Bijlage 2AD Programma van eisen

Dit Programma van Eisen (PvE) beschrijft de minimale functionele, technische, beveiligings-, beheer- en continuïteitseisen voor de levering, implementatie, migratie, beheer en doorontwikkeling van een geïntegreerde oplossing voor cameratoezicht (CCTV), toegangscontrole (TRS) en inbraakdetectie ten behoeve van Gemeente Barneveld.

Het PvE vormt een integraal onderdeel van de aanbestedingsdocumenten. Alle eisen in dit document gelden als minimumeisen, tenzij expliciet anders vermeld.

Functionele eisen - CCTV en TRS

1.1 Algemeen

Nr.	Omschrijving
A-003a	Opdrachtnemer ondersteunt het Gegevensbeheer van Opdrachtgever door onderscheid te maken tussen minimaal de volgende Gegevenscategorieën: • camerabeelden; • toegangslogs; • auditlogs; • alarmmeldingen; • bezoekersregistraties. Per Gegevenscategorie moeten bewaartermijnen, autorisaties, classificaties en verwijdertermijnen afzonderlijk configureerbaar zijn.
A-004	Opdrachtnemer garandeert gedurende de contractperiode een maandelijkse beschikbaarheid van: • 99,8% voor de Centrale Managementomgeving; • 99,9% voor kritische beveiligingsfuncties; Gemeten per kalendermaand. Gepland onderhoud binnen overeengekomen onderhoudsvensters wordt niet meegerekend. (Gepland onderhoud buiten kantooruren wordt hierbij buiten beschouwing gelaten). Het systeem en de applicatie dienen te voldoen aan de onderstaande beschikbaarheids- en continuïteitseisen: 1. Centrale managementomgeving o De Centrale managementomgeving voor beheer, monitoring, rapportage en configuratie heeft een minimale beschikbaarheid van 99,8% per kalendermaand, exclusief vooraf aangekondigd onderhoud.

	○ Gepland onderhoud wordt minimaal vijf werkdagen vooraf aangekondigd en vindt bij voorkeur buiten kantooruren plaats. 2. Kritische beveiligingsfuncties ○ Kritische beveiligingsfuncties, waaronder toegangscontrole, inbraakdetectie, alarmverwerking en lokale cameraregistratie, hebben een minimale beschikbaarheid van 99,9% per kalendermaand. ○ Uitval van de Centrale managementomgeving mag niet leiden tot uitval van deze kritische beveiligingsfuncties. 3. Lokale autonome werking ○ Deurcontrollers, toegangslezers, inbraakdetectiecomponenten en andere kritische beveiligingscomponenten blijven volledig operationeel bij verlies van verbinding met de Centrale managementomgeving of internetverbinding. ○ Lokale autorisaties, deurfuncties, alarmfuncties en logging blijven beschikbaar gedurende de verstoring. ○ Synchronisatie van Gegevens vindt automatisch plaats zodra de verbinding is hersteld. 4. Kwartaalrapportage (oplevering rapportage 15 werkdagen na kwartaal) ○ Opdrachtnemer rapporteert per kwartaal over gerealiseerde beschikbaarheid, storingen, incidenten, oorzaken en genomen herstelmaatregelen. ○ De beschikbaarheid wordt gemeten over de volledige productieomgeving en onderbouwd met meetgegevens.
NF-A-001	De Applicatie wordt geleverd als een SaaS (software als een service).
A-004a	De Opdrachtgever zoekt een hybride beveiligingsarchitectuur bestaande uit: • een centraal SaaS-managementplatform voor beheer, monitoring, rapportage en configuratie; • lokaal aanwezige camera's, deurcontrollers en inbraakdetectiecomponenten; • lokale operationele continuïteit bij uitval van internetverbindingen of SaaS-diensten; • lokale fail-over mogelijkheden voor toegangscontrole en inbraakdetectie; • cloudbeheer zonder verstoring van primaire beveiligingsfuncties. Kritische beveiligingsfuncties blijven operationeel bij verlies van verbinding met de Centrale managementomgeving.

A-005	Het Systeem / CCTV / TRS biedt centrale beheer- en monitoringmogelijkheid vanaf iedere werkplek.
A-006	Opdrachtgever kan zelfstandig rollen aanmaken, wijzigen en verwijderen en per rol autorisaties toekennen voor objecten, locaties, rapportages, configuraties en beheerfuncties conform het least-privilege-principe.
A-006a	**Authenticatie en toegangsbeveiliging** Het Systeem ondersteunt federatieve authenticatie via gangbare standaarden waaronder minimaal SAML 2.0 en OpenID Connect. De oplossing ondersteunt: • SAML 2.0 en/of OpenID Connect; • Single Sign-On; • Multi-Factor Authentication (MFA); • Conditional Access beleid van Opdrachtgever. Lokale accounts zijn uitsluitend toegestaan indien technisch noodzakelijk en worden afzonderlijk beheerd en met MFA beveiligd.
A-006b	**Logging, Audittrail en Forensische Ondersteuning** Het Systeem ondersteunt centrale logging, auditing, monitoring en rapportage voor CCTV, toegangscontrole, inbraakdetectie en de Centrale managementomgeving. 1. Vastlegging gebeurtenissen Het Systeem registreert minimaal de volgende gebeurtenissen: • gebruikersaanmeldingen en afmeldingen; • succesvolle en mislukte authenticatiepogingen; • toegangsgebeurtenissen; • wijziging van autorisaties; • configuratiewijzigingen; • systeemstoringen; • alarmmeldingen; • beveiligingsincidenten; • export van camerabeelden; • export van persoonsgegevens; • gebruik van beheerfunctionaliteiten; • wijzigingen in logging- en beveiligingsinstellingen. 2. Inhoud logregels Elke logregel bevat minimaal: • datum en tijd (UTC en lokale tijd); • unieke gebeurtenisidentificatie;

	• gebruiker, systeemcomponent of serviceaccount; • uitgevoerde actie; • betrokken object; • resultaat van de actie; • bronlocatie of IP-adres indien van toepassing. 3. Audittrail Alle beheeracties, configuratiewijzigingen en autorisatiewijzigingen worden opgenomen in een niet-manipuleerbare Audittrail. De Audittrail ondersteunt: • forensisch onderzoek; • incidentonderzoek; • accountantscontroles; • ENSIA-verantwoording; • BIO2-audits. 4. Bewaartermijnen Het Systeem ondersteunt afzonderlijk configureerbare bewaartermijnen voor: • camerabeelden; • toegangslogs; • auditlogs; • alarmmeldingen; • bezoekersregistraties. Minimaal gelden de volgende bewaartermijnen: Auditlogs: • minimaal 24 maanden. Toegangslogs: • Zone 1 t/m 3: minimaal 3 maanden; • Zone 4: minimaal 12 maanden. Camerabeelden: • maximaal 28 dagen tenzij een incident een langere bewaartermijn rechtvaardigt. 5. Integriteit Logginggegevens: • zijn niet wijzigbaar of verwijderbaar door reguliere gebruikers; • zijn controleerbaar op integriteit; • blijven behouden bij upgrades; • zijn exporteerbaar voor onderzoeksdoeleinden. 6. Monitoring

	Het Systeem genereert automatisch meldingen bij: • foutieve inlogpogingen; • ongeautoriseerde toegangspogingen; • mislukte authenticaties; • wijzigingen in autorisaties; • wijzigingen in beveiligingsinstellingen; • systeemstoringen; • uitval van camera's; • uitval van controllers; • opslagproblemen; • beveiligingsincidenten. 7. Integratie Logginggegevens kunnen worden ontsloten via open standaarden en API's ten behoeve van SIEM-, monitorings-, audit- en analysetoepassingen. Het Systeem ondersteunt minimaal: • Syslog; • REST API; • JSON-export. 8. Rapportage Geautoriseerde gebruikers kunnen logging- en auditgegevens: • raadplegen; • filteren; • exporteren; • rapporteren;zonder tussenkomst van Opdrachtnemer.
A-007	Het Systeem / CCTV / TRS biedt exportfunctionaliteit met watermerk en digitale handtekening voor bewijslast.
A-008	Het Systeem / CCTV / TRS biedt alarmering bij systeemfalen, schijfstoringen en camera-uitval.
A-009	Het Systeem verwerkt en slaat alle Gegevens op binnen de Europese Economische Ruimte (EER).
A-010	Architectuur Opdrachtgever Het Systeem sluit aan op: • BIO2; • AVG; • GEMMA-principes; • Common Ground-principes; • Open Standaardenbeleid Overheid;

	• API-first uitgangspunten; • Principes van Gegevensminimalisatie en Gegevensbronhouderschap.

1.2 Integratie en netwerkinfrastructuur

Nr.	Omschrijving
IN-001	Het CCTV en TRS moeten volledig geïntegreerd zijn. De Opdrachtnemer is verantwoordelijk voor de samenhang tussen alle systemen. Daarnaast zijn de volgende Koppelingen vereist: Koppeling — Type — Vereist/Optioneel CCTV <-> TRS — Gebeurteniskoppeling: camera-activatie bij toegangsevent — Vereist TRS <-> Brand- en inbraakinstallatie — Alarmkoppeling (I/O): blokkade lezers bij gewapend alarm — Vereist TRS <-> Microsoft EntraID — SAML 2.0/LDAP: SSO en tweefactorauthenticatie — Vereist CCTV/TRS <-> Gebouwbeheersysteem — API/Protocol — Optioneel
IN-002	**Integratievereisten:** • Bij een ongeautoriseerde toegangspoging activeert het systeem automatisch de dichtstbijzijnde camera • Bij een brandalarm worden alle nooduitgangen automatisch ontgrendeld (fail-safe) • Bij een inbraakalarm worden alle lezers in het betreffende gebied geblokkeerd • De oplossing ondersteunt standaard Koppelingen met Microsoft Entra ID en AFAS via gedocumenteerde API's of standaardconnectoren. • Alle Koppelingen werken via open standaarden: ONVIF (CCTV), OSDP (lezers), SOAP/REST (API) • Koppelingen functioneren ook bij offline server: controllers werken zelfstandig • De oplossing ondersteunt een API-first architectuur waarbij alle primaire beheer- en integratiefuncties beschikbaar zijn via gedocumenteerde API’s
IN-002a.	**Leveranciersonafhankelijkheid** De oplossing moet leverancier-onafhankelijk worden ingericht. Opdrachtnemer levert bij oplevering: • volledige API-documentatie; • export van configuraties; • export van gebruikers- en autorisatiestructuren; • export van logginggegevens;

	• export van camerabeelden in gangbare formaten; • migratiedocumentatie ten behoeve van toekomstige vervanging van de oplossing. Voor deze exportmogelijkheden gelden geen aanvullende licenties
IN-003	**Netwerkinfrastructuur** • Dedicated beveiligings-VLAN (logische scheiding van bedrijfsnetwerk) > eigen netwerklijn • Gigabit Ethernet connectiviteit minimum • PoE switches (IEEE 802.3at/bt) voor camera's en controllers (deels aanwezig) • Bekabeling minimaal Cat6 UTP, bij voorkeur Cat6a • Gebruik bestaande kabeltracés waar mogelijk • Redundante netwerkverbindingen voor kritieke componenten • VPN voor remote toegang beheer (verplicht in combinatie met tweefactor-authenticatie) • Firewall segmentatie beveiligingsnetwerk • Network Access Control (NAC) voor netwerkaansluitingen buiten het gebouw, specifiek voor paslezers bij slagboom en fietsenstalling • Paslezers buiten het gebouw: extra fysieke bescherming van de netwerkaansluiting

IN-004	**Cyberbeveiliging (zie A-006b)**
	• Alle communicatie versleuteld via TLS 1.3
	• Sterke wachtwoordvereisten: minimaal 12 tekens met complexiteitseisen
	• Tweefactorauthenticatie verplicht voor remote toegang en beheer
	• Hardening van alle apparaten: onnodige diensten uitschakelen, standaardwachtwoorden wijzigen, beveiligingsinstellingen op veilige waarden conform CIS Controls en OWASP-richtlijnen
	• Opdrachtnemer installeert firmware- en software-updates: beveiligingspatches conform onderstaande prioriteitsindeling:
	  • P1 (Kritiek): binnen 48 uur;
	  • P2 (Hoog): binnen 7 alenderdagen;
	  • P3 (Middel): binnen 30 kalenderdagen;
	  • P4 (Laag): binnen 90 kalenderdagen.
	Indien een patch niet binnen de gestelde termijn kan worden geïnstalleerd, treft Opdrachtnemer binnen 48 uur passende mitigerende maatregelen op basis van een gedocumenteerde risicoafweging en informeert hij Opdrachtgever schriftelijk over de risico's, maatregelen en geplande hersteltermijn.
	• Geïsoleerd managementnetwerk: beheer- en productieverkeer gescheiden
	• Bij een beveiligingsincident of Gegevenslek: melding aan Opdrachtgever binnen 8 Opdrachtnemer meldt beveiligingsincidenten en (vermoedelijke) Gegevenslekken onverwijld en uiterlijk binnen 4 uur na constatering aan Opdrachtgever.
	De melding bevat minimaal:
	  • aard van het incident;
	  • getroffen systemen;
	  • vermoedelijke impact;
	  • reeds genomen maatregelen;
	  • verwachte hersteltijd.
	• Multi-Factor Authentication is verplicht voor alle beheerdersaccounts, ongeacht of toegang lokaal of op afstand plaatsvindt.

1.3 Technische eisen (algemeen)

Nr.	Omschrijving
TA-001	**Installatie en bekabeling** • Alle installaties conform NEN 1010 (elektrotechnische installaties) en NEN-EN 50173 (gestructureerde bekabeling) • Bij oplevering kabeldocumentatie en labelen verplicht; elk kabel uniek genummerd en traceerbaar • Gebruik bestaande kabeltracés waar mogelijk; nieuwe tracés alleen waar technisch noodzakelijk

	• De SaaS-oplossing blijft tijdens implementatie-, configuratie- en onderhoudswerkzaamheden minimaal 99,5% beschikbaar per kalendermaand. Geplande werkzaamheden die kunnen leiden tot een onderbreking van de dienstverlening worden uitsluitend uitgevoerd binnen overeengekomen Onderhoudsvensters buiten Bedrijfsuren, tenzij sprake is van een Spoedeisende Situatie. De Opdrachtnemer informeert de Opdrachtgever hierover ten minste vijf (5) werkdagen vooraf. • Afstemming met projectleider verbouwing Gemeentehuis over fasering en planning • Alle buiteninstallaties weerbestendig uitgevoerd conform IP-classificaties (IP68)
TA-002	**Documentatie** Bij oplevering van het CCTV- en TRS-systeem levert de Opdrachtnemer de volgende documentatie aan in het Nederlands: • Complete technische documentatie van alle componenten, specificaties) • Netwerktopologie en IP-adressenlijst • As-built (revisie) tekeningen en bedradingsschema's • Configuratiedocumentatie en instellingen van het CCTV en TRS systeem • Cameraplan conform NEN 62676-4 met snapshots van alle camera's bij oplevering • Gebruikershandleidingen in het Nederlands • Beheerhandleidingen in het Nederlands • Procedures: privacy, back-up/restore en calamiteiten • Wachtwoordendocument in verzegelde envelop; bewaard door Facilitaire Dienst • DAP (Dossier Afspraken en Processen): vastgelegd vóór ingebruikname, ondertekend door beide partijen **Het DAP bevat minimaal:** • Overzicht overlegstructuur en contactpersonen • Inhoud en frequentie van periodieke rapportages • Processen voor incidentmelding, wijzigingsaanvragen en escalatie • Verdeling beheertaken tussen Opdrachtgever en Opdrachtnemer • SLA-afspraken en KPI's
TA-003	**Garantie** Op alle geleverde hardware geldt: • minimaal 5 jaar fabrieksgarantie; • next business day vervanging voor kritische componenten; • firmware-ondersteuning gedurende minimaal 7 jaar.
TA-005	**Opleverdocumentatie** Bij definitieve oplevering levert Opdrachtnemer aan: • Volledig ingevuld cameraplan conform NEN 62676-4 met snapshots alle camera's • As-built tekeningen van beide locaties

	• IP-adressenlijst en netwerktopologie definitief • Configuratiedocumentatie alle systemen • Bewijs van aanmelding camera's bij Camera in Beeld (Politie) • Getekende verwerkersovereenkomst • Getekend DAP • Wachtwoordendocument in verzegelde envelop • Trainingsmateriaal en aanwezigheidslijsten training

2. Programma van eisen - CCTV

2.1 Algemene eisen

Nr.	Omschrijving
F1-001	De BIO2 is de vernieuwde basisnorm voor informatiebeveiliging binnen de Nederlandse overheid, gekoppeld aan de Cyberbeveiligingswet (Cbw). Gemeenten passen de BIO2 toe als richtinggevend kader. De belangrijkste eisen voor fysieke beveiliging: • Zonering: indeling in beveiligingszones. • Toegangscontrole: autorisatie vereist voor toegang tot beveiligde zones. • Logging conform eis A-006b. • *Controle autorisa*ties: minimaal halfjaarlijks; voor Zone 4 minimaal per kwartaal. • Alarmering: 24/7 inbraakalarm gekoppeld aan alarmcentrale. • Cameratoezicht: op toegangswegen en beveiligde ruimtes. • Overvalplan: met afspraken over aanrijroutes en contacten politie. • Alarmknoppen: in wachtruimten, spreekkamers en bij publiekscontact. • Scheiding netwerken: beveiligingssystemen op gescheiden netwerk (VLAN). • Hardening: beveiligde configuratie van alle componenten. • Remote beheer: alleen via tweefactorauthenticatie en VPN. Conform BIO2 wordt het gebouw ingedeeld in vier beveiligingszones met oplopende beveiligingsniveaus. Voor Zone 4 geldt een extra autorisatie die minimaal elk kwartaal wordt gecontroleerd. BHV-ers hebben toegang tot alle ruimten, controleer daarom periodiek of er geen misbruik wordt gemaakt van deze toegangsrechten. Zie voor de uitwerking tabel 1 Beveiligingsniveaus.
F1-002	Alle camera's die zicht hebben op de openbare ruimte worden geregistreerd bij Camera in Beeld (Politie). De huidige registratie betreft 13 buitencamera's van het Gemeentehuis. Opdrachtnemer zorgt voor aanmelding van nieuwe en gewijzigde camera's bij Camera in Beeld, voor zowel Gemeentehuis als De Werf.
F1-003	Camera-installaties voor beveiligingsdoeleinden voldoen aan NEN 62676-4.
F1-004	Snel opvragen van beelden via zoekfunctie op tijd, datum, camera en gebeurtenis.
F1-005	Live viewing vanaf verschillende werkstations en mobiel; beveiligd via tweefactorauthenticatie.
F1-006	Beeldopname vindt continu plaats: bewegingsdetectie is geen primaire opnamemodus.

F1-007	Integratie met toegangscontrolesysteem (beelden koppelen aan toegangsevents) en integratie met brand- en inbraakinstallatiesysteem.

Nr.	Omschrijving zone	Omschrijving zone
Zone 0	Terrein rondom gebouw (buitengebied).	Vrij toegankelijk; binnenterrein/rijwielstalling via slagboom/TRS.
Zone 1	Publiekshal met receptie.	Vrij toegankelijk tijdens openingstijden; receptie geeft permissie voor Zone 2.
Zone 2	Vergadercentrum, bestuursruimten regelmatig toegankelijk voor publiek (Oude Raadszaal, fractiekamers, perskamer).	Alleen met begeleiding of na autorisatie receptie.
Zone 3	Werkruimten alleen voor geautoriseerde medewerkers: bestuursruimten college B&W, crisiscentrum, restaurant, kantoorwerkplekken inclusief publiekszaken.	Alleen met geldige toegangspas (TRS).
Zone 4	Extra beveiligde ruimten: laad-/losvoorzieningen, kluis paspoorten/contant geld, archieven, server- en netwerkruimten, off-site back-up locatie.	Alleen met speciale autorisatie; extra logging; kwartaalcontrole autorisaties.

Tabel 1 Beveiligingsniveaus

2.2 Technische specificaties camera's

Nr.	Omschrijving
T2-001	De minimale technische specificaties van de binnen camera's zijn: Specificatie — Uitwerking Resolutie — Minimaal 1080p (Full HD), bij voorkeur 4K voor kritieke locaties Beeldfrequentie — Minimaal 25 fps, bij voorkeur 30 fps Beeldhoek — Minimaal 90° horizontaal, variabel afhankelijk van locatie Dag/nacht functionaliteit — IR of low-light technologie voor beelden bij weinig licht WDR — Wide Dynamic Range verplicht voor locaties met tegenlicht Digitale zoom — Minimaal 4x zonder kwaliteitsverlies Compressie — H.265/H.264 voor efficiënte opslag Voeding — PoE (Power over Ethernet) - IEEE 802.3af/at Vandalismebestendig — IK10 voor kritieke locaties (entree, publieke ruimten) Audio (optioneel) — Microfoon voor specifieke locaties indien gewenst Behuizing — Discreet design, wit of zwart Montage — Plafond- of wandmontage afhankelijk van locatie

<table>
<tr><td>T2-002</td><td>De minimale technische specificaties van de buiten camera’s zijn:<table>
<tr><th>Specificatie</th><th>Omschrijving</th></tr>
<tr><td>Resolutie</td><td>Camera's leveren voldoende beeldkwaliteit om identificatie mogelijk te maken overeenkomstig NEN-EN-IEC 62676-4 voor de beoogde observatie-, herkennings- of identificatiedoelstelling.</td></tr>
<tr><td>Beeldfrequentie</td><td>Minimaal 25 fps</td></tr>
<tr><td>Beeldhoek</td><td>Minimaal 90° horizontaal, variabel afhankelijk van locatie</td></tr>
<tr><td>Weerbescherming</td><td>Minimaal IP66 (stof- en waterdicht)</td></tr>
<tr><td>Temperatuurbereik</td><td>-30°C tot +60°C voor Nederlandse klimaat</td></tr>
<tr><td>Infrarood nachtzicht</td><td>Minimaal 30 meter bereik, bij voorkeur 50 meter</td></tr>
<tr><td>WDR</td><td>Wide Dynamic Range verplicht</td></tr>
<tr><td>Optische zoom</td><td>Bij voorkeur 4x of hoger voor parkeerplaatsen/toegangswegen</td></tr>
<tr><td>Compressie</td><td>H.265/H.264</td></tr>
<tr><td>Voeding</td><td>PoE (Power over Ethernet) - IEEE 802.3at/bt voor PTZ</td></tr>
<tr><td>Vandalismebestendig</td><td>IK10 verplicht</td></tr>
<tr><td>Anti-condensatie</td><td>Verwarming tegen condensvorming</td></tr>
<tr><td>Verlichting</td><td>IR LED's of eventueel ingebouwde witte LED's</td></tr>
<tr><td>Behuizing</td><td>Weerbestendige dome of bullet behuizing</td></tr>
<tr><td>Montage</td><td>Muur-, paal- of plafondmontage afhankelijk van locatie</td></tr>
</table></td></tr>
<tr><td>T2-003</td><td>Voor specifieke locaties zoals parkeerplaatsen en grote buitengebieden kunnen Pan-Tilt-Zoom (PTZ-) camera's wenselijk zijn voor actieve monitoring. Deze camera’s voldoen aan de volgende eisen:
Optische zoom: minimaal 20x
Pan range: 360° continue rotatie
Tilt range: minimaal -15° tot +90°
Presets: minimaal 256 instelbare posities
Tours: automatische rondgang langs presets
Auto-tracking (optioneel): automatisch volgen bewegende objecten
Alle overige eisen conform buitencamera's
</td></tr>
</table>

2.3 Opslag en recording

Nr.	Omschrijving
O2-001	**Network Video Recorder (NVR) / Storage** - Opslagcapaciteit: minimaal 28 dagen continue opname alle camera's in Full HD/4K + 20% overcapaciteit voor toekomstige uitbreiding - Redundantie: RAID 5 of 6 configuratie voor Gegevensveiligheid - Hot-swappable schijven: schijven verwisselbaar zonder systeem uit te schakelen - Harde schijven: enterprise/surveillance grade schijven (24/7 rating)

	• Back-up: automatische back-up naar tweede locatie of Cloud (minimaal 7 dagen) • Overschrijving: automatische overschrijving oudste beelden na 28 dagen • Opnamemodi: continue opname + pre/post-alarm opname bij events • Simultane opname: alle camera's simultaan opnemen zonder frameverlies • Alarm bij storing: automatische melding bij schijffouten, vollopende opslag • Failover: bij uitval hoofdsysteem: automatische overschakeling naar back-up • RPO maximaal 4 uur voor CCTV en 1 uur voor TRS • RTO maximaal 8 uur voor CCTV en 4 uur voor TRS. Jaarlijkse fail-over- en hersteltesten zijn verplicht. Testresultaten worden gedeeld met Opdrachtgever.
O2-002	**Beeldkwaliteit opname** • Resolutie: conform camera-specificaties (min. 1080p binnen, 4MP buiten) • Framerate: minimaal 25 fps per camera • Compressie: H.265 voor optimale balans kwaliteit/opslagruimte • Bitrate: aanpasbaar per camera (constant of variabel) • Dual stream: hoge kwaliteit voor opname, lagere kwaliteit voor live viewing (bandbreedte) • Kwaliteitsniveaus: instelbaar per camera afhankelijk van belangrijkheid • Pre-alarm recording: minimaal 10 seconden vóór alarm • Post-alarm recording: minimaal 30 seconden na alarm

2.4 Video Management Software

Nr.	Omschrijving
V2-001	**Algemene VMS-eisen** • Nederlandstalige interface (volledig) • Intuïtieve bediening: minimale training nodig voor dagelijks gebruik • Multi-monitor ondersteuning (minimaal 2 schermen) • Webbased toegang voor remote viewing (beveiligd) • Mobiele apps voor iOS en Android • ONVIF compliant voor camera-integratie • API beschikbaar voor Koppelingen met andere systemen • Microsoft EntraID / LDAP integratie met SSO via SAML 2.0 • Schaalbaar: uitbreidbaar met meer camera's en locaties zonder beperkingen • Tweefactorauthenticatie voor beheerders en remote toegang • Sessies worden automatisch beëindigd na instelbare periode van inactiviteit • Na drie foutieve inlogpogingen wordt account geblokkeerd
V2-002	**Live viewing functionaliteit** • Configureerbare lay-outs: 1x1, 2x2, 3x3, 4x4 en custom • Drag-and-drop camera's naar monitors

	• PTZ-bediening: pan/tilt/zoom met muisbesturing • Digitale zoom in live beeld • Instant playback: direct terug kunnen kijken zonder live te verlaten • Alarm pop-ups bij events • Audio (indien van toepassing) • Snapshot functie • Grafische plattegronden met cameraposities (kaart-view) • Sequence viewing: automatische roulatie door camera's
V2-003	**Playback en zoekfunctionaliteit** • Timeline-based playback: intuïtieve tijdlijn • Multi-camera playback: meerdere camera's synchroon terugkijken • Snelle zoekfunctie op: datum, tijd, camera, alarm, beweging • Smart search: zoeken op beweging binnen bepaald gebied • Thumbnail view: snel overzicht van opgenomen periode • Variable speed playback: 0.25x tot 32x snelheid • Frame-by-frame: nauwkeurige analyse • Digitale zoom in playback zonder kwaliteitsverlies • Bookmarks: markeren belangrijke momenten
V2-004	**Export en bewijslast** • Export naar standaard formaten (AVI, MP4) • Exporteren met native player (opslaan van videobeelden in het oorspronkelijke, onbewerkte formaat) • Watermerk en digitale handtekening tegen manipulatie • Exporteren naar USB, netwerkschijf en e-mail • Meerdere camera's in één export • Metadata: datum, tijd, camera en locatie • Print snapshots met metadata • Exportrechten apart toekennen per gebruiker
V2-005	**Privacy en beveiliging** • Privacy masking: afschermen privacygevoelige gebieden (vaste maskers) • Gebruikersbeheer: granulaire rechten per gebruiker/groep • Audit trail: volledige logging van alle gebruikersacties • Automatische uitlog na inactiviteit • Sterke wachtwoordeisen (complexiteit, rotatie) • Tweefactor authenticatie (optioneel maar aanbevolen) • Versleutelde communicatie (TLS/SSL) • Versleutelde opslag (optioneel) • Toegang beperken tot specifieke camera's per gebruiker

	• Export-rechten apart toekennen (niet iedereen mag exporteren) • Alle Gegevens verwerkt en opgeslagen binnen de EER

V2-006	**Intelligente analysefuncties**
	
	• Indien AI- of videoanalysefunctionaliteit gebruikmaakt van cloudverwerking:
	  • vindt verwerking plaats binnen de EER;
	  • worden geen beelden gebruikt voor modeltraining;
	  • blijft Opdrachtgever eigenaar van alle Gegevens.
	• Slimme analysefuncties zijn geen harde eis maar sterk gewenst voor toekomstbestendigheid:
	• Bewegingsdetectie: instelbare zones en gevoeligheid
	• Lijnkruising: alarm bij overschrijden virtuele lijn
	• Object detectie: herkennen voertuigen, personen
	• Loitering detectie: alarm bij te lang stilstaan
	• Intrusion detection: alarm bij betreden verboden gebied
	• Kentekenherkenning (ANPR): bij in-/uitgangen parkeren (werf)
	• Gezichtsherkenning maakt geen onderdeel uit van de opdracht. Toepassing hiervan is uitsluitend toegestaan indien hiervoor een afzonderlijke wettelijke grondslag aanwezig is, een aanvullende DPIA is uitgevoerd en Opdrachtgever hiervoor expliciet schriftelijke toestemming heeft verleend.
	• Sabotagedetectie: alarm bij verplaatsing, afdekking, defocus camera
	• Audio-detectie: glasbreuk, agressie, schreeuwen (optioneel t.b.v. spreekkamer)
	• People counting: tellingen bezoekers (optioneel)

V2-007	**Rapportage** • Standaard rapporten: events, alarmen, systeemgezondheid, gebruikersactiviteit • Custom rapporten: zelf samenstellen • Exporteren naar PDF, Excel, CSV • Automatische rapportage: periodiek versturen per e-mail • Dashboard: real-time overzicht systeemstatus.
V2-008	Bij Gegevens- of informatie-uitwisseling binnen de Applicatie of tussen applicaties of tussen Applicatie en gebruikers, moet de Gegevens-integriteit zijn gewaarborgd. Dit betekent dat de Gegevens niet van buitenaf gelezen of gemuteerd kan worden.

3. Programma van eisen - TRS

3.1 Algemene eisen

Nr.	Omschrijving
A2-001	• Centraal beheer van alle toegangsrechten via één systeem. • Real-time registratie van in- en uitgangen (logging). • Bewaartermijn eventlogging moet ingesteld kunnen worden, liefst vanaf 0 of 1 dag. • Tijdzone management: toegang op specifieke tijden/dagen. • Anti-passback: voorkomen dat één pas meerdere personen doorlaat. • First person in / Last person out: registratie voor faciliteiten. • Alarmering bij ongeautoriseerde toegangspogingen. • Noodontgrendeling: alle deuren ontgrendelen bij calamiteit. • Fail-safe / fail-secure per deurtype configureerbaar. • 24/7 operationeel, ook bij netwerkuitval (offline modus). PS back-up minimaal 4 uur voor alle componenten. • Integratie met brand- en inbraakinstallatie: automatisch blokkeren toegang bij alarm. • Het moet mogelijk zijn om autorisaties toe te kennen aan individuele kaarthouders of aan een groep kaarthouders. • Autorisatiematrix op één scherm toonbaar of afdrukbaar op maximaal twee pagina's. • Koppelingen met verschillende typen toegangspunten van verschillende Opdrachtnemers moet mogelijk zijn. • Het Systeem moet de mogelijkheid ondersteunen om kaarthouderinformatie afzonderlijk of in bulk te bewerken. • Het Systeem biedt een uniforme zoekfunctie (zoek gelijktijdig in alle kaarthoudergegevens), directe validatie (directe feedback over of de informatie in een veld geldig is) en directe resultaten (directe zoekresultaten tijdens het typen).
A2-003	Het Systeem maakt het mogelijk om op elk moment in de toekomst en in kleine stapjes (per deur, met bedrade en draadloze toegangscontrole, inbraakdetectoren en lockers) eenvoudig en onbeperkt uit te breiden van apparaten (inclusief bedrade en draadloze toegangsdeuren, inbraakdetectoren en lockers) te vergroten, zonder prestatieverlies, de noodzaak om meer te rekenen dan de daadwerkelijke uitbreiding, en het gebruik van andere/nieuwe systeemsoftware.
A2-004	De oplossing ondersteunt minimaal 100 gelijktijdige beheerderssessies zonder merkbare degradatie van prestaties.

A2-005	Het Systeem stuurt automatisch een waarschuwing via e-mail en sms naar geselecteerde contacten als instellingen in het systeem zijn gewijzigd. Het Systeem maakt het mogelijk om in te stellen welke wijzigingen zo'n waarschuwing zullen activeren.
A2-006	Het Systeem moet meerdere oplossingen ondersteunen om systeemgebruikers toe te voegen en te authenticeren. • Lokale systeemaccounts: een beheerder moet in staat zijn om gebruikersaccounts, gebruikersrollen en gebruikerssjablonen lokaal aan te maken. • Systeemaccounts die door LDAP worden beheerd: het systeem gebruikt lokale accounts, maar LDAP beheert de gebruikersnaam en het wachtwoord, maakt nieuwe accounts aan en wijst een gebruikersrol en/of gebruikerstemplate toe aan een gebruiker. Als de LDAP-server uitvalt, moet het systeem gebruikers ondersteunen om nog steeds in te loggen met hun lokale accountinstellingen, aangezien deze door de LDAP-server zijn ingesteld bij de laatste inloging met LDAP. • Single sign-on (SSO) beheerd door SAML: Het Systeem moet het gebruik van gangbare inbraakdetectiesystemen die gebruikmaken van open standaarden of aantoonbaar gelijkwaardige integratiemogelijkheden. • Single sign-on (SSO) beheerd door SPNEGO: Het Systeem moet het gebruik van een Kerberos-server ondersteunen zodat gebruikers automatisch kunnen inloggen met hun Windows-domeininloggegevens. Deze optie moet ook met LDAP kunnen werken.
A2-007	Het Systeem moet vanaf elk werkstation toegankelijk zijn via een webgebaseerde gebruikersinterface via het lokale gebied/wide area network (LAN/WAN), zonder dat specifieke systeemclientsoftware op werkstations hoeft te worden geïnstalleerd. Het zal compatibel zijn met ten minste Microsoft Edge, Google Chrome, Safari en Mozilla Firefox. Het Systeem moet beveiligde communicatie (ten minste https) tussen het werkstation en de server ondersteunen.
A2-008	Het Systeem staat toe dat het aantal gelijktijdige sessies per systeemgebruiker wordt begrensd, om te voorkomen dat gebruikers hun account delen of op meerdere locaties inloggen.
A2-009	Het Systeem meldt zich automatisch af na een definieerbare verlengde periode van inactiviteit (sessietime-out).
A2-010	Het Systeem schakelt automatisch accounts uit van systeemgebruikers en beheerders die een definieerbaar maximaal aantal foute inlogpogingen overschrijden. Na succesvol inloggen toont het systeem of eerdere mislukte inlogpogingen hebben plaatsgevonden.
A2-011	Het Systeem maakt het mogelijk om systeemgebruikers te authenticeren tegen een externe LDAP-directory.

3.2 Identificatiemiddelen en hardware

Nr.	Omschrijving
I2-001	Het Systeem ondersteunt SOAP, RESTful en ODBC om kaarthouder-, toegangskaart- en autorisatiegegevens bidirectioneel in realtime uit te wisselen. Dit maakt het systeem mogelijk om te functioneren als zowel slave-systeem als master-systeem.
I2-002	Het Systeem zal een socket-interface bieden voor realtime uitwisselingsgegevens. Dit stelt een derdepartijsysteem in staat om alle systeemveldhardware te beheren en alle systeemgebeurtenissen en alarmen te ontvangen.
I2-003	Het Systeem maakt het mogelijk om te integreren met toegangscontrolesystemen van derden via een SOAP-webservice en een database-import/export (ODBC) om kaart-, toegangskaart- en autorisatiegegevens bidirectioneel in realtime uit te wisselen. Dit maakt het systeem mogelijk om te functioneren als zowel slave-systeem als master-systeem.
I2-004	Hardware componenten: • Kaartlezers communiceren via een OSDP (Open Supervised Device Protocol), waarvoor een getwiste, afgeschermde kabel die geschikt is voor RS-485 communicatie gebruikt wordt. Een kabeltype 2x2x0,22 mm^2 of 2x2x0,5 mm^2 twisted pair shielded. Eén pair voor A/B data en één pair voor voeding. OSDP Secure Channel is de huidige best practice die Opdrachtgever eist. • RFID-lezers per soort zone: binnen IK08, buiten minimaal IP65 en IK10 • Communicatieprotocol lezers: OSDP • Elektrische sloten: • Elektromagnetisch voor nooduitgangen (fail-safe) • Elektromotorsloten voor beveiligde ruimtes (fail-secure) • REX-sensoren: PIR of radar • Centrale voeding met UPS back-up minimaal 4 uur • Paniekknoppen op locaties met publiekscontact en spreekkamers

3.3 Toegangscontrolesoftware

Nr.	Omschrijving
TS2-001	**Algemene eisen:** • Nederlandstalige interface, volledig en intuïtief • Centraal beheer van gebruikers en autorisaties • Realtime monitoring van alle toegangspunten • Grafische plattegronden met status per deur • Export naar Excel en PDF • Automatische back-ups vereist

	• Schaalbaar zonder beperkingen in gebruikers, transacties of locaties
TS2-002	**Integratie-eisen:** • Koppeling met Microsoft EntraID (grote voorkeur) via SAML 2.0 met SSO • Koppeling met brand- en inbraakinstallatie: automatisch blokkeren lezers bij gewapend alarm
TS3-003	**Beveiliging en privacy:** • Tweefactorauthenticatie voor beheerders en remote toegang • Sessies automatisch beëindigd na instelbare periode van inactiviteit • Na drie foutieve inlogpogingen wordt account geblokkeerd • Geen kopieën van toegangsgegevens behalve voor beschikbaarheid • Alle Gegevens worden verwerkt en opgeslagen binnen de EER • Opdrachtnemer kan niet zelfstandig toegang verlenen aan eigen medewerkers tot Gegevens van Opdrachtgever. Toegang verlenen tot Gegevens van Opdrachtgever verloopt te allen tijde via (de functioneel beheerder van) Opdrachtgever.
TS3-004	**Gebruikersbeheer:** • Individuele accounts, geen groeps- of afdelingsaccounts • Autorisaties halfjaarlijks gecontroleerd; Zone 4 minimaal per kwartaal • Procedure voor vergeten pas: tijdelijke genummerde pas na legitimatie • Procedure voor verloren pas: directe blokkade via centraal systeem met registratie van toegangshistorie vanaf moment van verlies
TS3-005	**Bezoekersbeheer:** • Bezoekers worden geregistreerd bij aankomst via receptie • Identificatiemiddel gekoppeld aan TRS: toegang beperkt tot geautoriseerde zones en tijden • Automatische blokkade bezoekerspas bij vertrek • Registratie bijgehouden: naam, organisatie, contactpersoon, tijdstip in en uit
TS3-006	Het moet mogelijk zijn om, per vervoerdertype (werknemer, bezoeker, aannemer, voertuig), de periode te definiëren waarvoor vervoerdergegevens in het Systeem worden opgeslagen.
TS3-007	Het Systeem moet een verschil maken in de Gegevensopslagperiode per dag voor verschillende Gegevenstypen • Carriers zonder badges verwijderen. • Carriers verwijderen • Verwijderde carriergegevens wissen
TS3-021	Het Systeem zal een volledig aanpasbare kaart van gebouwen en hun plattegronden bieden om geselecteerde beveiliging kritische locaties en apparaten weer te geven. De kaart zal op

	verdiepingen kunnen inzoomen om verschillende detailniveaus te tonen. De kaart zal de realtime status van beveiligingsapparaten (inclusief sensoren, sloten en lezers) en alarmen visualiseren, inclusief hun exacte locatie, door audio- en visuele signalen te genereren (zowel kleur als vorm van iconen zijn definieerbaar).
TS3-022	Wanneer een deel van een gebouw is opgedeeld in meerdere kaarten, toont het systeem aan de systeemgebruiker waar de kaart zich bevindt ten opzichte van de rest van het gebouw dat wordt bekeken, om situationeel inzicht te bieden.
TS3-023	Alarmen moeten van elk geselecteerd gebeurtenistype zijn, gegenereerd door de toegangscontrole, inbraakdetectie of IP-videobewakingssystemen. Het Systeem maakt het mogelijk om alarmen te prioriteren (zoals kritiek, hoog, medium of laag belangrijkheid) en geselecteerde alarmen te markeren met definieerbare kleuren. Het Systeem zal automatisch specifieke alarmen doorsturen naar specifieke systeemgebruikers. Het Systeem stelt de systeembeheerder in staat om te filteren welke systeemgebruikers welke gebeurtenissen en alarmen kunnen zien.
TS-024	Voor elk verschillend alarm staat het systeem toe dat automatisch een e-mail en sms-bericht naar geselecteerde contacten worden gestuurd.
TS-025	Het Systeem zal onderscheid maken tussen de volgende typen kaarthouders: • Werknemers. • Bezoekers. • Aannemers (werknemers van derdepartijbedrijven die werken op de toegangsgecontroleerde locatie). • Voertuigen.
TS-026	Het Systeem ondersteunt onbeperkte autorisatiesjablonen en kaarthoudergroepen en bepaalt welke systeemgebruikers het specifieke sjabloon of de groep aan kaarthouders mogen toewijzen. Sjablonen bestaan uit één of meer: • Enkele toegangspunten en groepen toegangspunten (bijvoorbeeld alle deuren binnen een bepaalde verdieping) die de kaarthouder kan benaderen. • Vrij definieerbare dag-/tijdschema's, die aangeven op welke dag van de week en op welke exacte data en tijden kaarthouders toegang krijgen tot de geselecteerde (groep van) toegangspunten. Het Systeem maakt het mogelijk om verschillende dag-/tijdschema's per (groep van) toegangspunten in te stellen (bijvoorbeeld een dag-/tijdschema voor alle deuren en een ander dag-/tijdschema voor de hoofdingang). De lokale tijd bij het betreffende toegangspunt geldt voor het dag-/tijdschema.
TS-027	Het Systeem maakt het mogelijk om de autorisatie van kaarthouders te bepalen door hen één of meer:

	• Autorisatietemplates. • Kaarthoudersgroepen. • Handmatige autorisatie voor groepen toegangspunten en individuele toegangspunten.
TS-028	Het Systeem koppelt autorisaties aan kaarthouders (die personen of voertuigen kunnen zijn), niet aan de toegangskaart die door de kaarthouder wordt bezit. Alle toegangskaarten zijn inactief, tenzij toegewezen aan een kaarthouder. Het ondersteunt de toewijzing van meerdere toegangskaarten aan enkele kaarthouders, zonder dat deze kaarthouders meerdere keren hoeven te worden geregistreerd.
TS-029	Het Systeem maakt het mogelijk om zowel één als meerdere kaarthouders gelijktijdig te bewerken, waaronder: • Blokkeer/deblokkeer geselecteerde kaarthouders, inclusief het registreren van de reden van blokkering. Dit blokkeert de kaarthouder en blokkeert automatisch alle bijbehorende toegangskaarten. • Bekijk en bewerk de informatie en autorisatie van een kaarthouder. • Verander het type kaarthouder. • Verplaats kaarthouders van de ene aparte groep (bijvoorbeeld een afdeling) naar een andere. • Haal toegangskaarten op en (ont)blokkeer de toegangskaarten. • Verwijder kaarthouders.
TS-030	Het Systeem biedt de mogelijkheid om: • geef een vervangende toegangskaart en registreer de reden van vervanging (bijvoorbeeld verloren). Dit zal de originele toegangspas automatisch en onmiddellijk blokkeren. • trek de vervangende kaart in, die de originele kaart zal deblokkeren en de vervangende kaart automatisch en onmiddellijk ongeldig maakt.
TS-031	Het Systeem maakt het mogelijk om vervangende toegangspassen opnieuw te gebruiken voor andere kaarthouders zonder dat de kaarthouderinformatie en gebeurtenisgeschiedenis van een kaarthouder worden beïnvloed.
TS-032	Het Systeem stuurt automatisch een e-mail en sms-bericht naar de betreffende kaarthouder als hun toegangskaart is vervangen of ingetrokken.
TS-033	Wijzigingen met betrekking tot toegangskaarten worden binnen minder dan 1 seconde door het hele systeem verspreid (mogelijke netwerklatentie wordt niet meegenomen).
TS-034	Om de efficiëntie te verhogen en menselijke fouten te verminderen, zal het systeem automatisch autorisaties van kaarthouders bijwerken als aan een of meer gedefinieerde criteria en regels wordt voldaan, met behulp van voorwaardelijke constructies zoals 'als',

	'en', 'of', 'groter dan', 'minder dan', 'gelijk', 'dan'-logica. Alle velden in het systeem, inclusief door de gebruiker gedefinieerde velden, moeten beschikbaar zijn voor het definiëren van criteria en regels. Voorbeelden zijn: • Blokkeer automatisch werknemers die hun baan verlaten (beheerd in HR-software van derden). • Gespecificeerde toekenningen worden toegekend aan kaarthouders die in een bepaalde afdeling werken. Als de afdeling verandert, worden de toestemmingen automatisch bijgewerkt. • Toestemmingen van kaarthouders die van gebouw veranderen worden automatisch bijgewerkt.
TS-035	Nieuwe kaarthouders en wijzigingen in autorisatie worden binnen minder dan 1 seconde geactiveerd door het hele systeem (mogelijke netwerklatentie wordt niet meegenomen).
TS-036	Het Systeem blokkeert automatisch kaarthouders van wie de toegangspassen gedurende een bepaalde periode niet zijn gebruikt. Het zal bepaalde kaarthouders in staat stellen vrijgesteld te zijn van automatische blokkering.
TS-037	Het Systeem blokkeert automatisch kaarthouders zodra hun dienstverband is beëindigd, wat geregistreerd is in een HRM-systeem van een derde partij.
TS-038	Het Systeem kan een kaarthouder blokkeren op basis van een vooraf bepaalde gebeurtenis.
TS-039	Het Systeem staat toe dat de kaarthouder automatisch wordt geblokkeerd als de geldigheid van zijn gegevens is verlopen. Als de betreffende kaarthouder een aannemer is, ondersteunt het systeem automatisch het blokkeren van de bijbehorende Opdrachtnemer. Het Systeem maakt het mogelijk om automatisch een e-mail en sms-bericht te sturen om de kaarthouder een bepaald aantal dagen van tevoren te informeren dat hun gegevens bijna verlopen. Het staat automatisch blokkeren toe als reactie op het verlopen van een kaarthouderveld, inclusief paspoort, foto, certificaten (bijv. veiligheidsinstructies) en werkvergunning.
TS-040	Het Systeem weigert automatisch geblokkeerde kaarthouders toegang bij alle toegangspunten en toont de reden voor blokkering in de gebruikersinterface.
TS-041	Het Systeem biedt de mogelijkheid om per credential een vervaldatum in te voeren voor automatische blokkering van een credential na een bepaalde datum.
TS-042	Het Systeem zal anti-pass back (APB) bieden om te voorkomen dat mensen geselecteerde zones en toegangspunten betreden door een toegangskaart van een kaarthouder te hergebruiken die het betreffende zone/toegangspunt niet eerder heeft verlaten. Als er

	sprake is van een APB-overtreding, genereert het systeem een alarmgebeurtenis en staat de volgende soorten respons toe: • Zachte APB: toegang wordt verleend; Er wordt alleen een alarmgebeurtenis naar geselecteerde personen gestuurd. • Getimede APB: toegang tot de APB-zone wordt voor een bepaalde periode geweigerd nadat de kaarthouder die APB-zone is binnengegaan. • Geteld APB: de kaarthouder wordt geblokkeerd na een bepaald aantal APB-overtredingen. • Harde APB: toegang tot de APB-zone wordt geweigerd.
TS-043	Het Systeem garandeert de voortdurende volledige werking van APB wanneer de server niet beschikbaar is.
TS-044	Het Systeem staat Opdrachtnemers (derden, bijvoorbeeld schoonmaakbureaus) die op de toegangsgecontroleerde locatie werken toe en geeft toestemming aan hun geselecteerde aannemers (werknemers van een Opdrachtnemer). Het zal onderscheid maken tussen aannemers van hoofdOpdrachtnemers (rechtstreeks ingehuurd) en van onderaannemers (ingehuurd door andere derde partijen). Het Systeem koppelt aannemers aan een verantwoordelijke host of contactpersoon.
TS-045	Het Systeem moet het mogelijk maken om projecten te definiëren waarvoor Opdrachtnemers en hun aannemers ter plaatse werken. Aannemers hebben alleen toegang als ze gekoppeld zijn aan een actief project. Projecten moeten ten minste specificeren: • De aard van het werk en de locatie. • Hoeveel en welke specifieke aannemers aan dit project mogen werken. • De projectperiode waarin het werk zal plaatsvinden. Alle toestemmingen voor toegang van aannemers worden automatisch geblokkeerd buiten deze periode. • Of de Opdrachtnemers en hun aannemers beschikken over de vereiste vrij definieerbare certificering, bijvoorbeeld veiligheidsinstructies. Het zal automatisch aannemers blokkeren van wie de certificeringen zijn verlopen en automatisch een e-mail en sms-bericht sturen om de betrokken aannemers een vastgesteld aantal dagen van tevoren te informeren als hun certificering bijna verloopt.
TS-046	Het Systeem staat het toe om een tijdelijke en permanente weigering van toegang uit te vaardigen voor alle kaarthouders die bij een bepaalde Opdrachtnemer in dienst zijn.

3.3.1 Logbeheer en Audittrail

TS3-008	Het Systeem moet toestaan om de periode waarin gebeurtenissen worden opgeslagen in het gebeurtenislogboek in te stellen.
TS3-009	Het Systeem moet de mogelijkheid ondersteunen om na die periode alle gebeurtenisgegevens te verwijderen of de gebeurtenisgegevens na die periode te archiveren.
TS3-010	Alleen toegestane gebruikers mogen de gearchiveerde logboekgebeurtenissen bekijken.
TS3-011	Het Systeem moet de beperking ondersteunen van het aantal dagen dat een gebruiker kan terugkijken in het gebeurtenislogboek.
TS3-012	Het Systeem moet de beperking ondersteunen van het aantal dagen dat een gebruiker terug kan kijken in het auditspoor.
TS3-013	Het Systeem moet alle zoekopdrachten die een gebruiker uitvoert opslaan in het gebeurtenislogboek.
TS3-014	Het Systeem moet toestaan dat het auditspoor voor een definieerbare (inclusief onbeperkte) tijd in een ophaalbaar bestand wordt bewaard. Als er een tijdslimiet is ingesteld, verwijdert het systeem automatisch alle opgeslagen gebruikersacties, gebeurtenissen en alarmen die deze limiet overschrijden. Upgrades en updates van het systeem hebben geen invloed op de compatibiliteit van het auditspoor.
TS3-015	Het Systeem ondersteunt geautomatiseerde archivering van auditspoor-gebeurtenissen na een gedefinieerde bewaarperiode van de systeemdatabase naar een bestand op de server om de impact op de systeemprestaties in de tijd te verminderen.
TS3-016	Het Systeem stelt de systeemgebruiker in staat snel te zoeken tussen live en gearchiveerde auditsporen vanuit de gebruikersinterface. Gebeurtenissen in het gebeurtenislogboek worden weergegeven in zowel centrale servertijd als lokale tijd.
TS3-017	Het Systeem maakt het mogelijk om alle geregistreerde gebruikersacties, gebeurtenissen en alarmen op te vragen en weer te geven. Het Systeem maakt het mogelijk om queries op te slaan.
TS3-018	Het Systeem maakt het mogelijk om in te stellen welke systeemgebruikers het auditspoor mogen opvragen en zien.

TS3-019	Het Systeem moet alle zoekopdrachten die een gebruiker uitvoert opslaan in het gebeurtenislogboek.
TS3-020	Voor elke systeemgebruiker moet het systeem filteren welke geregistreerde gebeurtenissen en alarmen toegankelijk zijn. Het Systeem stelt de systeemgebruiker in staat om te filteren op het type gebeurtenis en alarm, evenals op geografische locatie (bijvoorbeeld alleen toegangscontrole-evenementen die in een bepaald gebouw worden gegenereerd).

3.4 Integratie en netwerkinfrastructuur

Nr.	Omschrijving
IN2-001	**Algemene eisen:** • Nederlandstalige interface, volledig en intuïtief • Centraal beheer van gebruikers en autorisaties • Realtime monitoring van alle toegangspunten • Grafische plattegronden met status per deur • Volledige auditspoor van alle gebruikersacties • Export naar Excel en PDF • Automatische back-ups vereist • Schaalbaar zonder beperkingen in gebruikers, transacties of locaties
IN2-002	**Integratie-eisen:** • Koppeling met Microsoft EntraID (grote voorkeur) via SAML 2.0 met SSO • Koppeling met brand- en inbraakinstallatie: automatisch blokkeren lezers bij gewapend alarm
IN3-003	**Beveiliging en privacy:** • Tweefactorauthenticatie voor beheerders en remote toegang • Sessies automatisch beëindigd na instelbare periode van inactiviteit • Na drie foutieve inlogpogingen wordt account geblokkeerd • Logging van toegangsevents: bewaartermijn conform zoneringsplan Zone 1-3: minimaal 3 maanden Zone 4 (extra beveiligd): minimaal 1 jaar • Geen kopieën van toegangsdata behalve voor beschikbaarheid • Alle Gegevens verwerkt en opgeslagen binnen de EER • Opdrachtnemer kan niet zelfstandig toegang verlenen aan eigen medewerkers tot Gegevens van Opdrachtgever

IN3-004	**Gebruikersbeheer:** • Individuele accounts, geen groeps- of afdelingsaccounts • RBAC: gebruiker krijgt alleen toegang tot locaties en tijden die passen bij zijn rol • Autorisaties halfjaarlijks gecontroleerd; Zone 4 minimaal per kwartaal • Procedure voor vergeten pas: tijdelijke genummerde pas na legitimatie • Procedure voor verloren pas: directe blokkade via centraal systeem met registratie van toegangshistorie vanaf moment van verlies
IN4-005	Het Systeem maakt integratie mogelijk met gangbare inbraakdetectiesystemen die gebruikmaken van open standaarden of aantoonbaar gelijkwaardige integratiemogelijkheden. Ten minste om: • Automatisch de autorisatie intrekken om inbraakgebieden van kaarthouders te activeren en onschadelijk te maken van wie de toegangscontrolerechten in het toegangscontrolesysteem zijn geblokkeerd. • Lokaal inbraakgebieden bewapenen en deactiveren met geautoriseerde toegangskaarten. Als de kaarthouder een vervangende kaart ontvangt, kan hij/zij deze automatisch gebruiken in het inbraaksysteem. • Voorkom het activeren van inbraakgebieden als toegangspunten binnen dat gebied nog open zijn. Dit werkt zelfs als de server offline is. • Blokkeer automatisch alle toegangspunten door de kaartlezers binnen een inbraakgebied te blokkeren terwijl het inbraakgebied is geactiveerd. De LED van de kaartlezer zal de kaarthouders informeren dat zij niet naar binnen kunnen vanwege het bewapende inbraakgebied. Dit werkt zelfs als de server offline is.

3.5 Inbraakdetectie en interface

Nr.	Omschrijving
ID2-001	Het Systeem kan de inbraakautorisatie beheren in hetzelfde systeem als de toegangscontroleautorisaties.
ID2-002	Het Systeem ondersteunt de toewijzing van inbraakautorisaties op basis van sjablonen aan kaarthouders. Kaarthouders kunnen meerdere templates hebben.
ID3-003	Via een webgebaseerde gebruikersinterface maakt het inbraaksysteem het mogelijk om te beheren wie gemachtigd is om elk individueel inbraakgebied te activeren en te deactiveren. Dit maakt het mogelijk om op afstand toegangskaarten en pincodes toe te wijzen en te wijzigen die worden gebruikt voor het activeren en onschadelijk maken van inbraakgebieden, wat betekent dat dit niet vereist dat je lokaal aanwezig hoeft te zijn op de locatie van de betreffende inbraakgebieden.
ID3-004	Het Systeem blokkeert automatisch de autorisatie om inbraakgebieden te activeren en te deactiveren door kaarthouders die zijn geblokkeerd voor toegang tot het

	toegangscontrolesysteem en van personen van wie het werk eindigt, dat geregistreerd is in een derdepartijsysteem.
ID3-005	Het Systeem maakt het mogelijk om elk inbraakgebied op afstand te activeren en te deactiveren via een webgebaseerde gebruikersinterface
ID3-006	Het Systeem maakt het mogelijk om te koppelen met het toegangscontrolesysteem om te voorkomen dat een inbraakgebied wordt geactiveerd als toegangspunten binnen dat gebied nog open zijn, zonder dat extra deurmonitoringcontacten of bedrading nodig zijn anders dan die voor toegangscontrole.
ID3-007	Wanneer een inbraakgebied is geactiveerd, blokkeert het systeem automatisch alle toegangspunten binnen dat gebied door de kaartlezers te blokkeren. Dit gebeurt via een softwareinterface, niet door het verbinden van in- en uitgangen, en werkt zelfs als de server offline is.

3.6 Cyberbeveiliging

Nr.	Omschrijving
C2-001	Het Systeem moet de communicatie tussen alle componenten versleutelen met TLS1.3-certificaten. Dit geldt voor de communicatie; • tussen de Applicatie en de Applicatieserver. • tussen de database en de Applicatieserver. • tussen de controller en de Applicatieserver. • tussen controllers (peer-to-peer).
C2-002	De controllers ondersteunen 802.1x EAP-TLS voor Network Access Control (NAC).
C2-003	Het Systeem zal in staat zijn certificaten te beheren.
C2-004	Naast de TLS 1.3-certificaten voor het Systeem en de Applicatie zullen ook de 802.1x-certificaten van de controllers beheersbaar zijn.
C2-005	Het Systeem en de Applicatie krijgt zijn eigen unieke certificaten.
C2-006	Het Systeem heeft een certificaatmanager aan boord, die alle certificaten van het hele systeem bijhoudt en bijwerkt.
C2-007	Het Systeem moet een lokale ondertekenaar aan boord hebben, zodat alle certificaten vanuit de Applicatie kunnen ondertekenen.
C2-008	Het Systeem ondersteunt het SCEP-protocol voor het ondertekenen van certificaten door een externe Public Key Infrastructure (PKI). Op deze manier kunnen certificaten worden

	ondertekend door een certificeringsinstantie (CA) die al voor andere doeleinden wordt gebruikt.
C2-011	Controllers moeten in staat zijn om op elk moment een SAM te bevatten voor het opslaan van DESFire-sleutels en digitale certificaten, zonder dat controllerhardware anders dan het installeren van de SAM zelf hoeft te veranderen.
C2-012	Controllers staan het mogelijk om de DESFire-sleutels en digitale certificaten op afstand bij te werken via een beveiligde, versleutelde verbinding.
C2-013	Het Systeem zal SAM AV2 en SAM AV3 ondersteunen.
C2-014	De controllers van het systeem zullen in transparante modus kunnen communiceren met badge-lezers. Dit betekent dat de badgelezers geen kaartsleutels mogen bevatten om de Gegevens te ontsleutelen. Op deze manier worden alle gevoelige Gegevens op controllerniveau opgeslagen, aan de veilige kant van de deur.
C2-015	De controllers van het systeem kunnen in transparante modus communiceren, met eigen badge-lezers. Daarnaast zal het gebruik van badge-lezers van derden ook worden ondersteund via het SSCPv2-protocol.
C2-016	De oplossing voldoet aantoonbaar aan: • BIO2; • ISO 27001; • ISO 27017 (voor SaaS-diensten); • ISO 27018 (voor verwerking van persoonsgegevens); • relevante NCSC-richtlijnen; • AVG.
C2-017	Opdrachtnemer en eventuele partijen die het SaaS-platform hosten of beheren beschikken over een geldige ISO 27001-certificering die relevant is voor de aangeboden dienstverlening.

3.7 Identificaties en kwalificaties

Nr.	Omschrijving
IK2-001	Het Systeem zal onbeperkte uitbreiding van toegangskaarten op elk moment in de toekomst mogelijk maken zonder dat systeemhardware en -software hoeven aan te passen.

IK2-002	Het Systeem ondersteunt de toewijzing van meerdere toegangsmiddelen aan kaarthouders die voldoen aan de geldende wet- en regelgeving van beveiliging. Het Systeem is in staat om gelijktijdig meerdere toegangskaarttechnologieën te bedienen.
IK2-003	Het Systeem moet in staat zijn om alle informatie die op een toegangskaart is opgeslagen te lezen, inclusief UID (Card Serial Number, CSN), gecodeerde sectorgegevens en gecodeerde Applicatiegegevens (bestandsgegevens).
IK2-004	Het Systeem zal een gebruikersinterface hebben die meerdere DESFire-Applicatiebestanden op hetzelfde badge kan lezen.
IK2-005	Het Systeem zal een gebruikersinterface hebben die elk type DESFire-badge kan lezen dat wordt gebruikt voor toegangscontrole.
IK2-006	Het Systeem ondersteunt het gebruik van mobiele inloggegevens op basis van een applicatie op de smartphone om het gebruik van een NFC- of QR-code als identificatie mogelijk te maken.
IK2-007	Het Systeem ondersteunt het gebruik van mobiele inloggegevens die zijn opgeslagen in het veilige element van de smartphone (de portemonnee) om het gebruik van de NFC-chip als identificatie mogelijk te maken.
IK2-008	Het Systeem zal de OSS Mobile Access (OSS-MA) open standaard ondersteunen voor gebruik van externe mobiele sloten.

4. Niet-Functioneel

4.1 Cyberrisico

Nummer	Omschrijving
NF-A-002	Opdrachtnemer maakt voor het uitvoeren van de Opdracht geen gebruik van leveranciers, onderaannemers of leveranciers van deze onderaannemers die onder EU-sancties vallen.
A-003	Voor cameratoezicht en toegangsregistratie is een Data Protection Impact Assessment (DPIA) verplicht. De DPIA is uitgevoerd in april 2026 door de teamleider facilitair en de privacy officer van Opdrachtgever. De functionaris gegevensbescherming heeft het DPIA voorzien van advies. De privacy officer van Opdrachtgever zorgt voor actualisatie van de DPIA in samenwerking met Opdrachtnemer. Opdrachtnemer werkt hier te allen tijde aan mee door het aanleveren van o.a. de gevraagde informatie.

4.2 Organisatie Opdrachtnemer

4.2.1 Doorontwikkeling Product

Nummer	Omschrijving
NF-O-004	Opdrachtnemer heeft een ontwikkel-agenda van de geplande wijzigingen (features, technische vernieuwing en beveiligingsverbeteringen) met een tijdshorizon van 12 maanden.

4.2.2 Ondersteuning Opdrachtgever

Nummer	Omschrijving
NF-O-011	De Opdrachtnemer stelt aan het einde van de implementatiefase een DAP (Detail Afspraken en Processen) op samen met de Opdrachtgever. De eerste door beide partijen goedgekeurde DAP wordt toegevoegd als bijlage aan de Overeenkomst. Als er wijzigingen zijn, wordt de DAP bijgewerkt. Nieuwe versies van de DAP hoeven niet aan de Overeenkomst worden toegevoegd mits beide partijen akkoord zijn met de wijzigingen. In de DAP wordt o.a. opgenomen: - Welke overleggen er zijn, welke onderwerpen in welk overleg worden besproken en met welke regelmaat de overleggen worden ingepland - Welke contactpersonen er zijn voor welke activiteiten (inclusief de contactgegeven) - Wat de inhoud is van de periodieke rapportage - Hoe processen verlopen (denk aan melden incidenten, aanvragen wijzigingen en escalaties) etc. - In het DAP wordt vastgelegd welke beheertaken door de Opdrachtgever worden uitgevoerd en welke door de Opdrachtnemer.
NF-O-014	**Opdrachtnemer** beschikt over één servicedesk die fungeert als Single Point of Contact voor het melden van incidenten, serviceverzoeken, wijzigingsverzoeken en vragen over de dienstverlening. De servicedesk is op werkdagen van 09:00 tot 17:00 uur telefonisch en per e-mail bereikbaar. Opdrachtnemer bevestigt iedere melding binnen **30 minuten** na ontvangst en kent daarbij een prioriteit toe conform de overeengekomen SLA. Opdrachtnemer informeert de door Opdrachtgever aangewezen contactpersoon gedurende de afhandeling van de melding over de voortgang: • P1: minimaal elke **60 minuten**; • P2: minimaal iedere **4 uur**; • P3: minimaal iedere **werkdag**; • P4: op verzoek van Opdrachtgever.

	Voor Prioriteit 1-incidenten is Opdrachtnemer bereikbaar van maandag tot en met vrijdag van **06:00 tot 23:00 uur**. Buiten deze tijden is een noodnummer beschikbaar voor het melden van Prioriteit 1-incidenten. Een **Prioriteit 1-incident** betreft: • volledige uitval van een kritische beveiligingsfunctie; • ernstige verstoring van de Toegangscontrole; • ernstige verstoring van het CCTV-systeem; • een Beveiligingsincident met directe impact op de beschikbaarheid, integriteit of vertrouwelijkheid van de Dienstverlening. Inschrijver levert bij zijn Inschrijving een concept-SLA aan. De in het PvE opgenomen service-eisen gelden daarbij als minimale eisen waaraan de SLA moet voldoen.

4.2.3 Overleggen met Opdrachtgever

Nummer	Omschrijving
NF-O-021	Gedurende de looptijd van de Overeenkomst vindt het strategisch overleg éénmaal per jaar plaats tussen Opdrachtgever en Opdrachtnemer. Onderwerpen zijn o.a. a. de behaalde resultaten en performance van het afgelopen jaar ten opzichte van de SLA - afgezet tegen de eisen en voorwaarden in de Overeenkomst, b. ontwikkelingen bij Opdrachtgever op langere termijn, c. bedrijfsontwikkelingen bij de Opdrachtnemer, d. de roadmap van de Opdrachtnemer (van minimaal een jaar), e. duiding van de technische en/of functionele ontwikkelingen die voor de Opdrachtgever van belang zijn en marktontwikkelingen. f. de Overeenkomst wordt geëvalueerd g. afspraken worden gemaakt over de volgende periode van samenwerking. Eventueel wordt de DAP aangepast als er wijzigingen zijn geweest in het afgelopen jaar. Het initiatief, de organisatie en de verslaglegging ligt bij de Opdrachtnemer. Aanwezig zijn minimaal de accountmanager van de Opdrachtnemer en vanuit de Opdrachtgever de Applicatie-eigenaar en contractmanager.

4.2.4 Processen

Nummer	Omschrijving
NF-O-030	Opdrachtnemer behoort haar “Business Continuity Management” (BCM) proces adequaat te hebben georganiseerd, waarbij de volgende aspecten zijn geadresseerd: verantwoordelijkheid voor “Business Continuity Management”, beleid en procedures,

	bedrijfscontinuïteitsplanning, verificatie en updaten en computercentra. Dit b.v. gedaan op basis van ISO22301 of gelijkwaardige norm.
NF-O-032	Opdrachtnemer stelt direct (uiterlijk binnen 8 uur) op de hoogte van veiligheidsincidenten (bijvoorbeeld een Gegevens-lek of security-incident) en de bijbehorende ICT-oplossingtermijn. Opdrachtnemer informeert hierbij over het feit of de 'bedreiging' wel of niet adequaat is opgelost en de eventuele gevolgen en impact van het veiligheidsincident als wel het oplossen hiervan. Wie binnen de Opdrachtnemer en de Opdrachtgever elkaar informeren wordt vastgelegd in het gezamenlijke DAP (Dossier Afspraken en Protocollen). De contactgegevens van de verantwoordelijke personen worden ook in de DAP vastgelegd.
NF-O-033	Opdrachtnemer heeft procedures voor correctief, preventief en adaptief onderhoud. De upgrades, updates en (security) patches die hieruit voortvloeien worden via een beschreven ontwikkel- en testproces tijdig, geautoriseerd en getest doorgevoerd. In dit proces is aangegeven op welke momenten wordt gecommuniceerd naar de klant, hoe een eventuele roll-back wordt uitgevoerd wanneer een wijziging onverhoopt fouten geeft en hoe bij het uitrollen wordt omgegaan met Koppelingen met een andere applicatie die de Opdrachtnemer of de klant hebben gelegd. Afspraken hierover worden in her DAP vastgelegd.
NF-O-035	Opdrachtnemer garandeert medewerking bij periodieke Audits door Opdrachtgever op het geheel van taken en verantwoordelijkheden van de Opdrachtnemer
NF-O-037	Opdrachtnemer laat minimaal eenmaal per jaar een onafhankelijke penetratietest uitvoeren op de productieomgeving en verstrekt een managementsamenvatting van de resultaten aan Opdrachtgever.

4.3 Product Opdrachtnemer

4.3.1 Betrouwbaarheid

Nummer	Omschrijving
NF-P-007	Opdrachtnemer heeft een back-up-, disaster- en recoveryprocedure die gedocumenteerd, getest, operationeel en goedgekeurd is door de opdrachtgever. De basis hiervoor zijn de afgesproken RTO en RPO bij calamiteiten. De test moet minimaal één keer per jaar worden uitgevoerd en gerapporteerd aan Opdrachtgever.
NF-P-009	Back-up niet muteerbaar: Een back-up is 'niet muteerbaar' – dus kan niet meer worden aangepast of verwijderd vanaf de originele locatie nadat die is weggeschreven. Dit voorkomt dat bij een ransomware aanval de back-ups onherstelbaar worden

	beschadigd. De verwijdering van back-ups dan alleen door een geautoriseerd verwijderingsproces.

4.3.2 Beveiligbaarheid

Nummer	Omschrijving
NF-P-014	Alleen medewerkers die door de Opdrachtgever zijn toegewezen, kunnen toegang krijgen tot de Applicatie. Nadat de medewerkers zijn identificatie en authenticatie op basis van de Opdrachtgever identity store (Azure Active Directory) krijgen de medewerkers daadwerkelijk toegang tot de Applicatie. De identity store moet aangroepen worden met SAML 2.0 protocol met EntraID.
NF-P-018	Opdrachtnemer kan geen toegang tot functies, rollen of Gegevens binnen de Applicatie verlenen aan eigen medewerkers of onderaannemers. Uitsluitend Opdrachtgever kan dergelijke autorisaties verstrekken. Deze beperking geldt niet voor toegang tot de technische infrastructuur die noodzakelijk is voor beheer- en onderhoudswerkzaamheden.
NF-P-019	De inlogmethode die gebruikt wordt door de beheerder van de Opdrachtnemer om toegang tot de hardware, software en netwerk is: met twee factor authenticatie.
NF-P-022	Sessies via welk device dan ook, behoren authentiek te zijn voor elke gebruiker en worden automatisch inactief na een instelbaar aantal minuten en uitgelogd na een separaraat aantal minuten.
NF-P-024	Na het uitvoeren van een transactie via de GUI of API van een applicatie blijven de gemuteerde Gegevens consistent. Wanneer een transactie door een gebruiker of fout in de Applicatie wordt afgebroken dan brengt de Applicatie de Gegevens weer in de consistente toestand voor de transactie.
NF-P-027	Hardening servers: Veilig maken configuratie systeemomgevingen van de Applicatie: - Overbodige functies in de omgeving zijn uitgezet - Niet gebruikte bestanden, software, documentatie op het systeem worden verwijderd - Beveiligingsinstellingen worden veilige waarden aan toegekend; - Standaard wachtwoorden worden gewijzigd. Tevens wordt de effectiviteit van de hardening regelmatig (geautomatiseerd) geaudit Hierbij worden de richtlijnen gebruikt van CIS2 en OWASP richtlijnen Security Configuration & Vulnerable and Outdated components. N.B. Dit geldt ook voor de training, test en acceptatie omgeving.

NF-P-028	Het Gegevensverkeer dat bij de Opdrachtnemer binnenkomt of uitgaat wordt bewaakt en geanalyseerd op kwaadaardige elementen middels detectievoorzieningen vergelijkbaar met het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties), GDI (Generieke Digitale Infrastructuur) of SOC/SIEM (Security Operations Center / Security Information & Event Management). Bij de detectie en/of analyse worden acties uitgezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen Gegevens en informatiesystemen.
NF-P-029	De Gegevens en informatie in de tenant van de SAAS-omgeving van de Opdrachtgever zijn tijdens transport, bewerking en opslag duurzaam geïsoleerd van beheer functies en Gegevens en informatie van andere klanten van de Opdrachtnemer.
NF-P-031	**Opdrachtnemer** installeert beveiligingspatches binnen 48 uur (kritiek), 7 dagen (hoog), 30 dagen (middel) en 90 dagen (laag) na beschikbaarstelling. Indien tijdige installatie niet mogelijk is, treft Opdrachtnemer binnen 48 uur mitigerende maatregelen op basis van een gedocumenteerde risicoafweging en informeert hij Opdrachtgever hierover.
NF-P-032	De processen en het verwerken van Gegevens in de Applicatie en Koppelingen moeten voldoen aan “privacy by design and default” (zie hiervoor Handleiding Privacy by Design van Ministerie van Justitie en Veiligheid).
NF-P-137	Opdrachtnemer verleent volledige medewerking aan migratie naar een opvolgende leverancier. Hierbij worden geen aanvullende licentie- of exportkosten in rekening gebracht voor: • configuraties; • autorisaties; • loggegevens; • camerabeelden; • documentatie.
NF-P-040	Opdrachtnemer verleent gedurende de looptijd van de Overeenkomst medewerking aan ENSIA-Audits, Audits van Opdrachtgever en accountantscontroles en verstrekt de daarvoor benodigde bewijsstukken binnen 10 werkdagen na verzoek van Opdrachtgever.
NF-P-043	Opdrachtnemer werkt op verzoek van Opdrachtgever mee aan een DPIA en levert de daarvoor benodigde informatie binnen 10 werkdagen aan. Indien een DPIA vereist is, mogen eventuele uit de DPIA voortvloeiende noodzakelijke beheersmaatregelen niet openstaan bij ingebruikname van het Systeem.
NF-P-046	Een logregel bevat in geen geval Gegevens die tot het doorbreken van de beveiliging kunnen leiden.

NF-P-048	Na 3 foutieve inlogpogingen wordt het gebruikersaccount geblokkeerd. Het deblokkeren moet plaatsvinden met een inlogmethode met twee factor authenticatie.
NF-P-049	Verwerking Gegevens in Europese Economische Ruimte (EER): Alle Gegevens (inclusief back-up en logging) moeten binnen de EER verwerkt worden (uitspraak Schrems II). Dit geldt dus voor de (back up) servers en de (back up) servers van eventuele subverwerkers.
NF-P-053	De beheerder van de Opdrachtgever kan zelf de benodigde gebruikers rollen definiëren in de Applicatie en daar de autorisaties aan toekennen.
NF-P-054	Voor het vastleggen van brongegevens van de Applicatie in andere applicaties geldt het volgende Toegangscontrole systeem: geen kopieën Cameratoezicht: minimalisatie van het aantal kopieën en versie van de brongegevens in de andere applicatie is bekend.
NF-P-055	Cryptografiebeleid: De Opdrachtnemer heeft een cryptografiebeleid waarin minimaal de volgende onderwerpen zijn uitgewerkt: (a) Wanneer cryptografie ingezet wordt. (b) Wie verantwoordelijk is voor de Implementatie product. (c) Wie verantwoordelijk is voor het sleutelbeheer. (d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.
NF-P-057	Rol Gebaseerde Toegang (RBAC): De Opdrachtgever kan een gebruiker op basis van zijn rol toegang geven tot de functies, gegevensattributen, Informatieobjecten (documenten) en rapporten in de Applicatie die nodig zijn om de werkzaamheden die bij zijn rol horen uit te voeren (need to know and have) uit te voeren. Hiernaast wordt vastgelegd welke bewerking (raadplegen, toevoegen, wijzigen, verwijderen, vernietigen, downloaden, uploaden) de gebruiker op welke gegevensattributen en Informatieobjecten mag uitvoeren. Daarnaast kan de functioneel beheerder van de Opdrachtgever zelfstandig de rollen en rechten (autorisaties) voor gebruikers instellen op scherm, formulier en/of dossierniveau.
NF-P-058	Autorisatieprofielen voor de verschillende voorgedefinieerde rollen kunnen worden gewijzigd. De Gegevens die standaard zichtbaar zijn voor iedereen worden zoveel mogelijk beperkt. Het moet mogelijk zijn om bepaalde vertrouwelijke zaken standaard af te schermen.
NF-P-060	Gegevens en informatie worden versleuteld opgeslagen en uitgewisseld met applicaties buiten het netwerk van de Opdrachtgever volgens actuele NCSC c.q.

	OWASP richtlijnen Cryptographic. Bij vertrouwelijke en geheime informatie moet niet alleen tijdens het transport worden versleuteld maar ook de inhoud van het bericht.
NF-P-061	De Gegevens en informatie in de Applicatie zijn altijd eigendom van Opdrachtgever en moet hier te allen tijde toegang toe hebben, waar nodig ondersteund door Opdrachtnemer. Opdrachtnemer gebruikt deze Gegevens en informatie niet voor eigen doeleinden, tenzij Opdrachtgever daar natuurlijk toestemming voor heeft gegeven.

4.3.3 Bruikbaarheid

Nummer	Omschrijving
NF-P-072	De gebruikersinterface van de Applicatie biedt consistente navigatie, iconografie en interface-elementen op alle pagina's en apparaten.
NF-P-073	Gebruikers merken niet dat Gegevens uit andere bronapplicaties komen.
NF-P-077	Een gebruiker ziet alleen die schermen en menu-items waarvoor de gebruiker zelf is geautoriseerd.
NF-P-081	De Applicatie moet volledig voldoen aan de geldende internationale norm WCAG, niveau A en AA (zoals aangewezen in norm EN301 549). Stuur als bijlage bij de aanbieding, een door een ter zake kundige expert opgesteld toegankelijkheidsrapport mee (met vermelding van de onderzoeksmethode WCAG-EM en voorzien van datum). Een automatisch gegenereerd toegankelijkheidsrapport of screenshot uit een kantoorapplicatie of validatietool volstaat niet. a. Stuur ook wanneer de Applicatie op de inschrijfdatum gedeeltelijk voldoet, een door een ter zake kundige expert opgesteld toegankelijkheidsrapport mee (met vermelding van de onderzoeksmethode WCAG-EM en voorzien van datum). Een automatisch gegenereerd toegankelijkheidsrapport of screenshot uit een kantoorapplicatie of validatietool volstaat niet. b. Indien de aangeboden Applicatie op de inschrijfdatum nog niet digitaal toegankelijk is: geef aan in welke mate de aangeboden Applicatie voldoet. Beschrijf dit voor elke publicatie-omgeving/e-loket én interne (werk)omgeving of module. Geef tevens aan hoe de roadmap eruitziet om binnen redelijke termijn te komen tot een blijvend, volledig digitaal toegankelijke Applicatie.

4.3.4 Flexibiliteit

Nummer	Omschrijving

NF-P-093	De Applicatie, omgeving waar de Applicatie draait, en het netwerk zijn schaalbaar. De Opdrachtgever kan gebruikers toevoegen of verwijderen tegen de binnen de aanbesteding afgesproken licentieprijzen. De Applicatie is dusdanig schaalbaar dat geen beperking plaatsvindt in de hierin opgeslagen Gegevens, aantallen gebruikers, transacties, verwerkingssnelheid, gebruikersperformance/ snelheid of instellingen en nog steeds wordt voldaan aan de afgesproken SLA en KPI's. Zo spoedig mogelijk worden hardware en softwaremiddelen bijgeschakeld als aan voorgaande niet kan worden voldaan.

4.3.5 Functionaliteit Algemeen

Nummer	Omschrijving
NF-P-111	De in de Applicatie opgeslagen Gegevens blijven duurzaam toegankelijk (vindbaar, beschikbaar, leesbaar, interpreteer baar, betrouwbaar en toekomstbestendig; voor iedereen die daar recht op heeft en voor zo lang als noodzakelijk) gedurende de looptijd van de Overeenkomst.
NF-P-118	Informatieobjecten en bijbehorende metadata kunnen onherstelbaar worden vernietigd op basis van de opgegeven waardering en / of bewaartermijn en ingangsdatum bewaartermijn. Dat geldt voor alle door de Opdrachtnemer gebruikte fysieke en virtuele opslaglocaties.
NF-P-121	Ten aanzien van export en migratie geldt: 1. Het moet mogelijk zijn om een export te maken van Informatieobjecten, bijbehorende metadata en gekoppelde bestanden op basis van opgegeven zoekcriteria, ten behoeve van bijvoorbeeld overbrenging naar een E-depot, DMS of een andere applicatie. 2. Bij een export kan de metadata mee geëxporteerd worden op een zodanige manier dat het verband tussen Informatieobjecten en metadata intact blijft. 3. Bij een export kan metadata in een gangbaar machinaal leesbaar bestandsformaat geleverd worden, zoals XML.
NF-P-122	Opdrachtnemer kan garanderen dat geen Gegevens meer terug in de Opdrachtnemer omgeving kunnen worden geplaatst na formele vernietiging. (vaak staan Gegevens nog op server Opdrachtnemer, of in back-ups).
NF-P-134	Opdrachtnemer mag geen informatie vernietigen tenzij Opdrachtgever hier schriftelijk om verzoekt. Als Gegevens of informatie worden vernietigd door de Opdrachtnemer, dient een verklaring te worden opgeleverd waarin minimaal wordt aangegeven om welke informatie het gaat, hoe de selectie heeft plaatsgevonden en op welk moment de vernietiging heeft plaatsgevonden.

NF-P-146	De Applicatie moet de volgende uitvoerformaten voor rapporten kunnen ondersteunen: Word, Rich Tekst Format (RTF), Excel, Comma Seperated Value (CSV), XML, PDF.
NF-P-153	Rapportages zijn real time beschikbaar.
NF-P-154	Rapportages met statistieke bevatten nooit persoonlijke Gegevens.

4.3.6 Onderhoudbaarheid

Nummer	Omschrijving
NF-P-171	De Applicatie is (inclusief eventuele losse modules) webbased. Dit betekent dat alle functionaliteit via een webbrowser toegankelijk moet zijn op basis van HTML 5/HTTPS zijn zonder installatie van Applicatie of plug-ins of add-ons op de apparaat van de eindgebruiker. De volgende webbrowsers moeten minimaal worden ondersteund: Microsoft Edge, Chrome en Safari.
NF-P-174	Onderhouds- en releasewerkzaamheden leiden niet tot verstoring van kritische beveiligingsfuncties. Geplande werkzaamheden worden minimaal vijf werkdagen vooraf aangekondigd.
NF-P-175	Nieuwe versies van de Applicatie: Een nieuwe versie van de Applicatie en de Koppelingen die worden beheerd door de Opdrachtnemer moeten zonder te testen door de Opdrachtgever in productie kunnen worden gezet. Bij wijzigingen in het Gegevensmodel van de Applicatie zijn bij uitrol ook de standaard Koppelingen met de bijbehorende documentatie aangepast. N.B. Koppelingen die door Opdrachtgever heeft laten ontwikkelen, moeten wel eerst met de nieuwe versie worden getest. De Opdrachtnemer moet dan de versie eerst in de acceptatie-omgeving ter beschikking worden gesteld voordat deze in productie wordt gezet. Om genoeg tijd te hebben om te testen moet de Opdrachtnemer minimaal 4 weken van de voren een nieuwe versie aankondigen.

4.3.7 Prestatie en efficiëntie

Nummer	Omschrijving
NF-P-182	Rapportages: De doorlooptijd voor een rapportage is afhankelijk van de totaal opgevraagde gegevensset, niet van de hoeveelheid aanwezige Gegevens. Rapportages mogen niet langer duren dan 1 minuut. Uitgaande voldoende netwerk bandbreedte tussen de locatie waar de Applicatie wordt gehost en gebruiker.
NF-P-183	Transacties en zoekopdrachten: Transacties, raadplegingen mogen niet langer duren van 1,5 seconden in 90% van de

	gevallen. Zoekschermen moeten binnen 5 seconden een resultaat opleveren. Dit bij 15 gelijktijdige gebruikers en voldoende netwerk bandbreedte tussen de locatie waar de Applicatie wordt gehost en gebruiker.

4.3.8 Uitwisselbaarheid

Nummer	Omschrijving
NF-P-190	Het versturen van e-Mailberichten vanuit de Applicatie vindt plaats via de mailserver van Opdrachtgever.
NF-P-193	De Applicatie kan API's van andere externe applicaties gebruiken om Gegevens of informatie te kunnen ophalen (ophalen van verbruiksgegevens).
NF-P-194	Gebruik API-Koppelingen externe applicaties: De Applicatie kan API's van andere externe applicaties gebruiken om Gegevens of informatie te kunnen muteren of een mutatie c.q. actie kunnen initiëren.
NF-P-197	De bronapplicatie moet op basis van doorgegeven gebruikersaccount kunnen bepalen welke Gegevens en informatie een gebruiker van een afnemende applicatie kan ophalen of muteren via de standaard API-Koppelingen van de Applicatie.
NF-P-198	Applicaties behoren veilige API's te gebruiken voor import en export van Gegevens (OWASP ASVS 2020: V13).
NF-P-200	De Applicatie heeft standaard Koppelingen om alle Gegevens en informatie die zijn vastgelegd in de Applicatie op te halen.
NF-P-201	Koppelingen worden technisch uitgevoerd volgens (inter)nationale standaarden. • REST (REpresentational State Transfer) • JSON (JavaScript Object Notation) • W3C webservices (SOAP/XML) • StUF ZGW en BG etc • OGC standaarden En moeten eenduidig en duidelijk zijn gedocumenteerd bij oplevering van de Applicatie.
NF-P-202	Er is actuele documentatie beschikbaar van de standaard API's van de Applicatie en gerealiseerde Koppelingen door de Opdrachtnemer. Bij nieuwe versies van de Applicaties waarin het Gegevensmodel is aangepast wordt de aangepaste API-documentatie beschikbaar gesteld.
NF-P-206	De Applicatie moet de Koppelingen krijgen zoals gespecificeerd in de bijgevoegde lijst.

4.4 Implementatie product

4.4.1 Migratie Gegevens

Nummer	Omschrijving
NF-I-004	De Opdrachtgever beoordeelt de door de Opdrachtnemer uitgevoerde migratie tijdens de implementatiefase, op basis van het overeengekomen migratie- en testplan. Eventuele uitval van Gegevens tijdens de migratie, wordt door de Opdrachtnemer opgelost en opnieuw gemigreerd. De Opdrachtgever beoordeelt de migratie en inrichting van de Applicatie en geeft al dan niet pas na schriftelijk akkoord toestemming voor de livegang.
NF-I-001A	Bij migratie van Gegevens en informatie uit bestaande bronapplicaties naar nieuwe Applicaties worden Gegevens of informatie niet toegevoegd of hersteld. Wanneer tijdens de migratie blijkt dat Gegevens ontbreken of moeten worden hersteld dan moet dit plaatsvinden in de bronapplicatie.
NF-I-002	De Opdrachtnemer draagt zorg voor de migratie van Gegevens en informatie uit de bestaande applicatie naar de Applicatie. Dit geldt niet voor de autorisatiegegevens. De Opdrachtnemer doet dit in overleg met de huidige (vorige) Opdrachtnemer. De Opdrachtgever bepaalt welke Gegevens uit de bestaande applicatie naar de Applicatie worden geconverteerd.

4.4.2 Opleiding

Nummer	Omschrijving
NF-I-011	De volgende groepen moeten worden opgeleid: • Medewerker/ gebruikers (circa 20 key-users) • Functioneel beheerder (4-6 personen) De training is on-site bij Opdrachtgever en volledig in de Nederlandse taal (inclusief trainingsmateriaal). De training is afgerond vóór formele oplevering en ingebruikname.

4.4.4 Uitvoering

Nummer	Omschrijving
NF-I-001A	Na het sluiten van de overeenkomst wordt door Opdrachtnemer een Implementatieplan opgesteld, conform GIBIT-artikel 6.3. Dit Implementatieplan is een uitbreiding van het ingediende Plan van Aanpak bij Gunningscriterium K.1 in het

	Aanbestedingsdocument en wordt na goedkeuring door opdrachtgever gebruikt om de werkzaamheden te plannen.
NF-I-171B	Tijdens de implementatie bespreekt de aanbieder alle parameters van het pakket met de (functioneel) beheerders van de Opdrachtgever. Het gaat hier om parameters die de beheerders zelf kunnen instellen en wijzigen, maar óók die de aanbieder zelf instelt voor de gemeente.
NF-I-017A	Gedurende de implementatieperiode wordt wekelijks een overzicht verschaft van status en planning van de werkzaamheden. Hierbij wordt gerefereerd aan het Plan van Aanpak dat bij inschrijving is ingediend.

4.5 Overeenkomst

4.5.1 Beëindiging

Nummer	Omschrijving
NF-P-136	Opdrachtnemer levert uiterlijk binnen 30 kalenderdagen na beëindiging van de overeenkomst: • alle configuraties; • alle loggegevens; • alle camerabeelden binnen bewaartermijnen; • alle autorisatiestructuren; • alle documentatie; • in open en machine leesbare formaten. De overdracht wordt uitgevoerd conform een vooraf overeengekomen exitplan.

4.5.2 Beveiliging

Nummer	Omschrijving
A-001	Opdrachtnemer verstrekt op verzoek alle informatie die noodzakelijk is voor Audits, DPIA's, AVG-verzoeken en ENSIA-verantwoording. Opdrachtnemer treft alle technische en organisatorische maatregelen die noodzakelijk zijn voor een rechtmatige verwerking van persoonsgegevens binnen CCTV-, toegangscontrole- en inbraakdetectieprocessen.
A-002	Het nieuwe systeem moet privacy-vriendelijk zijn ontworpen (Privacy by Design) en standaard de meest privacy-vriendelijke instellingen gebruiken (Privacy by Default): • Privacy masking: gezichten en kentekenplaten afschermen waar niet noodzakelijk.

	• Versleuteling: communicatie en opslag zijn versleuteld. Duidelijke signalering: bordjes die aangeven dat er cameratoezicht is.
NF-F-001	Het instellen van, het uitwisselen van Gegevens met en besturen van de gebruikte camera's mogen alleen via een vast netwerk worden uitgevoerd.
NF-F-003	De Gegevensuitwisseling tussen de Applicatie, applicaties en de fysieke middelen zoals camera's, toegangslezers, brandmelders en inbraaksensoren moet plaatsvinden via één vast netwerk dat gescheiden is van het netwerk voor medewerkers.

4.5.3 Duurzaamheid

Nummer	Omschrijving
DU-001	Apparatuur voldoet minimaal aan: • RoHS-richtlijn; • WEEE-richtlijn; • CE-markering.
DU-002	Leverancier beschikt over een proces voor hergebruik en verantwoorde afvoer van afgeschreven apparatuur.
DU-003	Apparatuur heeft een verwachte technische levensduur van minimaal 7 jaar.

Bijlage 1

Koppelingenmatrix

Koppeling	Eigenaar	Protocol	Richting
TRS - Entra ID	Gemeente	SAML/OIDC	Bi
CCTV - TRS	Opdrachtnemer	ONVIF/API	Bi
TRS - Inbraak	Opdrachtnemer	OSDP/API	Bi
TRS - AFAS	Gemeente	REST/API	Bi
CCTV - Camera in Beeld	Opdrachtnemer	Webservice	Uni

Prioriteitsclassificatie

P1 Kritiek

Een kwetsbaarheid waarvoor:

- actief misbruik plaatsvindt of zeer waarschijnlijk is;
- onbevoegde toegang tot Systemen, Gegevens of beheerfuncties mogelijk is;
- de beschikbaarheid van het CCTV- of TRS-Systeem ernstig wordt bedreigd;
- geen afdoende tijdelijke mitigerende maatregel beschikbaar is.

Hersteltermijn: binnen 48 uur na beschikbaarstelling van de patch.

P2 Hoog

Een kwetsbaarheid waarvoor:

- misbruik aannemelijk is;
- vertrouwelijkheid, integriteit of beschikbaarheid van het Systeem aanzienlijk kan worden aangetast;
- tijdelijke mitigerende maatregelen beschikbaar zijn;
- de bedrijfsvoering niet direct stilvalt.

Hersteltermijn: binnen 7 kalenderdagen na beschikbaarstelling van de patch.

P3 Middel

Een kwetsbaarheid waarvoor:

- misbruik beperkt waarschijnlijk is;

- de impact op vertrouwelijkheid, integriteit of beschikbaarheid beperkt is;
- aanvullende voorwaarden nodig zijn voor misbruik;
- voldoende mitigerende maatregelen beschikbaar zijn.

Hersteltermijn: binnen 30 kalenderdagen na beschikbaarstelling van de patch.

P4 Laag

Een kwetsbaarheid waarvoor:

- misbruik onwaarschijnlijk is;
- de impact beperkt is;
- geen directe gevolgen voor de beveiliging of beschikbaarheid van het Systeem worden verwacht;
- de kwetsbaarheid voornamelijk een technisch of administratief risico vormt.

Hersteltermijn: binnen 90 kalenderdagen na beschikbaarstelling van de patch.