

# **Levering, Implementatie en Onderhoud van Toegangscontrolesystemen voor Verzamelcontainers GFE**

## **Bijlage 1 Programma van Eisen**

# Minimum-eisen

In deze bijlage beschrijft Opdrachtgever het Programma van Eisen waar gegadigde aan moet voldoen om aan deze Offerteaanvraag te kunnen deelnemen. Eisen zijn dus minimale randvoorwaarden waaraan de Offerte dient te voldoen om voor de beoordeling in aanmerking te komen.

## Algemene Eisen

| Algemene eisen |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nr.            | Omschrijving                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Alg-1          | <p>De levering betreft toegangscontrolesystemen voor verzamelcontainers, welke worden geplaatst voor het inzamelen van GFE(T), zijnde vooral groente, fruit en etensresten. De verzamelcontainers betreffen ten minste twee types: (1) een containerbehuizing voor een 240 liter minicontainer met een inwerpvoorziening (klep) voor zakken van circa 30 liter en (2) een semi-ondergrondse onderlosser met Kinshofer opnamesysteem.</p>                                                                                                          |
| Alg-2          | Een compleet toegangscontrolesysteem bestaat ten minste uit: een centrale SaaS oplossing plus een aantal decentrale fysieke componenten: een bedieningsconsole, waarin opgenomen een communicatiesysteem, een voedingsunit (accu / batterij), een elektronisch slot, een kabelboom en bevestigings- en beschermingsmateriaal.                                                                                                                                                                                                                                                                                                        |
| Alg-3          | De inschrijver garandeert een technische levensduur van minimaal 5 jaar. Onder technische levensduur wordt verstaan: het voldoen aan de specificaties volgens de gestelde eisen. Leverancier dient gedurende deze periode onderdelen indien nodig te vervangen. De kosten hiervan maken onderdeel uit van de jaarlijkse onderhoudskosten en mogen niet apart in rekening worden gebracht.                                                                                                                                                                                                                                            |
| Alg-4          | De inschrijver garandeert gedurende de technische levensduur onderdelen of complete systemen te kunnen leveren in gelijkwaardige uitvoering en minimaal gelijkwaardige kwaliteit. De levertermijn, voor losse onderdelen, bedraagt maximaal 5 werkdagen. Opdrachtgever kan geen voorraad van onderdelen aanhouden.                                                                                                                                                                                                                                                                                                                   |
| Alg-5          | Alle onderdelen, aansluitingen en bevestigingen met betrekking tot de decentrale toegangscontrolesysteemcomponenten zijn waterdicht en waterbestendig.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Alg-6          | De decentrale toegangscontrolesysteemcomponenten zijn vervaardigd van duurzame materialen en zijn geheel voorzien van een coating of andere bescherming zodat roestvorming binnen de levensduur van 5 jaar niet zal voorkomen. Het toegepaste materiaal en de constructie zijn zodanig dat vervorming van het toegangscontrolesysteem door normaal gebruik tijdens de levensduur wordt voorkomen en dat het toegangscontrolesysteem bestand is tegen ruw en onjuist gebruik. Hetgeen wil zeggen dat ruw of onjuist gebruik geen directe nadelige invloed heeft op het functioneren en de veiligheid van het toegangscontrolesysteem. |

|        |                                                                                                                                                                                                                     |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alg-7  | De decentrale toegangscontrolesysteemcomponenten dienen bestand te zijn tegen inwerking van seizoensinvloeden, temperaturen, grond-, regen- en pekelwater, percolaat en andere inwerkingen van huishoudelijk afval. |
| Alg-8  | Alle decentrale toegangscontrolesysteemcomponenten zijn vlak en glad afgewerkt en mogen geen scherpe randen hebben.                                                                                                 |
| Alg-9  | Het toegangscontrolesysteem dient geschikt te zijn om in de toekomst gemakkelijk te combineren met een vulgraadsensor, waarbij gebruik wordt gemaakt van de communicatie-oplossing van het toegangscontrolesysteem. |
| Alg-10 | Inschrijver levert bij inschrijving foto's/afbeelding/tekeningen aan waarop het complete decentrale toegangscontrolesysteem van alle kanten zichtbaar is.                                                           |
| Alg-11 | Inschrijver levert bij inschrijving de gebruikershandleiding voor aanbieden pas/druppel en software (uitlezen data, uploaden whitelist, etc.).                                                                      |
| Alg-12 | Inschrijver levert bij inschrijving de voorschriften aan te leveren voor montage, onderhoud en reparaties.                                                                                                          |
| Alg-13 | Inschrijver levert een Service Level Agreement aan en gedurende de contractperiode wordt deze door de leverancier bijgewerkt.                                                                                       |
| Alg-14 | Gemeente is in alle gevallen eigenaar van alle data (loggegevens, whitelists, systeemgegevens).                                                                                                                     |

## Eisen Voedingsunit

| Eisen Voedingsunit |                                                                                                                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nr.                | Omschrijving                                                                                                                                                                                                                    |
| VDU-1              | De voedingsunit levert voldoende voeding, die noodzakelijk is voor het gehele systeem (inclusief eventuele vulgraadsensor als deze geen eigen voeding heeft) tijdens alle in Nederland voorkomende weertypen en temperaturen.   |
| VDU-2              | De voedingsunit heeft een minimale gegarandeerde levensduur van 2,5 jaar gebaseerd op 250 klep/trommelopeningen per week en twee ledigingen per week. Deze levensduur start na ingebruikname van de voedingsunit.               |
| VDU-3              | Een voedingsunit die uitgeput raakt dient op afstand tijdig gesignaleerd te kunnen worden. De resterende tijd tot uitvallen van de voedingsunit dient ruim voldoende te zijn voor het leveren en vervangen van de voedingsunit. |
| VDU-4              | Het is mogelijk om op afstand de spanning en temperatuur uit te lezen door opdrachtgever.                                                                                                                                       |
| VDU-5              | De voedingsunit is gemakkelijk te vervangen.                                                                                                                                                                                    |
| VDU-6              | De voedingsunit heeft een beschikbaarheid van 99,5 % en maakt geen gebruik van zonnepanelen.                                                                                                                                    |

## Eisen Console (Bedieningsunit Display)

| Eisen Console (Bedieningsunit Display) |                                                                                                                                                 |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Nr.                                    | Omschrijving                                                                                                                                    |
| CON-1                                  | De console heeft een glad oppervlakte, zonder scherpe uitstekende randen.                                                                       |
| CON-2                                  | De console heeft een eenvoudig begrijpelijke Nederlandstalige bedieningsinstructie die goed leesbaar is en leesbaar blijft bij direct zonlicht. |

|        |                                                                                                                                                                                 |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CON-3  | De console is goed sluitend te monteren in een universele uitsparing in de containerbehuizing, zonder naden, uitstekende oppervlaktes en opbouw van onderdelen.                 |
| CON-4  | De console geeft een volmelding bij het bereiken van een instelbaar aantal klep/trommelbewegingen (en volmelding van de mogelijk toekomstig te plaatsen vulgraadsensor).        |
| CON-5  | De console is waterdicht, waardoor er bijvoorbeeld geen mogelijkheid is dat er vocht achter de display komt en de bedieningsinstructie onleesbaar wordt.                        |
| CON-6  | De console is geschikt voor Mifare pasjes/druppels. Enkele Mifare pasjes die in Amsterdam worden gebruikt worden aangeleverd ten behoeve van de praktijkbeoordeling.            |
| CON-7  | De console is geschikt voor NFC-identificatie in combinatie met een applicatie op een mobiele telefoon. Een alternatief met dezelfde functionaliteit mag ook worden aangeboden. |
| CON-8  | De console heeft de mogelijkheid om een vulgraadsensor aan te sluiten, waarmee op basis van de sensor een volmelding wordt getoond.                                             |
| CON-9  | De console is eenvoudig op afstand te configureren vanuit de software/backoffice.                                                                                               |
| CON-10 | Wanneer de inwerpvoorziening wordt ontsloten wordt ten behoeve van slechtzienden een geluidsignaal afgegeven.                                                                   |
| CON-11 | Wanneer de inwerpvoorziening wordt ontsloten en het geluidsignaal is afgegeven is er voldoende tijd om de inwerpvoorziening te openen.                                          |
| CON-12 | Het slot sluit automatisch korte tijd na het dichtvallen van de inwerpvoorziening.                                                                                              |

## Eisen Slot

| Eisen Slot |                                                                                                                                                                                                                                                                    |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nr.        | Omschrijving                                                                                                                                                                                                                                                       |
| SLOT-1     | Het elektronisch slot is eenvoudig te monteren en toe te passen op verschillende inwerpvoorzieningen zoals verschillende kleptechnieken en een trommel.                                                                                                            |
| SLOT-2     | Het slot is in sterkte instelbaar.                                                                                                                                                                                                                                 |
| SLOT-3     | <p>Het elektronisch slot is universeel en heeft een T-vorm en wordt gebruikt in combinatie met een toegangscontrolesysteem. Zie bijgevoegde afbeelding voor een voorbeeld.</p>  |
| SLOT-4     | Het slot is idiotproof waardoor bij hardhandig willen openen van een door het slot afgesloten inwerpopening de inwerpvoorziening gesloten blijft. Het slot kan niet eenvoudig geforceerd of gesaboteerd worden.                                                    |

## Eisen Kabelboom

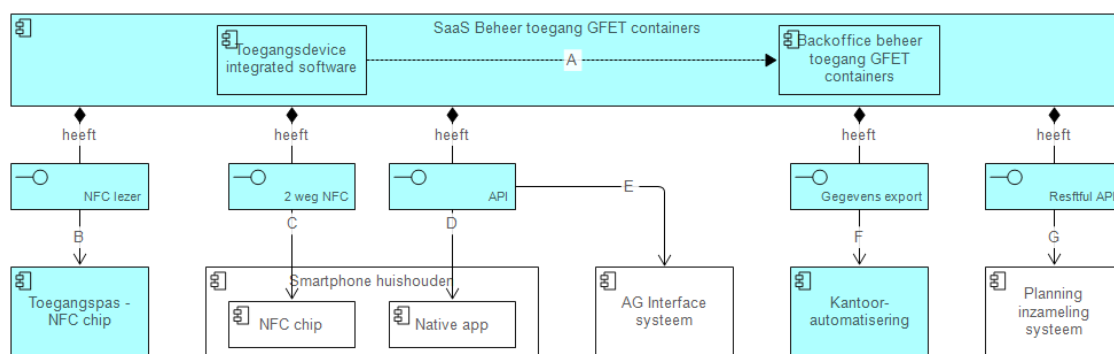
| Eisen Kabelboom |                                         |
|-----------------|-----------------------------------------|
| Nr.             | Omschrijving                            |
| KAB-1           | De kabelboom is eenvoudig te vervangen. |

|       |                                                             |
|-------|-------------------------------------------------------------|
| KAB-2 | De kabelboom is waterdicht inclusief de aansluitingspunten. |
| KAB-3 | De kabelboom is voorzien van universele stekkers            |

## Eisen ICT

| Eisen ICT |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nr.       | Omschrijving                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| ICT-1     | Leverancier biedt een Toegangscontrolesysteem in de vorm van een SaaS oplossing. De software dient middels configuratie ingericht te kunnen worden ten behoeve van Opdrachtgever.                                                                                                                                                                                                                                                                                                                                              |
| ICT-2     | De SaaS oplossing dient minimaal 350.00 huishoudens aan te kunnen.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| ICT-3     | De SaaS oplossing garandeert een beschikbaarheid van minimaal 99,5 %.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| ICT-3     | De SaaS oplossing is geschikt om met een mobiele App op iOS en Android toestellen toegang te geven tot de verzamelcontainers zonder gebruik te hoeven maken van een pasje of druppel. Inschrijver stelt software libraries, API's of documentatie beschikbaar waarmee een derde partij een app kan ontwikkelen voor het realtime activeren van de smartphone ten behoeve van het openen van bepaalde containers. De eventueel daarmee samenhangende kosten zoals licentiekosten dienen opgevoerd te worden in het prijzenblad. |
| ICT-4     | De SaaS oplossing is geschikt om volgens de STOSAG data uit te wisselen                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| ICT-5     | Er is sprake van een automatische real-time of ten minste dagelijkse communicatie tussen ieder decentraal toegangscontrolesysteem (verzamelcontainer) en de centrale SaaS oplossing, waarbij ten minste dagelijks een actueel beeld van de gegevens van iedere verzamelcontainer kan worden opgevraagd.                                                                                                                                                                                                                        |
| ICT-6     | Het dient mogelijk te zijn om handmatig vanuit de SaaS oplossing op ieder gewenst moment gegevens op te halen uit ieder decentrale toegangscontrolesysteem (verzamelcontainer).                                                                                                                                                                                                                                                                                                                                                |
| ICT-7     | Het dient mogelijk te zijn om via een Application Programming Interface (API) gegevens op te halen met betrekking tot identificatie en de operationele toestand van een toegangscontrolesysteem, de autorisatielijst en de loggegevens. Hiermee kan een automatische onttrekking van alle data uit de SaaS-oplossing plaatsvinden.                                                                                                                                                                                             |
| ICT-8     | Het dient mogelijk te zijn een vulgraadindicatie op basis van aantal stortingen/pasaanbiedingen real time op te vragen / uit te lezen.                                                                                                                                                                                                                                                                                                                                                                                         |
| ICT-9     | De leverancier is verantwoordelijk voor het mogelijk maken van communicatie tussen de SaaS oplossing enerzijds en de decentrale toegangscontrolesysteemcomponenten anderzijds.                                                                                                                                                                                                                                                                                                                                                 |
| ICT-10    | Het uploaden van batches en het doorvoeren van mutaties met betrekking tot de toegang met behulp van Mifare pasjes/druppels (whitelist) en accountgegevens van de mobiele app worden binnen 3 werkdagen door leverancier uitgevoerd als een gebruikersvriendelijke oplossing ontbreekt waarbij opdrachtgever dit zelf kan invoeren in de SaaS-oplossing.                                                                                                                                                                       |
| ICT-11    | Onderdeel van de opdracht is het verzorgen van upgrades en updates van zowel de centrale SaaS oplossing als van de decentrale bedieningsconsole gedurende de gehele contractperiode gericht op een optimale werking van het gehele systeem.                                                                                                                                                                                                                                                                                    |
| ICT-12    | Inschrijver conformeert zich aan de Open Standaarden van Forum Standaardisatie voor: <ul style="list-style-type: none"> <li>• authenticatie, autorisatie en identificatie;</li> <li>• beveiligde, betrouwbare verbindingen;</li> </ul>                                                                                                                                                                                                                                                                                         |

|        |                                                                                                                                                                                                                                                                                        |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | <ul style="list-style-type: none"> <li>• beveiligde, betrouwbare berichten- en/ of bestandsuitwisseling;</li> <li>• metadatering;</li> <li>• digitale bestandsformaten.</li> </ul> <p>Zie: <a href="https://www.forumstandaardisatie.nl/">https://www.forumstandaardisatie.nl/</a></p> |
| ICT-13 | De SaaS oplossing biedt de mogelijkheid om in de toekomst via een Restful API geautomatiseerd, realtime te koppelen met een Planning inzameling systeem voor het doorgeven van een indicatie volmelding, zie onderstaande figuur.                                                      |
| ICT-14 | De SaaS oplossing biedt de mogelijkheid om wekelijks gegevens te exporteren in (CSV of XML) richting een kantoorautomatiseringsoplossing van Assetmanagement (gemeente Amsterdam).                                                                                                     |
| ICT-15 | Soortelijke schaalbaarheid: de hardware (device) en architectuur van de oplossing dienen herbruikbaar te zijn voor toekomstig toegangsbeheer van inzamel fracties textiel en luiers waarbij rekening wordt gehouden met het gewenste onderscheid in fracties.                          |



**Figuur 1.** Eindsituatie Applicatie Integratie GFET - vereiste interfaces en koppelingen (A tot en met G).

| Koppeling | Toelichting                                                                                                                                                                                                                  |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A         | Realtime 4G netwerk communicatie tussen toegangsdevice- en backoffice-component van de SaaS.                                                                                                                                 |
| B         | Oplossing levert een NFC lezer interface die mogelijk maakt om het toegangsdevice te openen d.m.v. een toegangspas.                                                                                                          |
| C         | Oplossing levert een 2 weg NFC interface die de mogelijkheid biedt om in de toekomst het toegangsdevice te openen met een NFC bechipte smartphone.                                                                           |
| D en E    | Oplossing levert een API interface om in de toekomst geautomatiseerd, realtime te kunnen koppelen met een native toegangsapp op een smartphone, en het AG interface systeem voor het uitwisselen van toegangsrecht mutaties. |
| F         | Oplossing biedt de mogelijkheid om wekelijks gegevens te exporteren in (CSV of XML) richting een kantoorautomatiseringsoplossing van Assetmanagement.                                                                        |
| G         | Oplossing biedt de mogelijkheid om in de toekomst via een Restful API geautomatiseerd, realtime te koppelen met een Planning inzameling systeem – bijvoorbeeld RO - voor het doorgeven van een indicatie volmelding.         |

## Eisen Informatiebeveiliging & Privacy

| Eisen Informatiebeveiliging & Privacy |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nr.                                   | Omschrijving                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SEC-1                                 | De aanbieder moet voldoen aan NCSC beveiligingsrichtlijnen voor webapplicaties "https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties (of equivalent)                                                                                                                                                                                                                                                                                                                                            |
| SEC-2                                 | De applicatie voldoet aan de meest actuele OWASP richtlijnen: <a href="https://owasp.org/www-project-top-ten/">https://owasp.org/www-project-top-ten/</a> . Webapplicaties en mobiele apps worden ieder jaar op de laatst bekende versie van de OWASP (top 10) norm getoetst d.m.v. een veiligheidstest die door een onafhankelijke derde wordt uitgevoerd. De Inschrijver levert hiervoor jaarlijks een rapportage of een TPM verklaring aan van een onafhankelijke derde partij. De aanbieder levert de verklaring 2019 of recenter bij offerte |
| SEC-3                                 | Bij koppelingen (in- en uitgaand) biedt de applicatie een mechanisme om het datatransport te versleutelen (bijvoorbeeld SSL/TLS).                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SEC-4                                 | Toegang tot de SaaS oplossing via een Internet Browser vindt versleuteld plaats ("https") met TLS1.2 of hoger.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SEC-5                                 | In het kader van de Algemene Verordening Gegevensverwerking (AVG) tekent inschrijver een Verwerkersovereenkomst.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SEC-6                                 | De data van de SaaS oplossing wordt gehost in een EU land plus Noorwegen, Liechtenstein, IJsland, min Groot-Brittannië.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SEC-6                                 | Het is mogelijk dat alle rollen (medewerker, leidinggevende, professional en functioneel beheerder) via een Internet browser, zonder additionele plugins of andere software, gebruik kunnen maken van de SaaS applicatie. De SaaS applicatie is voor deze rollen een "Zero Footprint" web-applicatie.                                                                                                                                                                                                                                             |
| SEC-8                                 | Voor authenticatie en autorisatie van de SaaS oplossing dient gebruik te worden gemaakt van de IAM voorziening van de gemeente Amsterdam.                                                                                                                                                                                                                                                                                                                                                                                                         |
| SEC-9                                 | De aanbieder is verplicht bij onderaanneming (bijv. de ontwikkeling van software) met zijn onderaannemers te regelen via schriftelijk vastgelegde afspraken, inclusief doorlegging van verwerkersovereenkomst met gemeente Amsterdam. Daarin wordt in elk geval vastgelegd: intellectueel eigendom, kwaliteitsaspecten, beveiligingsaspecten, aansprakelijkheid, escrow en reviews. Desgevraagd geeft hij deze afspraken ter inzage aan Opdrachtgever.                                                                                            |
| SEC-10                                | Wachtwoorden moeten zijn samengesteld op basis van de geldende beveiligingseisen (bijv. NIST 800-63) en mogen niet leesbaar worden opgeslagen maar voorzien zijn van een salt (van 32 bits of meer, een gecodeerde HMAC-hash met SHA-1, SHA-2 of SHA-3 en het "stretching" -algoritme PBKDF2 met ten minste 10.000 iteraties).                                                                                                                                                                                                                    |
| SEC-11                                | Een admin of superuser account is voor exclusief gebruik door Functioneel Beheer                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SEC-12                                | De functioneel beheerder dient, indien nodig, extra rechten (raadplegen, mutatie- en beheerrechten, etc.) aan rollen en profielen te kunnen toewijzen, zodat er verschillende rollen ondersteund kunnen worden.                                                                                                                                                                                                                                                                                                                                   |
| SEC-13                                | De gebruiker van de remote hosting applicatie dient zelf het wachtwoord te kunnen wijzigen middels een vastgestelde procedure.                                                                                                                                                                                                                                                                                                                                                                                                                    |

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SEC-14 | De logging dient alleen toegankelijk te zijn voor daartoe door de gemeente Amsterdam benoemde bevoegde gebruikers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SEC-15 | Log bestanden dienen toegankelijk te zijn of moeten aansluiten op de SIEM oplossing van gemeente Amsterdam<br>Data logging                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SEC-16 | Inlogpogingen moeten beperkt zijn tot slechts 4 foutieve pogingen per keer met een lockperiode 5 minuten voordat weer kan worden ingelogd. Dit om bruteforcing te voorkomen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SEC-17 | Uitzonderingen en informatiebeveiligingsgebeurtenissen worden gelogd en minimaal voor 3 maanden te worden bewaard. Op aanvraag van de gemeente Amsterdam worden deze ter beschikking gesteld                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SEC-18 | <p>De aanbieder is ISO 27001 gecertificeerd of gelijkwaardig en toont dit, d.m.v. een TPM verklaring, aan ten aanzien van:</p> <ol style="list-style-type: none"> <li>Verwerker is ISO 27001 (of gelijkwaardig) gecertificeerd;</li> <li>Verwerker toont zelf aan dat hij aan de eisen uit de Baseline Informatiebeveiliging Overheid (BIO) voldoet (door een GAP analyse inclusief overzicht van genomen maatregelen);</li> <li>Verwerker levert eenmalig bij gunningen jaarlijks een audit of TPM: een ISAE 3402 type 2 rapport, waarmee een onafhankelijke externe auditor rapporteert over de opzet, bestaan en werking van beheersmaatregelen;</li> <li>Verwerkingsverantwoordelijke ontvangt jaarlijks dit rapport en heeft een right-to audit om eventueel aanvullend te toetsen;</li> </ol> <p>De Verwerker hanteert een integriteitscode dan wel een interne gedragscode voor zijn medewerkers waaruit blijkt dat de medewerkers en door de Verwerker ingeschakelde derden de vertrouwelijkheid in acht nemen. (artikel 28 lid 3 AVG: verwerker moet bewijsbaar integere medewerkers in dienst hebben), afgedekt met getekende geheimhoudingsovereenkomst. Verwerker levert persoonlijke VOG aan voor betrokken medewerkers die activiteiten uitvoeren.</p> |
| SEC-19 | <p>Pen- en Hacktesten.</p> <ol style="list-style-type: none"> <li>De aangeboden applicaties zijn in acceptatie fase aan een veiligheidstest onderworpen en bevindingen zijn aantoonbaar verholpen voordat deze in productie gaat.</li> <li>Alvorens de toepassing door gemeente Amsterdam in gebruik genomen wordt, wordt/is een zgn. Pen- en Hacktest uitgevoerd. De uitvoering van de Pen- en Hacktest vindt plaats, of heeft aantoonbaar plaatsgevonden, door een onafhankelijke partij.</li> <li>Inschrijver draagt de kosten voor de Pen- en Hacktest;</li> </ol> <p>Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SEC-20 | Voor de Remote hosting cloud-basedoplossing wordt (logische) netwerksegmentatie toegepast waarbij productie, acceptatie en test omgevingen met verschillende beveiligingsniveaus van elkaar gescheiden worden.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SEC-21 | Verkeer tussen de verschillende segmenten wordt gefilterd (minimaal op IP) en verkeer wordt alleen toegestaan in overeenstemming met applicatie behoeftigheden                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SEC-22 | Data van de gemeente mag niet voor andere dan de beoogde gebruikers beschikbaar komen. In geval van "multi-tenancy" oplossingen mogen API-services en netwerk-services shared zijn, maar data opslag niet. De data is alleen per tenant toegankelijk en opgeslagen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SEC-23 | In het geval van multi-tenancy; moeten virtuele servers of applicaties geïsoleerd zijn van andere virtuele servers en applicaties van de andere tenants                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

|        |                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SEC-24 | Een systeem of systeemoplossing die toegang verschaffen hebben een uniek inlogaccount en uniek certificaat.                                                                                                                                                                                                                                                                                       |
| SEC-25 | Verbindingen tussen cliënt (webbrowser/app) en de (SaaS) server dienen versleuteld (minimaal SSL) plaats te vinden op basis van een Extended Validation SSL certificaat (zowel intern als extern). Bij verwerking van bijzondere persoonsgegevens dienen deze gegevens aanvullend versleuteld via de bestaande SSL verbinding dan wel via een versleutelde tunnel plaats te vinden (SSH/VPN/SFTP) |
| SEC-26 | Bij systeemkoppelingen (in- en uitgaand) van data met een hogere van integriteit en vertrouwelijkheid vindt er wederzijds systeemauthenticatie plaats door middel van certificaten ("Two Way SSL").                                                                                                                                                                                               |
| SEC-27 | Er is een backup policy overeengekomen die gebaseerd is op de eisen en wensen van de gemeente Amsterdam. Backup media wordt conform deze policy opgeslagen en periodiek gecontroleerd op herstelbaarheid                                                                                                                                                                                          |
| SEC-28 | De aanbieder heeft een actief patchbeleid, procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICTvoorzieningen en levert deze aan.                                                                                                                                                                    |
| SEC-29 | De aanbieder moet proactief en onmiddellijk beveiligingsincidenten/datalekken melden aan de gemeente Amsterdam.                                                                                                                                                                                                                                                                                   |
| SEC-30 | De aanbieder heeft een uitgewerkt protocol om cyberaanvallen te weren of de eventueel geleden schade op een gestructureerde en adequate manier op te lossen.                                                                                                                                                                                                                                      |
| SEC-31 | Malafide code detectie (anti-virus) is actief voor alle data van gemeente Amsterdam.                                                                                                                                                                                                                                                                                                              |

## Onderhouds- en reparatie-eisen

| Onderhouds- en reparatieeisen |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nr.                           | Omschrijving                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| OND-1                         | Inschrijver levert gedurende de gehele contractperiode onderhoud en reparatie op het complete toegangscontrolesysteem. De onderhouds- en reparatieperiode vangt direct aan na levering van het toegangscontrolesysteem. Uitgangspunt voor het gebruik van het toegangscontrolesysteem is 250 klepbewegingen per week en een technische levensduur van tenminste 5 jaar. Bij de inzet van een voedingsunit met een levensduur korter dan 5 jaar wordt het vervangen van de voedingsunit onderdeel van de onderhouds- en reparatiewerkzaamheden. Werkzaamheden door anderen dan de leverancier hebben geen invloed op het onderhoud, tenzij leverancier kan aantonen dat deze werkzaamheden niet volgens de verstrekte voorschriften zijn uitgevoerd en hierdoor reparatie of vervanging noodzakelijk is. |

## Eisen Levering

| Eisen Levering |              |
|----------------|--------------|
| Nr.            | Omschrijving |

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LEV-1 | Ten aanzien van nieuw te plaatsen verzamelcontainers dienen de decentrale toegangscontrolesysteemcomponenten aangeleverd te worden op de locatie van de leverancier de verzamelcontainers. Plaats, tijdstip en omvang van levering geschieden in overleg met de Opdrachtgever. De leverancier van de verzamelcontainers is nog niet bekend, maar de levering zal plaatsvinden in batches van ten minste 10 stuks en de plaats zal gelegen zijn in Nederland. Transportkosten worden niet apart vergoed en dienen dus onderdeel te zijn van de aanbiedingsprijs. |
| LEV-2 | Het toegangscontrolesysteem dient als één geheel, volledig werkend na installatie, te worden geleverd. Indien eventueel afmontage noodzakelijk is na plaatsing in de verzamelcontainer komt dit voor rekening van de inschrijver. De combinatie dient geheel te functioneren bij oplevering (na montage).                                                                                                                                                                                                                                                       |
| LEV-3 | Levering dient maximaal 8 weken na afroep plaats te vinden. Er dient rekening mee gehouden te worden dat de eerste afroep plaatsvindt direct na gunning en bestaat uit 150 toegangscontrolesystemen.                                                                                                                                                                                                                                                                                                                                                            |

## Eisen Rapportages

| Eisen Rapportages |                                                                                                                                                                              |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nr.               | Omschrijving                                                                                                                                                                 |
| RAP-1             | Leverancier stelt online rapportages ter beschikking waarop beschikbaarheid, storingen, gebruik, en, indien van toepassing, vullingsgraad te zien zijn.                      |
| RAP-2             | De rapportages hebben een exportfunctie in ieder geval csv formaat, opdat Opdrachtgever zelf over deze gegevens kan beschikken, en in kan lezen in een eigen rapportagetool. |

## Beheereisen

| Beheereisen |                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nr.         | Omschrijving                                                                                                                                                                                                                                                                                                                                                                        |
| Beh-1       | De leverancier stelt bij bekende 'bugs' bijbehorende workarounds beschikbaar.                                                                                                                                                                                                                                                                                                       |
| Beh-2       | In geval van een storing kan de container ook niet ontgrendeld worden.                                                                                                                                                                                                                                                                                                              |
| Beh-3       | In geval van contact met technisch applicatiebeheer en de Opdrachtgever is de voertaal Nederlands                                                                                                                                                                                                                                                                                   |
| Beh-4       | Opdrachtgever krijgt bij een fout in het systeem een duidelijke instructie in gebruikerstaal hoe deze fout op te lossen.                                                                                                                                                                                                                                                            |
| Beh-5       | Opdrachtgever wordt actief geïnformeerd bij systeemfouten middels e-mailnotificatie of andere actieve foutenlog.                                                                                                                                                                                                                                                                    |
| Beh-6       | Het servicewindow is ten minste op maandag, dinsdag, woensdag, donderdag en vrijdag van 07.30 - 18.30 uur. Uitzondering hierop vormen de officiële nationale feestdagen zoals bepaald door de Rijksoverheid. Tijdens dit servicewindow dienen medewerkers van Leverancier telefonisch bereikbaar te zijn. Gedurende 24 x 7 dient het mogelijk te zijn om de servicedesk te emailen. |
| Beh-7       | De Service Desk voert uitsluitend de Nederlandse taal.                                                                                                                                                                                                                                                                                                                              |
| Beh-8       | Incidenten worden voorzien van een prioriteit:                                                                                                                                                                                                                                                                                                                                      |

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | <ol style="list-style-type: none"> <li>1. Incidenten die leiden tot volledige uitval van één of meer bedrijfskritische procesonderdelen. Deze Incidenten komen in de Service Management rapportage tot uiting in een verlaagd beschikbaarheid percentage.</li> <li>2. Incidenten die ernstig impact hebben op de dienstverlening en die leiden tot een uitval of verminderde dienstverlening voor een groot deel van de gebruikers</li> <li>3. Incidenten die een beperkte impact hebben, die slechts voor enkele gebruikers merkbaar zijn, uitval van niet-bedrijf kritische applicatie.</li> </ol>                                              |
| Beh-9  | Indien incidenten/meldingen niet adequaat worden opgevolgd wordt geëscaleerd conform door de Gemeente en de Leverancier ingerichte escalatieprocedure op 3 niveaus (Strategisch/Tactisch/Operationeel).                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Beh-10 | De Leverancier stelt een contactpersoon aan die aangesproken kan worden over de voortgang c.q. afhandeling van een incident of melding                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Beh-11 | Bij iedere change levert de Leverancier releasedocumentatie en is verantwoordelijk voor het uitvoeren van de technische test. De Gemeente is verantwoordelijk voor de acceptatietest.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Beh-12 | De Leverancier voert alleen gepland onderhoud uit in het onderhoudswindow (vastgelegd in de SLA) en stelt de Opdrachtgever daarvan op de hoogte. Leverancier stuurt een risico analyse van gepland onderhoud aan gemeente en na akkoord Opdrachtgever kan het onderhoud worden uitgevoerd.                                                                                                                                                                                                                                                                                                                                                        |
| Beh-13 | De Leverancier is verantwoordelijk voor het opstellen van een Exit Plan na het beëindigen van de overeenkomst.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Beh-14 | <p>De Leverancier dient een Service Level Agreement aan te leveren en dient afspraken met prestatie-indicatoren ten aanzien van de volgende onderwerpen ter accordering voor te leggen aan de Opdrachtgever:</p> <ul style="list-style-type: none"> <li>• Bereikbaarheid</li> <li>• Beschikbaarheid</li> <li>• Incidentmanagement</li> <li>• Securitymanagement</li> <li>• Change management</li> <li>• Releasemanagement</li> <li>• Serviceraapportages</li> <li>• Servicegesprekken</li> </ul> <p>Leverancier is verantwoordelijk voor het actueel houden van de SLA en dient wijzigingen ter accordering voor te leggen aan Opdrachtgever.</p> |
| Beh-15 | <p>De Leverancier is verantwoordelijk voor het nader uitwerken en bijhouden van afspraken in:</p> <ol style="list-style-type: none"> <li>1. DAP (Dossier Afspraken en Procedures): procedures met de leverancier</li> <li>2. DFA (Dossier Financiële Afspraken): financiële afspraken.</li> </ol> <p>Deze documenten dienen vervolgens ter accordering te worden voorgelegd aan Opdrachtgever.</p>                                                                                                                                                                                                                                                |

## Eisen Informatiebeheer

| Eisen Informatiebeheer |                                                                                                                                             |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Nr.                    | Omschrijving                                                                                                                                |
| IB-1                   | De applicatie beschikt over een niet-muteerbare audit-trail waarin automatisch registratie en opslag van de volgende gegevens plaats vindt: |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <ol style="list-style-type: none"> <li>1. Alle handelingen (functionaliteiten) die door gebruikers met betrekking tot metagegevens, processen, documenten, dossiers of andere objecten worden verricht,</li> <li>2. De gebruiker, datum en tijd van de uitvoering van de handeling. Hierdoor dient het mogelijk te zijn om alle handelingen ook achteraf te kunnen volgen.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| IB-2 | <p>De applicatie moet functionaliteit bevatten die Opdrachtgever in staat stelt om de gewenste dan wel wettelijke bewaartermijnen te handhaven:</p> <ol style="list-style-type: none"> <li>1. Er moet een bewaartermijn kunnen worden ingericht op basis van een geïdentificeerd werkproces en er moeten metadata over de bewaartermijn en einddatum van het proces kunnen worden toegevoegd.</li> <li>2. Van informatieobjecten die voor vernietiging in aanmerking komen, moeten op basis van het jaar van vernietiging overzichten kunnen worden gecreëerd.</li> <li>3. Informatieobjecten en bijbehorende metadata moeten onherstelbaar kunnen worden vernietigd op basis van de als zoekcriteria (metadata) opgegeven waardering/vernietigingstermijn.</li> <li>4. Van de vernietiging moet een verklaring worden opgeleverd waarin minimaal wordt aangegeven om welke informatie het gaat, dat de vernietiging volledig is uitgevoerd en om hoeveel data het gaat (TB, MB, etc.)</li> <li>5. Inschrijver garandeert dat bij een backup-recovery geen gegevens terug in productie worden gezet die formeel al vernietigd zijn.</li> </ol> |
| IB-3 | <p>Het moet mogelijk zijn om een export te maken van bestanden en bijbehorende metadata op basis van opgegeven zoekcriteria, ten behoeve van bijvoorbeeld overdracht naar een andere omgeving, zoals bij het einde van de overeenkomst. De onderlinge samenhang tussen gegevens, indien van toepassing, kan worden blijven gelegd (bijv.: metadata en bestanden, relationele database) om informatieverlies te voorkomen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |