Bijlage 4. Programma van Eisen

Inhoud

Aanbestedingseisen Inhoudelijk 1

Aanbestedingseisen IM&ICT Algemeen 1

Aanbestedingseisen IM&ICT Data 2

Aanbestedingseisen ICT & Security eisen 3

Aanbestedingseisen informatiebeheer vakapplicatie 6

Aanbestedingseisen IM&ICT Integratie 9

Aanbestedingseisen IM&ICT Mobile Devices 10

Aanbestedingseisen IM&ICT Technische Infrastructuur 10

Aanbestedingseisen IM&ICT Overig 10

Aanbestedingseisen Inhoudelijk

Nr	Eis
IH1	Inhoudelijke eis 1 *Trainingen op het gebied van Informatieveiligheid, BIO, WPG, AVG, privacy binnen materiewetten gemeente.*

Aanbestedingseisen IM&ICT Algemeen

Nr	Eis
A1	**SLA** Opdrachtnemer stuurt binnen 10 kalenderdagen na opdrachtverlening een concept SLA mee welke als uitgangspunt voor de overeenkomst dient. Het SLA moet minimaal de volgende onderwerpen bevatten: - Structurele updates van de server en software die ervoor zorgen dat de veiligheid, performance en betrouwbaarheid van de oplossing gewaarborgd blijft. - Reactie- en oplostijden bij incidenten. - Procesafspraken in verband met incidenten en onderhoud. Zie bijlage voor voorbeeld.
A2	**Toegankelijkheid** De oplossing voldoet aan de toegankelijkheidseisen EN 301 549 (WCAG 2.1 AA/ WCAG 2.2)/ laatst actuele versie. We begrijpen dat dit een gezamenlijke inspanning is om

	hieraan te voldoen. Opdrachtnemer moet ons echter wel in staat stellen hieraan te kunnen voldoen. Opdrachtnemer is verantwoordelijk voor het technisch deel, opdrachtgever voor het contentdeel.
A3	**Afhankelijkheden van derden** De leverancier dient duidelijk aan te geven welke afhankelijkheden er zijn van onderaannemers. Indien de leverancier gebruik maakt van onderaannemers zijn de voorwaarden opgesomd in dit document ook van toepassing op de onderaannemers.

Aanbestedingseisen IM&ICT Data

Stuurinformatie en rapportages (algemene info)
Er wordt onderscheid gemaakt tussen stuurinformatie en rapportages op operationeel niveau en stuurinformatie op strategische en tactisch niveau.

Binnen de applicatie voor bewustwordingscampagne Informatieveiligheid en Privacy zijn de dagdagelijkse en operationele rapportages beschikbaar. Deze rapportages zijn eenvoudig aan te maken door de functioneel beheerder binnen de applicatie zelf.

Gebruikers kunnen deze rapportages zelf opstarten binnen de applicatie voor bewustwordingscampagne Informatieveiligheid en Privacy.

Strategische en tactische informatie wordt gepubliceerd in de Business Intelligence-omgeving van de opdrachtgever, waardoor het management, de directie en het bestuur deze informatie op een centrale locatie kunnen raadplegen. Strategische en tactische rapportages zijn voor de scope van de aanbesteding voor instrumenten bewustwordingscampagne Informatieveiligheid en Privacy niet van toepassing.

Nr	Eis
D1	**Eigenaarschap:** De opdrachtgever is en blijft eigenaar van de data in de applicatie.
D2	**Kosten data beschikbaar stellen** Er worden geen extra kosten in rekening gebracht voor het beschikbaar stellen van de data.
D3	**Vernietiging data:** Informatie kan definitief worden vernietigd (de gemeente is hierbij in de lead). Leverancier maakt samen met gemeente afspraken rondom verantwoorde vernietiging in overeenstemming met het bewaar- en vernietigingsbeleid van de opdrachtgever. De gemeente heeft zich geconformeerd aan de selectielijst 2020. Het vernietigingsbeleid is gebaseerd op de archiefwet.
D4	**Bewaren data**: Informatie kan in zijn originele digitale vorm worden overdragen naar een systeem waarin de informatie gearchiveerd wordt.
D5	**Integratie netwerk gemeente met extern:** Koppelingen tussen het netwerk van opdrachtgever en de 'buitenwereld' extern vinden standaard plaats via een Data gateway voorziening van de opdrachtgever. Verbindingen worden opgezet via https.
D6	**Operationele informatie** Binnen de applicatie zijn de dagdagelijkse en operationele rapportages beschikbaar. In deze rapportages is minimaal de onderstaande informatie overzichtelijk visueel weergegeven:

	- Per team kan worden getoond per training welke persoon de training op welke datum met goed gevolg heeft afgerond ○ Het moet tevens mogelijk zijn om de aantallen op teamniveau te raadplegen (anoniem) - Overige gegevens nodig voor accountability doeleinden
D7	**Rapportage eenvoudig aan te maken** Deze operationele rapportages zijn eenvoudig aan te maken door de key-user binnen de applicatie zelf
D8	**Opstarten operationele rapportages door gebruikers** Gebruikers kunnen deze operationele rapportages zelf opstarten binnen de applicatie.

D9	**Datakwaliteit** -> gegevens dienen zo correct mogelijk worden ingevoerd.
	• Verplichte velden zijn echt verplicht
	• Gebruiken van veldvalidatieregels in de applicatie zoals:
	  ○ Bij telefoonnummer kunnen alleen cijfers worden ingevoerd.
	  ○ Een datum-tijdveld accepteert alleen geldige datums en tijden
	  ○ Een valutaveld accepteert alleen geldbedragen
	• Gebruiken van invoermaskers
	  ○ Een invoermasker kan gebruikers bijvoorbeeld verplichten om datums in een Europese notatie in te voeren, zoals 14-02-2024.
	• Door – waar mogelijk – keuzelijsten te gebruiken in plaats van vrije tekst

D10	Leverancier en applicatie moeten rechten van betrokkenen kunnen borgen, bijv. inzageverzoek of verzoek tot verwijdering

Aanbestedingseisen ICT & Security eisen

Nr	Eis
	Algemeen
IS1	De te leveren (web)applicatie/dienst voldoet aan de Baseline Informatiebeveiliging Overheid. https://bio-overheid.nl/
IS2	De complete omgeving, dus alle (web)applicaties en onderliggende infrastructuur zijn ingericht conform de verplichte standaarden van het Forum Standaardisatie: zie link. https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht
	Beheerorganisatie
IS3	De medewerkers van de opdrachtnemer (beheerorganisatie) hebben een recente Verklaring Omtrent Gedrag (VOG) of beschikken over een Screening van Justitie.
	Authenticatie
IS4	De aangeboden oplossing maakt geen gebruik van lokale gebruikers, maar sluit aan op de gemeentelijke authenticatiemogelijkheden, LDAPS of Entra AD Connect. Het is niet toegestaan andere authenticatiemethodes te gebruiken of een eigen systeem in het netwerk van de Opdrachtgever te plaatsen.
IS5	Ten behoeve van accountsynchronisatie wordt gebruik gemaakt van Entra AD Connect, SSO / SAML.

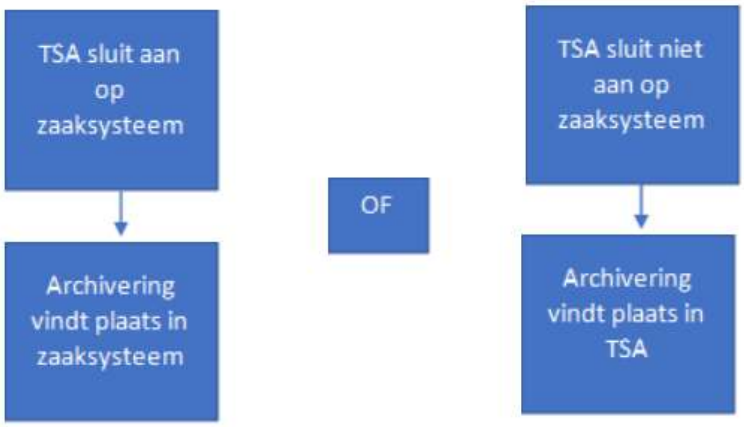
IS6	Alle accounts dienen persoonsgebonden te zijn.
	Web Services
IS7	In de response headers wordt de versie van de webserver of service niet meegestuurd.
IS8	Foutmeldingen geven geen details weer die misbruik mogelijk maken.
IS9	Al het webverkeer wordt middels TLS getransporteerd (https). Zie hiervoor ook de eisen voor TLS.
IS10	Alleen de benodigde HTTP-request methoden worden gebruikt. (B.v. GET, POST, PUT, DELETE)
IS11	Connecties via http worden automatisch doorverwezen naar https middels een http response status code 3xx.
IS12	De webserver stuurt securityheaders mee in de response headers. Voor een actueel overzicht van mee te sturen securityheaders zie: https://owasp.org/www-project-secure-headers/ Voor de Content Security Policy (CSP) geldt de volgende aanscherping: Onveilige configuraties zoals het gebruik van 'unsafe-inline' en 'unsafe-eval' zijn niet toegestaan. Het whitelisten van bronnen kan uitsluitend via een secure verbinding (https). De website heeft een A+ rating op https://securityheaders.com/
IS13	De webapplicatie is minimaal beschermd tegen OWASP top 10 aanvallen. https://owasp.org/www-project-top-ten/
IS14	De webapplicatie is conform de ict-beveiligingsrichtlijnen voor webapplicaties van het NCSC gebouwd. https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties
IS15	Voor mobiele apps, dient de inschrijver aan de ICT-beveiligingsrichtlijnen voor mobiele apps te voldoen. https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-mobiele-apps. Zie ook richtlijnen document MDM van de opdrachtgever. Ook zijn de apps altijd beschikbaar in Apple of Android store, geen sideloaded apps toegestaan.
IS16	Een webbased userinterface is zonder beperking van functionaliteit benaderbaar door de laatste twee versies van de meest gangbare en ondersteunde browsers Microsoft Edge is een vereiste (aanvullend Google Chrome, Apple Safari en Mozilla Firefox) zonder gebruik te maken van NPAPI plug-ins (zoals Flash, Silverlight, ActiveX, etc.)
IS17	Gebruikte Cookies zijn voorzien van de attributen ‘Secure’ en ‘HttpOnly’. Cookies met gevoelige informatie hebben een korte levensduur en maken gebruik van het ‘SameSite’ attribuut met als waarde ‘Strict’ of ‘Lax’.
	E-mail
IS18	Binnen de Opdrachtgever verloopt mailverkeer met een (sub)domein uitsluitend via onze exchange server. Hierdoor kunnen we het serviceaccount en het mailverkeer beter beheren en controleren. De volgende standaarden worden toegepast: SPF, DKIM, DMARC, STARTTLS, DANE.

	Domain Name System (DNS)
IS19	Wordt door opdrachtnemer een ‘eigen’ domein gebruikt, dan moet DNSSEC (Domain Name System Security Extensions) worden toegepast.
IS20	Domeinen waarvoor certificaten zijn uitgegeven dienen CAA records (DNS Certification Authority Authorization) te publiceren.
IS21	Voor controle slagen via forum standaardisatie van het 'eigen' domein n.a.v. deze technische eisen moet de gemeente een CNAME op het eigen domein aanmaken met bijhorend overheidscertificaat die in de applicatie toegevoegd dient te worden.
	Transport Layer Security (TLS)
IS22	Indien een domeinnaam wordt gebruikt die niet eigendom is van Opdrachtgever, dient de opdrachtnemer een officieel erkend certificaat te gebruiken. Die voldoet aan de eisen van forum standaardisatie en die alleen voldoende of sterke cipher suites gebruikt.https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1
IS23	TLS is volgens de richtlijnen van het NCSC ingericht. https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1
IS24	De server is zo ingericht en onderhouden dat deze een A+ rating behaalt op SSL Labs. https://www.ssllabs.com/ssltest/index.html
	Governance
IS25	De inschrijver en eventuele onderaannemers zijn ISO27001/2 (Informatiebeveiliging) gecertificeerd en/of is in het bezit van een geldige ISAE3402 SOC2 assurance rapportage en/of levert ten tijde van de inschrijving jaarlijks een TPM-verklaring over de gehele dienstverlening inclusief onderaannemers, uitgegeven door een IT Auditor (RE en/of CISA), waarmee assurance wordt afgegeven over de kwaliteitsaspecten integriteit, beschikbaarheid en vertrouwelijkheid in opzet, bestaan en werking. De jaarlijkse kosten van de TPM worden meegenomen in de totale kosten van de aangeboden dienstverlening.
IS26	De opdrachtnemer ondertekent bij gunning en vooraf aan de POC de vrijwaringsverklaring waardoor de Opdrachtgever pentesten kan (laten) uitvoeren op de aangeboden oplossing. De template van deze vrijwaringsverklaring kan bij de Opdrachtgever worden opgevraagd.
IS27	De opdrachtnemer werkt kosteloos mee aan audits uitgevoerd door of in opdracht van de aanbesteder. Deze audits worden uitgevoerd door of onder verantwoordelijkheid van een RE of CISA.
	Cloud
IS28	De ICT-infrastructuur van de geboden oplossing is in zijn geheel ondergebracht in een datacenter binnen de EER. (Niet van toepassing bij On Premise installatie).
	Koppelingen
IS29	De geboden oplossing ondersteunt zowel IPv4 als IPv6. Voor Cloud oplossingen dienen beide actief te zijn.
IS30	Koppelingen/verbindingen tussen systemen en/of services (ook als deze op hetzelfde systeem draaien) worden door opdrachtnemer bij inschrijving inzichtelijk gemaakt in een protocol matrix, waarin de verkeerstromen zijn opgenomen. Deze matrix bestaat minimaal uit de volgende velden:

	• Source IPv(4/6) • Source Port • Destination IPv(4/6) • Destination Port • Layer 4 protocol (bijv. TCP/UDP/...) Application protocol (bijv.: http/https/smtp/dns/...).
IS31	Koppelingen vanuit de SaaS omgeving van de opdrachtnemer naar derden (bv andere SaaS omgevingen) lopen ten allen tijden via de integratie laag (reverse proxy) van de Opdrachtgever. Rechtstreekse koppelingen zijn dus niet toegestaan.
IS32	Koppelingen met onze integratie laag hebben minimaal het onderstaande beveiligingsniveau: REST architectuur: TLS & API Key SOAP / StUF architectuur: TLS Mutual Authentication
IS33	Het aanbieden van RDP-koppelingen (of vergelijkbaar) evenals het gebruik van Remote Desktop Gateway is niet toegestaan.
	Versiebeheer
IS34	De webapplicatie en onderliggende ICT-componenten zijn altijd up-to-date. Opdrachtnemer mag maximaal 1 stabiele patch aan het einde van de train (bijv 1.0.0.1)achterlopen, mits deze versie nog volledig wordt ondersteund door de betreffende leverancier van dat component en geen kwetsbaarheden bevat.
	Security Incidenten
IS35	Security incidenten worden onverwijld (binnen 4 uur), na hiervan op de hoogte te zijn, gemeld bij de Opdrachtgever.
IS36	Bij security incidenten worden de gevolgen zo snel mogelijk ongedaan gemaakt dan wel beperkt, waardoor het incident onder controle wordt gebracht. Over de genomen maatregelen wordt de Opdrachtgever geïnformeerd.

Aanbestedingseisen informatiebeheer vakapplicatie

Er zijn twee opties om te voldoen aan goed informatiebeheer. Of er wordt gekoppeld met het zaaksysteem waarbij de archivering en vernietiging ook plaatsvindt in het zaaksysteem. Of de taakspecifieke applicatie (TSA) beschikt over een eigen archiefsysteem dat voldoet aan een aantal eisen.
Zijn beide opties (uiterste geval!) niet mogelijk dan moet voorzien worden in een analyse en een plan van aanpak hoe informatiebeheer (bewaren en vernietigen) dan kan worden geborgd. Dit geldt ook voor het geval de oplossing gebaseerd is op de Common Ground gedachte.



In het geval van de aanbesteding instrumenten bewustwordingscampagne Informatieveiligheid en Privacy geldt dat er niet wordt aangesloten op een zaaksysteem.

TSA sluit niet aan op zaaksysteem

Nr	Eis	Toelichting
	Bewaren	
IB1	Informatie (bestanden en metadata) moet toegankelijk en duurzaam blijven tijdens de geldende bewaartermijn.	**Toegankelijk** betekent vindbaar, beschikbaar, leesbaar, interpreteerbaar en betrouwbaar voor degenen die er recht op hebben, vanaf het moment van ontstaan en voor zolang als noodzakelijk (gerelateerd aan geldende bewaartermijn). **Duurzaam** betekent dat de toegankelijkheid van de informatie bestand is tegen veranderingen van elke aard. Deze **geldende bewaartermijn** kan variëren van 6 weken tot 20 jaar (na in werking treding nieuwe Archiefwet is de termijn uiterlijk 10 jaar).
	Authenticiteit en integriteit	
IB2	De integriteit van een digitaal bestand en van de bijbehorende metadata moet kunnen worden gewaarborgd	Er moet gewaarborgd worden tegen onbedoelde en ongeautoriseerde wijzigingen, beschadigingen en verwijdering.
	Vernietigen	

IB3	Het moet mogelijk zijn vernietigingslijsten/ overzichten te genereren op basis van een vooraf ingestelde vernietigingstermijn	Deze vernietigingstermijn wordt bij voorkeur opgesteld op zaak- of procesniveau
IB4	Het moet mogelijk zijn deze vernietigingslijsten als bestandsvorm op te slaan	
IB5	Het moet mogelijk zijn deze vernietigingslijsten te kunnen distribueren	
IB6	Het moet mogelijk zijn op basis van deze vernietigingslijsten de informatieobjecten (zaak, metadata, documenten) te kunnen vernietigen	
IB7	Het moet mogelijk zijn een bewijs van vernietiging te kunnen opslaan in een bestandsvorm	De vernietigingslijst en het bewijs van vernietiging moeten blijvend bewaard worden
IB8	Het moet mogelijk zijn de vernietigingslijst te voorzien van een specifieke set aan metadata: zaaknummer (of uniek identificatienummer), omschrijving zaak/proces, startdatum zaak/proces, resultaat van de zaak/proces, einddatum van afhandeling, bewaartermijn)	
IB9	De applicatie biedt de mogelijkheid tot definitief vernietigen van alle gegevens en bestanden, ook backups	Opdrachtnemer garandeert dat back-ups na een overeengekomen termijn vernietigd worden en dat na beëindiging van de overeenkomst alle achtergebleven informatie wordt vernietigd.
IB10	Leverancier moet applicatie privacy by design & by default inrichten	

Bij de onderhanden aanbesteding is de wens dat de applicatie voor bewustwordingscampagne Informatieveiligheid en Privacy geïntegreerd kan worden met de e-learning module van het gemeentelijke personeelsadministratiesysteem AFAS. AFAS beschikt ook over een module om conform bovenstaande eisen gegevens en bestanden te kunnen archiveren en vernietigen. Indien uw applicatie een zodanige integratie met AFAS biedt, en de opdrachtgever hiervan gebruik wil maken, dat de gegevens en bestanden in uw applicatie in AFAS gearchiveerd en vernietigd kunnen worden conform bovenstaande eisen, dan hoeft uw applicatie niet aan bovenstaande eisen IB3 t/m IB8 te voldoen. Vereist is dan wel dat zodra gegevens zijn uitgewisseld met AFAS, deze direct in de applicatie voor bewustwordingscampagne Informatieveiligheid en Privacy worden vernietigd, zodat er geen sprake is van meervoudige opslag van gegevens en bestanden.

Aanvullende vragen (geen eisen) (tenzij deze ook bij eisen/ wensen/ vragen zaaksysteem worden opgenomen)

1. Welke bestandsformaten kunnen worden opgeslagen in de applicatie?
2. Is het mogelijk bewaar- en vernietigingstermijnen in te stellen (bij voorkeur op zaakniveau)? Zo ja, toon dit aan.
3. Is het mogelijk deze termijnen per zaak handmatig aan te passen (in geval van uitzondering van vernietiging)? Zo ja, toon dit aan.
4. Wat is de retentietermijn van back-ups?

Algemeen digitaal informatiebeheer

Nr	Eis	Toelichting
IB10	Indien binnen de applicatie gebruik wordt gemaakt van algoritmes dan moeten de algoritmes in een leesbaar formaat kunnen worden opgeslagen en tevens buiten de applicatie worden bewaard	Indien gebruik gemaakt wordt van algoritmes dan dient de gemeente deze openbaar te maken. (Selectielijst 2020)
IB11	Indien de oplossing gebruik maakt van een algoritme, dient vooraf de ontwerpdocumentatie incl. input en output overlegd te worden ter archivering	Indien gebruik gemaakt wordt van algoritmes dan dient de gemeente deze openbaar te maken. (Selectielijst 2020). De gemeente dient zich te kunnen verantwoorden over de uitvoering van zijn taken. Indien in een proces een algoritme de beslissingen neemt i.p.v. de ambtenaar moet de gemeente zich kunnen verantwoorden over deze beslissingen.

Aanbestedingseisen IM&ICT Integratie

Nr	Eis
IN1	Uw oplossing biedt in beginsel een integratie met de e-learning module van het gemeentelijke AFAS personeelsadministratiesysteem. Het moet teven mogelijk zijn om hier geen gebruik van de maken indien de opdrachtgever dat wenst.

Aanbestedingseisen IM&ICT Mobile Devices

Nr	Eis/Wens
M1	Uw oplossing is dusdanig geprogrammeerd dat ze herkennen op welke apparaat de applicatie wordt geopend en hier hun schermopbouw op aanpassen (responsive design).
M2	Een mobiele applicatie (app) maakt geen gebruik van dataopslag op het apparaat of in een andere cloud dan het bronsysteem.
M3	Belanghebbenden werken altijd met de meest actuele versie van een App. Adviezen van de Informatie Beveiligings Dienst (IBD) worden hierin opgevolgd.
M4	Bij een zakelijke app voor belanghebbenden die de gemeente in gebruik neemt, heeft de leverancier reeds bij het ontwerp en realisatie van de app goed over de beveiliging nagedacht (security by design).
M5	Een app die in gebruik wordt genomen dient te voldoen aan de Baseline informatiebeveiliging. Op basis van dataclassificatie moet de App mogelijk aan extra maatregelen voldoen.

Aanbestedingseisen IM&ICT Technische Infrastructuur

Nr	Eis/Wens
T1	Gegevens uit productieomgeving worden niet gebruikt in (O)T(A)-omgevingen (tenzij deze zijn geanonimiseerd en de gegevenseigenaar toestemming heeft gegeven).
	Performance
T2	Uw oplossing is in staat om alle interactieve gebruikersinterfaces (o.a. het schakelen tussen velden en schermen) voor de rollen eindgebruikers en functioneel beheerders in ten minste 80% van de gevallen binnen 3 seconden te tonen. Dit geldt niet voor het eventueel genereren van overzichten en rapportages, en uploaden van bestanden.
T3	Uw oplossing toont bij ten minste 90% van de gevallen binnen ten minste 2 seconden de zoekresultaten als sprake is van een eenvoudige zoekopdracht.

Aanbestedingseisen IM&ICT Overig

Nr	Eis
O1	Eis: Het recht op de nieuwste versies van het geleverde platform is inbegrepen bij het aanbod en de prijs.