Eisen Cybersecurity

Bijlage bij Raamovereenkomst:
2025-SB-815
TLC – levering en onderhoud

Opdrachtgever	Gemeente Utrecht Afdeling BOR Tractieweg 2 3524 AP Utrecht
Datum	30 maart 2026
Status	Definitief
Projectcode	2025-SB-815
Opsteller	V. de Weger

Inhoud

Cybersecurity eisen en bepalingen

NB: **XXXXXXXXXXXXXXXX**: invullen na gunning.

De in dit document opgenomen cybersecurity-eisen en bepalingen zijn opgesteld om de digitale weerbaarheid van TLC's van de gemeente te borgen. Deze installaties maken onderdeel uit van de operationele technologie (OT) van de gemeente en vervullen een directe rol in de uitvoering van de publieke taak. Verstoring, manipulatie of uitval van deze systemen kan gevolgen hebben voor verkeersveiligheid, doorstroming en het vertrouwen in de gemeentelijke dienstverlening. Om die reden worden aan de leverancier/Opdrachtnemer en aan de te leveren systemen expliciete eisen gesteld op het gebied van cybersecurity.

Bij het opstellen van deze eisen en bepalingen is aangesloten bij de **Baseline Informatiebeveiliging Overheid (BIO2), versie 1.3**. De BIO2 beschrijft het normenkader dat overheidsorganisaties toepassen om informatiebeveiliging en cyberweerbaarheid structureel in te richten.

De maatregelen uit de BIO2 zijn primair gericht op de interne organisatie van de gemeente. In de praktijk worden echter belangrijke onderdelen van de OT-keten – zoals ontwerp, productie, onderhoud en softwareontwikkeling – uitgevoerd door marktpartijen. Om te voorkomen dat er lacunes ontstaan in de beveiliging van deze keten, vertaalt de gemeente relevante BIO2-maatregelen naar concrete verplichtingen voor de Opdrachtnemer.

De in dit document opgenomen teksten vormen daarmee een nadere uitwerking van BIO2-maatregelen voor zover deze betrekking hebben op de ontwikkeling, levering, configuratie, het beheer en het onderhoud van TLC-systemen. De gemeente kiest er nadrukkelijk voor om de uitvoering van een aantal beveiligingsmaatregelen bij de leverancier en de onderhoudsaannemer te beleggen. Die beschikken immers over de technische kennis van het systeem, de ontwikkelomgeving en de softwarecomponenten waaruit de installatie is opgebouwd. Door deze verantwoordelijkheden expliciet te wordt geborgd dat cybersecurity vanaf het ontwerp en gedurende de gehele levensduur van de installatie onderdeel is van de dienstverlening.

Project- en procesgegevens

Algemene projectbeschrijving

Levering en onderhoud Traffic Light Controllers, besteknummer 2025-SB-815.

Omvang van het werk

Het werk bestaat in hoofdzaak uit:

1.	Levering van Traffic Light Controllers
2.	Na levering gedurende 15 jaar (2e lijns) onderhoud van Traffic Light Controllers

Betrokken partijen

XXXXXXXXXXXXXXXX

Namen van in te schakelen deskundigen

CISO Gemeente Utrecht: **XXXXXXXXXXXXXXXX**
Installatiebeheerder Gemeente Utrecht: **XXXXXXXXXXXXXXXX**

Eisen en bepalingen

In dit document wordt onderscheid gemaakt tussen **eisen** en **bepalingen**. Dit onderscheid is bewust aangebracht omdat beide een verschillende functie hebben in de contractrelatie.

Eisen beschrijven eigenschappen of capaciteiten waaraan de te leveren systemen of de organisatie van de Opdrachtnemer moeten voldoen. Het gaat hierbij bijvoorbeeld om eisen aan logging, toegangsbeveiliging, netwerksegmentatie, patchbeheer of het bestaan van beveiligingsbeleid. Eisen zijn in beginsel toetsbaar en kunnen tijdens de uitvoering van het contract worden gecontroleerd.

Bepalingen regelen de wijze waarop Opdrachtgever en Opdrachtnemer gedurende de contractperiode met elkaar samenwerken op het gebied van cybersecurity. Het gaat hierbij bijvoorbeeld om afspraken over incidentmelding, het delen van kwetsbaarheden, medewerking aan onderzoeken of het afstemmen van wijzigingen die invloed kunnen hebben op de veiligheid van de installatie. Bepalingen richten zich daarmee niet primair op de technische eigenschappen van het systeem, maar op het gedrag en de verantwoordelijkheden van partijen tijdens de uitvoering van het werk.

Door eisen en bepalingen te combineren ontstaat een samenhangend kader waarin zowel de technische beveiliging van de installatie als de organisatorische samenwerking tussen gemeente en leverancier/onderhoudsaannemer wordt geregeld. Dit draagt bij aan een beheersbare en transparante uitvoering van de cybersecurityverplichtingen gedurende de volledige levenscyclus van de TLC.

1 Beleid voor gegevensbescherming

BIO2 O-maatregel-nummer	Eisen aan de TLC, de productie/levering van de TLC en het onderhoud van de TLC
5.01.01	**Eis 1: De Opdrachtnemer beschikt over een door de directie vastgesteld informatiebeveiligingsbeleid dat van toepassing is op het ontwerp, de productie, levering en het onderhoud van TLC-systemen.** **Het beleid beschrijft ten minste:** • **verantwoordelijkheden voor informatiebeveiliging en OT-security;** • **de relatie met bedrijfscontinuïteitsmanagement (BCM);** • **de toewijzing van verantwoordelijkheden binnen ketens van informatiesystemen;** • **de wijze waarop het beleid periodiek wordt geëvalueerd.** De Opdrachtnemer toont naleving aan door middel van één van de volgende bewijsmiddelen: a. Een samenvatting van het (OT) gegevensbeveiligingsbeleid aan ten aanzien van **het ontwerp, de productie, levering en onderhoud** van TLC's, welke goedgekeurd is door de directie van de Opdrachtnemer. In de samenvatting wordt tenminste beschreven: - De strategische uitgangspunten die de Opdrachtnemer hanteert ten aanzien van gegevensbeveiliging van VRI's/TLC's. - Hoe het gegevensbeveiligingsbeleid zich verhoudt tot cyberweerbaarheid wetgeving (Cbw -- NIS2 --, Verordening cyberweerbaarheid -- CRA --) en standaarden (ISO-27001). - Inbedding van het beleid in de organisatie van de Opdrachtnemer. - Afstemming op algemene beleid van beveiliging en gegevensbeveiliging van de Opdrachtgever. - Welke functionarissen verantwoordelijk zijn voor het uitvoeren van taken en bevoegdheden op het gebied van gegevensbeveiliging. - De frequentie waarmee het gegevensbeveiligingsbeleid wordt geëvalueerd . - De bevordering van het beveiligings bewustzijn van alle betrokken medewerkers. b. Een geldig ISO27001 certificaat met een scope die het ontwerp, de productie, levering en onderhoud van TLC's omvat. c. Een onafhankelijke auditverklaring.
5.08.01	**Bepaling 2: Indien de Opdrachtnemer voornemens is een cybersecurity-gerelateerde maatregel te implementeren die direct of indirect de elektrotechnische of verkeerskundige veiligheid van de installatie kan beïnvloeden, geldt het volgende:** **1. De Opdrachtnemer is verplicht om voorafgaand aan de implementatie van de maatregel in overleg te treden met de Opdrachtgever.** **2. De Opdrachtnemer dient een schriftelijke risicoanalyse te overleggen waarin de (mogelijke) gevolgen van de maatregel voor de elektrotechnische en/of verkeerskundige veiligheid zijn opgenomen.** **3. De implementatie van de betreffende maatregel mag uitsluitend plaatsvinden na voorafgaande schriftelijke instemming van de Opdrachtgever.** **4. Zonder deze instemming is implementatie van de maatregel niet toegestaan en kan de Opdrachtgever verdere uitvoering opschorten of aanvullende voorwaarden stellen.**

6.01.01	**Eis 3: De Opdrachtnemer beschikt over een vastgesteld screenings- en integriteitsbeleid voor medewerkers en ingehuurde contractanten die werkzaamheden uitvoeren aan TLC-systemen.** **Dit beleid omvat ten minste:** • **bewustwording van informatiebeveiligingsverplichtingen;** • **ondertekening van geheimhoudingsverklaringen;** • **naleving van beveiligingsprocedures van de Opdrachtgever.** De Opdrachtnemer toont naleving aan door middel van één van de volgende bewijsmiddelen: a. De Opdrachtnemer verklaart dat de medewerkers die voor de Opdrachtgever werkzaamheden verrichten zijn gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging. Geldende regelingen en instructies voor deze omgang zijn eenvoudig toegankelijk voor deze medewerkers. De Opdrachtnemer behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de Opdrachtgever. De medewerkers hebben een ondertekende geheimhoudingsovereenkomst getekend. b. Een geldig ISO27001 certificaat met een scope die het ontwerp, de productie, levering en onderhoud van TLC's omvat. c. Een onafhankelijke auditverklaring.
8.01.02	**Eis 4: De Opdrachtnemer beschikt over beleid voor het veilig gebruik van mobiele apparatuur die wordt ingezet voor beheer en onderhoud van TLC-installaties.** **Het beleid vereist ten minste dat:** • **uitsluitend door de Opdrachtnemer beheerde apparaten worden gebruikt;** • **apparaten voorzien zijn van actuele beveiligingsupdates;** • **medewerkers geïnstrueerd zijn over veilig mobiel werken.** De Opdrachtnemer toont naleving aan door middel van één van de volgende bewijsmiddelen: a. De Opdrachtnemer verklaart dat: a. medewerkers zijn zich bewust van het veilig werken met mobiele apparatuur en gegevensdragers. b. mobiele apparatuur actief worden onderhouden met patches en geen onnodige of irrelevante applicaties bevatten die niet nodig zijn voor het beheer en onderhoud van de TLC. c. voor beheer en onderhoud van VRI's door middel van mobiele apparaten alleen gebruik mag worden gemaakt van door de Opdrachtnemer beheerde apparaten ("Managed devices") waarop beveiligingsbeleid van toepassing is. d. alle betrokken medewerkers zich bewust zijn van de gevaren van mobiel werken. b. Een geldig ISO27001 certificaat met een scope die het ontwerp, de productie, levering en onderhoud van TLC's omvat. c. Een onafhankelijke auditverklaring.
8.04.01	**Eis 5: Toegang tot broncode, ontwikkeltools en softwarebibliotheken die worden gebruikt voor TLC-systemen wordt door de Opdrachtnemer beheerd via een formeel toegangsbeheerproces.** De Opdrachtnemer toont naleving aan door middel van één van de volgende bewijsmiddelen: a. De Opdrachtnemer verklaart dat de toegang tot de broncode van de systeem software (zijnde niet de verkeersregelingen) van de TLC beperkt is tot daarvoor geautoriseerde personen en tegen onbedoeld wijzigen wordt beschermd. b. Een geldig ISO27001 certificaat met een scope die het ontwerp, de productie, levering en onderhoud van TLC's omvat.

	c. Een onafhankelijke auditverklaring.

2 Incidentbeheer en continuïteit management

BIO2 O-maatregel-nummer	Eisen aan de TLC, de productie/levering van de TLC en het onderhoud van de TLC
5.20.04	**Bepaling 6: De Opdrachtnemer verleent medewerking aan het verzamelen, veiligstellen en beschikbaar stellen van digitaal bewijsmateriaal met betrekking tot cybersecurityincidenten.**
5.20.05	**Bepaling 7: De Opdrachtnemer meldt kwetsbaarheden en informatiebeveiligingsincidenten die relevant zijn voor de dienstverlening aan de Opdrachtgever conform geldende cyberweerbaarheidswetgeving.** **Eis 8: In voortgangsrapportages van de Opdrachtnemer worden informatiebeveiligingsincidenten en de getroffen herstelmaatregelen opgenomen.**
5.24.07	**Bepaling 9: De onderhoudspartij:** **- voert werkzaamheden uit conform gemeentelijk beleid en vastgestelde procedures.** **- levert proactief input over operationele risico's, storingspatronen en beheerafhankelijkheden.**
5.26.02	**Bepaling 10: Informatiebeveiligingsincidenten worden afgedaan via een incidentbeheerproces. In het incidentbeheerproces is opgenomen dat incidenten indien relevant gemeld worden bij de in wet- en regelgeving aangewezen toezichthouders.**
5.27.01	**Eis 11: Informatiebeveiligingsincidenten worden door de Opdrachtnemer geanalyseerd om achterliggende oorzaken vast te stellen en verbetermaatregelen te identificeren.**
5.27.02	**Bepaling 12: De analyses van informatiebeveiligingsincidenten, inclusief de achterliggende oorzaken en de verbeteringen worden breed gedeeld met relevante partners om herhaling en toekomstige incidenten te voorkomen.**
5.28.01	**Eis 13: De Opdrachtnemer bewaart informatie met betrekking tot een (vermoedelijk) informatiebeveiligingsincident minimaal drie jaar. Dit betreft onder meer de informatie benodigd voor de analyse (waaronder logging), de oplossing en het advies.**
5.30.01	**Bepaling 14: De Opdrachtnemer werkt desgevraagd mee aan het door de Opdrachtgever opstellen van een continuïteitsplan, waarin mogelijke risico's/scenario's beschreven worden die de continuïteit van de systemen van de Opdrachtgever negatief kunnen beïnvloeden. Denk hierbij bijvoorbeeld aan stroom storingen, kabelschade, fysieke beschadiging, brand van de straatkast, inbraak, ramp of andere crisis situaties. Het plan geeft aan wat de impact is voor de dienstverlening van de Opdrachtgever en welke mitigerende maatregelen er door de Opdrachtnemer geïmplementeerd zijn.**
8.13.01	**Eis 15: Opdrachtnemer heeft een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld. 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.**
8.13.03	**Bepaling 16: Tijdens de onderhoudsperiode worden backups van de TLC software opgeslagen op een door de Opdrachtgever aangegeven locatie.**
8.13.04	**Bepaling 17: De Opdrahtnemer werkt desgevraagd mee aan het door de Opdrachtgever opstellen van een recoveryplan, waarmee o.a. een cyberaanval op de IT en OT wordt afgedekt.**

3 Ketenmanagement

BIO2 O-maatregel-nummer	Eisen aan de TLC, de productie/levering van de TLC en het onderhoud van de TLC
5.09.01	**Bepaling 18: De Opdrachtnemer geeft bij aanvang van het contract inzicht in de keten van toeleveranciers en eventuele risico's daarin, inclusief de afspraken en risicoverdeling m.b.t. (cyber)security.**
5.21.04	**Bepaling 19: Gedurende de looptijd geeft de Opdrachtnemer veranderingen in de keten van toeleveranciers door, inclusief risico's daarin. Dit omvat minimaal kwetsbaarheden en informatiebeveiligingsincidenten die de dienstverlening aan de overheidsorganisatie kunnen raken.**
8.07.01	**Eis 20: Ten behoeve van de TLC geïnstalleerde software en firmware moeten afkomstig zijn van vertrouwde bronnen.**
8.30.01	**Eis 21: Interne maatregelen van de Opdrachtnemer voor systeemontwikkeling zijn onverkort van toepassing op uitbestede ontwikkeling, aangevuld met maatregelen die volgen vanuit uitbestedingen.**

4 Kwetsbaarheden beheer

BIO2 O-maatregel-nummer	Eisen aan de TLC, de productie/levering van de TLC en het onderhoud van de TLC
5.14.04	**Eis 22: De Opdrachtnemer levert een lijst of overzicht van toegestaan netwerkverkeer (inbound en outbound) ter goedkeuring aan de Opdrachtgever. Het doel is alleen minimaal noodzakelijk verkeer toe te staan. De default instelling is deny-by-default.**
8.01.01	**Eis 23:** **a. Er mogen geen IP of andere netwerkgegevens in de vorm van stickers of documentatie in de straatkast aanwezig zijn.** **b. Er mogen geen aanmeldgegevens of andere digitale identiteiten in de straatkast genoteerd worden of achterblijven in de straatkast na werkzaamheden.** **c. Ongebruikte netwerkaansluitingen moeten uitgeschakeld of in-actief gemaakt worden.**
8.08.01	**Bepaling 24: Indien de Opdrachtgever melding maakt van een patch dan dient de Opdrachtnemer daarvoor een implementatieadvies ter kennis te brengen van de Opdrachtgever. Daarbij gelden de volgende doorlooptijden:** **1. voor een kritieke patch: maximaal 48 uur na melding door de Opdrachtgever, gerekend vanaf de eerstvolgende werkdag;** **2. voor een niet kritieke patch: maximaal twee maanden na melding door de Opdrachtgever.** **De Opdrachtnemer dient de patch, na Acceptatie door de Opdrachtgever van het implementatieadvies, conform het advies te realiseren.** **Indien de Opdrachtgever melding maakt van een patch dan dient de Opdrachtnemer voor de uitrol te voldoen aan de volgende doorlooptijden:** **1. voor een kritieke patch: maximaal 48 uur na melding door de Opdrachtgever, gerekend vanaf de eerstvolgende werkdag;** **2. voor een niet kritieke patch: maximaal twee maanden na melding door de Opdrachtgever.**
8.08.04	**Eis 25: Bedieningsprocedures behoren door de Opdrachtnemer te worden gedocumenteerd en beschikbaar te worden gesteld aan de Opdrachtgever.**
8.16.01	**Bepaling 26: Bij ontdekte nieuwe dreigingen (aanvallen) worden deze binnen geldende juridische kaders verplicht gedeeld met de daarvoor aangewezen Computer Emergency Response Team (CERT).**

5 Logging

BIO2 O-maatregel-nummer	Eisen aan de TLC, de productie/levering van de TLC en het onderhoud van de TLC
8.15.01	**Eis 27: Een logregel bevat minimaal:** **- Actie: de gebeurtenis of handeling die heeft plaatsgevonden.** **- Object: waarop de gebeurtenis of handeling effect had (bijvoorbeeld welk bestand, proces of systeem).** **- Resultaat: het resultaat van de gebeurtenis of handeling.** **- Oorsprong: het apparaat of de netwerklocatie van waaruit de gebeurtenis of handeling in gang is gezet.** **- Actor: identificatie van de persoon die of het proces dat de gebeurtenis in gang heeft gezet.** **- Tijdstempel: datum en tijdstip waarop de gebeurtenis of handeling plaatsvond.**
8.15.02	**Eis 28: Een logregel bevat nooit gegevens die tot het doorbreken van de beveiliging kunnen leiden.**
8.15.03	**Eis 29: Een overzicht van logbestanden die worden gegenereerd is gedocumenteerd en wordt beschikbaar gesteld aan de Opdrachtgever.**
8.15.04	**Eis 30: De bewaartermijn van logbestanden en gegevens in het Security Incident en Event Monitoring (SIEM) worden risicogericht bepaald, rekening houdend met het scenario dat aanvallers langdurig binnen zijn.**
8.15.05	**Eis 31: Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als informatiebeveiligingsincident via de procedure voor informatiebeveiligingsincidenten.**
8.16.03	**Eis 32: Logging en ontsluiting ten behoeve van SOC.** **De Opdrachtnemer draagt er zorg voor dat de installatie zodanig is ingericht dat beveiligingsrelevante gebeurtenissen worden vastgelegd, beschermd en beheerd.** **De Opdrachtnemer waarborgt dat deze loggegevens op verzoek van de Opdrachtgever zonder aanvullende kosten of beperkingen ontsloten kunnen worden naar een door of namens de Opdrachtgever ingerichte Security Operations Center (SOC)-dienstverlening.** **De ontsluiting voldoet minimaal aan de volgende voorwaarden:** **- Ondersteuning van gestandaardiseerde logprotocollen (bijv. syslog, API, of gelijkwaardig);** **- Mogelijkheid tot near real-time levering van loggegevens;** **- Borging van integriteit, volledigheid en tijdsynchronisatie van logdata;** **- Documentatie van het logformaat en de semantiek van gebeurtenissen;** **- Geen afhankelijkheid van leveranciersspecifieke tooling voor uitlezing.**
8.16.04	**Eis 33: Actieve netwerkcomponenten zijn voorzien van logging en monitoring van die logging om afwijkende gebeurtenissen te kunnen waarnemen en daarop te reageren.**
8.18.02	**Eis 34: Het gebruik van systeemhulpmiddelen wordt gelogd.** **De logging is een halfjaar beschikbaar voor onderzoek.**

6 Ontwerp

BIO2 O-maatregel-nummer	Eisen aan de TLC, de productie/levering van de TLC en het onderhoud van de TLC
5.20.06	**Eis 35: De TLC dient zodanig te worden ontworpen, gebouwd en geconfigureerd dat:** **1. De VRI te allen tijde in staat is zelfstandig (standalone) het verkeer te regelen, ook in het geval van uitval, verstoring of afwezigheid van enige netwerkverbinding met externe systemen of centrale verkeersmanagementsystemen.** **2. In situaties van netwerkuitval dient de TLC minimaal haar laatst ingestelde verkeersregelingen, dan wel een vooraf vastgestelde fallback-regeling, zelfstandig en correct te kunnen uitvoeren zonder dat de verkeersveiligheid of verkeersdoorstroming in gevaar komt.** **3. Herstel van de netwerkverbinding mag geen verstoring veroorzaken in de autonome verkeersregeling en moet zonder herstart van de TLC kunnen plaatsvinden.**
8.03.01	**Eis 36:** **a. Het openen en sluiten van de segmenten van de straatkast wordt door middel van deurcontacten automatisch gemeld en in de elektronische logboeken van de automaat en de beheercentrale vastgelegd.** **b. De bedienconsole van de TLC (Web GUI) meldt ongebruikte sessies automatisch af na maximaal 15 minuten.** **c. Het bedieningspaneel mag bij niet ingelogde sessies geen (netwerk)configuratie gegevens tonen.**
8.07.04	**Eis 37: De Opdrachtnemer garandeert dat gebruikte software, inclusief firmware, bij levering:** **a. gecontroleerd is op malware,** **b. dat de herkomst geverifieerd is en** **c. dat de software actueel is.**

7 Segmentering

BIO2 O-maatregel-nummer	Eisen aan de TLC, de productie/levering van de TLC en het onderhoud van de TLC
7.01.02	**Eis 38: De straatkast van de VRI moet uit de volgende fysiek apart afsluitbare segmenten (beveiligingszones) bestaan:** **- Automaatdeel ; bevat besturingselektronica en datacommunicatie apparatuur** **- Energiedeel; bevat het aansluitbord op de stroomvoorziening van de netbeheerder** **- Bedienpaneel; lokale bediening van de VRI door beheerders en politie.**
8.05.01	**Eis 39: De TLC ondersteunt expliciete configuratie van externe IP-diensten (zoals DNS, NTP en logging) en levert deze diensten niet zelf.** **Bepaling 40: Tijdens de onderhoudsperiode maakt Opdrachtnemer uitsluitend gebruik van de door de Opdrachtgever beschikbaar gestelde voorziening voor beheer en onderhoud op afstand ten behoeve van de VRI. Alternatieve methodes voor beheer op afstand zoals bijvoorbeeld TeamViewer en andere vormen van "back door" toegang zijn nadrukkelijk niet toegestaan omdat deze het beveiligingsbeleid van de Opdrachtgever nadelig beïnvloedt.**

8 Toegangsbeveiliging

BIO2 O-maatregel-nummer	Eisen aan de TLC, de productie/levering van de TLC en het onderhoud van de TLC
5.15.01	**Eis 41:** **a. Er moeten fysieke maatregelen toegepast worden om de datacommunicatie apparatuur en de daarop aangesloten netwerkbekabeling af te schermen van de openbare ruimte.** **b. De gemeente stelt cilindersloten ter beschikking voor de verschillende segmenten van de straatkast.** **c. Het gebruik van persoonlijke apparatuur (Bring Your Own Device) voor beheer en onderhoud van een VRI installatie op straatniveau is niet toegestaan. Voor dit doel dient de Opdrachtnemer een beheerd en veilig apparaat ter beschikking te stellen.**
5.16.01	**Eis 42: Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.**
5.16.02	**Eis 43:** **a. Indien lokaal op de TLC gebruik wordt gemaakt van groepsaccounts wordt dit afgestemd met de Opdrachtgever.** **b. De Opdrachtgever bepaalt de autorisaties voor toegang tot de TLC. In basis wordt hierbij gebruik gemaakt van de IVERA indeling.** **Bepaling 44: Tijdens de onderhoudsperiode van een installatie brengt de Opdrachtnemer uitsluitend wijzigingen aan op de accounts van de TLC op aanvraag van de Opdrachtgever. Het maken en/of aanpassen van accounts met bijzondere rechten is niet toegestaan.**
5.17.01	**Eis 45: Gedurende de FAT procedure van een TLC dienen alle fabriekswachtwoorden vervangen te worden door wachtwoorden aangeleverd door de Opdrachtgever. De FAT is het moment waarop het wachtwoordbeleid van de Opdrachtgever van start gaat.** **Bepaling 46: Indien de TLC geen gebruik kan maken van centrale authenticatie dient de Opdrachtnemer een register bij te houden waaruit blijkt welke personen bevoegdheden hebben gekregen en welke functie zij bekleden.**
5.18.01	**Eis 47: De Opdrachtnemer waarborgt dat de TLC, inclusief de specifieke applicatiesoftware, het besturingssysteem en alle overige systeemcomponenten, maar exclusief de regelapplicatie, is voorzien van geïntegreerde security-logging conform de normen uit de Baseline Informatiebeveiliging Overheid (BIO2). De logging moet ten minste voorzien in:** **- Registratie van beveiligingsrelevante gebeurtenissen, waaronder authenticatiepogingen (geslaagd en niet geslaagd), software-updates, beheerhandelingen en pogingen tot ongeautoriseerde toegang.** **- Scheiding van functionele logging en security-logging, waarbij beveiligingslogbestanden onafhankelijk van de verkeerskundige logbestanden worden opgeslagen en beheerd.** **- Documentatie van logformats, loginhoud en bewaartermijnen, zodat de Opdrachtgever de logging eenvoudig kan integreren in de bredere beveiligingsmonitoring en auditprocessen.** **Afwijkingen van de loggingfunctionaliteit, beperkingen of uitsluitingen worden vooraf schriftelijk gemeld en zijn slechts toegestaan na expliciete schriftelijke instemming van de Opdrachtgever.**

5.18.02	**Eis 48: Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld.**
7.06.01	**Eis 49: Toegang tot de straatkast is gelimiteerd tot daarvoor geautoriseerd en bevoegd personeel voor het uitvoeren van hun werkzaamheden.**
8.07.03	**Eis 50: De gebruikte antimalware-software en bijbehorende herstelsoftware zijn actueel en wordt ondersteund door periodieke updates.**
8.18.01	**Eis 51: Alleen bevoegd personeel heeft, op die momenten dat toegang strikt noodzakelijk is, toegang tot systeemhulpmiddelen.**
8.19.01	**Eis 52: Het is niet toegestaan ongeautoriseerde software op de installaties te installeren.** **Eis 53: De Opdrachtnemer levert ter autorisatie voor aanvang van de FAT een overzicht aan van alle gebruikte software componenten.**
8.20.02	**Eis 54:** **a. De segmenten van de straatkast zijn voor verschillende toepassingen. Gebruikers zijn alleen geautoriseerd voor specifieke segmenten van de straatkast die passen bij hun functie.** **b. Communicatie interfaces voor data en voor beheer dienen gescheiden te zijn.**
8.21.01	**Eis 55: Communicatie met een cloud/SaaS of gemeentelijke backoffice dient alleen geauthenticeerd en versleuteld plaats te vinden.**
8.21.02	**Eis 56: TLC-systemen mogen alleen communiceren via vooraf door de Opdrachtgever geautoriseerde beveiligde netwerken (bijv. VPN, DNS, NTP, VLOG, TLEX).**
8.21.04	**Eis 57: Communicatie met de TLC zoals VLOG, IVERA, CCOL commando parser en andere interfaces dienen over een encrypted channel plaats te vinden.**
8.22.01	**Eis 58:** **a. De TLC wordt geïnstalleerd in een beveiligde netwerkzone conform de inrichting verstrekt door de Opdrachtgever.** **b. Toegang tot de (applicaties van de) TLC is gebaseerd op rollen en daarbij passende rechten.**
8.24.04	**Eis 59: Verbindingen met de TLC vinden plaats over een met minimaal TLS versie 1.3 beveiligde verbinding.**
8.27.01	**Eis 60: De algemeen gangbare principes van security by design zijn uitgangspunt bij de ontwikkeling en inrichting van software en systemen. Hieronder valt tenminste, maar niet uitsluitend:** **- Standaardwachtwoorden moeten verwijderd of gewijzigd worden.** **- Niet-noodzakelijke services en poorten moeten worden uitgeschakeld.** **- De TLC genereert beveiligings- en systeemlogregels en kan deze afleveren aan een centrale logvoorziening.** **- Security logging moet standaard geactiveerd zijn.** N.B. Netwerkverkeer van de VRI/TLC wordt op aangeven van de Opdrachtgever per functionaliteit verdeeld over verschillende VLANs. Zo is er bijvoorbeeld een separaat VLAN voor IO, voor beheer, en voor verkeersgegevens.

9 Wijzigingbeheer en testen

BIO2 O-maatregel-nummer	Eisen aan de TLC, de productie/levering van de TLC en het onderhoud van de TLC
8.29.01	**Eis 61:** **a. Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.** **b. Van de resultaten van de testen wordt verslag gemaakt.**
8.31.01	**Eis 62: De Opdrachtnemer draagt zorg voor de beschikbaarheid van representatieve testfaciliteiten ten behoeve van TLC's om tests in de productieomgeving te voorkomen.**
8.31.02	**Eis 63: Significante wijzigingen in de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar kan hiervan worden afgeweken.**
8.32.01	**Eis 64: In het wijzigingsbeheerproces is minimaal aandacht besteed aan:** **- het administreren van wijzigingen, met de resultaten van het testplan;** **- een risicoafweging van mogelijke gevolgen van de wijzigingen, inclusief een beschreven rollbackplan;** **- de goedkeuringsprocedure voor wijzigingen.**
8.34.01	**Eis 65: Voor de levering van de TLC wordt bij de FAT een securitytest uitgevoerd. Dit omvat minimaal:** **-verificatie van remote access (alleen toegang via geautoriseerd toegangspad)** **-verificatie van netwerksegmentatie (alleen geautoriseerde datastromen)** **-verificatie van hardening (geen standaardaccounts, alleen noodzakelijke poorten open)**

10 Overig

BIO2 O-maatregel-nummer	Eisen aan de TLC, de productie/levering van de TLC en het onderhoud van de TLC
7.10.02	**Eis 66: Gegevensdragers zoals flashkaart/USB-sticks en andere verwijderbare media die gegevens van de Opdrachtgever bevatten mogen alleen de organisatie verlaten of elders opnieuw worden ingezet nadat de inhoud onherstelbaar is verwijderd.**