Bijlage 1: Programma van eisen

Door voor deze aanbesteding een inschrijving in te dienen, verklaart inschrijver zich onvoorwaardelijk en volledig akkoord met onderstaande eisen. Eventuele voortvloeiende kosten uit onderstaande eisen dient inschrijver te verwerken in de prijsopgave. Onderstaande eisen kunnen dus niet leiden tot extra kosten.

Algemene eisen	
Eis	**Omschrijving**
1.	Opdrachtnemer is gehouden om bij de uitvoering van deze opdracht te allen tijde volledig te voldoen aan alle geldende Nederlandse wet- en regelgeving, alsmede aan van toepassing zijnde Europese wet- en regelgeving en overige relevante voorschriften en normen. Daarnaast dient opdrachtnemer te handelen conform de bepalingen van GIBIT 2023, waarin gemeentelijke inkoopvoorwaarden voor ICT-diensten en producten zijn vastgelegd en Opdrachtnemer dient gedurende de uitvoering van de opdracht tevens rekening te houden met het bepaalde in het inkoopbeleid.
2.	Alle documentatie van de processen en de systemen, evenals overige relevante informatie, dient door Opdrachtnemer up-to-date te worden gehouden en aan Opdrachtgever ter beschikking te worden gesteld. Opdrachtgever heeft te allen tijde het recht deze documentatie op te vragen en in te zien.
3.	Alle systeemlogging wordt ingesteld op Nederlandse tijd (CET/CEST), zodat gegevens eenvoudig door Opdrachtgever kunnen worden ingezien en gecontroleerd.
4.	Opdrachtgever heeft gedurende de volledige looptijd van de overeenkomst het recht om gebouwen dan wel gebouwdelen aan de overeenkomst, onder dezelfde condities als de oorspronkelijke gebouwen, toe te voegen of om gebouwen dan wel gebouwdelen kosteloos uit de overeenkomst te verwijderen.
5.	Onderaannemers voldoen aan dezelfde (beveiligings)eisen als Opdrachtnemer zelf en Opdrachtnemer is hiervoor verantwoordelijk.
6.	Na gunning dient als onderdeel van de implementatie door Opdrachtnemer een plan te worden uitgewerkt en voorgelegd te beoordeling over de wijze van verificatie en (acceptatie)test, inclusief verantwoordelijkheden van Opdrachtnemer en Opdrachtgever, de te hanteren criteria, de planning van tests per locatie en de wijze waarop bevindingen worden geregistreerd, opgevolgd en vrijgegeven voor definitieve acceptatie. De verificatie omvat tevens de correcte werking van het gebruik van tags/passen voor het veilig en betrouwbaar vrijgeven van printopdrachten en voor de kilometerregistratie in voertuigen, inclusief eventuele koppelingen met bestaande systemen.

Personeelseisen	
Eis	**Omschrijving**
7.	Alle door opdrachtnemer ingezette personen bij opdrachtgever spreken en communiceren in het Nederlands, gedragen zich passend in de gebouwen van opdrachtgever en zijn herkenbaar via bedrijfskleding of legitimatie. Opdrachtnemer waarborgt naleving van alle interne regels, huisregels en toepasselijke wet- en regelgeving, inclusief veiligheidsvoorschriften. Voor inzet bij opdrachtgever dient opdrachtnemer voor alle betrokken medewerkers over een geldige Verklaring Omtrent het Gedrag (VOG) te beschikken.
8.	Zowel de Opdrachtnemer, het bedrijf dat de feitelijke installatiewerkzaamheden uitvoert, als het in te zetten personeel dienen te beschikken over de juiste opleidingen, kennis, certificeringen en de ontwikkelingen in de markt. Zij zijn op de hoogte van de nieuwste ontwikkelingen op het gebied van toegangs- en sluitsystemen en zijn vertrouwd met de relevante procedures, werkmethoden, processen, materialen, machines en uit te voeren werkzaamheden. Het in te zetten personeel beschikt over de vereiste documenten en opleidingen om de toegewezen werkzaamheden verantwoord en vakbekwaam uit te voeren. Tijdens de uitvoering van werkzaamheden is te allen tijde minimaal één persoon met een geldige VOL-VCA-certificering aanwezig, evenals ten minste één persoon die aantoonbaar bekend is met de inrichting en specifieke omstandigheden van de betreffende locatie(s). Bij ziekte, vakantie of andere redenen van afwezigheid van personeel van Opdrachtnemer, dient Opdrachtnemer voor adequate vervanging te zorgen. Opdrachtnemer is verantwoordelijk voor het waarborgen van de continuïteit en kwaliteit van de werkzaamheden.
9.	Het personeel van Opdrachtnemer draagt zorg voor een schoon, opgeruimd en veilig werkterrein. Hiertoe worden passende maatregelen genomen ter voorkoming van vervuiling, beschadiging of verlies van bouwmaterialen, en ter waarborging van de veiligheid van de installatie, het gebouw, eigen medewerkers, alsmede van bezoekers en medewerkers van Opdrachtgever.

Systeem vereisten	
Eis	**Omschrijving**

10.	De hardware voor toegangscontrole moet worden geplaatst in een afgeschermde ruimte en voldoen aan Zero Trust-principes, waarbij alle communicatie wordt geauthentiseerd en geautoriseerd. Alle verbindingen naar en van deze hardware moeten uitsluitend via beveiligde protocollen verlopen.
11.	Bij storingen of uitval moet het systeem zodanig zijn ingericht dat alle locaties zelfstandig operationeel blijven. Dit betekent dat alle deuren toegankelijk blijven op basis van de laatst geladen autorisaties vóór het optreden van de storing. Deze functionaliteit blijft gegarandeerd beschikbaar totdat het systeem volledig is hersteld.
12.	Het systeem dient gelijktijdig gebruik door meerdere personen volledig te ondersteunen, zonder functionele beperkingen, dataverlies of prestatievermindering.
13.	Het systeem moet het aanmaken van tags en toegangspasjes ondersteunen met verschillende autorisatieniveaus. In het systeem moet het mogelijk zijn om toegangsrechten voor medewerkers centraal te beheren via een beheerportaal, inclusief rechten voor fysieke objecten zoals gebouwen, gebouwonderdelen en zones. Daarbij geldt dat Facilitaire Dienstverlening (FD) beschikt over de centrale beheerfunctionaliteit en decentrale beheerders de mogelijkheden hebben om een eigen subset van beheertaken uit te voeren.
14.	Voor kritieke ruimtes, zoals serverruimtes, moet het systeem een extra autorisatiestap ondersteunen. Toegang tot deze ruimtes wordt pas verleend nadat een groepsmanager IT Beheer de aanvraag heeft goedgekeurd.
15.	Het openen van deuren dient op afstand te kunnen plaatsvinden via het centrale beheerportaal, zodat medewerkers met de juiste autorisaties deuren kunnen openen zonder fysiek aanwezig te zijn. Daarbij dient audio- en visuele communicatie mogelijk te zijn, zodat medewerkers op afstand kunnen zien en horen wie toegang vraagt alvorens de deur te openen. Daar waar in huidige situatie nu ook al mogelijk is, dan moet dit blijven werken.
16.	Opdrachtnemer levert een oplossing waarbij sloten, cilinders, beslag en lezers, overeenkomstig de SKG normen afgestemd op de huidige situatie, zodanig zijn uitgevoerd dat deze niet eenvoudig kunnen worden verwijderd of gemanipuleerd en bestand zijn tegen oppervlakkige beschadigingen, zoals krassen, zonder direct defect te raken, zodat de fysieke integriteit en continuïteit van het toegangscontrolesysteem onder normale gebruiksomstandigheden te allen tijde gewaarborgd blijft.
17.	Alle keuzes voor hergebruik of vervanging worden vastgelegd in het technisch dossier, inclusief onderbouwing op basis van inspectie en levensduurcriteria.
18.	De fysieke oplossing (waaronder toegangspassen en –tags) dienen beveiligd te zijn tegen kopiëren en klonen, conform de huidige stand der techniek en geldende beveiligingsnormen.

Service	
Eis	**Omschrijving**
19.	Bij aanvang en na afronding van de werkzaamheden meldt het personeel van Opdrachtnemer zich aan en af bij de contactpersoon van Opdrachtgever en informeert deze over de uitgevoerde werkzaamheden. Indien de werkzaamheden niet afgerond kunnen worden, dient een schriftelijke rapportage te worden opgesteld waarin zowel de voorgestelde vervolghandelingen als de redenen voor het niet afronden van de werkzaamheden worden beschreven.
20.	Opdrachtnemer biedt een centraal Servicepunt telefonisch bereikbaar op werkdagen van 08:00–17:00 uur en een online Service Portal voor vragen etc. Berichten, verzonden buiten kantooruren, worden binnen één werkdag beantwoord. Toegang tot het aanmeldproces (ticket, telefonische of e-mailondersteuning) is uitsluitend toegestaan voor vooraf geautoriseerde medewerkers van Opdrachtgever.
21.	De reactie- en oplostermijnen zijn als volgt: **Kritieke storingen** (veiligheid in gevaar, deur blijft open of nooduitgang defect): binnen **2 uur** (24/7) **Belangrijke storingen** (deur werkt niet, maar er is een alternatieve route): **4 tot 8 uur** (vaak binnen kantooruren). **Niet-kritieke storingen** (comfort, cosmetisch): **1 werkdag**. Wanneer het realiseren van een permanente oplossing niet mogelijk blijkt binnen de genoemde oplostermijnen dan is een realiseren van een tijdelijke oplossing noodzakelijk. Opdrachtnemer garandeert 24/7 bereikbaarheid en storingsdienst voor het opvolgen en oplossen van storingen.
22.	De beschikbaarheid van het systeem bedraagt minimaal 99,5% per maand, uitgaande van een 24/7 service venster. Onderhoud kan overdag plaatsvinden, mits de bedrijfsvoering geen hinder ondervindt. Overig preventief en correctief onderhoud vindt uitsluitend plaats binnen het afgesproken venster: dagelijks tussen 22:00 en 06:00 uur. Gepland onderhoud wordt minimaal 5 werkdagen vooraf aan opdrachtgever gecommuniceerd en mag de beschikbaarheid tijdens reguliere uren niet beïnvloeden.
23.	Opdrachtnemer handelt klachten, van welke aard ook, binnen vijf (5) werkdagen af.
24.	Opdrachtnemer verzorgt een uitgebreide training en instructie voor alle betrokken medewerkers, minimaal gericht op:

	• Het correct gebruik van het systeem. • Het beheer, profielmanagement, zone management, bloktijden en de toekenning van toegangsrechten.

KPI's	
Gedurende de contractperiode zal Opdrachtgever de kwaliteit van de geleverde dienstverlening beoordelen aan de hand van onderstaande kritische prestatie-indicatoren (KPI). Het doel hiervan is om de kwaliteit van dienstverlening te borgen en te verbeteren en zo actief te werken aan een duurzame relatie.	
Eis	**Omschrijving**
25.	KPI: Systeembeschikbaarheid • **Definitie:** Het percentage van de tijd dat het toegangscontrolesysteem volledig operationeel is en gebruikers toegang kunnen krijgen zonder storingen. • **Doelwaarde:** ≥ 99,5% operationeel per kalendermaand. • **Meetmethode:** Monitoring van systeemlogs en incidentmeldingen; uitvaltijd wordt geregistreerd en vergeleken met de totale operationele tijd van het systeem. • **Rapportage:** Maandelijks aan Opdrachtgever.
26.	KPI: Naleving van beveiligings- en auditvereisten • **Definitie:** Het percentage van periodieke systeem- en gebruiksaudits dat voldoet aan gemeentelijke en wettelijke eisen. • **Doelwaarde:** 100% conformiteit. • **Meetmethode:** Auditrapporten door interne of externe auditor; inclusief naleving van AVG, privacy en toegangsbeheerbeleid. • **Rapportage:** Jaarlijks of na elke audit.
27.	KPI: Registratie Storingen en opvolging • **Definitie:** Het percentage storingen dat correct geregistreerd, toegewezen en afgehandeld wordt binnen de afgesproken termijnen. • **Doelwaarde:** 100% registratie; ≥ 95% afgehandeld binnen SLA-termijnen. • **Meetmethode:** Servicemanagementsysteem; periodieke controle op volledigheid en opvolging. • **Rapportage:** Maandelijks.
28.	Verantwoordelijk voor monitoren Voor de monitoring van de KPI's legt de Opdrachtgever de verantwoordelijkheid bij de Opdrachtnemer. Opdrachtnemer dient aan te tonen dat bovenstaande KPI behaald is middels valide en aantoonbaar betrouwbare informatie. Bij aanvang van de overeenkomst draagt Opdrachtnemer een plan van aanpak aan over de wijze van monitoren, de wijze van rapporteren, beheersmaatregelen en mogelijke verbetermaatregelen. Het is naar oordeel van Opdrachtgever of de aanpak van Opdrachtnemer voldoende is, zo niet, dient Opdrachtnemer zijn aanpak hierop aan te passen.
29.	Consequenties bij niet realiseren KPI`s In overleg met Opdrachtgever op basis van realistische verwachtingen stelt Opdrachtnemer bij het niet realiseren van de KPI stelt binnen twee weken na constatering een verbeterplan op. Het verbeterplan wordt geaccordeerd door Opdrachtgever en vervolgens binnen twee weken ten uitvoer gebracht. In het plan staat aangegeven wanneer acties tot resultaat leidt. Het hierboven genoemde laat alle overige rechten van Opdrachtgever, die zij onder meer op basis van de Overeenkomst en de GIBIT 2023 heeft, onverlet.

Communicatie en rapportage	
Eis	**Omschrijving**
30.	Het systeem moet de mogelijkheid bieden automatisch periodiek een overzicht te genereren van alle toegekende toegangsrechten per ruimte, ter ondersteuning van periodieke audits en interne controles.
31.	De oplossing wordt ingezet voor het opstellen en beschikbaar stellen van operationele, tactische en strategische managementinformatie, inclusief stuurinformatie binnen processen. Dit gebeurt via geïntegreerde rapportagetools en dashboards. De software moet KPI's en statistieken kunnen meten en periodieke rapportages genereren over het gebruik van toegangspassen en tags, inclusief overzichten per gebruiker en per ruimte, zonder extra beheerverplichtingen.
32.	Opdrachtnemer is contractueel verantwoordelijk voor goede dienstverlening en stemt jaarlijks een planning voor evaluatiegesprekken af met Opdrachtgever: operationeel wekelijks (indien nodig), tactisch/operationeel minimaal vier keer per jaar, en strategisch minimaal één keer per jaar.
33.	Kwartaal: Opdrachtnemer levert per kwartaal digitale managementinformatie per locatie, ter voorbereiding op het kwartaal- en strategisch overleg. In het overleg wordt de rapportage besproken. Minimaal dient de volgende informatie opgenomen te zijn: • Incident- en wijzigingsstatistieken. • Beschikbaarheid.

	• Serviceniveau-afwijkingen. • Resultaten van backuptesten • Ontwikkelingen en kansen. • Samenwerkingsevaluatie. • KPI-prestaties en SROI-invulling. • Verbetervoorstellen bij escalaties.
34.	Jaarlijks: Er wordt minimaal jaarlijks een pentest bij Opdrachtnemer uitgevoerd op het SaaS-omgeving of na een grote wijziging op het systeem waarna kwetsbaarheden op basis van het gelopen risico tijdig worden verholpen. Deze is bij ingebruikname uitgevoerd en de rapportage is beschikbaar, inclusief risicoanalyse.
35.	Partijen werken samen volgens onderstaand communicatieschema:

Type overleg / communicatie	Frequentie	Doel	Deelnemers	Documentatie
Operationeel overleg	Wekelijks (indien nodig)	Voortgang storingen, klachten	Operationeel team	Actielijst binnen 48 uur
Tactisch overleg	4x per jaar	KPI's, incidentstatistieken, verbeterpunten	Contractmanager, Opdrachtnemer	Verslag + KPI-rapportage
Strategisch overleg	1x per jaar	Evaluatie samenwerking, strategische ontwikkelingen	Directie / Management	Jaarverslag + evaluatie
Kwartaalrapportage	Per kwartaal	Managementinformatie per locatie	Opdrachtnemer aan Opdrachtgever	Rapportage in centraal systeem
KPI rapportage	Per half jaar	Managementinformatie	Opdrachtnemer aan Opdrachtgever	Rapportage in centraal systeem
Pentest rapportage	Jaarlijks / na grote wijziging	Beveiligingscontrole	IT Security team	Rapportage + risicoanalyse

Facturatie eisen	
Eis	**Omschrijving**
36.	Alle kosten die met de levering samenhangen, zijn inbegrepen in de ingediende prijzen. Verzend- en leveringskosten mogen derhalve niet afzonderlijk in rekening worden gebracht.
37.	Opdrachtnemer dient gefaseerd te factureren per locatie. Per locatie geldt de volgende betalingsstructuur voor de implementatie: • 30% van het aan het betreffende locatie toe te rekenen opdrachtbedrag mag vooraf worden gefactureerd; • 70% van het aan het betreffende locatie toe te rekenen opdrachtbedrag mag pas worden gefactureerd nadat de locatie door Opdrachtgever formeel is geaccepteerd en na goedgekeurd engineeringspakket (Blokschema's, Projecteringstekeningen, Aansluitschema's, Specs van de te gebruiken producten).. De eerste locatie, inclusief de centrale voorzieningen, wordt uitgevoerd als pilot, waarvan de acceptatie als voorwaarde geldt voor de voortgang van de implementatie van de overige locaties. Facturen dienen gespecificeerd te worden per locatie (of per groep locaties indien Opdrachtgever besluit deze samen te factureren), zodat uitvoering, oplevering en facturatie transparant en controleerbaar zijn.
38.	Opdrachtnemer factureert achteraf op maandbasis een maandelijkse vaste beheervergoeding waarin de licentiekosten en de kosten voor preventief onderhoud zijn opgenomen.
39.	Opdrachtnemer factureert na uitvoering van het werk de kosten voor het correctieve onderhoud. Deze facturatie gebeurt op basis van de Topdesk meldingen. Dit nummer dient ook te worden vermeld op de factuur.
40.	De factuuradresgegevens zijn opgenomen in de Overeenkomst, Bijlage 2A. De factuur dient minimaal de volgende gegevens te bevatten: • NAW-gegevens Opdrachtnemer; • WBS code Opdrachtgever (per locatie); • naam en contactgegevens contactpersoon Opdrachtgever; • datum van levering diensten; • omschrijving van de geleverde diensten; • totaalfactuurbedrag; • totaal prijs inclusief btw; • btw-tarief; • btw bedrag in euro's.

	De digitale factuur wordt in PDF-formaat verstuurd aan het factuuradres van de gemeente Deventer
41.	De maandelijkse beheersvergoeding kan, na schriftelijke goedkeuring van Opdrachtgever, één keer per jaar per 1 januari, voor het eerst per 1 januari 2028, worden verlaagd/verhoogd op basis van het CBS-prijsindexcijfer voor "Financiële en zakelijke diensten" bedrijfstak/branche "IT en informatiedienstverlening". Opdrachtnemer kondigt de prijsaanpassing schriftelijk aan, uiterlijk op 31 oktober voor het daaropvolgende jaar. De indexatie wordt als volgt berekend: Voorbeeld voor het eerste jaar: 2e kwartaal 2027 – 2e kwartaal 2026 / 2e kwartaal 2026 x 100. Overige (tussentijdse) prijsverhogingen worden niet geaccepteerd. Deze bepaling geldt ook voor de optiejaren indien daar gebruik van wordt gemaakt.

Informatievoorziening- /informatiebeveiligingseisen	
Eis	**Omschrijving**
42.	Opdrachtnemer blijft gedurende de gehele duur van de overeenkomst ISO27001 (of gelijkwaardig) gecertificeerd en levert dit certificaat inclusief verklaring van toepasselijkheid bij eerste verzoek aan.
43.	Data dat wordt opgeslagen in de Cloud-omgeving blijft eigendom van Opdrachtgever. Data is altijd toegankelijk voor Opdrachtgever en moet te allen tijde eenvoudig door Opdrachtgever uit de Cloud-omgeving kunnen worden gehaald wanneer daartoe aanleiding voor wordt gezien.
44.	Alle data van Opdrachtgever (zowel digitaal als niet-digitaal, inclusief back-updata) wordt na afloop van het contract binnen 30 dagen na overdracht aan Opdrachtgever verwijderd of vernietigd conform DIN-norm 66399. Dit wordt schriftelijk bevestigd. De exit strategie en werkwijze die hierbij worden gehanteerd, worden tijdens de implementatie aangeleverd door Opdrachtnemer, ter beoordeling van Opdrachtgever. Hierin wordt tevens het (export)bestandstype vastgelegd.
45.	De omgeving van Opdrachtgever is gescheiden van andere klanten, wat het niet mogelijk maakt om toegang te krijgen tot de dienst vanuit een andere klant. Opdrachtnemer dient de SaaS-omgeving logisch of fysiek gescheiden te houden van andere tenants.
46.	Opdrachtnemer draagt zorg voor het up-to-date houden van de software tegen kwetsbaarheden en maakt alleen gebruik van producten die binnen de 'vendor lifecycle' vallen. Opdrachtnemer neemt hier gepaste maatregelen op waarbij rekening te houden met de OWASP top 10. (Web)interfaces die via het internet benaderbaar zijn, mogen door Opdrachtgever worden gescand op kwetsbaarheden.
47.	Systemen welke 24x7 open staan voor remote overname door de leverancier worden niet toegestaan. Remote beheer is bijvoorbeeld wel mogelijk indien de apparatuur, zoals een bridge box, verbinding heeft met een centraal systeem bij de leverancier. Dit betreft dus een sessie van de apparatuur aan de zijde van DOWR naar de leverancier en niet andersom.
48.	Er worden alleen technieken en protocollen gebruikt die als veilig worden beschouwd en noodzakelijk zijn voor de oplossing (hardening). Hier wordt voldaan aan de standaarden van het Forum Standaardisatie van het Ministerie van Binnenlandse Zaken. Hier wordt gedurende de looptijd van het contract aan voldaan. Als er wijzigingen plaatsvinden in de standaarden worden deze ook toegepast door Opdrachtnemer.
49.	Data at rest en in transit in de Cloud-omgeving is versleuteld. Uitzonderingen zijn niet toegestaan. Alle gevoelige data moet minimaal worden versleuteld met AES-256 (data-at-rest) en TLS 1.2 of hoger (data-in-transit). Websites hebben een score van A of A+ bij ssllabs.com.
50.	Opdrachtnemer voert minimaal halfjaarlijks volledige back-uptests uit en toont schriftelijk aan dat deze succesvol zijn uitgevoerd. Deze resultaten worden opgenomen in de periodieke managementrapportage. Voor een SaaS-oplossing geldt dat back-ups moeten voldoen aan de overeengekomen RPO (Recovery Point Objective) en RTO (Recovery Time Objective), inclusief herstelprocedures en verificatie van data-integriteit. Opdrachtnemer moet aantonen dat back-ups versleuteld worden opgeslagen, zowel in transit als in rest, en dat deze voldoen aan relevante compliance- en beveiligingsstandaarden (bijv. ISO 27001, AVG). Daarnaast moet een plan voor disaster recovery en business continuity beschikbaar zijn, inclusief testresultaten en verbeteracties.
51.	Het systeem moet Single Sign-On (SSO) ondersteunen via OAuth2 met MFA, bij voorkeur op basis van OIDC of SAML, gekoppeld aan de bestaande Identity Provider van de Opdrachtgever. Toegang vindt uitsluitend plaats op basis van rollen en attributen (RBAC). Daarnaast moet het mogelijk zijn om legacy login-methoden volledig uit te schakelen, zodat alleen moderne, veilige authenticatiestandaarden worden toegepast.
52.	Auditlogs van alle activiteiten moeten beschikbaar en exporteerbaar zijn.
53.	Inloggen door Opdrachtnemer, ten behoeve van ondersteuning op de SaaS-systeem van de Opdrachtgever, vindt plaats via een Entra ID gastaccount vanuit de Identity provider van de Opdrachtgever waarbij MFA zal worden afgedwongen.
54.	De applicatie verstuurt bij voorkeur e-mail via Microsoft Graph API (Azure App-registratie). Dit wordt beperkt aan de kant van Inschrijver door het gebruik van Application RBAC, zodat alleen geautoriseerde mailboxen en functies beschikbaar zijn. Wanneer dit niet mogelijk is, kan bij uitzondering SMTP-relay via de mailserver van DOWR worden toegepast, mits voldaan wordt aan de specifieke aansluitvoorwaarden. Rechten binnen de applicatie worden doorgegeven via groepslidmaatschappen of applicatierollen die gekoppeld zijn aan de App-registratie. Deze rechten kunnen binnen de applicatie worden gebruikt voor het toewijzen van rollen en permissies.

55.	Persoonsgegevens worden uitsluitend opgeslagen en verwerkt binnen de Europese Unie en andere EER-landen, conform de vereisten van de Algemene Verordening Gegevensbescherming (AVG) en toekomstige privacywetgeving.
56.	Bescherming tegen Distributed Denial of Service (DDoS)-aanvallen moet structureel worden gewaarborgd om de beschikbaarheid en continuïteit van diensten te garanderen.
57.	Gebruikers die zijn/of worden uitgeschakeld binnen de gesynchroniseerde of gekoppelde identity provider van Opdrachtgever moeten onmiddellijk de toegang tot ruimtes en gerelateerde omgevingen worden ontzegd, waarbij directe intrekking van toegangsrechten een vereiste is.
58.	De opdrachtnemer dient ieder datalek of beveiligingsincident, evenals iedere situatie waarin een dergelijk lek of incident wordt vermoed, onverwijld en uiterlijk binnen 24 uur na ontdekking te melden aan de opdrachtgever, conform het vastgestelde Security Incident Response Plan.
59.	Logging wordt minimaal 3 jaar bewaard en voldoet aan de volgende eisen, inclusief alle privileged acties: - Herleidbaar tot een natuurlijk persoon of gebruikersnaam. - De gebeurtenis. - Waar mogelijk en van toepassing de identiteit van het werkstation of de locatie. - Waar mogelijk en van toepassing de host naam. - Naam van de toepassing. - Het object waarop de handeling werd uitgevoerd. - Het resultaat van de handeling. - De datum en het tijdstip en de duur van de gebeurtenis.
60.	Automatische veranderingen aan verbruikte ingekochte capaciteit als gevolg van automatisch opschalen van resources worden tijdig aan Opdrachtgever gecommuniceerd als dit resulteert in hogere kosten.
61.	Opdrachtgever heeft het recht om een audit/pentest uit te voeren of te laten uitvoeren om te controleren of aan alle contractuele eisen wordt voldaan. Daarnaast kan Opdrachtgever een audit laten uitvoeren wanneer daartoe aanleiding bestaat, bijvoorbeeld na een datalek of beveiligingsincident. De kosten voor de audit/pentest is voor rekening van Opdrachtgever.

Informatievoorziening- /architectuureisen	
Eis	**Omschrijving**
62.	Indien meerdere diensten worden aangeboden, dienen deze via één publiek IP-adres ontsloten te worden, waarbij Network Address Translation (NAT) als vereiste geldt voor inkomend verkeer via de firewall.
63.	Het systeem ondersteunt gegevensuitwisseling primair via gestandaardiseerde en goed gedocumenteerde API-koppelingen conform de REST-API Design Rules. Bestandsuitwisseling via SFTP, XML of CSV is alleen toegestaan indien technisch noodzakelijk en expliciet goedgekeurd door DOWR. Opdrachtnemer implementeert vastgestelde API-standaarden binnen zes maanden en bouwt API's volgens REST/JSON en OAS 3.x. Koppelvlakken worden volledig gedocumenteerd. Alle koppelingen sluiten aan op het integratieplatform van Opdrachtgever en maken verplicht gebruik van de API-gateway.
64.	Het systeem dient een volledig webnative en webresponsive SaaS-oplossing te zijn, toegankelijk via moderne webbrowsers zonder afhankelijkheid van Citrix of RDP. De leverancier dient te specificeren op welk platform (bijv. Azure, AWS, eigen datacenter) en besturingssysteem de oplossing draait, en of gebruik wordt gemaakt van containerisatie (zoals Kubernetes) of een webapplicatieplatform (zoals Azure App Services)
65.	Alle certificaten die worden gebruikt voor de SaaS-oplossing en de bijbehorende API's mogen niet gebaseerd zijn op wildcard-certificaten (zoals *.domein.nl). Certificaten moeten specifiek per domein of subdomein worden uitgegeven en voldoen aan actuele beveiligingsstandaarden, inclusief ondersteuning voor TLS 1.3 en sterke sleutelparen.
66.	De oplossing betreft een standaardapplicatie. Geen maatwerk voor Opdrachtgever.
67.	Opdrachtnemer zorgt dat alle noodzakelijke digitale onderdelen van de oplossing voldoen aan de vereisten van WCAG 2.1 niveau AA, zoals verankerd in de Europese norm EN 301 549 voor digitale toegankelijkheid. Dit omvat onder meer toegankelijke gebruikersinterfaces, leesbare schermteksten, navigatie via toetsenbord, voldoende contrast, duidelijke labels, en compatibiliteit met hulpmiddelen zoals schermlezers.
68.	De oplossing moet uitbreidbaar zijn met nieuwe beveiligingsdomeinen en technologieën zonder platformvervanging. Gedurende de looptijd van de overeenkomst voldoet de oplossing aan alle toepasselijke wettelijke standaarden, de open standaarden zoals vermeld op de Pas-toe-of-leg-uit-lijst, en de landelijke gemeentelijke standaarden, voor zover deze van toepassing zijn op het werkingsgebied van de oplossing.

Informatievoorziening- /privacy eisen	
Eis	**Omschrijving**
69.	Wanneer de rolverdeling tussen Opdrachtnemer en Opdrachtgever die van Verwerker en Verantwoordelijke is, dient Opdrachtnemer voor gunning een overzicht aan te leveren van de door hem ingeschakelde derden en onderaannemers, waarin de identiteit, vestigingsplaats en een beschrijving van de werkzaamheden van de derden of onderaannemers zijn opgenomen.

70.	Indien het systeem algoritmes waaronder kunstmatige intelligentie bevat, dan dient deze data ten alle tijden binnen de tenant/systeem van de opdrachtgever te blijven.
71.	Opdrachtnemer verstrekt zijn eigen register van verwerkingen en het privacy statement aan Opdrachtgever binnen twee maanden na start van de overeenkomst.

Informatievoorziening- /koppelingen	
Eis	**Omschrijving**
72.	De tag voldoet aan Mifare Desfire EV3. De tag moet de huidige koppelingen en integraties ondersteunen, zie hiervoor het blokschema.

Duurzaamheidseisen	
Eis	**Omschrijving**
73.	Opdrachtnemer is verplicht zich aantoonbaar in te spannen om de milieubelasting van de werkzaamheden en de te leveren producten tot een minimum te beperken. Het voldoen aan alle geldende milieuwet- en regelgeving geldt hierbij als absolute minimumnorm. Opdrachtnemer dient gedurende de uitvoering van de opdracht tevens rekening te houden met het bepaalde in het inkoopbeleid en de Nul-emissiezone in Deventer, zie Nul-emissiezone Deventer.
74.	Opdrachtnemer is verantwoordelijk voor het retournemen van alle verpakkingsmaterialen. Alle materiaalresten, emballage, verpakkingsmiddelen en door de werkzaamheden van Opdrachtnemer ontstane verontreinigingen dienen onverwijld door Opdrachtnemer te worden opgeruimd en op correcte wijze afgevoerd.
75.	Opdrachtnemer neemt, waar mogelijk, reeds aanwezige producten retour en streeft daarbij naar een maximale circulariteit conform de circulariteitsladder. Eventuele opbrengsten of hergebruikopties worden vooraf met Opdrachtgever besproken en afgestemd.
76.	Opdrachtnemer biedt, voor zover technisch en praktisch mogelijk, oplossingen die de levensduur van producten verlengen, producten reviseren en hergebruik stimuleren.
77.	Opdrachtnemer realiseert binnen de looptijd van de opdracht een Social Return on Investment (SROI) ter waarde van minimaal 2% van de opdrachtsom. Deze verplichting wordt ingezet om maatschappelijke meerwaarde te creëren, bijvoorbeeld door het bieden van werk- of leerplekken aan mensen met een afstand tot de arbeidsmarkt, het aanbieden van stageplaatsen of leerwerktrajecten, of door andere activiteiten die bijdragen aan inclusiviteit en duurzame werkgelegenheid. Opdrachtnemer stemt de invulling en uitvoering van de SROI-verplichting vooraf af met Opdrachtgever en rapporteert periodiek over de voortgang en realisatie.