Gemeente Amsterdam

Ingenieursbureau

Bijlage 5 Programma van Eisen

Projectnaam:	**Aanbesteding Digitale toegang Team Licht**
Kenmerk:	AI 2026-0011
Datum:	19 november 2026
Versie:	1.2

Inhoud

1 Inleiding 4

2 Definities 5

3 Algemene eisen 8
3.1 Eisen m.b.t. duurzaamheid 9
3.2 Eisen m.b.t. kwaliteitsmanagement en normering 10
3.3 Eisen m.b.t. veiligheid 10
3.4 Eisen m.b.t. communicatie en overleg 11
3.5 Eisen m.b.t. uitvoering 11
3.6 Eisen m.b.t. vergunningen en ontheffingen 12
3.7 Bijzondere uitvoeringsvoorwaarde social return 13

4 Eisen m.b.t. BIO2 14
4.1 Organisatorische maatregelen 14
4.2 Personeelsmaatregelen 25
4.3 Fysieke beveiliging 25
4.4 Systeembeveiliging 26

5 Sluitplan 31

6 Eisen levering Hardware 32
6.1 Algemene eisen Hardware 32
6.2 Eisen aan Mechatronische cilinders 32
6.3 Eisen aan fysiek Openingsmiddel 33

7 Eisen levering Software 34
7.1 Technische eisen aan Software 34
7.1.1 Hosting en infrastructuur 34
7.1.2 Beheer van de Toegangsbeheerapplicatie 35
7.1.3 Verbindingen 35
7.2 Functionele eisen Toegangsbeheerapplicatie 36
7.3 Smartphone applicatie eisen 37

8 Eisen Opleiden, Trainen en Oefenen (OTO) 39

9 Eisen implementeren, configureren en testen Toegangsbeheerapplicatie 40
9.1 Proces 40
9.2 Eisen aan testen 40

10 Eisen Testen & In bedrijfstellen vervanging 41
10.1 IFAT 41
10.2 ISAT 41

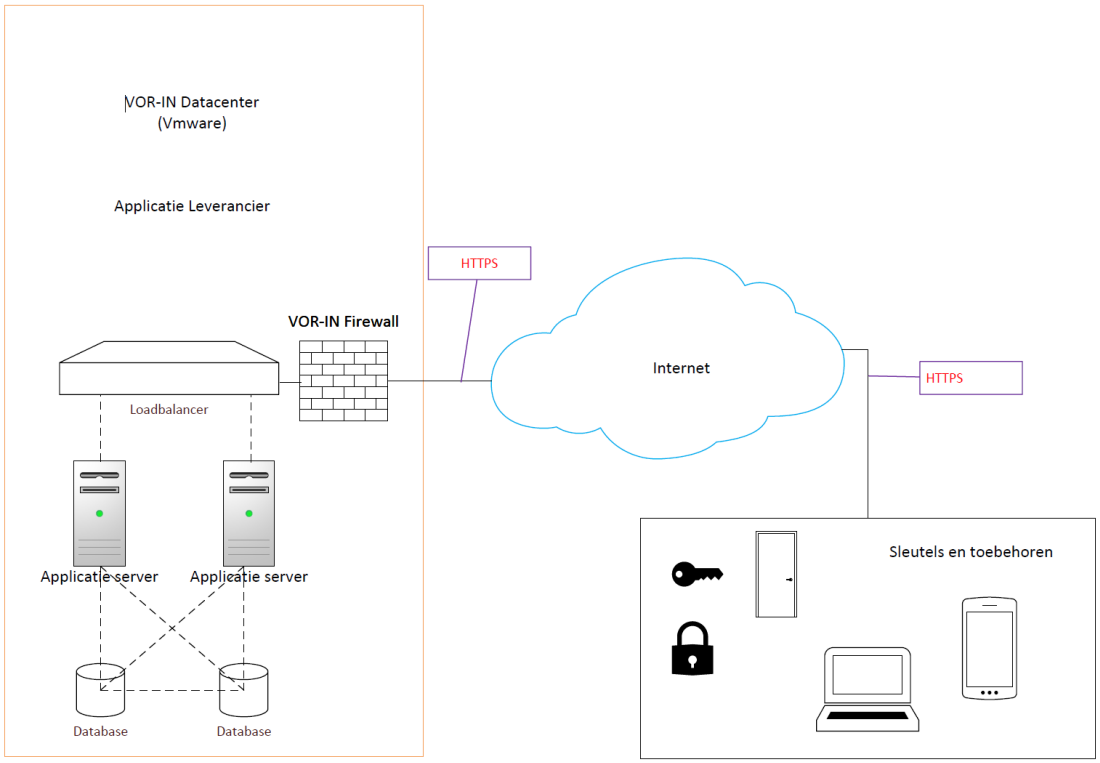
11 Eisen Opleverdossier 43

12 Eisen Beheer & Onderhoud **44**

Bijlagen **46**

1 Inleiding

Voor u ligt het Programma van Eisen voor het leveren en plaatsen van een digitaal toegangssysteem en het installeren, bedrijfsvaardig opleveren en onderhouden van een Toegangsbeheerapplicatie hiervoor, zoals schematisch weergegeven in Figuur 1. Dit document beschrijft de eisen voor de te leveren inspanningen, prestaties, hardware en software voor de Raamovereenkomst AI2026-0011. De volledige scope wordt beschreven in de Aanbestedingsleidraad.



Figuur 1: Schematische weergave Toegangsbeheerapplicatie

2 Definities

Begrip	Omschrijving
Active Directory	Een centrale opslagplaats voor het beheer van gebruikers, computers, wachtwoorden en toegangsrechten. AD zorgt voor veilige authenticatie en autorisatie, waardoor beheerders netwerkbeleid kunnen afdwingen en resources kunnen beheren.
Asset	Een verzameling van dezelfde objecten, zoals bijvoorbeeld Verkeersregelinstallaties (VRI).
Audit-logging	Controle registratie waarin wordt vastgelegd "wie, wat, wanneer en welk object"
AVG	Algemene Verordening Gegevensbescherming. De AVG regelt hoe organisaties binnen de Europese Unie (EU) moeten omgaan met persoonsgegevens.
BIO2	Baseline Informatiebeveiliging Overheid 2, de vernieuwde uniforme norm voor informatiebeveiliging binnen de Nederlandse overheid.
BIV	"Beschikbaarheid", "Integriteit" en "Vertrouwelijkheid"
BRL 9101	Nederlandse beoordelingsrichtlijn (procescertificaat) voor het veilig ontwerpen, plaatsen en onderhouden van tijdelijke verkeersmaatregelen bij werk in uitvoering en evenementen. Het garandeert dat wegafzettingen voldoen aan de CROW-richtlijnen 96A/96B
Cilinder	Het bewegende binnenste deel van een Slot die het fysieke ont- en vergrendeling van een Slot borgt. Drijft het Slot aan en bedient het Slot. ON vervangt binnen deze aanbesteding de huidige cilinders voor Mechatronische cilinders die werken binnen de digitale toegang oplossing die Opdrachtnemer aanbiedt.
Contractaannemer	Opdrachtnemer van de gemeente Amsterdam die vanuit andere overeenkomsten diensten en/of leveringen verzorgen voor assets waar de Digitale toegang oplossing voor uitgerold gaat worden. Bijvoorbeeld het onderhoud van de VRI-kasten.
DAP	Dossier Afspraken en Procedures. Beschrijft operationele werkafspraken tussen Opdrachtnemer en Opdrachtgever.
Digitale toegang	Het geheel van Toegangbeheerapplicatie, Mechatronische cilinders, Openingsmiddelen en onderlingen verbindingen.
GVB	Gemeentelijk Vervoerbedrijf. Het GVB is het openbaarvervoerbedrijf van Amsterdam en verzorgt het vervoer met trams, bussen, metro's en veerponten in en rond de stad.
IFAT	Integrated Factory Acceptance Test
ISAT	Integrated Site Acceptance Test
ITIL	Information Technology Infrastructure Library

Mechatronische cilinder	Cilinder die wordt toegepast binnen de digitale toegang oplossing die Opdrachtnemer aanbiedt.
OG	Opdrachtgever, de gemeente Amsterdam
ON	Opdrachtnemer voor dit contract
Openingsmiddel	Het object of combinatie van objecten die de gebruiker aanwendt voor het ontgrendelen van de cilinder in het slot, niet zijnde een smartphone van een gebruiker.
OVL	Openbare Verlichting. Elektrische installaties voorzien van lichtpunten (armaturen met 1 of meerdere lichtbronnen) die zijn aangebracht op een lichtmast of bevestigd aan een kunstwerk. OVL heeft als doel om ook bij duisternis het wegverkeer verkeersveilig te laten functioneren
PH-test	Penetration and Hacking test
RF	Radiofrequent
SB	Systeem Beheer
Slot	Mechanisme dat een deur of luik beveiligt. De Cilinder is hier onderdeel van.
SPIN	SPIN (Systeem Planning en Informatie Nederland) is een portaal van Rijkswaterstaat voor het aanvragen van verkeersmaatregelen op rijkswegen.
Toegangsbeheerapplicatie	Centraal systeem voor het aansturen van de Mechatronische cilinders en het registreren van handelingen binnen het systeem.
TVM	Een TVM (Tijdelijke Verkeersmaatregel) is een tijdelijke aanpassing van de verkeerssituatie op de openbare weg, nodig voor of evenementen, om de veiligheid en doorstroming te garanderen met behulp van bijvoorbeeld borden, afzettingen, omleidingen of verkeersregelaars.
V&G-plan	Een V&G-plan (Veiligheids- en Gezondheidsplan) is een document dat wordt opgesteld om de veiligheid en gezondheid van werknemers en anderen te waarborgen tijdens een bouwproject of andere risicovolle werkzaamheden. Het is verplicht vanuit de Arbowet.
VGCU	V&G-coördinator uitvoeringsfase
VIS	De Asset VIS (Verkeersinformatiesystemen) omvat verschillende type installaties waaronder verkeerscamera's, pollers, bewegwijzering en verschillende displays.
VRI	Een VRI (Verkeersregelinstallatie) is een installatie die het verkeersaanbod op kruispunten detecteert en regelt door middel van verkeerslichten. De installatie bestaat uit een regelkast, detectielussen, verkeerslichten en bijbehorende software en zorgt voor een veilige en efficiënte afwikkeling van het gemotoriseerde en ongemotoriseerde verkeer. Alle VRI's zijn georganiseerd binnen de gelijknamige Asset VRI.

WIOR	WIOR (Werken In de Openbare Ruimte) is een Amsterdamse verordening die regels stelt voor werkzaamheden in de openbare ruimte, zoals graven, bouwen en het plaatsen van objecten. Het doel is om veiligheid, bereikbaarheid en leefbaarheid te waarborgen en werkzaamheden goed te coördineren.
WLS	De WLS (Wet Lokaalspoor) is wetgeving die o.a. regels stelt aan werkzaamheden op en rondom metro- en traminfrastructuur.
WVA	Indien er gewerkt wordt in het areaal van een tunnel dient er WVA (Werkvergunningsaanvraag) tunnel aangevraagd te worden bij de Tunnelbeheerorganisatie (TBO).

Deze definities zijn aanvullend op de definities uit de Aanbestedingsleidraad.

3 Algemene eisen

Als toelichting op en/of ter verduidelijking van de eisen wordt verwezen naar Bijlage 5H – Demarcatie Opdrachtgever-Opdrachtnemer.

eis - 1	Opdrachtnemer (ON) realiseert een volledig functionerend en correct geïnstalleerd werkend systeem conform de eisen uit dit PvE bestaande uit alle geleverde componenten en benodigde integraties met andere systemen: • Active Directory; • E-mail notificaties via bestaande relay server van Opdrachtgever (OG). De aangeboden en gerealiseerde producten dienen één geïntegreerd geheel te vormen.
eis - 2	De ON moet alle eisen in het PvE verifiëren. Hiervoor stelt ON zelf een verificatiematrix op. ON levert de verificatiematrix ter akkoord bij OG aan binnen zes weken na de definitieve gunning. De verificatiematrix geldt als basis voor de verificatierapportage om te verifiëren dat er aan de eisen is voldaan en wordt als bijlage bij een verzoek ten behoeve van een prestatieverklaring aangeleverd.
eis - 3	De minimale beschikbaarheid van de Toegangsbeheerapplicatie op jaar basis, zijnde 24 uur/dag en 365 dagen/jaar, is 99,6% uitgezonderd de tijd voor planbare systeempatches en updates.
eis - 4	Niet-beschikbaarheid van de Toegangsbeheerapplicatie mag alleen in overleg met OG en onder gecontroleerde omstandigheden plaatsvinden vanwege de grote operationele gevolgen.
eis - 5	ON is geboden een Projectteam te mobiliseren voor het vakkundig uitvoeren van de opdracht. Hierin dient zij onder meer samen te werken met de gebruikers van het toegangsbeheersysteem. Dit zijn onder meer medewerkers van OG, gecontracteerde onderhoudspartijen en dienstverleners en stakeholders zoals bijvoorbeeld de politie.
eis - 6	In het geval dat OG om extra werkzaamheden vraagt die ON bij derden moet uitzetten, worden facturen direct middels een AWR naar de OG gestuurd. De ON mag de volgende aannemersvergoeding hanteren; • Diensten maximaal 10%; • Vergunningen en leges maximaal 8%; • Leveringen maximaal 5%. De AWR wordt enkel goedgekeurd door OG bij aantonen van betaling in combinatie met de factuur van de aangedragen aannemer of leverancier.
eis - 7	ON stelt binnen vijf werkdagen na gunning van de opdracht een organisatieschema beschikbaar van zijn organisatie met daarin benoemd de sleutelfunctionarissen en hun plaatsvervangers die in de verschillende rollen als gevolg van de overeenkomst betrokken zijn. ON geeft daarbij een escalatiemodel met functionarissen van zowel OG als ON alsmede de criteria om naar een volgend niveau te escaleren.

	In het organisatieschema wordt tevens vastgelegd wie namens OG welke bevoegdheden heeft. Het organisatieschema wordt door ON aangepast aan wijzigingen in de organisatie van OG en ON. De rollen die ten minste in het organisatieschema moeten terugkomen zijn: ON • Contractmanager • Projectleider • Technisch specialist • V&G coördinator • Super user • Chief Information Security Officer (CISO) OG • Asset manager • Contractmanager • Projectleider • Asset beheerder • Aanspreekpunt Systeem Beheer • Aanspreekpunt Servicedesk Team Licht • Toezichthouder / Directievoerder • Chief Information Security Officer (CISO)
eis - 8	ON dient na gunning een gedetailleerd implementatieplan per asset op te stellen, welke na goedkeuring van de OG, volgens plan uitgevoerd wordt. Dit implementatieplan kent de volgende fasering: 1. Implementatie Toegangsbeheerapplicatie op VORIN 2. Functionele configuratie en test van de Toegangsbeheerapplicatie per asset, voorafgaand aan het in bedrijfstellen/"live" gaan van de Toegangsbeheerapplicatie op VORIN . 3. Uitrol van de Cilinders in combinatie met de Toegangsbeheerapplicatie per asset in de openbare ruimte, incl. ISAT per object.

3.1 Eisen m.b.t. duurzaamheid

eis - 9	Alle in te zetten voertuigen moeten tenminste voldoen aan de eisen zoals die gelden in de milieuzones, zie https://www.amsterdam.nl/verkeer-vervoer/milieuzones-uitstootvrije-zones/
eis - 10	Per 1 januari 2025 dienen alle vervoers- en transportbewegingen ten behoeve van de uitvoering van de Overeenkomst uitstootvrij te zijn. Uitstootvrij betekent zonder uitlaatemissie van broeikasgassen, verontreinigende gassen en deeltjes. Dit geldt voor de voertuigcategorieën M1, M2, M3, N1 en N2 (zie rdw.nl/particulier/paginas/voertuigcategorieën).

eis - 11	Per 1 januari 2025 dienen (mobiele) werktuigen en (stationaire) machines die ten behoeve van de uitvoering van de Overeenkomst worden ingezet uitstootvrij te zijn. Uitstootvrij betekent zonder uitlaatemissie van broeikasgassen, verontreinigende gassen en deeltjes. Dit geldt voor de machinecategorieën Mini (<19kW) en Klein (19-56kW). Middel en Groot dienen ook Uitstootvrij te zijn, mits technisch en economisch mogelijk.

3.2 Eisen m.b.t. kwaliteitsmanagement en normering

eis - 12	ON moet tijdens de hele looptijd van deze Raamovereenkomst blijven voldoen aan de geschiktheidseisen uit de Aanbestedingsleidraad.
eis - 13	Deze normeringen dienen van toepassing te zijn op de aangeboden hard- en software: • Cyberbeveiligingswet en NIS2 • NEN-EN 15684:2021 duurzaamheidsklasse 6, klimatologische klasse 4, veiligheidsklasse F, systeem managementklasse 2 en inbraakwerendheid klasse 2.
eis - 14	Het door ON in te zetten personeel in de openbare ruimte dient minimaal te beschikken over een VCA-B of aantoonbaar gelijkwaardig certificaat. Voor leidinggevende geldt dat zij in het bezit zijn van een VCA-VOL of aantoonbaar gelijkwaardig certificaat.

3.3 Eisen m.b.t. veiligheid

eis - 15	ON is verplicht te allen tijde een veilige werkomgeving te creëren conform de ARBO wet voor de uitvoering van werkzaamheden, voor de eigen medewerkers en andere gebruikers van de openbare ruimte. Voor uitvoering van werkzaamheden die niet plaatsvinden binnen gedefinieerde parameters van het verkeer wordt de ON geachte de juiste verkeersmaatregelen zoals pionnen tot zijn beschikking te hebben én te plaatsen, zodat een veilige werkplek wordt gecreëerd. De werkzaamheden worden uitgevoerd zoals omschreven in de richtlijnen die zijn vastgesteld in de Bouw-Cao, artikel 70 en het Handboekwegafzetting CROW96a en 96b. Voor toegepaste figuren wordt verwezen naar Bijlage 5F BLVC Uitvoeringsplan en Bijlage 4 - Prijzenblad Digitale Toegang Team Licht rubriek Verkeersmaatregelen Voor de bepalingen voor het aanvragen en verkrijgen van de noodzakelijke vergunningen en ontheffingen wordt verwezen naar par. 3.5
eis - 16	ON legt uiterlijk 4 weken na de start van de overeenkomst een V&G-plan uitvoeringsfase voor aan de OG. De eisen waaraan het V&G-plan uitvoeringsfase aan moet voldoen, staan gespecificeerd in Bijlage 5A V&G-plan ontwerpfase, hoofdstuk 3 “Wettelijke verplichtingen”.

eis - 17	Opdrachtnemer is verplicht een V&G-coördinator uitvoeringsfase (VGCU) aan te stellen.
eis - 18	De VGCU heeft minimaal 3 jaar aantoonbare ervaring in veiligheidskundige taken zoals het opstellen van V&G plannen en V&G dossiers en het maken van BTO keuzes op basis van de arbeidshygiënische strategie passend bij de scope van het project.
eis - 19	De taken en plichten van de VGCU staan gespecificeerd in de Bijlage V&G-plan ontwerpfase, hoofdstuk 3 "Wettelijke verplichtingen"

3.4 Eisen m.b.t. communicatie en overleg

eis - 20	Binnen 10 werkdagen na gunning organiseert ON een Project Startup met OG. Bij deze Project Startup moeten tenminste de personen aanwezig zijn zoals benoemd in eis - 7.
eis - 21	Tijdens de projectmatige vervanging wordt (minimaal) maandelijks een bouwvergadering gehouden met tenminste de vaste agendapunten: • Veiligheid; • Status update informatiebeveiliging; • Actie en besluitenlijst; • Planning en voortgang (stand en aandachtspunten); • Afwijkingen/Wijzigingen; • Rondvraag.
eis - 22	In de beheerfase vindt per kwartaal een kwartaaloverleg plaats. Deze overleggen vinden binnen twee weken na het aflopen van het desbetreffende kwartaal plaats.
eis - 23	ON inventariseert de agendapunten voor de kwartaaloverleggen, deelt de agenda één week voor het overleg met de deelnemers, notuleert en deelt de notulen uiterlijk twee weken na het betreffende kwartaaloverleg. Vaste agendapunten zijn: • Verslag/status CISO; • Financiële update (o.a. totale uitputting contract vanaf start overeenkomst); • De voortgang van lopende Nadere Opdrachten; • Advies ter optimalisering van de uitvoering of afspraken m.b.t. het beheer van het areaal in het geheel of een installatie in het bijzonder.
eis - 24	Tijdens het kwartaaloverleg van kwartaal vier wordt tevens het hele afgelopen kalenderjaar geëvalueerd (o.a. DAP bespreken/bijstellen).

3.5 Eisen m.b.t. uitvoering

eis - 25	De transitie van de bestaande situatie (o.b.v. conventionele cilinders en sleutels) naar de eindsituatie (o.b.v. mechatronische cilinders en Openingsmiddelen) dient gefaseerd per asset gerealiseerd te worden.
eis - 26	De transitie dient per asset met de projectleider van het vervangingsproject overlegd en afgestemd te worden.

eis - 27	Aan het einde van de werkdag zijn de objecten waarvan de Cilinder die dag op de planning stond om vervangen te worden, te openen met het nieuwe of het bestaande Openingsmiddel. OG moet daarnaast altijd toegang houden tot de kast om bijvoorbeeld te kunnen reageren op calamiteiten.
eis - 28	Voorafgaand aan het vervangen en in bedrijfstellen van de eerste Cilinder binnen een nadere opdracht beschikken de in het sluitplan toegewezen gebruikers over het nieuwe Openingsmiddel.
eis - 29	Voor het in bedrijfstellen van een Mechatronisch slot zijn de toegangsrechten van de relevante stakeholders in de Toegangsbeheerapplicatie geactiveerd.

3.6 Eisen m.b.t. vergunningen en ontheffingen

eis - 30	Tijdens werkzaamheden beschikt de ON over de juiste vergunningen, ontheffingen, e.d. conform landelijke of Amsterdamse regelgeving. Deze worden op eerste verzoek aan handhavers, door OG aangewezen directievoerders of inspecteurs getoond.
eis - 31	ON vraagt vergunningen of ontheffingen zelf aan. ON mag eventuele legeskosten volgens eis - 6 verrekenen.
eis - 32	ON dient in Amsterdam te werken volgens procedures vastgelegd in de WIOR-verordening en nadere regels. Zie ook: Werken in de openbare ruimte (WIOR) - Gemeente Amsterdam.
eis - 33	ON dient te werken volgens de geldende regels voor werken nabij tram, metro of bus, te verkrijgen bij de regelgevende instanties (vergunningenloket van de GVB). Zie ook: gvb-zakelijk-vergunning-aanvragen-wls | GVB
eis - 34	ON dient te werken volgens de geldende regels voor werken op Rijkswegen. Zie ook: https://www.rws.nl/SPIN
eis - 35	ON dient te werken volgens de geldende regels voor werken op Provinciale wegen. Zie ook: https://www.noord-holland.nl/Producten_op_alfabet/Toestemming_tijdelijke_verkeersmaatregelen_weg
eis - 36	ON dient te werken volgens de geldende regels ten aanzien van werkzaamheden nabij tunnels, zoals vastgelegd in Bijlage 5B Werkrichtlijnen tunnels versie 2.4.
eis - 37	Bij alle werkzaamheden in de openbare ruimte dient ON de leidraad 'Zo werken wij in Amsterdam op straat' (ZWIA) te volgen. Deze leidraad is beschikbaar op www.amsterdam.nl. https://www.amsterdam.nl/parkeren-verkeer/werken-openbare-ruimte/handboek-zwia/
eis - 38	Bij alle werkzaamheden, zowel aanleg als onderhoud, dient ON rekening te houden met de zone zwaar verkeer Amsterdam. Zie ook: https://www.amsterdam.nl/parkeren-verkeer/zone-zwaar-verkeer-amsterdam/
eis - 39	ON dient te werken conform de geldende RVV-ontheffingsregels. Zie ook: https://www.amsterdam.nl/ondernemen/vergunningen-ondernemers/

3.7 Bijzondere uitvoeringsvoorwaarde social return

Inzake de bijzondere uitvoeringsvoorwaarde social return wordt verwezen naar Bijlage 5G: Social Return.

4 Eisen m.b.t. BIO2

De eisen in Hoofdstuk 4 van dit PvE zijn 1-op-1 afgeleid van de BIO2. Bij elke eis staat het BIO2-overheidsmaatregelnummer in rood. Dit nummer geeft aan van welke maatregel de eis is afgeleid. BIO2-overheidsmaatregelen waar in dit hoofdstuk of in de ISO 27001 niet naar worden verwezen, zijn niet van toepassing op deze opdracht.

4.1 Organisatorische maatregelen

eis - 40	5.01.01 **Informatiebeveiligingsplan** ON heeft aantoonbaar informatiebeveiligingsbeleid in de eigen organisatie geïmplementeerd en legt dit vast in het Informatiebeveiligingsplan. Dit beleid voorziet tenminste in de volgende hoofdzaken: 1. De wijze waarop de openingsmiddelen en hun uitgifte en beheer is beveiligd. 2. De continuïteit van de bedrijfsvoering is geborgd in geval van hacking, malware attacks en andere vormen van cybercriminaliteit. 3. De inrichting van de eigen organisatie. Beschrijf de rollen en verantwoordelijkheden van de functionarissen ten aanzien van bedrijfscontinuïteit en verantwoordelijkheden voor het onderhouden van het informatiebeveiligingsbeleid. 4. De specifieke verantwoordelijkheden, taken en bevoegdheden van de functionaris belast met de informatiebeveiligingsfunctie. 5. De maatregelen die zijn genomen in het kader van privacybescherming. Beschrijf hoe het gebruik van privacy gevoelige gegevens is geminimaliseerd, hoe privacy gevoelige gegevens worden beschermd. 6. De wijze waarop actief veiligheidsbewustzijn van medewerkers van ON wordt bevorderd. Trainingen worden periodiek herhaald en zijn zowel voor medewerkers als bestuurders van toepassing. Bestuurders kunnen aanvullend aantonen dat zij voldoende kennis en vaardigheden hebben om de gevolgen van Informatiebeveiligingsrisico's te beoordelen op de diensten en/of producten die de organisatie levert. 7. De interne procedures voor het afhandelen van informatiebeveiligingsincidenten. 8. ON neemt in het informatiebeveiligingsplan een separate paragraaf op met daarin de beschrijving van de rol van de Chief Information Security Officer (CISO) of gelijkwaardig. Beschrijf bevoegdheden en de wijze waarop onafhankelijkheid en zelfstandigheid voor het adviseren en rapporteren aan de leiding van de organisatie is geborgd.

	9. ON neemt in het informatiebeveiligingsplan een separaat hoofdstuk op gericht op de werknemers van de organisatie waarin expliciet en helder geformuleerd is wat de gedragsregels ten aanzien van het veilig gebruik van bedrijfsmiddelen zijn. Deze regels zijn opgenomen in het contract van de medewerkers. 10. De Plan-Do-Check-Act cyclus waarmee informatiebeveiligingsbeleid wordt onderhouden en jaarlijks vastgesteld door de leiding van de organisatie.
eis - 41	5.01.02 **Informatiebeveiligingsplan** • Het informatiebeveiligingsbeleid moet tenminste elk jaar beoordeeld en zo nodig bijgesteld moeten worden om te zorgen dat deze voortdurend passend, adequaat en doeltreffend blijft. • Het informatiebeveiligingsbeleid moet bij reorganisatie of veranderingen in de verantwoordelijkheidsverdeling beoordeeld en zo nodig bijgesteld worden. • Het informatiebeveiligingsbeleid moet bij elke wijziging opnieuw ter beschikking worden gesteld aan de OG.
eis - 42	5.02.01 **Rollen en verantwoordelijkheden** Zie eis - 41 (5.01.02)
eis - 43	5.02.02 **Chief Information Security Officer (CISO)** Zie eis - 40 en eis - 41 (5.01.01 en 5.01.02)
eis - 44	5.03.01 **Functiescheiding** ON moet beschrijven in het informatiebeveiligingsplan welke maatregelen er zijn genomen om documentatie, configuraties, hard- en software, licenties e.d. van de OG te beschermen tegen onbedoeld ter beschikking stellen aan andere klanten of relaties van de ON zonder voorafgaande toestemming van de OG.
eis - 45	5.04.01 **Training** De ON verklaart dat deze een training verzorgt en jaarlijks herhaalt voor alle medewerkers die voor de ON werkzaamheden gaan verrichten ten aanzien van informatiebeveiliging op het gebied van bewustzijn, regels en verplichtingen. De bestuurders overleggen schriftelijk bewijs dat zij voldoende kennis en vaardigheden hebben om gevolgen van informatiebeveiligingsrisico's te beoordelen op de diensten en/of producten die de organisatie levert.
eis - 46	5.04.02 + 5.04.03 **Gedragsregels** ON neemt in het Informatiebeveiligingsplan een separaat hoofdstuk op gericht op de werknemers van de organisatie waarin expliciet en helder geformuleerd is wat de gedragsregels ten aanzien van het veilig gebruik van bedrijfsmiddelen zijn. Deze regels zijn van toepassing op intern en extern personeel alsmede vrijwilligers. Deze

	regels zijn opgenomen in het contract van de medewerkers. Medewerkers zijn actief gewezen op deze gedragsregels
eis - 47	5.05.01 **Organogram** ON levert een organogram met schriftelijke toelichting aan waaruit blijkt welke functionarissen welke rollen vervullen in het kader van Informatiebeveiliging, welk mandaat bij welke rol hoort en hoe dit organogram en toelichting jaarlijks wordt geactualiseerd. Het document is voorzien van een datum en versienummer.
eis - 48	5.06.01 **Belangengroepen** ON maakt het mogelijk dat werknemers met een rol op het vlak van Informatiebeveiliging seminars, cursussen, trainingen e.d. kunnen bezoeken op het vlak van Operationele Technologie (OT) en informatiebeveiliging om daarmee een actueel beeld van het dreigingslandschap en mogelijke oplossingen te behouden. Opgedane kennis en inzichten worden actief met de overige werknemers gedeeld in het kader van bewustzijn op het vlak van informatiebeveiliging.
eis - 49	5.07.01 **Informatiebeveiligingsdreigingen** ON wijst formeel de taak aan de functionaris belast met informatiebeveiliging toe zich te abonneren op de RSS en/of nieuws feed van het Nationaal Cyber Security Centrum (https://www.ncsc.nl/), de binnenkomende meldingen te beoordelen op relevantie en passende acties uit te zetten om bedreigingen of kwetsbaarheden te mitigeren. ON wijst formeel de taak aan de functionaris belast met Informatiebeveiliging toe tenminste maandelijks relevante log bestanden te scannen op afwijkend, ongewenst of verdacht gedrag van systemen met als doel hacking of intrusion attempts te kunnen herkennen. Eventuele bevindingen zorgen voor snelle, passende en relevante mitigerende maatregelen.
eis - 50	5.08.01 **Risicomanagement** ON maakt bij nieuwe informatiesystemen en bij significante wijzigingen op bestaande informatiesystemen een expliciete risicoafweging op basis van de door de organisatie vastgestelde risicomanagementmethodiek, om risico's te identificeren en in voldoende mate te beheersen en ook voor het vaststellen van de nieuwe of herziene beveiligingseisen. De risicomanagementmethodiek moet ook voorzien in het voorkomen van ongecontroleerde wijzigingen aan systemen. ON maakt een beknopt verslag waaruit de keuzes en onderbouwing van de wijzigingen blijkt en voegt dit toe aan het klantdossier. Het klantdossier kan door OG op aanvraag ingezien worden.
eis - 51	5.09.01 **Inventaris**

	ON onderhoudt actief een lijst van alle hard- en software componenten die ON levert en onderhoudt die deel uitmaken van de Digitale toegang oplossing voor OG. In de inventaris worden tenminste alle zaken opgenomen die relevant zijn op het gebied van Informatieverwerking, cybersecurity, netwerkvoorzieningen en Clouddiensten. Uit deze inventaris moet tenminste de status van de componenten in het kader van Lifecycle management blijken. Het gebruik van non-supported of end-of-life apparatuur / software is niet toegestaan en ON dient voor tijdige vervanging te zorgen. De volledigheid en actualiteit van de inventaris wordt ten minste 1x per jaar geactualiseerd en ter beschikking gesteld aan OG.
eis - 52	5.10.01 **Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen** ON heeft voor gebruik in de eigen organisatie regels opgesteld ten aanzien van aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen. Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen behoren te worden vastgesteld, gedocumenteerd en geïmplementeerd.
eis - 53	5.12.01 De ON respecteert de classificatie die door de OG aan datasets of andere gegevens is gegeven en hanteert daarvoor passende beschermingsmaatregelen. Bijvoorbeeld persoonsgegevens, digitale identiteiten (zoals inloggegevens en TLS certificaten) dienen beter beschermd te worden dan bijvoorbeeld een verkeersregeling in CCOL code.
eis - 54	5.13.01 ON hanteert tenminste twee verschillende informatieclassificaties met als doel privacygevoelige informatie, bijvoorbeeld persoonsgegevens en locaties van het openingsmiddelen ~~sleutel~~gebruik door eindgebruikers, te kunnen onderscheiden van meer algemene documentatie zoals as-built documentatie en technische specificaties. ON legt hiervoor een gebruikersclassificatieschema (welke persoon mag welke documenten lezen/wijzigen) ter goedkeuring voor aan OG.
eis - 55	5.14.01 **Internetfacing-informatiesystemen** ON heeft zijn eigen IT/OT omgeving goed beveiligd. ON heeft procedures beschreven en geïmplementeerd die moeten borgen dat deze eigen omgeving actief wordt onderhouden, cybersecurity risico's worden beoordeeld en op passende wijze worden gemitigeerd. Internetfacing-informatiesystemen en e-mail berichtenverkeer moeten blijvend voldoen aan de verplichte standaarden zoals deze beschreven staan op de website van het Forum voor Standaardisatie (https://www.forumstandaardisatie.nl/). Hierop wordt gestuurd met de metingen van de website Internet.nl (https://internet.nl/) Daarbij dienen alle onderdelen te worden ingesteld zodat een optimale beveiliging wordt bereikt zonder afbreuk te doen aan de functionaliteit van de geboden dienst.
eis - 56	5.14.02

	Beveiligingscertificaten ON maakt voor zijn systemen bij openbaar webverkeer van gevoelige gegevens gebruik van ten minste publiek vertrouwde Organization Validated (OV)-certificaten. ON maakt voor het beveiligen van interne datastromen gebruik van de actuele editie van het Transport Layer Security (TLS 1.3) protocol. De keuze wie de daarvoor benodigde certificaten uitgeeft, ON of OG, wordt afgestemd met de OG. Gedurende de looptijd van het contract bestaat de mogelijkheid dat hogere of afwijkende eisen aan certificaten worden gesteld voortkomend uit een risicoanalyse, aansluitvoorwaarden of wetgeving. ON dient zich hieraan te conformeren.
eis - 57	5.14.04 Van alle internetfacing-informatiesystemen, webapplicaties, IP-adressen en API's is een actuele registratie. ON levert as-built documentatie op waaruit tenminste duidelijk blijkt welke componenten zijn geïmplementeerd en hoe deze onderling communiceren. Van interfacing componenten dient specifiek het gebruikte protocol en de wijze van beveiliging te worden opgegeven.
eis - 58	5.15.01 **Vertrouwde zones** ON krijgt uitsluitend toegang tot relevante delen van het besturingsnetwerk van OG. Hiervoor wordt verplicht gebruik gemaakt van de telewerkvoorziening van de OG. Het gebruik van remote access tools, VPN's, directe SSH-koppelingen en vergelijkbaar is niet toegestaan. Te allen tijde moet het voor OG mogelijk blijven audit-trails ten aanzien van het gebruik van het besturingsnetwerk vast te leggen t.b.v. forensische analyses.
eis - 59	5.16.01 **Geldigheid van autorisaties** Autorisaties verstrekt door OG hebben een maximale geldigheid van 1 jaar en zullen automatisch verlopen. ON zorgt zelf voor tijdige verlenging voor zijn medewerkers door 1 maand voor het verlopen contact op te nemen met de Servicedesk van de OG om verlenging aan te vragen. ON meldt actief bij de Servicedesk van OG als er sprake is van personele mutaties die aanpassing van verstrekte autorisaties noodzakelijk maken.
eis - 60	5.16.02 **Gebruiksregels voor verstrekte autorisaties** ON accepteert gebruiksregels ten aanzien van autorisaties: Groepsaccounts of het gedeeld gebruik van accounts is niet toegestaan. De telewerkvoorziening van OG is gebaseerd op persoonlijke accounts en aangevuld met een smartphone applicatie gebaseerde Multi-factor authenticatie. Openingsmiddelen beheer: voor eisen ten aanzien van openingsmiddelen beheer zie hoofdstuk 5 Sluitplan
eis - 61	5.17.01 (1) Centrale authenticatie: Toegang voor eindgebruikers ("sleutelhouders") is gebaseerd op een Multilfactor authenticatiesysteem. Dit kan bijvoorbeeld in de vorm van een smartphone

	gebaseerde applicatie die het openingsmiddel valideert bij de Toegangsbeheerapplicatie waarbij de persoonlijke smartphone als authenticatiemiddel fungeert. (2) Centraal beheer: Alle digitale identiteiten voor de correcte werking van de uitgifte van de openingsmiddelen zijn op afstand vanuit het besturingsnetwerk van de OG te beheren. (5) Monitoring: • De tooling moet een actueel overzicht van verstrekte en actieve identiteiten kunnen tonen. • De tooling moet een audit trail die het gebruik van de digitale identiteiten weergeeft vastleggen. • De tooling registreert nadrukkelijk ook mislukte inlogpogingen. • De tooling registreert in de audit log ook het wijzigen van autorisaties en stuurt een alert naar de functioneel beheerder als rechten van een account verhoogd of uitgebreid worden. • Onverwachte of ongecontroleerde wijzigingen moeten als een informatiebeveiligingsincident vastgelegd en afgehandeld worden. (6) Functioneel beheer: De toegang tot de tooling is gebaseerd op een rollen en rechten structuur. Er is tenminste voorzien in een rol t.b.v. de functioneel beheerder. Deze beheerder is in staat om de actuele credentials te overzien en te beheren.
eis - 62	5.17.02 **Wachtwoordmanager** De ON biedt aan alle medewerkers die inloggegevens van OG ontvangen een wachtwoordmanager of vergelijkbare oplossing aan en verplicht deze te gebruiken.
eis - 63	5.17.03 **Afdwingen van wachtwoordbeleid** Zie 5.17.01 voor de eisen aan tooling tbv wachtwoordbeheer.
eis - 64	5.18.01 **Monitoring van accounts** Zie 5.17.01 voor de eisen aan tooling tbv monitoring van accounts.
eis - 65	5.18.02 **Toegangsrechten** OG levert gebruikersnamen en initiële wachtwoorden van de personen die namens de OG toegang tot de cilinder/straatkast nodig hebben (inclusief rolverdeling) aan de ON. ON koppelt deze gegevens aan de juiste rollen en rechten. De resulterende autorisatiematrix moet door OG opvraagbaar te zijn in de Toegangsbeheerapplicatie.
eis - 66	5.19.01 **Informatiebeveiliging bij inkoop** Deze BIO-interpretatie geeft invulling aan de gestelde eisen ten aanzien van

	informatiebeveiliging. BIV-rating Beschikbaarheid (B) Hoog Integriteit (I) Middel Vertrouwelijkheid (V) Middel
eis - 67	5.20.03 **Contracteisen valideren** ON toont aan dat aan alle gestelde eisen op het gebied van informatiebeveiliging is voldaan in opzet, bestaan en werking, op basis van onderzoeken van onafhankelijke derden. Deze onderzoeken hebben een scope die dekkend is voor de gecontracteerde dienstverlening. Hierbij is expliciet aandacht voor de toeleveringsketen en hoe de leverancier zijn leveranciersmanagement ingeregeld heeft, zie eis - 71 (5.21.01.). Dit toont de leverancier jaarlijks opnieuw aan.
eis - 68	5.20.04 **Externe audits** ON staat toe en werkt mee aan audits op het vlak van informatiebeveiliging op initiatief van de OG. Bevindingen worden in een beschermende context per omgaande gedeeld tussen OG en ON met als doel kwetsbaarheden te identificeren en mitigerende maatregelen te kunnen treffen. De manier waarop en wanneer deze audit plaatsvindt, wordt na gunning in overleg met ON vastgelegd.
eis - 69	5.20.05 **Delen van kwetsbaarheden** ON is transparant over kwetsbaarheden in de dienstverlening en informatiebeveiligingsincidenten waaronder datalekken. Dit stelt OG in staat om passend te reageren onder meer door te rapporteren en mitigerende maatregelen te treffen. Kwetsbaarheden en incidenten met een acuut karakter moeten direct aan de Servicedesk van de OG ter registratie als informatiebeveiligingsincident worden gemeld.
eis - 70	5.20.06 **Exit strategie inzake overgang op andere partij** In geval van dispuut met OG, of anderszins contractbeëindiging is de ON verplicht mee te werken aan een gecontroleerde overdracht zodanig dat de operatie in de openbare ruimte van Amsterdam ongestoord doorgang kan vinden. Voor dit doel levert ON een uitwerking aan van de exit-strategie in deze uitvraag.
eis - 71	5.21.01 **Supply chain management**

	Voorafgaand aan het afsluiten van de overeenkomst geeft de leverancier inzicht in de keten van toeleveranciers en in hoeverre de verplichtingen en eisen zijn doorgelegd aan de toeleveranciers. Ook toeleveranciers dienen aan alle eisen m.b.t. de BIO 2.0 te voldoen.
eis - 72	5.21.02 Voorafgaand aan het afsluiten van de overeenkomst geeft de leverancier inzicht in de keten van toeleveranciers en eventuele risico's daarin. De gemeente beoordeelt of de risico's acceptabel zijn.
eis - 73	5.21.03 **Beveiligingseisen doorleggen** De overheidsorganisatie borgt dat de beveiligingseisen aan de leverancier onverminderd van toepassing zijn op de keten van toeleveranciers, tenzij die eisen niet relevant zijn gezien de aard van de dienstverlening door de toeleverancier. Indien informatiebeveiligingseisen zijn uitgesloten, maakt de leverancier dat inzichtelijk, inclusief een onderbouwing.
eis - 74	5.21.04 **Supply chain management** ON is verplicht gedurende de looptijd van leverings- en onderhoudscontracten veranderingen in de keten van toeleveranciers door te geven, inclusief risico's daarin. Dit omvat minimaal kwetsbaarheden en informatiebeveiligingsincidenten die de dienstverlening aan de OG kunnen raken.
eis - 75	5.22.01 **Chief Information Security Officer (CISO)** ON stelt een vaste functionaris aan met de rol van Chief Information Security Officer (CISO) of gelijkwaardig. De CISO: • is als de proceseigenaar verantwoordelijk voor het jaarlijks beoordelen dat de ON voldoet aan de gestelde informatiebeveiligingseisen. • is de functionaris die eventuele beveiligingsrisico's beoordeeld namens de ON. • is de functionaris die mitigerende maatregelen laat implementeren. • is de primaire contactpersoon voor de CISO van OG voor informatiebeveiliging. • is de functionaris die samen met de CISO van OG eventuele rest-risico's beoordeelt en formeel accepteert. De CISO van ON is verantwoordelijk voor het oplossen van informatiebeveiligingsincidenten of dat deze tot een met OG afgestemd acceptabel rest-risico worden gereduceerd.
eis - 76	5.23.01 **Cloud Service Providers en digitale autonomie** OG hecht waarde aan digitale autonomie en het reduceren van vendor lock-in situaties. OG hanteert het beleid dat applicaties uitsluitend on-premises worden gehost. De smartphone App communiceert rechtstreeks met de on-premises Toegangsbeheerapplicatie.
eis - 77	5.24.01

	Melden van Informatiebeveiligingsincidenten Onderdeel van het informatiebeveiligingsbeleid is dat ON voorziet in een duidelijke en voor iedere medewerker toegankelijk meldloket, bijvoorbeeld de Servicedesk van ON, waar informatiebeveiligingsincidenten, kwetsbaarheden en verbetervoorstellen kunnen worden gemeld en geregistreerd. De meldprocedure en de daarbij horende taken en verantwoordelijkheden van het meldloket zijn beschreven.
eis - 78	5.24.04 **Rapportage verplichting** Taak voor de CISO rol en aanvullend op eis - 75 (5.22.01): De CISO of gelijkwaardig van ON is er verantwoordelijk voor dat er per incident gerapporteerd wordt over de opvolging van informatiebeveiligingsincidenten naar de CISO van OG. Informatiebeveiliging maakt onderdeel uit van de maandelijkse voortgangsoverleggen.
eis - 79	5.24.06 **Beveiliging van toeleveringsketens.** De beveiliging van toeleveringsketens is onderdeel van de risicoanalyse voor de ON. In de risicoanalyse wordt rekening gehouden met: • specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener; • de algemene kwaliteit van de producten; • de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures.
eis - 80	5.24.07 **Incidentmeldingen uitwisselen tussen OG en ON** 1. De incidentprocedure en dienstverlening van het meldloket van ON voorziet in tijdige afhandeling en melding richting OG zodat OG kan voldoen aan de wettelijke termijn om informatiebeveiligingsincidenten te melden bij het Nationale Cyber Security Incident Response Team (CSIRT). 2. Meldingen van CSIRT ontvangen door OG kunnen worden doorgezet naar het meldloket van ON ter oplossing of mitigatie van het probleem.
eis - 81	5.25.01 **Doormelden van informatiebeveiligingsincidenten** Meldingen van informatiebeveiligingsincidenten door ON aan OG worden afgedaan via het incidentbeheerproces. Deze meldingen worden indien relevant gemeld bij toezichthouders volgens de bepalingen uit de betrokken wet- en regelgeving zoals de Cyberbeveiligingswet, de Archiefwet en de Algemene verordening gegevensbescherming (AVG).
eis - 82	5.27.01 **Analyse van incidenten** ON is verplicht beveiligingsincidenten te analyseren met als doel te leren en te voorkomen van toekomstige beveiligingsincidenten. Na analyse dienen de mitigerende maatregelen bekend gemaakt te worden aan OG.
eis - 83	5.28.01 **Bewaartermijnen**

	• De ON is verplicht log bestanden of ander bewijsmateriaal ten aanzien van informatiebeveiligingsincidenten ten minste drie jaar te bewaren. • De ON is verplicht technische hulpmiddelen zoals logging en monitoring toe te passen voor het verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen. • De ON stelt een continuïteitsplan op waarin mogelijke risico's/scenario's beschreven worden die de continuïteit van de systemen van de OG negatief kunnen beïnvloeden. Denk hierbij bijvoorbeeld aan stroomstoringen, kabelschade, fysieke beschadiging, brand van de straatkast, inbraak, ramp of andere crisissituaties. Geef aan wat de impact is voor de dienstverlening en welke mitigerende maatregelen er geïmplementeerd zijn. • Het continuïteitsplan wordt minimaal jaarlijks gecontroleerd op geldigheid en bruikbaarheid. Het plan is voorzien van een duidelijke titel, versienummer, publicatiedatum en auteur.
eis - 84	5.30.01 **Testen van noodvoorzieningen en procedures** Werking van noodvoorzieningen zoals UPS, bereikbaarheid van IT voorzieningen, bereikbaarheid voor een service engineer voor acute situaties gedurende slechte of extreme weerscondities wordt door ON aannemelijk gemaakt door het implementeren van passende procedures of werkafspraken.
eis - 85	5.30.02 **Kritieke systemen** ON levert een lijst aan van kritieke systemen die nodig zijn voor de dienstverlening aan OG. ON beschrijft kans en impact van een verstoring van deze systemen. ON beschrijft de passende mitigerende maatregelen die zijn genomen om de kans of impact van een verstoring tot een minimum te beperken.
eis - 86	5.31.01 **Wettelijke, statutaire, regelgevende en contractuele eisen** Eisen van wettelijke, statutaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen te voldoen behoren te worden vastgesteld, gedocumenteerd en actueel gehouden.
eis - 87	5.32.01 **Intellectuele-eigendomsrechten** Voor zover van toepassing wordt verwezen naar Bijlage 2A - De Algemene Inkoopvoorwaarden van de gemeente Amsterdam.
eis - 88	5.33.01 **Bewaartermijnen** De OG heeft voor alle informatie(systemen) in selectielijsten de bewaartermijn vastgelegd, rekening houdend met de eigen bedrijfsdoelstellingen en wet- en regeling, zoals de archiefwet en privacywetgeving. Bewaartermijnen worden na gunning gedeeld met ON. De ON heeft deze termijnen ook praktisch ingeregeld en toetst periodiek de werking hiervan.

eis - 89	5.34.01 **Privacy en bescherming van persoonsgegevens.** • De ON wijst een functionaris gegevensbescherming in het kader van de Algemene Verordening Gegevensbescherming (AVG) toe die toeziet op de veilige en correcte omgang met privacygevoelige gegevens. Te denken valt hierbij aan persoonsgegevens van medewerkers, toegang tot de logginggegevens. • De ON herziet periodiek het informatiebeveiligingsplan en controleert periodiek op naleving van privacyregels, informatieverwerking en procedures van het informatiebeveiligingsplan en wet en regelgeving. • ON sluit in het kader van Privacy een Verwerkersovereenkomst af (zie bijlage 1B)
eis - 90	5.35.01 **Information Security Management System (ISMS)** De ON beschrijft hoe de Plan Do Check Act cyclus ten aanzien van Information Security Management voor de dienstverlening is geborgd in de organisatie. Aanvullend worden (potentiële) Informatiebeveiligingsincidenten met een passende status en hun opvolging gelogd in een Service Management tool van de Servicedesk, of functioneel vergelijkbaar, van de ON. De tool kan op elk gewenst moment op verzoek van de OG een rapport leveren over openstaande en afgehandelde informatiebeveiligingsincidenten.
eis - 91	5.35.02 **Auditplan** Er wordt jaarlijks door een onafhankelijke partij een security audit uitgevoerd. Deel van deze audit betreft een PH-test. De test wordt uitgevoerd met een representatieve bijbehorende datakoppeling in een test omgeving. Bevindingen worden in een rapport vastgelegd en afspraken worden gemaakt over de tijdige oplossing van deze bevindingen. Bevindingen dienen opgelost te worden. • De bevindingen van een security audit worden vastgelegd in een rapport en gedeeld met de ON. • De gebruikte test methodiek is gebaseerd op publiek algemene geaccepteerde tests van OWASP en aangevuld met apparaat specifieke tests.
eis - 92	5.36.01 **Rapportage van incidenten** In de maand- en kwartaalrapportages dienen informatiebeveiligingsincidenten en hun afhandeling opgenomen te worden. ON maakt aannemelijk dat incidenten op afdoende wijze zijn afgehandeld. OG behoudt zich het recht voor gesloten incidenten te laten heropenen of verdere mitigerende acties van ON te verlangen.
eis - 93	5.37.01 **Gedocumenteerde bedieningsprocedures.** ON stelt gebruiks- en onderhoudshandleidingen ter beschikking aan eigen servicepersoneel en personeel van OG voor zover relevant waarbij nadrukkelijk rekening gehouden wordt met veilig werken in de zin van de Cyber Beveiligingswet en het naleven van vastgestelde onderhouds- en gebruiksprocedures. Doel is het

	voorkomen van ongeautoriseerde, ongecontroleerde wijzigingen aan de installatie of het onbedoeld verlagen van het beveiligingsniveau.

4.2 Personeelsmaatregelen

eis - 94	6.01.01 **Screening van personeel** • Gegevens van de medewerkers (werknemers en ingehuurd personeel) die werkzaamheden voor de gemeente Amsterdam uitvoeren, moeten per medewerker worden aangeleverd. Aangeleverd dient te worden: Naam en telefoonnummer, VOG en getekende geheimhoudingsovereenkomst. • Elke medewerker van de ON die werkzaamheden voor de gemeente Amsterdam gaat uitvoeren moet in bezit zijn van een Verklaring Omtrent Gedrag dat passend is voor de uit te voeren taken en werkzaamheden, en niet ouder zijn dan 3 jaar. • In het kader van privacy kan worden volstaan met het tonen van de VOG aan de OG.
eis - 95	6.03.01 **Training** De ON verklaart dat deze een training bewustzijn verzorgt voor alle medewerkers die voor de ON werkzaamheden gaan verrichten ten aanzien van informatiebeveiliging bewustzijn, regels en verplichtingen.
eis - 96	6.03.02 **Training** De medewerkers hebben de training bewustzijn - binnen drie maanden na indiensttreding - gevolgd. Dit dient aangetoond te worden aan de OG.
eis - 97	6.03.03 **Training** De ON zorgt bij aanstelling of interne overplaatsing van medewerkers en contractanten dat het belang van opleiding en training duidelijk wordt gemaakt waarbij actief elke 3 jaar deze training opnieuw gevolgd wordt.
eis - 98	6.08.01 **Melden van incidenten** Geconstateerde beveiligingsincidenten dienen direct en volledig volgens de vastgestelde procedure te worden gemeld en afgehandeld inclusief taken en verantwoordelijkheden van betrokkenen.

4.3 Fysieke beveiliging

eis - 99	7.02.01 **Melden van incidenten** De OG verleent de autorisaties voor toegang tot de sleutels.

eis - 100	7.14.01 **Veilig verwijderen of hergebruiken van apparatuur.** Onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.

4.4 Systeembeveiliging

eis - 101	8.03.01 & 8.03.02 **Gebruikersrollen en minimale rechten** De gebruikersrollen die geïmplementeerd zijn dienen te borgen dat toegang tot informatie en systeemfuncties tot het noodzakelijk minimum worden beperkt. ("Principle of least privilege")
eis - 102	8.05.01 **Toegang op afstand** Toegang tot de omgeving van de OG vindt uitsluitend plaats via de daarvoor beschikbare procedure.
eis - 103	8.09.01 **Configuratiebeheer** Documenten zoals configuratiebestanden, documentatie, prestatiegegevens, incidenten, storingen, wijzigingen etc. dienen tenminste gedurende de gehele gebruiksduur bewaard en onderhouden te worden. Documenten zijn voorzien van een versienummer en publicatiedatum.
eis - 104	8.10.01 **Wissen van informatie** Gedurende en aan het einde van de overeenkomst treedt ON in overleg met OG om afspraken te maken over overdracht of vernietiging van de documentatie.
eis - 105	8.12.01 **Voorkomen van gegevenslekken** Documentatie zoals bedoeld in eis - 103 (8.09.01) wordt in een beveiligde en selectief toegankelijke locatie door ON bewaard. ON houdt een autorisatiematrix bij waaruit duidelijk blijkt wie toegang heeft tot de documentatie en wat daar de redenen voortvloeiend uit het uitoefenen van de functie voor zijn. Doel is documentatie zo selectief mogelijk beschikbaar te stellen en het oneigenlijk delen van de vastgelegde informatie te voorkomen.
eis - 106	8.13.01 **Back-up beleid** ON hanteert een back-upbeleid waarin de eisen voor het bewaren en beschermen van tenminste de documenten zoals bedoeld in eis - 103 (8.09.01) zijn opgenomen. Er moet speciale aandacht zijn voor het beschermen van de back-up tegen ransomware-aanvallen en genomen maatregelen om de integriteit van de back-up te behouden.
eis - 107	8.13.02

	Dataverlies Op basis van een expliciete risicoafweging is bepaald dat het maximaal toegestane dataverlies twee dagen betreft en de maximale hersteltijd na een incident één werkdag is.
eis - 108	8.13.03 **Bescherming van de back-up** ON levert documentatie aan van de correcte wijze van back-up van de applicatie en de onderliggende database.
eis - 109	8.13.04 **Recovery test** ON levert documentatie aan van de correcte wijze van een restore van de applicatie en de onderliggende database.
eis - 110	8.15.01 **Eisen aan logging** ON configureert de Toegangsbeheerapplicatie en Openingsmiddelen zodat tenminste aan- en afmeldpogingen gelogd worden. De logregel van de Toegangsbeheerapplicatie bevat een datum-tijd stempel en herkomst IP nummers/gebruiker. De logregel van het Openingsmiddel bevat een datum-tijd stempel, openingsmiddel-ID, cilinder-ID en resultaat.
eis - 111	8.15.02 **Beperking aan log gegevens** Een logregel bevat nooit gegevens die tot het doorbreken van de beveiliging kunnen leiden.
eis - 112	8.15.03 **Logging van informatie** ON legt ter beoordeling een voorbeeld aan OG voor van gelogde Toegangsbeheerapplicatie informatie. OG behoudt zich het recht voor wijzigingen of aanvullingen in de gelogde informatie aan te vragen bij ON. De gelogde informatie moet voldoende zijn voor het uitvoeren van forensische analyses in geval zich een incident in het kader van informatiebeveiliging zou voordoen.
eis - 113	8.15.04 **Bewaartermijn gelogde informatie** Gelogde informatie wordt tenminste 6 maanden online beschikbaar gehouden en wordt ook meegenomen in back-up sessies.
eis - 114	8.15.05 **Bescherming van log gegevens** Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als informatiebeveiligingsincident via de procedure voor informatiebeveiligingsincidenten volgens eis - 77 t/m eis - 80 (5.24.01 t/m 5.24.07)
eis - 115	8.15.06 **Bescherming van log gegevens** ON werkt mee aan audits aangevraagd door OG. Back-up beleid, bescherming van loggegevens en bewaartermijnen kunnen binnen het bereik van de audit vallen.
eis - 116	8.16.03

	Bewaking en monitoring ON past bewaking en monitoring op zijn eigen omgeving toe en heeft passende procedures om bedreigingen te mitigeren. Onderdeel van de procedures is dat incidenten en afwijkingen worden geclassificeerd en OG, indien de aard van de verstoring ook een bedreiging kan vormen voor OG, direct op de hoogte wordt gesteld zodat deze ook mitigerende maatregelen kan inzetten. De procedures worden vastgelegd in het informatiebeveiligingsplan en ter inzage aan OG aangeboden.
eis - 117	8.18.01 Alleen bevoegd personeel heeft op die momenten dat toegang strikt noodzakelijk is toegang tot systeemhulpmiddelen.
eis - 118	8.18.02 **Bewaartermijn van log gegevens** ON is verplicht log gegevens voorzien van datum-tijdstempel en gebruiker tenminste 6 maanden te bewaren.
eis - 119	8.21.04 **Versleuteling van data verbindingen** Het is nadrukkelijk niet toegestaan secundaire netwerkverbindingen (zoals Wifi of extra Internetverbindingen) aan de openingsmiddelen toe te voegen. Al het netwerkverkeer dient via het besturingsnetwerk van OG afgehandeld te worden.
eis - 120	8.24.01 **Cryptografiebeleid** 1. Alle verbindingen met de Toegangsbeheerapplicatie vinden plaats over een met TLS versie 1.3 of nieuwer beveiligde verbinding. 2. Digitale certificaten ten behoeve van TLS verbindingen worden in de vorm van een back-up bestand (*.pfx) door opdrachtgever ter beschikking gesteld aan de opdrachtnemer voor implementatie. 3. De OG genereert en verstrekt de benodigde certificaten voor gebruik in de Toegangsbeheerapplicatie tenzij nadrukkelijk anders overeengekomen en vastgelegd is in het DAP dat op basis van technische of organisatorische redenen de ON deze certificaten verstrekt en onderhoud. 4. De ON beschrijft welke maatregelen er zijn genomen om de private key te beschermen tegen onbedoelde verspreiding. 5. Verplichte kenmerken van TLS-certificaten zijn: a. geldigheid maximaal 2 jaar; b. Sleutellengte minimaal 3072 tekens; c. Encryptieniveau minimaal SHA512 d. Wildcard certificaten zijn niet toegestaan; e. De common name van het certificaat is gelijk aan de FQDN van de applicatieserver; f. Self signed certificaten zijn niet toegestaan, wel domain-self-signed certificaten vanuit een centrale PKI-server binnen het beheer domein; g. Uitgifte van PKI-certificaten dient door de instantie PKI Overheid gedaan te worden;

	h. Wachtwoorden op backup bestanden van een PKI-certificaat zullen via een ander kanaal dan waarover het backupbestand wordt verstuurd aan de opdrachtnemer ter beschikking worden gesteld. Bijvoorbeeld verzending van het backup bestand per e-mail, en het bijbehorende complexe unieke wachtwoord wordt via een ander medium dan e-mail doorgegeven; i. Gedurende de gebruiksduur van de Toegangsbeheerapplicatie dienen TLS protocol versies gevolgd te worden en best-practices geïmplementeerd. De gebruikte protocollen en best-practices worden tenminste jaarlijks geëvalueerd en zo nodig bijgewerkt naar de meest actuele stand van de techniek.
eis - 121	8.24.03 **Forum Standaardisatie** Het forum Standaardisatie van de Nederlandse overheid beschrijft welke standaarden toegepast moeten worden. Zie hiervoor https://www.forumstandaardisatie.nl/open-standaarden. ON levert (besturings-)applicaties die communiceren volgens de gepubliceerde standaarden van het forum.
eis - 122	8.24.04 **Cryptografiebeleid** De basis kenmerken van TLS-certificaten zijn beschreven in eis - 120 (8.24.01) en zijn van toepassing op het moment van opdrachtgunning aan de ON. ON is verplicht actuele adviezen over cryptografiesterkte van het Nationaal Cyber Security Centrum (NCSC) van het ministerie van Justitie en Veiligheid en de unit weerbaarheid van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) van het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties op te volgen volgens het 'pas toe of leg uit'-principe.
eis - 123	8.25.01 **Beveiligen tijdens de ontwikkelcyclus** ON past het principe "security-by-design" toe bij het inrichten of uitrollen van de Toegangsbeheerapplicatie. Gedurende het installeren van deze applicatie is het nog toegestaan met eenvoudige fabriekswachtwoorden te ontwikkelen en testen. Bij het daadwerkelijk in gebruik nemen in de productieomgeving van OG dienen alle fabriekswachtwoorden verwijderd te zijn en het vastgelegde wachtwoordbeleid volledig geïmplementeerd te zijn. Direct na voltooiing van de IFAT is het moment waarop het wachtwoordbeleid van OG verplicht gevolgd moet gaan worden. Het wachtwoordbeleid van OG is als volgt: • Minimaal 12 tekens; • Complexiteitseisen; • Geldigheid van maximaal 2 jaar.
eis - 124	8.26.01 **Toepassingsbeveiligingseisen** Zie eis - 123 (8.25.01) voor "security-by-design".
eis - 125	8.29.01

	Acceptatietesten De FAT- en SAT- procedure beschrijvingen bevatten een separate paragraaf met daarin alle standaard uit te voeren controles op cybersecurity-, informatiebeveiliging- en privacyaspecten. Deze procedurebeschrijvingen worden in samenwerking met de OG opgesteld.
eis - 126	8.30.01 **Systeemontwikkeling en testen** Indien gebruik gemaakt wordt van uitbestedingen van werkzaamheden of delen daarvan dient een risicoafweging gemaakt te worden en afgestemd met de OG. Goedkeuring van de OG is vereist.
eis - 127	8.31.01 **Systeemontwikkeling en testen** In de productieomgeving van de OG mag niet worden getest. Alleen met voorafgaande goedkeuring door de OG en onder gecontroleerde omstandigheden kan hiervan worden afgeweken.
eis - 128	8.31.03 **Systeemontwikkeling en testen** 1. Wijzigingen moeten altijd eerst in een testomgeving worden getest alvorens zij in de productieomgeving worden geïmplementeerd. 2. Toestemming voor tests in de productieomgeving wordt door de OG verleent en moeten schriftelijk worden vastgelegd.
eis - 129	8.32.01 **Wijzigingsbeheer (change management)** De ON dient een procedure voor wijzigingen aan systeemcomponenten of instellingen die van invloed kunnen zijn op Informatiebeveiliging te hanteren waarmee de wijziging wordt geadministreerd, risicoafweging van mogelijke gevolgen van de wijziging wordt gemaakt, en de wijziging wordt goedgekeurd door de OG.
eis - 130	8.33.01 **Bescherming van testgegevens** Rapporten van een Pen & Hacking test of een audit moeten vertrouwelijk behandeld worden. Opslag en delen van deze informatie gebeurt alleen met gebruikmaking van veilige media. De informatie is alleen beschikbaar voor medewerkers van OG en ON die uit de aard van hun functie hierover moeten kunnen beschikken.

5 Sluitplan

eis - 131	ON stelt binnen 6 weken na het aanleveren van de toegangsmatrix (zie eis -133) een sluitplan per Asset op welke, na acceptatie door de OG, in de Toegangsbeheerapplicatie geïmplementeerd wordt.
eis - 132	T.b.v. het Sluitplan inventariseert de ON de eisen en wensen van de betrokken Assets en stemt deze af met de beheerders van de Assets.
eis - 133	De assetmanagers/Installatieverantwoordelijke zijn verantwoordelijk voor het toegangsbeleid en de toegangsmatrix. De vigerende toegangsmatrix wordt voor de voorafgaande eis gedeeld met ON. Zie ook eis - 65 (5.18.02)
eis - 134	Cilinders worden geregistreerd op basis van unieke cilinderinformatie en gegroepeerd via labels, waardoor een logisch en herbruikbaar autorisatiemodel ontstaat.
eis - 135	In het Sluitplan worden maatregelen uitgewerkt met betrekking tot ad Hoc toegang tot kasten in geval van storingen en/of calamiteiten.

6 Eisen levering Hardware

6.1 Algemene eisen Hardware

eis - 136	Het integrale Toegangsbeheersysteem dient minimaal 15 jaar te functioneren. Aanpassingen en/of vervangingen systeemonderdelen dienen gedurende deze periode backward compatible te zijn.

6.2 Eisen aan Mechatronische cilinders

eis - 137	De Mechatronische cilinders moeten betrouwbaar blijven functioneren bij temperaturen tussen -15 °C en 65 °C en een relatieve luchtvochtigheid tot 100%.
eis - 138	De Mechatronische cilinders dienen minimaal te voldoen aan IP-rating 55.
eis - 139	De te leveren Mechatronische cilinders dienen geschikt te zijn voldoen aan beveiligingseisen beschreven in NEN5089 minimaal conform SKG keurmerk klasse *** of vergelijkbaar.
eis - 140	De Mechatronische cilinders kunnen alleen ontgrendeld worden in combinatie met een geautoriseerd Openingsmiddel.
eis - 141	Gedurende de looptijd van de Raamovereenkomst geeft Opdrachtnemer minimaal 2 jaar garantie op geleverde Mechatronische cilinders met als ingangsdatum van de garantie de datum van succesvolle ISAT van de betreffende locatie. Indien de Mechatronische cilinder niet door Opdrachtnemer ingebouwd wordt geldt de datum van verzending aan Opdrachtgever of Contractaannemer als ingangsdatum van de garantie.
eis - 142	Mechatronische cilinders moeten, in het geval van het wegvallen van internetverbindingen, te openen zijn door een geautoriseerd Openingsmiddel.
eis - 143	De Mechatronische cilinders dienen zelfstandig te kunnen functioneren zonder voeding en/of internetverbinding.
eis - 144	Mechatronische cilinders worden geopend door smartphone of door de combinatie van smartphone en een Openingsmiddel
eis - 145	Mechatronische cilinders zijn onderhoudsarm. Er zijn geen of minimale onderhoudswerkzaamheden nodig voor instandhouding tijdens de levensduur. Inschrijver dient deze onderhoudswerkzaamheden in het prijzenblad te specificeren met daarbij de frequentie en stuksprijs exclusief tijdelijke verkeersmaatregelen.
eis - 146	Uitgangspunt is dat de vervanging van de huidige cilinders in beginsel zonder aanpassing van de kasten c.q. mastluik gerealiseerd kunnen worden. Uitzondering hierop zijn: • Aanpassing van de hevel ivm de aangeboden oplossing, waarbij de prijs van deze aanpassing in de inschrijfprijs is opgenomen • In uitzonderlijke gevallen dient voor het Slot en hevel een maatwerk oplossing ge-engineerd te worden. Voor een typical voorbeeld wordt

	verwezen naar Bijlage 5C Bestaande sloten assets. Verrekening van specials vindt plaats via post(en) (n.t.b.)

6.3 Eisen aan fysiek Openingsmiddel

Onderstaande eisen zijn van toepassing als er een fysiek openingsmiddel (niet zijnde smartphones) aangeboden wordt door Opdrachtnemer.

eis - 147	De Openingsmiddelen moeten betrouwbaar blijven functioneren bij temperaturen tussen -10 °C en 40 °C en een relatieve luchtvochtigheid tot 100%.
eis - 148	Het openingsmiddel dient minimaal te voldoen aan IP-rating 67
eis - 149	Opdrachtnemer geeft minimaal 2 jaar garantie op de geleverde openingsmiddelen. Ingangsdatum van de garantie is de datum van verzending van het openingsmiddel aan de Opdrachtgever.
eis - 150	Indien het Openingsmiddel een batterij heeft, dient de batterij van een Openingsmiddel eenvoudig vervangbaar te zijn.
eis - 151	De minimale bedrijfstijd van het openingsmiddel na 30 min laden is 3 maanden.
eis - 152	Het Openingsmiddel moet via de smartphone draadloos kunnen communiceren met de toegangsbeheerapplicatie voor het actualiseren van toegangsrechten. Deze eis geldt niet voor het openingsmiddel dat ingezet wordt als calamiteitenvoorzieningen zoals RF transponder, Key Fobs, etc.
eis - 153	De firmware van het Openingsmiddel kan te allen tijde op afstand bijgewerkt worden (update/upgrade).

7 Eisen levering Software

7.1 Technische eisen aan Software

7.1.1 Hosting en infrastructuur

eis - 154	ON Installeert de Toegangsbeheerapplicatie voor de Digitale toegang oplossing op door OG geleverde Virtuele Machines.
eis - 155	De Virtuele Machines, benodigd voor de Toegangsbeheerapplicatie, worden on-premise gehost in één van de Datacenters van de OG. Het virtualisatie platform is VMWare. Indien ON voor de online validatie functionaliteit gebruik maakt van een clouddienst, dan is dat mogelijk mits OG toestemming heeft gegeven.
eis - 156	ON krijgt de keuze tussen een actuele of voorlaatste versie van Microsoft Windows of RedHat Enterprise Linux als operating system volgens het n-1 principe.
eis - 157	De database moet gebruik kunnen maken van Microsoft SQL op Windows of PostgreSQL op Linux, afhankelijk van de gekozen architectuur en leverancierseisen. ON mag onderbouwd een suggestie doen voor een vergelijkbare database. Enkel na akkoord van OG mag deze ook gebruikt worden. Deze moet nog steeds voldoen aan het n-1 principe.
eis - 158	De Virtuele Machines worden ter beschikking gesteld met beperkte specificaties ten aanzien van RAM, Processoren en Storage. De ON treedt in overleg met OG over definitieve specificaties van de Virtuele Machines. Aanvragen worden op redelijkheid beoordeeld.
eis - 159	De OG beheert het operating system van de geleverde Virtuele Machines. Het beheer omvat ook de installatie van operating system updates en het oplossen en analyseren van eventuele technische issues.
eis - 160	De ON is gedurende de beheer- en onderhoudsperiode verantwoordelijk voor het onderhoud, configuratie en een beschrijving van de backup- en restore procedure van de Toegangsbeheerapplicatie.
eis - 161	Op aanvraag en wanneer zinvol geacht kan ook een Virtuele Machine ten behoeve van Acceptatie beschikbaar gesteld worden.
eis - 162	OG kan op het moment van gunning geen container-gebaseerde applicaties ondersteunen. ON moet een traditionele, op het operating system geïnstalleerde, applicatie leveren.
eis - 163	ON voorziet voor de stallatie van de Toegangsbeheerapplicatie op VORIN in een grafische weergave ("architectuurplaat") van de betrokken componenten waaruit hun onderlinge relatie blijkt. Deze weergave moet snel en eenduidig inzichtelijk maken waar zich de technische koppelvlakken bevinden (bijvoorbeeld de software component die gebruikt wordt voor online verificatie van gebruikersrechten zal

	verbonden moeten zijn met Internet) en waar softwarematige relaties liggen bijvoorbeeld in de vorm van middleware.

7.1.2 Beheer van de Toegangsbeheerapplicatie

eis - 164	Ten behoeve van toegang en beheer op afstand van de Toegangsbeheerapplicatie moet ON gebruik maken van de door OG beschikbaar gestelde Telewerkvoorziening (RDP-gateway met MFA). Alternatieve methodieken worden nadrukkelijk niet toegestaan. Zie ook eis - 58 (5.15.01).
eis - 165	Iedere medewerker van ON die toegang op afstand aanvraagt, installeert de MFA-applicatie op de eigen smartphone. Benodigde credentials ('referenties') worden vervolgens door de Servicedesk van OG verstrekt.
eis - 166	Accounts zijn persoonsgebonden.
eis - 167	Accounts worden alleen verstrekt aan medewerkers van ON.
eis - 168	Accounts worden aangevraagd via de procedure van de Servicedesk van OG.
eis - 169	Indien de Toegangsbeheerapplicatie op een RHEL operating system draait, dan zal een extra Microsoft Windows gebaseerde Stepping Stone Server toegevoegd worden. Op deze Stepping Stone Server worden de noodzakelijke beheer-tools in overleg met Systeembeheer geïnstalleerd.

7.1.3 Verbindingen

eis - 170	ON mag geen verbindingen vanuit de Virtuele Machine leggen met systemen buiten de VOR-IN omgeving zonder voorafgaande toestemming van OG. Dit betreft zowel verbindingen naar externe systemen ten behoeve van monitoring op afstand als verbindingen ten behoeve van beheer op afstand. Zie ook eis - 58 (5.15.01).
eis - 171	ON kan bij OG met onderbouwing van nut & noodzaak een beveiligde netwerkverbinding aanvragen tussen de Toegangsbeheerapplicatie en de monitoring omgeving van de ON.
eis - 172	Toepassing: de beveiligde verbinding mag nooit gebruikt worden ten behoeve van Remote Beheer. Uitgangspunt is dat er geen continue data-uitwisseling is tussen de Cilinder en systemen van de leverancier.
eis - 173	Filtering: de beveiligde verbinding wordt maximaal gelimiteerd door alleen verkeer tussen gedefinieerde systemen over vastgestelde protocollen toe te laten.
eis - 174	Techniek: de beveiligde verbinding wordt gerealiseerd in de vorm van een IP-SEC encrypted site-to-site VPN-verbinding.
eis - 175	Procedure: de Security Officer van OG voert een controle uit op de systemen van de leverancier.
eis - 176	Niet-beschikbaarheid van de Toegangsbeheerapplicatie mag alleen onder gecontroleerde omstandigheden plaatsvinden vanwege de grote operationele gevolgen.

eis - 177	Het melden van storingen, updates, speciale verzoeken, wijzigingen en dergelijke moet ON melden via de Servicedesk van OG.
eis - 178	Het updaten van de Toegangsbeheerapplicatie mag alleen plaatsvinden in overleg met de OG. Gepland onderhoud moet aangevraagd worden via de Servicedesk waarna Systeembeheer een afspraak maakt voor de installatie.

7.2 Functionele eisen Toegangsbeheerapplicatie

eis - 179	De Toegangsbeheerapplicatie biedt ruime mogelijkheden in het ontwerpen van autorisaties, rollenstructuren en datavelden. Deze vrijheid vereist echter een doordachte ontwerpkeuze. Het ontwerp wordt uitgewerkt in samenwerking met OG volgens de eisen in hoofdstuk 5 - Sluitplan.
eis - 180	Autorisatie dient mogelijk te zijn afhankelijk van minimaal: • Rol • Object • Type Asset • Compartiment van het object • Bedrijf • Contract
eis - 181	Een Openingsmiddel is te koppelen aan een of meerdere specifieke Mechatronische cilinders
eis - 182	Een Openingsmiddel is te koppelen aan meerdere sluitplannen (van de verschillende assets)
eis - 183	Het tijdsinterval waarvoor een openingsmiddel geautoriseerd is, is instelbaar voor onbepaalde tijd of bepaalde tijd.
eis - 184	Het is mogelijk om voor alle Openingsmiddelen een gebruiker(typen) in te stellen.
eis - 185	Het incidenteel inlezen van groepen personen moet mogelijk zijn via een standaard format waaronder Excel zonder bijkomende kosten en zonder extra inzet van ON.
eis - 186	In-, door- en uitstroom van personen en/of bedrijven dient OG te kunnen managen zonder bijkomende kosten en zonder extra inzet van ON.
eis - 187	De Toegangsbeheerapplicatie dient een overdrachts/uitgifteformulier te bevatten Dit formulier bevat tenminste: • Naam • Mobielnummer • Rol/functie • Werkgever • Autorisatieoverzicht van deze gebruiker;
eis - 188	De Toegangsbeheerapplicatie dient minimaal de volgende dashboards/reports te bevatten (“audit-trail”): • Overzicht van ontgrendelde Mechatronische cilinders met object ID, tijd en gebruiker; • Overzicht met meest recente statusveranderingen bijvoorbeeld wachtwoord wijzigingen en sleutel uitgifte en intrekkingen.

	• Overzicht met gebruikers waarbij binnen een instelbare periode geen acties zijn waargenomen • Overzicht per type Object • Overzicht per type Contract • Overzicht per type Contractant • Overzicht per type Rol/functie • Overzicht per openingsmiddel • Overzicht van geconfigureerde Mechatronische cilinders • Overzicht van geconfigureerde openingsmiddel
eis - 189	Het systeem moet flexibel genoeg zijn om mogelijke uitbreidingen op te nemen, zodat extra gebruikersgroepen en/of objecten eenvoudig kunnen worden toegevoegd.
eis - 190	Er dient zowel een test- als een productieomgeving aanwezig te zijn.
eis - 191	Indien het openingsmiddel verbinding heeft met het internet en aangeboden wordt aan een Mechatronische cilinder, dan wordt deze handeling/het ontgrendelen van de cilinder binnen enkele minuten zichtbaar in de Toegangsbeheerapplicatie.
eis - 192	Indien het openingsmiddel offline is en gebruikt en aangeboden wordt aan een Mechatronische cilinder, dan wordt deze handeling/het ontgrendelen van de cilinder binnen enkele minuten na het herstel van de internet verbinding zichtbaar in de Toegangsbeheerapplicatie.
eis - 193	Bij het aanbieden van het Openingsmiddel dient het systeem moet beschikken over audit-log/audit trail functionaliteit
eis - 194	De Toegangsbeheerapplicatie wordt beschermd via MFA.
eis - 195	Kopieerbeveiliging dient gewaarborgd te zijn door middel van encryptie met minimaal AES 128 en in de toekomst de hoogst haalbare beveiliging.
eis - 196	Alle geleverde Cilinders en Openingsmiddelen dienen ondersteund (functioneel en operationeel) te blijven na updates van de Toegangsbeheerapplicatie.
eis - 197	De autorisatie van een Openingsmiddel voor het ontgrendelen van Cilinders moet op afstand in te stellen zijn.
eis - 198	Nieuwe gebruikers of Openingsmiddelen kunnen "over-the-air" (per telefoon) worden geïntegreerd en hoeven niet lokaal beschikbaar te zijn voor de systeembeheerder
eis - 199	Wijzigingen van de autorisaties, blokkeringen etc. kunnen "over-the-air" (per telefoon) worden uitgevoerd en hoeven niet op locatie te worden uitgevoerd.
eis - 200	Elke gebruiker heeft een unieke identificatie en kan individueel worden vergrendeld.

7.3 Smartphone applicatie eisen

eis - 201	Alle benodigde smartphone applicaties (apps) zijn gratis verkrijgbaar in de Google Play Store en Apple App Store en bevatten alle noodzakelijke functies die de Toegangsbeheerapplicatie hiervan gebruikt zonder dat daar additionele kosten aan verbonden zijn.

eis - 202	Indien een app aangeboden wordt t.b.v. het ontgrendelen van Mechatronische cilinders dient deze geschikt te zijn voor de voorlaatste en laatste besturingssysteem versie van Android en IOS.

8 Eisen Opleiden, Trainen en Oefenen (OTO)

eis - 203	Stakeholders voor OTO zijn: • Systeembeheerder VOR-IN (3 personen) • Eindverantwoordelijke sluitplan per asset (4 personen) • Functionele beheerder van de applicatie (4 personen) • Servicedesk (4 personen) • Eindgebruikers van de applicatie (n.t.b. aantal personen)
eis - 204	De planning van OTO is onderdeel van de project startup, die gedefinieerd is in eis - 20.
eis - 205	Afhankelijk van de inhoud en omvang van de kennisoverdracht per stakeholder dienen trainingen afzonderlijk per stakeholder of in samengestelde groepen aangeboden te worden.
eis - 206	Training vindt plaats in de acceptatie omgeving welke gelijk is aan de productie omgeving (Hands-on, praktijkvoorbeelden, user-cases).
eis - 207	Trainingen worden fysiek op locatie van de gemeente Amsterdam gegeven.
eis - 208	Trainingen dienen gefaseerd aangeboden te worden i.v.m. de beschikbaarheid van personeel.
eis - 209	OTO Systeembeheerder VOR-IN: ON levert al het noodzakelijke voor hosting van de managementapplicatie inclusief een Training voor de doelgroep Systeembeheerder(s) en handleidingen.
eis - 210	OTO Eindverantwoordelijke sluitplan: ON levert al het noodzakelijke voor het inrichten en gebruik van de managementapplicatie inclusief een Training en handleidingen.
eis - 211	OTO Functioneel beheer: ON levert al het noodzakelijke voor de inrichting, gebruik en troubleshooting van de managementapplicatie inclusief een Training voor de doelgroep Functionele beheerder(s) en handleidingen.
eis - 212	OTO Servicedesk: ON levert al het noodzakelijke voor de inrichting, gebruik en troubleshooting van de managementapplicatie inclusief een Training voor de doelgroep Servicedesk en handleidingen.
eis - 213	OTO Eindgebruikers: ON biedt al het noodzakelijke voor de doelgroep eindgebruikers aan via E-learning inclusief gebruikershandleiding.
eis - 214	Handleidingen en overige naslagwerken worden digitaal beschikbaar gesteld.

9 Eisen implementeren, configureren en testen Toegangsbeheerapplicatie

9.1 Proces

eis - 215	De werkwijze met betrekking tot implementeren van de Toegangsbeheerapplicatie is: 1. Implementatie en test van de Toegangsbeheerapplicatie in de acceptatie omgeving van het VOR-IN netwerk; 2. Configuratie en test van de Toegangsbeheerapplicatie conform het Sluitplan en de overige hardware in de keten. 3. Integrale test van de Toegangsbeheerapplicatie in een acceptatieomgeving; 4. Inbedrijfstellen van de Toegangsbeheerapplicatie: Software in de "live" (productie) omgeving ontsluiten en in bedrijf stellen.
eis - 216	Na de in bedrijfstelling van de Toegangsbeheerapplicatie wordt deze gefaseerd ingericht per sluitplan conform het geaccepteerde implementatieplan van ON.

9.2 Eisen aan testen

eis - 217	ON is verantwoordelijk voor en toont aan dat de Toegangsbeheerapplicatie integraal functioneert op het VOR-IN netwerk.
eis - 218	ON is verantwoordelijk voor en toont aan dat het Sluitplan goed ingevoerd is in de Toegangsbeheerapplicatie.
eis - 219	Verschillende scenario's worden getest, waaronder minimaal: 1. Scenario-1: • Testen, 4 assetgroepen aanmaken met twee eindgebruikers per asset; • Testen, toekennen van rechten voor deze eindgebruikers; • Testen, correct functioneren toegang; • Testen, Intrekken rechten; • Testen, genereren rapportage met juiste informatie. 2. Scenario-2: Testen, ontvangst registratie in de toegangsbeheerapplicatie binnen 60 min waarbij de internet verbinding onderbroken wordt. 3. Scenario-3: Testen, ad hoc toegang verlenen bij calamiteit 4. Scenario-4 Testen of het logboek accuraat bijhoudt wie, wanneer de deur heeft geopend. 5. Scenario-5 Testen of meldingen worden ontvangen bij acties (openen, sluiten, foutmeldingen

10 Eisen Testen & In bedrijfstellen vervanging

Uitgangspunt voor het testen aanvangt is dat de software op VOR-IN is geplaatst, zowel vanuit systeembeheer als functioneel beheer. Daarmee is het volgende al werkzaam:

- Toevoegen en configureren van Mechatronische cilinders en Openingsmiddelen;
- Toegang van verschillende gebruikers tot applicatie en toegang tot assets;
- Toegang van Opdrachtnemer tot applicatie voor onderhoud/update werkzaamheden.

10.1 IFAT

Het doel van de IFAT is aantonen dat de configuratie van het sluitplan voor een specifieke Nadere opdracht correct uitgevoerd is.

eis - 220	ON stelt een IFAT protocol op. Het IFAT protocol moet minimaal bevatten; • Controle op alle relevante eisen van dit PvE ; • Een test om de succesvolle configuratie van het Sluitplan aan te tonen • Een test om de goede werking van de Mechatronische cilinders te verifiëren Naast het controleren van alle eisen/punten moet er ook ruimte zijn om restpunten vast te leggen.
eis - 221	ON dient ten minste vier weken voor de eerste IFAT datum het IFAT-protocol in bij OG ter goedkeuring.
eis - 222	ON dient ten minste twee voor de IFAT datum de ingevulde eisen verificatiematrix in bij OG.
eis - 223	Uiterlijk twee weken na de IFAT c.q. uitgevoerde IFAT onderdelen, wordt het ondertekende FAT-protocol met OG gedeeld.
eis - 224	Restpunten uit de IFAT worden uiterlijk 4 weken na de IFAT opgelost, de correcte werking aangetoond en vastgelegd.

10.2 ISAT

De ISAT betreft een ketentest van toegangsbeheerapplicatie t/m aan te sturen slot.

eis - 225	Opdrachtnemer stelt een ISAT protocol op. Het ISAT protocol moet minimaal bevatten; • Controle op alle relevante eisen van dit PvE; • Een ketentest van het hele systeem (o.a. mechanische werking en aansturing, audit trail) • Controle op geaccepteerde restpunten uit de IFAT.

	Naast het controleren van alle eisen/punten moet er ook ruimte zijn om restpunten vast te leggen.
eis - 226	ON dient ten minste vier weken voor de eerste ISAT datum het ISAT-protocol in bij OG ter goedkeuring.
eis - 227	Iedere afzonderlijk Slot (combinatie van bestaand Slot en nieuw geplaatste Mechatronische cilinder) wordt op integrale werking getest voordat deze inbedrijf gesteld wordt.
eis - 228	Uiterlijk twee weken na de ISAT c.q. uitgevoerde ISAT onderdelen, wordt het ondertekende ISAT-protocol met OG gedeeld.
eis - 229	Restpunten uit de ISAT worden uiterlijk 2 weken na de ISAT opgelost en de correcte werking aangetoond.

11 Eisen Opleverdossier

eis - 230	De ON dient na realisatie van de levering en installatie op locatie, per Nadere opdracht een opleverdossier in, aan te leveren in de Nederlandse taal. Het opleverdossier wordt digitaal aangeleverd en bevat minimaal de volgende onderdelen: • Ingevuld en ondertekend document "Opleverrapport Toegangsbeheersysteem" zie bijlage 5D; • Het Opleverdossier bevat minimaal de documenten en gegevens volgens bijlage 5E Inhoudsopgave Opleverdossier; • Lijst van softwareversies en firmware versies gebruikte apparatuur; • Functionele beschrijving van het Toegangsbeheersysteem; • Conformiteitsverklaring aan programma van eisen en regelgeving. • Productbladen/tekeningen sloten en Openingsmiddel • Montagehandleidingen Mechatronische cilinders • As-built tekeningen inclusief eventueel benodigde aanpassingen in PDF DGN conform NLCS teken standaard; • ISAT rapport, getekend voor akkoord; • Overzicht per asset van toegepaste Mechatronische cilinder(s) per object en eventuele afwijkingen ten opzichte van de standaard uitvoering per object
eis - 231	ON levert uiterlijk twee weken na de laatste succesvolle ISAT van de Nadere opdracht een volledig concept opleverdossier aan bij OG waarin slechts de verslagen van nog uit te voeren beproevingen in ontbreken.

12 Eisen Beheer & Onderhoud

eis - 232	Na realisatie van het Toegangsbeheersysteem zal de ON de door hem definitieve geplaatste producten overdragen aan de beheerder van de OG middels een decharge formulier.
eis - 233	De ON dient voor oplevering, start beheer en onderhoud, een definitieve (door de OG goed te keuren) Service Level Agreement(s) op te stellen waarin hij aangeeft hoe deze het Toegangsbeheer-systeem gaat onderhouden om het systeem gedurende de contractduur operationeel te houden, binnen de gestelde beschikbaarheidseisen.
eis - 234	Het resultaat van Beheer en Onderhoud moet zijn dat het Toegangsbeheersysteem operationeel en functioneel beschikbaar is en blijft.
eis - 235	Alle kosten voor OG voor Beheer en Onderhoud (uitgezonderd de gespecificeerde uitzonderingen waar ON geen financiële verantwoordelijkheid voor draagt als ook alle aanpassingen) worden berekend conform de eenheidsprijzen van het Prijzenblad (bijlage 4). Indien het Prijzenblad niet voorziet in bepaalde eenheidsprijzen worden marktconforme prijzen in rekening gebracht
eis - 236	De functionaliteit van de geleverde en geplaatste Toegangsbeheer-objecten dient de ON, gedurende de contractperiode, te garanderen vanaf het moment van een volledig geslaagde ISAT. Storingen zijn voor rekening van ON, met uitzondering van schades en storingen veroorzaakt door vandalisme & schades door o.a. aanrijdingen.
eis - 237	Correctief onderhoud dient te worden uitgevoerd op het Toegangsbeheersysteem-systeem c.q. apparatuur die onder verantwoordelijkheid van ON vallen. Onder correctief onderhoud wordt verstaan: het opsporen en herstellen van schade of storingen, nadat deze zijn geconstateerd of als deze op andere wijze zijn gebleken, bijv. uit de monitoring.
eis - 238	Schades of storingen die zijn veroorzaakt als gevolg van overmacht, derden en die niet vanuit het ontwerp, toegepaste materialen en installatie voorkomen hadden kunnen worden door de ON, worden per geval tussen ON en OG besproken en van acties voorzien. De onbeschikbaarheid van het systeem als gevolg van deze schade of defecten wordt dan niet meegerekend in de onbeschikbaarheid toe te rekenen aan de ON
eis - 239	In geval storingsherstel langer duurt dan 24 uur, stelt de ON een herstelprocedure op en stemt deze af met de OG. De herstelprocedure voorziet onder meer in: • Analyse van de storing, incl. inschatting van impact en omvang; • Diagnose van de oorzaak van de storing binnen 24 uur na storingsmelding incl. de planning van de uitvoering van de herstelwerkzaamheden, en eventuele maatregelen die getroffen moet worden om de gevolgen van de storing te beheersen; • Functieherstel.
eis - 240	Storingsmeldingen binnen kantooruren: storingen worden binnen kantooruren doorgegeven aan de beheerder en Servicedesk van de OG.

eis - 241	Storingsmeldingen buiten kantooruren: urgente storingen worden buiten kantoortijden telefonisch gemeld aan de verkeersleiding van de OG en per email aan de beheerder en Servicedesk van de OG. Kantooruren: van maandag tot en met vrijdag van 07:00 tot 16:00 uur.
eis - 242	Bij het melden van storingen wordt onderscheid gemaakt in twee urgentieniveaus; urgent en niet-urgent. Een urgente Storing betreft: • Uitval van een of meerdere objecten/onderdelen van het Toegangsbeheersysteem; • Ernstige schade aan het Toegangsbeheersysteem; Een niet-urgente Storing betreft: • Alle overige storingen. Reparatietijd: • Urgent: reparatietijd binnen 24 uur; • Niet urgent: reparatietijd binnen 72 uur. Aan een Storing kan door de OG een ander urgentieniveau toegekend worden dan aangegeven in bovenstaande definities
eis - 243	ON zorgt ervoor dat kwetsbaarheden in de gebruikte applicatie/code zo snel mogelijk gepatcht worden. (CVE's) *** nog iets anders verwoorden ***

Bijlagen

Bijlage 5A: V&G plan ontwerpfase
Bijlage 5B: Werkrichtlijnen tunnels 2.4
Bijlage 5C: Bestaande sloten assets
Bijlage 5D: Opleverrapport "Toegangsbeheersysteem"
Bijlage 5E: Inhoudsopgave Opleverdossier
Bijlage 5F: BLVC Uitvoeringsplan
Bijlage 5G: Social Return
Bijlage 5H: Demarcatie Opdrachtgever-Opdrachtnemer