.

Tijdens de voortgang overleggen wordt de vastgestelde agenda gevolgd en op dezelfde wijze genotuleerd door de Opdrachtnemer. In de notulen wordt een actielijst opgenomen, die door zowel de Opdrachtnemer als de Opdrachtgever dient te worden uitgevoerd, inclusief de benodigde deadlines. Deze gestructureerde aanpak zorgt voor heldere communicatie, transparantie en een efficiënte afhandeling van actiepunten binnen het Project.

2.1.4. Afwijkingen t.o.v. bestek

Gedurende het Project kan meer- en minderwerk ontstaan doordat er afwijkingen ten opzichte van de eisen worden geconstateerd door de Opdrachtgever of Opdrachtnemer. Alle wijzigingen dienen te worden verwerkt in een afwijkingsformulier dat door de Opdrachtgever wordt verstrekt. Een afwijkingsformulier bevat een titel, voor welke deelnemer of complete samenwerking de afwijking van toepassing is, een omschrijving van de afwijking ten opzichte van de eisen die zijn gesteld, de functionele en technische consequenties van de afwijking en de consequenties voor kosten en planning/oplevertermijn. Er moet ook een afwijkingsformulier ingevuld worden als de werkzaamheden geen consequenties heeft ten aanzien van de kosten of planning/oplevertermijn.

Na constatering van meer-, minderwerk of wijziging dient het afwijkingsformulier 5 werkdagen of zoveel eerder schriftelijk bij de projectleider van de Opdrachtgever aangeleverd te zijn. Een afwijkingsformulier moet worden goedgekeurd door de Opdrachtgever. Alleen een door de Opdrachtgever goedgekeurd en getekend afwijkingsformulier kan als afwijking worden gezien en kan, indien van toepassing, verrekend worden. Verrekening van afwijking vinden plaats als het project is opgeleverd of eerder indien dit gezamenlijk is overeengekomen.

Meerwerkkosten worden niet voldaan indien de werkzaamheden al hebben plaatsgevonden zonder een afwijkingsformulier in te leveren volgens bovenstaande procedure. Tevens blijft de boeteclausule, benoemd in de Dienstverleningsovereenkomst, voor de uiterste datum van oplevering van kracht indien door de afwijking de opleverdatum niet wordt gehaald.

2.2. Opleverfase

2.2.1. Garantie Opdrachtnemer

De geleverde systemen of de te leveren data voldoet minimaal aan de gestelde eisen die in dit programma van eisen en het bijbehorende de(e)l(en) zijn beschreven. Eventuele aanvullende functionaliteiten en diensten die tijdens de inschrijffase zijn aangeboden maken ook onderdeel uit van hetgeen werkend wordt opgeleverd.

Gedurende de volledige contractduur zal de Opdrachtnemer garanderen dat de geëiste functionaliteiten en diensten respectievelijk blijven functioneren en geleverd worden. Indien bij oplevering of tijdens de contractperiode blijkt dat de functionaliteit niet naar behoren werkt volgens hetgeen is geëist, worden eventuele aanpassingen kosteloos binnen twee kalenderweken na melding uitgevoerd. De verantwoordelijkheid voor de uitgevoerde aanpassingen ligt in dit geval bij de Opdrachtnemer.

2.2.2. Oplevering en Restpunten

Bij oplevering zijn geen ernstige gebreken vastgesteld waarbij de hoofdpst en/of overstortmonitoring door gebruikers niet toegepast kunnen worden om haar taken goed te kunnen uitvoeren. Dit geldt zowel voor de oplevering van de pilotfase als bij de oplevering van het totale implementatieproject.

De volgende onderdelen worden gezien als ernstige gebreken:

Hoofdpост:

Als ernstige gebrek wordt gezien:

- niet alle Objecten zijn in de Hoofdpост Werkend aanwezig;
- geen Werkende alarmering aanwezig zoals vooraf schriftelijk is afgestemd;
- geen communicatie mogelijk tussen hoofdpост en Object of vice versa;
- geen Werkende grafieken en rapporten;
- geëiste functies niet volledig Werkend aanwezig zijn in de Hoofdpост.

Restpunten zijn:

- Een rapport is nog niet volledig Werkend;
- Procesplaatjes zijn wat vormgeving betreft nog niet geheel in overeenstemming op een beperkt aantal punten;
- Opdrachtgever heeft bij bepaalde Objecten nog geen specifieke informatie verstrekt na de vastgelegde haalbare en overeengekomen deadline zodat een Object niet volledig kan worden ingericht;
- Gezamenlijk overeengekomen restpunten die niet als ernstig Gebrek worden gezien.

Levering van betrouwbare niveaumetingen:

Als ernstige gebrek wordt gezien:

- Dagelijks geen kwalitatieve data beschikbaar van overstorten over de periode vanaf moment na plaatsing apparatuur en oplevering met een minimale periode van 2 weken aan meetdata.

Restpunten zijn:

- Indien door toedoen van Opdrachtgever of door onvoorziene omstandigheden de meetwaarden nog niet juist zijn of nog niet opgenomen zijn in de Hoofdpост. Als dit zich voordoet kan door Opdrachtnemer aantoonbaar laten zien dat de data kan worden opgehaald en de data betrouwbaar is.

De oplevertermijn voor de pilotfase en voor de totale oplevering zijn in paragraaf 1.5 van de Aanbestedingsleidraad beschreven.

Als er geen ernstige gebreken worden vastgesteld maar er nog wel één of meerdere punten nog niet zijn opgeleverd dan wordt deze punten als restpunten bestempeld.

Alle restpunten moeten binnen 15 werkdagen na de opleverdatum afgehandeld zijn, tenzij anders overeengekomen. Indien restpunten niet binnen 15 werkdagen worden opgelost, wordt met terugwerkende kracht de oplevering ingetrokken en worden de eventueel daarbij reeds door Opdrachtnemer verzonden facturen niet voldaan. Tevens treedt dan alsnog de boeteclausule in werking die in de Dienstverleningsovereenkomst is opgenomen vanaf de dag dat de oplevering heeft plaatsgevonden (Zie paragraaf 2.9 van de Aanbestedingsleidraad).

2.2.3. Opleveren documentatie

De Opdrachtnemer levert alle toegepaste of gebruikte documenten die noodzakelijk waren voor de uitvoering van de werkzaamheden bij oplevering aan Opdrachtgever.

Alle object gerelateerde documentatie of bestanden, zoals koppelvlakken, worden opgeslagen in de te leveren hoofdpост van de Opdrachtgever.

3. ICT-EISEN

Er zijn diverse eisen op het gebied van ICT en veiligheid. In dit hoofdstuk worden de eisen beschreven die van toepassing zijn voor de hoofdpst en het leveren van betrouwbare niveaumetingen. Indien de Opdrachtnemer die betrouwbare niveaumetingen moet leveren gebruik maakt van een eigen systeem, dat tussen de meetapparatuur en de te leveren hoofdpst in perceel A in staat, dan moet ook aan de veiligheidseisen voldaan worden die in dit hoofdstuk zijn beschreven staan en waar "Hoofdpst" wordt vermeld.

3.1. Applicatie

3.1.1. Plugin's en webbrowsers

De hoofdpst (incl. beheeromgeving) is een web gebaseerde Software as a Service (SAAS) oplossing. Dit betekent dat de systemen met alle geëiste functies via internet als een service wordt aangeboden en geen software/plugin's op de computer, tablet of smartphone behoeven te worden geïnstalleerd om er gebruik van te maken. Software downloaden om verbinding te maken en/of in te loggen in een web omgeving valt hier ook onder. De systemen dienen tenminste van de volgende webbrowsers (met maximaal 2 versies lager dan de meest recente versie) volledig en goed te functioneren:

- Microsoft Edge
- Mozilla Firefox;
- Google Chrome;
- Apple Safari.

Voor het gebruik van de hoofdpst zijn geen systeemaanpassingen nodig op bestaande werkstations, servers, firewalls en andere onderdelen van de ICT-infrastructuur van Opdrachtgever.

Ook de beheeromgeving van de hoofdpst of van het systeem dat gebruikt wordt voor levering betrouwbare niveaumetingen dient aan de bovenstaande eisen te voldoen. Het is niet toegestaan om standaard instellingen aan webbrowsers te wijzigen om de hoofdpst of systeem voor het leveren van betrouwbare niveaumetingen te kunnen gebruiken.

3.1.2. App en responsive gebaseerd systeem

De webapplicatie is responsive zodat deze is toe te passen op tablet, smartphone, laptop en pc met breedbeeldscherm. Mocht de webapplicatie niet responsive zijn dan heeft een app voor een Android en Apple omgeving de voorkeur, echter als aanvulling op het web gebaseerde systeem.

3.2. Veiligheidseisen

De Cyberbeveiligingswet (CBW) is per augustus 2026 ingegaan waarbij de Baseline Informatiebeveiliging Overheid versie 2 (BIO2) vanaf dat moment van toepassing is. Dit betekent voor de Hoofdpst leverancier en leverancier van betrouwbare data dat zij zich aan de BIO2 moeten houden (de Opdrachtnemer moet altijd voldoen aan de meest recente versie van de BIO of diens opvolger gedurende de overeenkomst van kracht is). De software moet ontwikkeld zijn volgens de "secure by design" methode en de leverancier moet garanderen dat software en de upgrades/updates van de software (en firmware) het vitale proces niet in gevaar brengen en kwetsbaarheden direct worden opgepakt.

Dit betekent o.a. ook uitgebreide logging en auditing om snel te kunnen analyseren, robuustidentiteits- en toegangsbeheer, continuïteitsmaatregelen zodat uitval tot een minimum wordt beperkt en aantoonbaar is dat de softwareontwikkeling en bedrijfsvoering veilig zijn.

Omdat de BIO2 onvoldoende diepgaande technische invulling geeft aan een veilige omgeving en bedrijfsvoering wordt voor deze aanbesteding ook de Cyber Security Implementatie Richtlijn versie 3.4 en recenter (hierna CSIR) gehanteerd. De CSIR is voor de hoofdpst aangevuld met beheersmaatregelen uit de industriestandaard IEC 62443 om dekkend te zijn voor de beveiliging van procesautomatisering. De CSIR 3.4 is in bijlage A.3 opgenomen. Alleen de onderdelen die betrekking hebben op de verbindingen, koppelingen en de hoofdpst zijn van toepassing. De Opdrachtgever moet altijd voldoen aan de meest recente versie van de CSIR en minimaal weerstandsniveau 1 als uitgangspunt gebruiken.

Het Nationaal Cyber Security Centrum (NCSC) en Informatiebeveiligingsdienst (IBD) hebben richtlijnen opgesteld ten aanzien van de Zero Trust principes. De hoofdpst dient te voorzien in expliciete verificatie van elke toegangsbevoegdheid op basis van beschikbare datapunten (o.a. gebruikersidentiteit en apparaatstatus) conform het 'Never Trust, Always Verify'-principe.

De leverancier past voor de SaaS-oplossing de meest recente versies van “Veilige ontwikkel beveiligingseisen voor (web)applicaties” (zie Centrum informatiebeveiliging en privacy) en de NCSC ICT beveiligingsrichtlijnen voor webapplicaties toe.

Het is essentieel dat voor de hoofdpst TLS-encryptie (altijd de laatste beschikbare en geteste versie, momenteel 1.3) en bij mogelijk is voor de communicatie tussen de hoofdpst en de toekomstige besturingen. Derhalve dient de hoofdpst deze mogelijkheid te hebben. De Opdrachtnemer zet nieuwste versie van Transport Layer Security (TLS) Protocol in voor het beveiligen van verbindingen en de Opdrachtnemer volgt ten aanzien van datatransport conform de meest actuele beveiligingsrichtlijnen van de NCSC.

Voor het leveren van betrouwbare niveaumetingen waarbij push en/of pull technologie wordt gebruikt moet ook encryptie en een veilige verbinding toegepast worden.

Voor alle in te zetten producten die op enige wijze communiceren dienen te voldoen aan de Cyber Resilience Act (hierna CRA). Voor alle hardware en bijbehorende software die binnen de overeenkomst wordt geleverd (ongeacht eigenaarschap) moet een CE-markering hebben, apparatuur zonder CE-markering is niet toegestaan. Voor PLC's, controllers en routers geldt klasse II (hoog risico) en voor loggers zonder sturing geldt klasse I.

Hosting van de hoofdpst betreft een voldoende beveiligde fysieke en logische omgeving – bestaande uit alle benodigde software (zoals virtualisatiesoftware, firewalls, technisch beheertoolsing en back-up software) en hardware (zoals serverapparatuur, opslag, back-up apparatuur en netwerken).

Alle benodigde beveiligingsupdates van de gebruikte software worden binnen één werkdag geïnstalleerd. Als de beveiligingsupdate volgens de leverancier van de betreffende toegepaste software noodzakelijk is om snel te installeren, dan moet deze binnen 1 kalenderdag worden geïnstalleerd of zoveel eerder als mogelijk. De Opdrachtnemer stelt de hoofdpst beschikbaar, inclusief het uitvoeren van het (technisch) beheer van deze omgeving.

3.2.1. Beveiligingsstandaarden

Alle software behorend tot de hoofdpst is volgens relevante standaarden beveiligd, conformeert zich telkens aan de laatst bekende beveiligingsinzichten en is blijvend van voldoende kwaliteit. Richtlijnen van de Autoriteit Persoonsgegevens (AP), Nationaal Cyber Security Centrum (NCSC), Informatiebeveiligingsdienst voor gemeenten (IBD), Forum Standaardisatie en Open Web Application Security Project (OWASP) zijn hierbij normstellend.

3.2.2. Systeemprogrammatuur

Systeemprogrammatuur, zijnde non-applicatie programmatuur, zoals besturingssysteem, middleware en firmware dient altijd te kunnen voldoen aan het juiste beveiligingsniveau (patchlevel) aanbevolen door de fabrikant en volgens de wettelijke regels. Opdrachtnemer onderbouwt dat beveiligingsmaatregelen in de oplossing afdoende geregeld zijn (Security by Design). 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 Opdrachtnemer zal altijd bij inzetten van apparatuur en/of een nieuwe patch/update het juiste versienummer in de Hoofdpst invullen bij het betreffende Object in het daarvoor bestemde veld dat door de Hoofdpstleverancier beschikbaar is gemaakt.

3.3. Auditing

3.3.1. Algemeen

Opdrachtgever heeft het recht om de beveiligingseisen die van toepassing zijn op de hoofdpst door een onafhankelijke partij te laten auditen. Opdrachtnemer stelt Opdrachtgever in staat om periodiek toe te zien of de aanbieder van de hostingomgeving zijn verplichting tot adequate beveiliging nakomt.

3.3.2. Audit-logbestanden

Activiteiten van gebruikers (raadpleging en mutatie), uitzonderingen en informatiebeveiligings-gebeurtenissen worden vastgelegd in audit-logbestanden die vanuit een applicatie-interface en via een standaard koppelveld naar het SIEM-systeem van Opdrachtgever, te allen tijde door Opdrachtgever kunnen worden geraadpleegd voor nadere analyse. Op verzoek van de Opdrachtgever, bijv. n.a.v. een beveiligingsincident, dienen relevante logs en auditgegevens aan de Opdrachtgever kosteloos aangeleverd te worden via een algemeen gehanteerd formaat.

3.3.3. Inhoud logbestanden

In audit-logbestanden wordt tenminste opgenomen: de gebeurtenis; de benodigde informatie die nodig is om een beveiligings-incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; 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.

3.3.4. ISO27001

De Opdrachtnemer dient een geldig ISO 27001-certificaat (of gelijkwaardig zoals expliciet NEN-ISO/IEC 27701, SOC 2 Type II of ISAE 3402 met relevante scope) te overleggen, afgegeven door een geaccrediteerde certificerende instelling (bijv. via RVA-register). Het certificaat moet de geleverde diensten (inclusief hoofdpst, SCADA/OT-systemen) omvatten, met bijvoeging van het meest recente auditrapport (max. 12 maanden oud) en Statement of Applicability (SoA). Gelijkwaardigheid wordt alleen geaccepteerd bij voorlegging van een onafhankelijke auditverklaring die BIO 2.0-conformiteit bevestigt, inclusief risicoanalyse voor ketenbeveiliging.

3.4. Autorisatie

De hoofdpst en biedt functionaliteit waarmee Opdrachtnemer kan garanderen dat een gebruiker slechts toegang heeft tot de gegevens die voor de uitoefening van zijn/haar functie nodig zijn (need to know/ least privileged). De hoofdpst voorziet in de mogelijkheid om autorisaties te baseren op Role Based Access Control (RBAC) en/of Attribute Based Access Control (ABAC) of soortgelijke.

De toegang, bedien- en gebruiksmogelijkheden moeten instelbaar zijn voor Opdrachtgever. Om rechten niet voor elke gebruiker te moeten wijzigen zijn gebruikers toe te kennen aan een gebruikersgroep waarop standaard rechten van toepassing zijn. Deze rechten zijn te overrulen door voor een betreffende gebruiker in de groep een specifiek recht toe te kennen op een bepaald onderdeel.

Hierbij moet onderscheid gemaakt worden in rechten zoals:

- Toegang krijgen tot de hoofdpst;
- Bekijken en lezen van informatie in de hoofdpst;
- Bekijken, lezen en muteren van systeeminstellingen in de hoofdpst;
- Accepteren, resetten en afhandelen van alarmen;
- Communicatie opzetten en bedienen van een object vanuit de hoofdpst;
- Wijzigen van instellingen van een object via de hoofdpst;
- Muteren van gegevens in de hoofdpst;
- Toegang tot de beheeromgeving waarin schematische weergaven, grafieken, rapporten, gebruikers en objecten gewijzigd/toegevoegd kunnen worden;
- Bekijken, lezen en muteren Realtime Controle procedures;
- Bekijken, lezen en muteren objecten binnen gebieden.

Eén of twee superusers van de hoofdpst heeft alle rechten in de hoofdpst.

3.5. Gegevensbescherming

3.5.1. Algemeen

Opdrachtnemer beveiligd alle gegevens die tot de (cloud)dienst behoren (ook die van niet-productieomgevingen) van Opdrachtgever op adequate wijze, zodanig dat bescherming wordt geboden tegen gegevensverlies als wel toegang tot gegevens door onbevoegden. Met "alle gegevens" wordt bedoeld zowel "data in use", "data in motion" als "data at rest" binnen Oplossing.

In de hoofdpst dienen alle opgeslagen gegevens te worden beschermd door middel van versleuteling conform de marktstandaarden zoals opgenomen bij het Forum Standaardisatie. De technische implementatielaag en versleutelingstechniek moet aantoonbaar voldoen aan deze standaarden en waarborgt dat bij onbevoegde toegang of een datalek uitsluitend versleutelde, nietszeggende en onleesbare data kan worden verkregen.

De omgeving waar de gegevens worden opgeslagen is gestationeerd in een land die behoort tot de Europese Economische Ruimte (EER).

3.5.2. Multi-tenancy

Bij multi-tenancy zijn afdoende maatregelen getroffen om te voorkomen dat gegevens van Opdrachtgever bedoeld of onbedoeld worden gedeeld met derden, dan wel worden gecombineerd met gegevens van andere klanten door

aggregatie of interferentie. De hoofdpост kan onafhankelijk van met andere klanten gedeelde infrastructuur en/of virtuele componenten worden ingericht en onderhouden.

3.5.3. Versleutelde verbinding

De hoofdpост wordt te allen tijde benaderd op basis van een versleutelde verbinding. Bij transport van vertrouwelijke informatie over onbetrouwbare netwerken, zoals het internet, wordt te allen tijde gebruikt gemaakt van versleutelde verbindingen en 2-factor authenticatie conform de laatste stand der techniek. Dit geldt ook indien er sprake is van toegang op afstand vanuit Opdrachtnemer, bijvoorbeeld voor ondersteunende werkzaamheden.

3.5.4. Verzenden emails

Bij het sturen 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 en IPv4 en IPv6, HTTPS en HSTS verkeer en kan hierop getoetst worden via www.internet.nl.

Bij gunning zal gedurende de looptijd van het contract de applicatie blijvend moeten voldoen aan een score op internet.nl van >90%, zowel voor de ICT Prestatie als voor de domeinnamen die het gebruikt.

3.5.5. Eigendom gegevens/veilig stellen data

Vanwege hosting buiten het domein van de Opdrachtgever is er enige onzekerheid dat gegevens beschikbaar blijven bij faillissement van de Opdrachtnemer of diens hostingpartij. Alle gegevens in de hoofdpост zijn en blijven te allen tijde eigendom van Opdrachtgever en mogen door Opdrachtnemer niet voor andere doeleinden worden gebruikt. Bij beëindiging van de overeenkomst worden alle gegevens overgedragen aan de Opdrachtgever in een leesbaar en standaard uitwisselformaat zonder meerkosten.

Alle gebruikte koppelvlakken worden toegevoegd in de hoofdpост onder bestanden/archief.

3.6. Identificatie & Authenticatie

3.6.1. Authenticatiedienst

De authenticatiedienst van Opdrachtnemer worden gekoppeld aan de authenticatiedienst van Opdrachtgever. Opdrachtnemer biedt een federatief koppelvlak aan voor uitwisseling van rollen en rechten. De verplichte standaard hiervoor is Microsoft Entra ID en SAML 2.0, alleen Azure AD. Opdrachtgever stelt praktische inrichtingseisen bij implementatie.

3.6.2. 2-factor authenticatie

Indien Opdrachtnemer niet kan aansluiten op het federatief koppelvlak van Opdrachtgever, biedt Opdrachtnemer zélf een sterke, in de markt gangbare, methode voor 2-factor authenticatie waarbij de 2de factor wordt gebaseerd op iets dat de gebruiker heeft en bij voorkeur in de vorm van een authenticator-app. Authenticatie via onbetrouwbare netwerken vindt te allen tijde plaats op basis van tenminste 2-factor authenticatie. SMS-verificatie of via spraak-verificatie is niet toegestaan.

3.6.3. Wachtwoord eisen

De hoofdpост biedt de mogelijkheid dat een gebruiker zélf zijn wachtwoord kan wijzigen waarbij eisen aan constructie, geldigheidsduur en toepassing zijn gebaseerd op het vigerende wachtwoordbeleid zoals in de CSIR is beschreven.

3.6.4. Versleuteling wachtwoord

Wachtwoorden worden bij invoer niet op het scherm getoond en worden versleuteld (gehasht) opgeslagen binnen de hoofdpост waarbij de versleutelde waarde niet zichtbaar kan worden gemaakt via beheerinterfaces of reverse engineering.

Er wordt geen gebruik gemaakt van voor gedefinieerde dan wel hard gecodeerde wachtwoorden in het algemeen en in het bijzonder bij standaard accounts. Accounts zonder wachtwoordbeveiliging zijn niet toegestaan.

3.6.5. Single Sign On

Single Sign On moet mogelijk zijn en kosteloos toegevoegd kunnen worden in een eventueel later stadium. Hierbij moet rekening worden gehouden dat elke gemeente, het waterschap en onderhoudspartijen haar eigen omgeving heeft, in de meeste gevallen is het een Microsoft Entra omgeving.

3.6.6. Administratie accounts

Opdrachtnemer geeft inzicht in hoe het aanvragen en muteren van toegang door gebruikers (inclusief toegang op afstand) plaatsvindt en hoe wachtwoorden worden toegewezen. De hoofdpst houdt een administratie van uitgegeven en ingetrokken accounts bij.

3.7. Informatieveiligheid

3.7.1. Vulnerability scan

Een vulnerability scanner op de hoofdpst wordt toegepast om continue zwakheden op te sporen van de applicatie en zijn verbindingen/netwerk. Zowel authenticated en unauthenticated scans worden toegepast. Zwakheden dienen te worden geclassificeerd/geprioriteerd volgens de tabel in sub-paragraaf 4.7.2 en opgelost te zijn binnen de gestelde termijn. Gevonden zwakheden worden aan de Opdrachtgever doorgegeven. Indien er mogelijk sprake is van oneigenlijk gebruik dan gaat er direct een melding (geautomatiseerd) naar de Opdrachtgever door middel van een email aan een nader te bepalen contactpersoon. De Opdrachtnemer zal direct actie ondernemen om de omgeving veilig te stellen.

3.7.2. Pentest

Er wordt minimaal jaarlijks een pentest uitgevoerd op de hoofdpst en bijbehorende verbindingen. Minimaal de meest voorkomende kwetsbaarheden in de OWASP-top 10 worden gescand.

De Opdrachtnemer is ervoor verantwoordelijk dat de pentest wordt uitgevoerd door een onafhankelijke partij waarmee de Opdrachtnemer geen enkel belang heeft. De onafhankelijke partij dient voorafgaand aan de pentest eerst worden beoordeeld door de Opdrachtgever. De Opdrachtgever heeft de mogelijkheid om de Opdrachtnemer te verplichten een andere pentestuitvoerder te selecteren.

De bevindingen worden geclassificeerd door onderstaand schema door de onafhankelijke partij. Alle testen en bevindingen en de eventueel te ondernemen/ ondernomen maatregelen worden schriftelijk aan de Opdrachtgever medegedeeld. Deze schriftelijke mededeling wordt maximaal 10 werkdagen nadat de pentest is uitgevoerd aangeleverd.

Eventuele aanpassingen n.a.v. de pentest worden geprioriteerd uitgevoerd volgens onderstaande tabel:

Classificatie	Omschrijving	Opgelost binnen
Laag	Laag risico op gecompromitteerde beveiligingscontrole met meetbare negatieve impact als resultaat.	30 werkdagen
Middelmatig	Middelmatig risico op gecompromitteerde beveiligingsinrichting met minimale financieel, reputatie, milieu en/of waterschade als resultaat.	10 werkdagen
Hoog	Hoog risico op gecompromitteerde beveiligingsinrichting met mogelijke (significante) financieel, reputatie, milieu en/of waterschade als resultaat.	2 werkdagen
Extreem	Extreem hoog risico op gecompromitteerde beveiligingsinrichting met mogelijke catastrofale financiële, reputatie, milieu en/of waterschade als resultaat.	1 werkdag

Indien de classificatie van het betreffende web security issue uit de pentest of vulnerability scan 'Extreem' of 'Hoog' is en gebruik van de hoofdpst niet verantwoord meer mogelijk is, dan wordt de hoofdpst tijdelijk afgesloten. De Opdrachtnemer neemt hiervoor de eindverantwoording. Situaties waarin meer dan normale kwetsbaarheden of risico's aanwezig zijn, worden onmiddellijk gemeld aan en besproken met de nog nader aan te wijzen hoofdcontactpersoon van de Opdrachtgever.

Alle kosten die gemaakt moeten worden om calamiteiten te voorkomen of calamiteiten op te lossen door toedoen van het stilleggen van systeem zijn voor de Opdrachtnemer.

De Opdrachtgever heeft toestemming om zelf een pentest te (laten) uitvoeren op de hoofdpst. De Opdrachtgever zal de Opdrachtnemer informeren indien zij de pentest zelf wil laten uitvoeren. Zonder meerkosten stelt de Opdrachtnemer een kopie-omgeving van de hoofdpst beschikbaar voor deze pentest.

Na gunning van de opdracht en vóór oplevering van de eerste gemeente laat de inschrijver een penetratietest (pentest) uitvoeren door een onafhankelijke (op geen enkele wijze gelieerd aan de inschrijver), binnen de sector erkende partij met aantoonbare ervaring met o.a. hoofdpsten. Het onderzoeksobject van de pentest omvat de door de inschrijver

geleverde en beheerde onderdelen van de ICT-prestatie. De planning/ scope van de pentest wordt altijd in afstemming met de Opdrachtgever bepaald. Indien de Opdrachtnemer in deze periode een pentest heeft uitgevoerd waarbij bewijsbaar de technische configuratie van de hoofdpst, versie en koppelingen met de hoofdpst identiek zijn dan volstaat het delen van de penetratietest resultaten.

Alle kosten voor de pentest, rapportage, her-tests en het doorvoeren van maatregelen zijn inbegrepen in de inschrijving. Bevindingen met een classificatie Hoog en Extreem dienen vóór oplevering van de eerste gemeente te zijn opgelost en gevalideerd middels een her-test.

Bevindingen met een classificatie Middelmatig en Laag dienen vóór totale oplevering te zijn opgelost, of te zijn voorzien van een door de inschrijver opgesteld en door de Opdrachtgever goedgekeurd plan van aanpak.

De resultaten van de pentest en de opvolging daarvan worden volledig kosteloos gerapporteerd aan de Opdrachtgever.

3.7.3. Oplossen beveiligingsincidenten

Opdrachtnemer start na melding/constatering van (beveiligings)incidenten direct met het oplossen ervan (ongeacht welke weekdag of tijdstip). Er wordt continue aan gewerkt om het beveiligingsprobleem zo spoedig mogelijk op te lossen. De beveiligingsrisico-indeling en de procedure is gelijk aan de hetgeen in paragraaf 4.7.2 is beschreven bij het vinden van een beveiligingsrisico na een pentest.

Indien sprake is van ransomware of gijzelsoftware waarbij de oorzaak is toe te schrijven aan de Opdracht-nemer dan is de Opdrachtnemer volledig verantwoordelijk voor het herstel. De beschikbaarheidsgaranties die in hoofdstuk 5 beschreven zijn in het PvE voor de onderdelen hoofdpst en overstortmonitoring zijn in dit geval nog steeds van toepassing, inclusief de daaraan gekoppelde boeteclausule en nevenkosten die gemoeid zijn indien de hoofdpst voor langere tijd niet beschikbaar is (zoals beschreven in de Dienstverleningsovereenkomst).

3.8. Meldplicht datalekken

3.8.1. Melden beveiligingsincidenten

Als Opdrachtnemer informatie van Opdrachtgever host op haar systemen, dienen (beveiligings)incidenten direct door Opdrachtnemer gemeld (uiterlijk binnen 12 uur) te worden aan de betrokken contactpersoon van Opdrachtgever.

Indien logging en auditgegevens relevant zijn voor een (lopend) onderzoek naar een (vermoed) informatiebeveiligingsincident, dienen deze gegevens veiliggesteld te worden en gedurende de volledige afhandelingstermijn en de daaropvolgende juridische verjaringstermijn (minimaal 5 jaar na incidentdatum) bewaard te blijven.

3.8.2. Kwalificatie datalek

In het geval de verwerking van persoonsgegevens door Opdrachtnemer deel uitmaakt van de af te nemen producten en/of diensten, accepteert Opdrachtnemer dat hij beveiligingsincidenten op het moment van onderkennen, direct meldt aan Opdrachtgever. Opdrachtgever beslist of een beveiligingsincident kan worden gekwalificeerd als datalek en zorgt in dat geval voor de melding aan de Autoriteit Persoonsgegevens en het in kennis stellen van de betrokkenen.

3.9. Privacy

Opdrachtnemer accepteert dat als er persoonsgegevens worden verwerkt binnen de hoofdpst er een verwerkersovereenkomst wordt afgesloten (zie Bijlage 2.2) met als basis het standaard VNG-model) als onderdeel van het contract.

3.10. Servicevoorwaarden

3.10.1. Patch- en Vulnerability Management

De Opdrachtnemer verhelpt kwetsbaarheden in de hoofdpst en de onderliggende infrastructuur conform de richtlijnen van het NCSC en de IBD.

Kritieke updates (Noodpatches):

Bij kwetsbaarheden met een hoog risico (bijv. CVSS-score > 7.0 of geclassificeerd als 'High/Critical' door NCSC/IBD) rolt de Opdrachtnemer de benodigde patches onverwijld uit, doch uiterlijk binnen 3 dagen na beschikbaarheid. Indien hiervoor (onvoorziene) downtime nodig is, wordt de Opdrachtgever hierover voorafgaand geïnformeerd. Deze noodpatches worden kosteloos doorgevoerd.

Reguliere updates:

Minder kritische beveiligingsupdates worden meegenomen in de eerstvolgende reguliere onderhoudscyclus (release window).

Informatievoorziening:

De Opdrachtgever wordt proactief geïnformeerd over de status van kritieke patches en de impact op de dienstverlening

3.10.2. DDoS maatregelen

De hoofdpst, inclusief de onderliggende infrastructuur, moet effectief zijn beveiligd tegen Distributed Denial of Service (DDoS) aanvallen op alle relevante lagen (netwerk-, transport- en applicatielaag), in lijn met de relevante publicaties van het NCSC, zoals de factsheet 'Continuïteit van online diensten' en de factsheet 'Technische maatregelen voor de continuïteit van online diensten'

3.10.3. Informatievoorziening

De Opdrachtgever wordt proactief geïnformeerd over de status van kritieke patches en de impact op de dienstverlening.

3.10.4. Testen

Alle betrokken systeemcomponenten zijn ontworpen en getest op het voorkomen van inbreuken op beschikbaarheid, integriteit en vertrouwelijkheid. Er wordt minimaal gebruik gemaakt van een test-, acceptatie- en productieomgeving om eventuele programmeerfouten zoveel mogelijk te voorkomen. Indien de Opdrachtgever dit wenst heeft zij de mogelijkheid om toegang te krijgen tot de acceptatieomgeving en kan zij zelf testen uitvoeren, alvorens de nieuwe versie van de programmatuur naar de productieomgeving wordt omgezet.

3.10.5. Back-up en recovery

Opdrachtnemer heeft een back-up en recovery beleid dat voldoet aan de eisen uit de CSIR en waarbij minimaal de volgende eisen van toepassing zijn op de back-up en restorevoorzieningen van Oplossing:

- De 3-2-1 regel wordt toegepast (3 kopieën (orgineel + 2 back-ups) op 2 verschillende media en 1 kopie off-site);
- Een incident op de ene locatie kan niet leiden tot schade op de andere locatie (ook niet in het geval van ransomware);
- De hoofdpst wordt bij calamiteiten binnen 1 kalenderdag hersteld;
- Gegevensverlies bedraagt maximaal 28 uur;
- Hersteltijd in geval van incidenten is maximaal 16 werkuren in 85% van de gevallen;
- Het restoren van back-ups wordt minimaal jaarlijks of na een grote wijziging getest waarbij recovery-procedures voortdurend worden bijgewerkt;
- Er is sprake van een reconstructiemechanisme als geen data verloren mag gaan;
- Back-ups worden beschermd tegen onbevoegde toegang;
- De data-integriteit van de hoofdpst en diens gekoppelde softwaresystemen dien gewaarborgd te zijn;
- Opdrachtnemer zorgt voor adequate afspraken over back-up en recovery en voldoet aantoonbaar aan relevante punten uit het beleid.

Het gebruik van een CMDB in een telemetriesysteem kan de algehele efficiëntie, betrouwbaarheid en onderhoud van het systeem verbeteren. Het stelt teams in staat om beter geïnformeerde beslissingen te nemen, snel problemen op te lossen en de levenscyclus van de apparaten effectief te beheren.

3.10.6. Cyber Resilience Act (CRA)

De nieuw in te zetten apparatuur die communiceert met de hoofdpst moet aantoonbaar voldoen aan de Cyber Security Act (CRA).