

Eis toegevoegd op datum	Eis Gewijzigd op datum	MR #	Purdue level	Onderwerp	Eis ID nr (Gemeente)	Eis tekst	Opmerking	Eis Status	Baseline standaard (SL 1 of SL 1' of SL 1'') (zie Hfd 3)	Toelichting	Organisatie	Baseline document versie (oude document versie bewaren)
24-jun-26		Installatie	0-1-2	Fysieke toegang	FT 1	Inbraakwering: De installatie dient een inbraakwerende behuizing te hebben met toegangsbeveiliging geregeld via fysieke of elektronische sloten en/of -sleutels (elektronische sloten hebben de voorkeur). Noot: Indien een afgesloten behuizing onmogelijk is, moeten rondom de installatie extra maatregelen genomen te worden om de fysieke toegang te ontmoedigen. Hiervoor dient de opdrachtnemer een risico analyse uit te voeren en dit te bespreken met de Gemeente Haarlem-Zandvoort. Enkele voorbeelden zijn: anti klim obstakels (op een paal), het afsluiten van toegangswegen (hekwerk, onderhoudsladder etc), een hek met een Art.461 bord, of vergelijkbare maatregelen.	Deze eis geldt met name voor kasten die in de openbare ruimte worden geplaatst (buitenruimte / straatkast zoals een VRJ) maar deze eis kan ook van toepassing zijn op kasten binnen (afgesloten) ruimtes.	Actief	IEC 62443-3-3 (systeem nivo), raakvlak met FR 1 en FR 2 als invulling		Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Fysieke toegang	FT 2	Inbraakwering: Componenten en/of apparatuur die zich buiten de (installatie) kast(en) bevinden en in de openbare/buiten ruimte gemonteerd worden dienen: - m.b.t. de behuizing voorzien te worden van bijv. veiligheidsschroeven, dropkeys, - vandalisme bestendig behuizing of door een afdoende beschermende bescherming.		Actief	IEC 62443-4-2 (component nivo - manipulatiebestendigheid van hardware in het "veld"), raakvlak met EDR 3.11 tamper resistance neemt toe door vandalisme bestendige behuizingen (zoals een hogere IK-klasse) tamper detection toepassen zoals open luik / open deur schakelaars met doormelding		Project en Beheer & Onderhoud	V1.0
					FT 4	Vandalisme: Er dienen maatregelen genomen te worden dat buiten bekabeling (energie en data) zie zichtbaar zijn, zodanig afgeschermd wordt dat de kabels niet verwijderd en/of doorgeknipt en/of veranderd/gewijzigd kunnen worden.					Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Fysieke toegang	FT 8	Vandalisme: Er dienen maatregelen genomen te worden dat apparatuur in openbare / buiten ruimte zodanig wordt geplaatst dat fysieke sabotage / vandalisme tot een minimum wordt beperkt. Voorbeeld hoogte en positie van de apparatuur en/of anti-klim obstakels op een paal , extra verstevigde behuizing/afscherming etc.		Actief			Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Logische toegang	LT 1	Account management: Toegestaan zijn: - Groepsaccounts op level 0-1 en - Privilege accounts op level 2 en hoger (via vb. LDAP, Active Directory) Noot: zie purdue model voor de definities van de levels		Actief			Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Logische toegang	LT 2	Controle: De Gemeente heeft het recht om controles uit te voeren op de naleving van het logische toegangsproces van de Opdrachtnemer.		Actief			Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Logische toegang	LT 3	Toegangsrechten: De toegangsrechten van alle medewerkers (bedienaars, beheerders en overig ondersteunend personeel) dienen minimaal eenmaal per halfjaar te worden beoordeeld en geactualiseerd in een formeel proces. Opvolging van de bevindingen wordt gedocumenteerd en wordt behandeld als een beveiligingsincident.		Actief			Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Logische toegang	LT 4	Toegangsbeheer: Alle type accounts (op alle levels) dienen op uniforme wijze te worden beheerd. Er dient een geborgde procedure te bestaan m.b.t. het toegangsbeheer bij functiewisseling of vertrek (in-, door- en uitstroming).		Actief	De norm eist in deel 2-1 dat er een gedocumenteerd proces is dat garandeert dat fysieke en digitale toegangsrechten direct worden aangepast bij een functiewijziging, en per direct worden ingetrokken zodra een medewerker (of externe partij) uit dienst treedt. Component Dit vereist dat apparaten (zoals netwerkswitches of HMI's) centrale authenticatie-protocollen ondersteunen (zoals RADIUS, TACACS+ of Active Directory integratie) zodat er geen lokale, losse accounts op de apparaten zelf beheerd hoeven te worden.		Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Logische toegang	LT 5	Toegangsbeleid: De Gemeente Haarlem-Zandvoort specificeert op welke wijze logische toegang (op afstand) plaatsvindt en welke beveiligingsmaatregelen van toepassing zijn zodat strikte toegang verzekerd wordt en blijft dat dit de enige manier is om (op afstand) toegang te krijgen tot de installatie. Bij remote toegang om beheer of diagnose activiteiten uit te voeren op het OT netwerk van de Gemeente Haarlem-Zandvoort dient gebruik te worden gemaakt van de diensten die de Gemeente Haarlem-Zandvoort hiervoor beschikbaar stelt.		Actief			Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Logische toegang	LT 6	Beheerders, bedienaars en overig ondersteunend personeel (dienen te) worden ondersteund in het beheren van hun wachtwoorden door het gebruik van een wachtwoordkluis.	welke eisen zijn van toepassing m.b.t. de digitale wachtwoordkluis	Actief	Een wachtwoordkluis is een organisatorisch hulpmiddel om te voldoen aan de eisen voor (IEC 62443-2-1: Security program requirements for IACS asset owners): Element: Personnel Security (Personeelsbeveiliging) Element: Operational Security Procedures (Operationele beveiligingsprocedures) De norm eist dat de organisatie ervoor zorgt dat medewerkers in staat zijn om vertrouwelijk en veilig om te gaan met inloggegevens. Het aanbieden van een wachtwoordkluis helpt voorkomen dat medewerkers wachtwoorden opschrijven op post-its of bewaren in onbeveiligde Excel-lijsten. Bij een audit voor SL 2 of hoger controleert een auditor ook onze processen (deel 2-1).		Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Logische toegang	LT 7	Wachtwoorden/pincodes: Standaard wachtwoorden en/of pincodes dienen: - per direct te worden gewijzigd, - gedeelde wachtwoorden/pincodes zijn niet toegestaan, en - eisen voor wachtwoordsterkte moeten indien mogelijk technologisch afgedwongen worden voor beheerdersaccounts. Zie CSIR voor Installaties - bijlage "CSR bijlage CSIR 7 Wachtwoorden".		Actief	Note: Uitwerken van een break-glass scenario als gedeelde accounts verboden zijn.		Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Logische toegang	LT 8	Inactiviteit: Bij inactiviteit moet de sessie na een bepaalde periode automatisch vergrendeld worden. Voor het bepalen van de 'periode', zie CSIR voor Installaties - bijlage "CSR bijlage 7 Wachtwoorden".		Actief	Altijd van toepassing bij HDS devices zoals IPC, Panel PC (HMI)		Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Logische toegang	LT 9	Lock-out: na X-aantal foutieve inlog pogingen wordt de lock-out tijd actief.		Actief	SL 2 en hoger		Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Logische toegang	LT 10	Versleuteling: De benodigde gegevens voor identificatie, authenticatie en autorisatie dienen in versleutelde vorm te worden uitgewisseld en opgeslagen.		Actief			Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Logische toegang	LT 11	Logging inlogpogingen: Er dient een audit log van inlogpogingen beschikbaar te zijn.		Actief	SL 2 en hoger		Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Logische toegang	LT 12	Audit en systeem logs moeten beschermd zijn tegen verlies, wijziging en onbevoegde toegang.		Actief			Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Logische toegang	LT 13	Least Privilege: Toegang tot de installatie is standaard geblokkeerd tenzij toegestaan en dient geïmplementeerd te worden volgens het principe van Least Privilege, waarbij zo min mogelijk rechten aan een gebruiker worden toegekend.		Actief	Volgens SR 2.1 moet het systeem standaard alle privileges blokkeren en pas vrijgeven na succesvolle autorisatie. Om het 'Least Privilege'-principe werkbaar te maken, vereist SR 2.2 (verplicht vanaf SL 2) dat er rollen worden gedefinieerd (bijvoorbeeld: Operator, Engineer, Administrator). Gebruikers krijgen vervolgens alleen de specifieke rol toegewezen die noodzakelijk is voor hun taken.		Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Logische toegang	LT 14	Wachtwoorden/pincodes: Wachtwoorden en/of pincodes dienen regelmatig te worden gewijzigd. Zie bijlage "CSR 7 Wachtwoorden" m.b.t. de frequentie van wijzigen.		Actief	SR 1.7 eist dat het systeem mechanismen heeft om authenticatiegegevens (zoals wachtwoorden, pincodes en certificaten) veilig te beheren, te distribueren en in te trekken. Het periodiek dwingen tot een wijziging is een directe invulling van dit beheerproces.		Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Logische toegang	LT 15	Wachtwoorden/pincodes: Wachtwoorden dienen niet zichtbaar te zijn tijdens het intypen en dienen versleuteld verstuurd te worden. Zie bijlage "CSR 7 Wachtwoorden" m.b.t. de frequentie van wijzigen. Noot: Bij o.a. webpagina's die niet goed beveiligd zijn, kan men de wachtwoorden lezen tijdens het intypen Daarnaast is het mogelijk om het http protocol met netwerktools te bekijken waarbij de wachtwoorden in plane tekst zichtbaar zijn.		Actief	SIL 1 maskeren van wachtwoorden SIL 2 en hoger, SR 4.3/EDR 4.3 eist dat er cryptografische mechanismen worden gebruikt om gevoelige data (zoals wachtwoorden en pincodes) te beschermen tijdens transport. In de praktijk betekent dit het uitsluiten van onbeveiligde protocollen (zoals HTTP of Telnet) en het verplicht stellen van beveiligde varianten (zoals HTTPS of SSH).		Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Digitale weerbaarheid	HARD 1	Attack Surface Reduction: Voor zover mogelijk dienen: - alle onnodige services/applicaties/software/netwerkiterfaces verwijderd of gedeactiveerd te worden, - het aantal netwerkverbindingen dient geminimaliseerd te worden, - alle default accounts dienen uitgeschakeld te worden. - Firmware Signing: Alleen door de fabrikant digitaal ondertekende firmware kan worden geladen,	Camera's	Actief			Project en Beheer & Onderhoud	V1.0
1-sep-26		Installatie	0-1-2	Digitale weerbaarheid	HARD 1	Attack Surface Reduction: Voor zover mogelijk dienen: - Zero Exposed Ports: De fysieke behuizing van de nodes mag geen enkele externe fysieke datapoort bevatten (zoals USB, RJ45 of seriële pinnen). Alle communicatie ten behoeve van onderhoud, service of configuratie dient uitsluitend via beveiligde, versleutelde draadloze protocollen plaats te vinden.				Aan buitenzijde van kasten, apparatuur etc mogen geen fysieke poorten zichtbaar zijn.	Project en Beheer & Onderhoud	V1.0

24-jun-26		Installatie	0-1-2	Digitale weerbaarheid	HARD 2	Versleuteling: de installatie dient zo ingesteld te worden dat het netwerkverkeer van de installatie (voor zover mogelijk) via versleutelde protocollen verloopt. Netwerkverkeer voor het configureren van de installatie is enkel toegestaan wanneer sprake is van versleuteling in het gebruikte communicatieprotocol (SSL, TLS 1.3) of in het kanaal waarlangs deze communicatie plaatsvindt. Noot: Versleuteling van netwerkverkeer kan op alle levels van het purdue model voorkomen. Veel installaties / apparatuur bevinden zich in de openbare / buiten ruimte waardoor netwerkversleuteling toegepast dient te worden. Onveilige protocollen mogelijk niet gebruikt worden.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Digitale weerbaarheid	HARD 3	Logging: De installatie moet logbestanden aanmaken waarin minimaal: - alle beheershandelingen en mislukte wijzigings- of inlogpogingen worden geregistreerd en - alle relevante bedienaarshandelingen (setpoints, configuratie/parameter) zijn vastgelegd.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Digitale weerbaarheid	HARD 4	Patching: de installatie dient zo ingesteld te worden dat updates voor de geïnstalleerde software minimaal eens per jaar ontvangen en uitgevoerd kunnen worden. Indien patches/firmware om bepaalde redenen bewust niet worden uitgevoerd, dient de afweging hiertoe schriftelijk te worden vastgelegd voorzien van een risicoafweging, inclusief een mitigatievoorstel. Indien zowel de kans op misbruik als de verwachte schade hoog zijn, wordt de betreffende patch in overleg met Opdrachtgever (direct) ingepland voor implementatie.	Patching	Actief	Overige VRIs			Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Digitale weerbaarheid	HARD 4	Patching: de installatie dient zo ingesteld te worden dat updates voor de geïnstalleerde software minimaal 2 keer per jaar ontvangen en uitgevoerd kunnen worden. Indien patches/firmware om bepaalde redenen bewust niet worden uitgevoerd, dient de afweging hiertoe schriftelijk te worden vastgelegd voorzien van een risicoafweging, inclusief een mitigatievoorstel. Indien zowel de kans op misbruik als de verwachte schade hoog zijn, wordt de betreffende patch in overleg met Opdrachtgever (direct) ingepland voor implementatie.	Patching	Actief	Overige VRIs	Baseline +		Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Digitale weerbaarheid	HARD 7	Back-up & Fail-safe: Bij uitval of compromitatie van software (onderdelen) dient de installatie per direct terug te vallen op een fail-safe modus om te verzekeren dat dit niet tot gevaarlijke situaties leidt. Er moeten back-ups beschikbaar zijn om het systeem/installatie vanuit de fail-safe modus te herstellen naar een veilig en functioneel werkend systeem en operationeel proces.		Actief				Project en Beheer & Onderhoud	V1.0
1-sep-26		Installatie	0-1-2	Digitale weerbaarheid	HARD 7.0	Back-up & Fail-safe: De nodes dienen uitgerust te zijn van een interne energiebuffer (bijv. een supercondensator/batterij). Bij acute fysieke sabotage of het doorknippen van de voedingskabel dient de node over voldoende reststroom te beschikken om het alarm inclusief de statusomstandigheden succesvol via het netwerk te verzenden alvorens uit te vallen.						Project en Beheer & Onderhoud	V1.0
24-jun-26		Installatie	0-1-2	Digitale weerbaarheid	HARD 8	Antimalware voorzieningen moeten worden ingezet in overeenstemming met de Gemeente Haarlem-Zandvoort, waarbij de opdrachtnemer, beheerder dient aan te kunnen tonen dat de antimalware software correct is geïnstalleerd en geconfigureerd. De juiste werking dient hierbij te worden aangetoond.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Netwerk	0-1-2	Monitoring	MON 1	De Opdrachtnemer dient indien de installatie welke niet (permanent) op het Security Operations Centre is aangesloten zijn medewerking te verlenen voor het incidenteel kunnen uitlezen van de lokale installatie netwerkverkeer of een specifiek deelinetwerk van de installatie.	Installatie is niet aangesloten op een SOC	Actief				Project en Beheer & Onderhoud	V1.0
28-jul-26		Netwerk	0-1-2	Monitoring	MON 2	De Opdrachtnemer dient over een operationeel proces te beschikken als onderdeel van het incidentmanagementproces voor het melden van incidenten aan de Gemeente Haarlem-Zandvoort.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Netwerk	0-1-2	Monitoring	MON 3	Logging Configuratie: De netwerkkapparatuur (bijv. virtuele) servers, routers, modems, firewalls) moet zo ingesteld worden dat (iedere poging tot) het veranderen van de configuratie gelogd wordt. Als er geen automatische analyse plaatsvindt, moeten deze loggegevens bij een storing geanalyseerd worden om onverwachte gebeurtenissen te herkennen.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Netwerk	0-1-2	Monitoring	MON 4	Real-time Monitoring van Data: Er dient real-time monitoring aanwezig te zijn op dataverkeer binnen het netwerk. Dit verkeer dient op een geautomatiseerde wijze geanalyseerd te worden om afwijkingen in bestaande patronen te herkennen. Gedetecteerde afwijkingen dienen voor minstens drie maanden te worden bewaard en moeten wekelijks een review ondergaan.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Netwerk	0-1-2	Monitoring	MON 5	Beschikbaarheidsmonitoring: Het netwerk moet zo ingericht worden dat er periodiek (Interval < 1h) een automatische check plaatsvindt of netwerkkapparatuur nog bereikbaar is. Wanneer een systeem niet reageert op deze check, dient dit gelogd en gemeld te worden. Deze uptime gegevens dienen bewaard te worden voor historische analyse. Noot: Bewaartermijn is 12 maanden (ringbuffer volgens First-In / First-out)		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Netwerk	0-1-2	Monitoring	MON 6	Kwetsbaarhedenmonitoring: Er dient regelmatig (ieder jaar) een scan uitgevoerd te worden op de netwerkkapparatuur (bijv. virtuele) servers, routers, modems, firewalls) om te bepalen of deze bekende kwetsbaarheden hebben. Deze scan dient: - op een wijze uitgevoerd te worden dat het functioneren van OT-installaties niet merkbaar gehinderd wordt, - op basis van de AS-IS informatie vastgelegd en bijgehouden in de CMDB		Actief				Beheer & Onderhoud	V1.0
24-jun-26		Netwerk	0-1-2	Netwerkkarchitectuur	NA 1	Opdrachtnemer draagt zorg voor en ziet erop toe dat bij netwerkkoppelingen tussen de installatie en de centrale netwerken van de Gemeente de aansluitvoorwaarden van de Gemeente in acht worden genomen. Voor remote logische toegang van personeel / medewerkers tot aan de installatie gekoppelde systemen moet de procedure gevolgd worden van de Gemeente waarbij de Installatie verantwoordelijke/-eigenaar de aanvraag verzorgt.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Netwerk	0-1-2	Netwerkkarchitectuur	NA 2	Netwerkdigram: Er dient een actueel overzicht te zijn van de architectuur van het netwerk (conform het purdue model) waarin is aangegeven welke systemen op welke netwerken zijn verbonden, hoe deze systemen met elkaar communiceren en welke protocollen hierbij gebruikt worden (bijv. een Entity Relationship Diagram, Database Model Diagram)		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Netwerk	0-1-2	Netwerkkarchitectuur	NA 3	Scheiding IT/OT omgeving: OT installaties/systemen dienen op level 0 t/m 3 geïnstalleerd te worden, de onderlinge communicatie verloopt dan via één of meer OT netwerken. OT netwerken (level 0 t/m 3) mogen nooit direct verbonden worden met het IT domein: Level 4 / 5 (KA omgeving) en level 6 (Datacenter / Cloud omgeving bij derde partijen). Indien een koppeling noodzakelijk is tussen OT en IT dient de infrastructuur ingericht te worden volgens de Purdue Enterprise Reference Architecture (PERA), waarbij er een duidelijke grens is aangebracht tussen het controle niveau (level 3) en het enterprise niveau (level 4, 5 & 6). Op deze grens dient een koppelvak met een extra laag authenticatie geïmplementeerd te worden. Zie CSIR bijlage 3 Noot: OT applicaties in de Cloud worden gezien als level 6 (SaaS). Deze applicaties mogen bij verstoring, uitval, compromitatie nooit de installatie (level 0 t/m 3) verstoren. Indien dit wel mogelijk is, dan dient de applicatie te verhuizen naar Level 3. Bij applicaties op level 6, zowel van IT als OT, zijn de SaaS eisen van toepassing. Dit is een separaat document aanvullend op de CSIR voor Installaties en deze baseline.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Netwerk	0-1-2	Netwerkkarchitectuur	NA 4	Segmentatie per OT type: Er dient een netwerk- en systeemscheiding aangebracht te worden tussen verschillende type OT installaties in het OT domein. Iedere OT type krijgt een eigen logisch- of fysiek netwerk, onderlinge communicatie dient tot een minimum beperkt te worden. OT systemen geplaatst in hun eigen netwerksegment kunnen uitsluitend met elkaar communiceren op vastgestelde koppelvakken die door de Gemeente Haarlem-Zandvoort bepaald en vastgelegd zijn. Zie CSIR bijlage 3 Bijv. Alle VRI's en bruggen hebben ieder een eigen netwerk. Communicatie tussen een VRI en brug is toegestaan uitsluitend op basis van vastgelegde principes).		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Netwerk	0-1-2	Netwerkkarchitectuur	NA 5	Segmentatie per installatie: Voor zover mogelijk dient ervoor gezorgd te worden dat er een netwerkscheiding is tussen verschillende installatie onderdelen. Bv Brug installatie: level 0 - veld IO, level 1 - control, level 2 - Scada. Zie CSIR bijlage 3		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Netwerk	0-1-2	Technische controle	TC 1	Koppelvlakken: Koppelvlakken tussen netwerksegmenten dienen zo ingericht te worden dat: 1. Communicatie niet van het ene naar het andere netwerksegment kan lopen zonder een centrale/speciale koppelvak te passeren en 2. Dataverkeer tussen netwerksegmenten geblokkeerd wordt tenzij dit plaatsvindt via goedgekeurde protocollen op vooraf gedefinieerde netwerkpopen en 3. Het dataverkeer dat door het koppelvak loopt gemonitord kan worden waar relevant.		Actief				Project en Beheer & Onderhoud	V1.0

24-jun-26		Netwerk	0-1-2	Technische controle	TC 2	Cryptografie: Binnen het netwerk dient waar mogelijk gebruik gemaakt te worden van protocollen die de voorkeur hebben van het NCSC of vergelijkbare organisaties. Waar mogelijk dienen openbare protocollen te worden verkozen boven een merkgelabeld protocol. Encryptie: Vereist: TLS1.3 Wanneer het voor een OT-systeem niet mogelijk is te communiceren via een veilig protocol, dienen aanvullende maatregelen genomen te worden om communicatie met deze systemen te beschermen, zoals additionele segmentatie, encryptie op verbindingsniveau, of vergelijkbare maatregelen.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Netwerk	0-1-2	Technische controle	TC 3	Hardening Netwerkkapitaal: Bij het configureren van netwerkkapitaal (bijv. (virtuele) servers, routers, modems, firewalls) dient rekening gehouden te worden met best-practices en hardening maatregelen die aanbevolen worden door de producent en/of cybersecurity expertisecentra (zoals bijv. NCSC, CIS, MITRE, DoD Cyber Exchange). Daarbij dient er voor alle netwerkkapitaal systemen ten minste voor gezorgd te worden dat: - De gebruikte software actief ondersteund wordt door de leverancier en dat aanbevolen (security) updates regelmatig geïnstalleerd worden - Alle niet-noodzakelijke diensten of applicaties op het systeem worden uitgeschakeld of verwijderd - Er gebruik gemaakt wordt van een anti-malware oplossing waar mogelijk, welke regelmatig (minimaal wekelijks) signature updates ontvangt.	Netwerk hardening, wekelijks	Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Netwerk	0-1-2	Technische controle	TC 4	Hardening systeem apparatuur / componenten: Bij het configureren van systemen en componenten (bijv. (virtuele) servers, PLC's, controllers, veldIO / frq regelaars etc) dient rekening gehouden te worden met best-practices en hardening maatregelen die aanbevolen worden door de producent en/of cybersecurity expertisecentra (zoals bijv. NCSC, CIS, MITRE, DoD Cyber Exchange). Daarbij dient er voor alle systemen / componenten ten minste voor gezorgd te worden dat: - De gebruikte software actief ondersteund wordt door de leverancier en dat aanbevolen (security) updates regelmatig geïnstalleerd worden - Alle niet-noodzakelijke diensten of applicaties op het systeem worden uitgeschakeld of verwijderd - Er gebruik gemaakt wordt van een anti-malware oplossing waar mogelijk, welke regelmatig (minimaal wekelijks) signature updates ontvangt.	Componenten / apparatuur, kwartaal	Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Netwerk	0-1-2	Technische controle	TC 5	Disaster Recovery: Er dient een recoveryplan opgesteld te worden om na uitval de installatie, netwerk(en) binnen een bepaalde periode (nader te bepalen per OT object type -> SLA onderbrengen) te kunnen herstellen. Voor het uitvoeren van dit plan dienen de volgende technische oplossingen te worden overwogen: - Back-ups van het OT netwerk en systeem delen die essentieel zijn voor het functioneren van het installatie (OP processen), - Redundancy-systemen, waardoor bij uitval overgeschakeld kan worden naar andere hardware zonder significante onderbreking. Noot: De bepaalde periode is door de Opdrachtgever bepaald of indien nog niet bepaald dan wordt deze periode in overleg met de Opdrachtgever nader bepaald per OT object type. De eis dient in de SLA opgenomen te worden t.b.v. beheer en onderhouds periode		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Netwerk	0-1-2	Technische controle	TC 6	Hardening systeem apparatuur / componenten: Bij het configureren van systemen en componenten (bijv. (virtuele) servers, PLC's, controllers, veldIO / frq regelaars etc) dient rekening gehouden te worden met best-practices en hardening maatregelen die aanbevolen worden door de producent en/of cybersecurity expertisecentra (zoals bijv. NCSC, CIS, MITRE, DoD Cyber Exchange). Daarbij dient er voor alle systemen / componenten ten minste voor gezorgd te worden dat: - De gebruikte software actief ondersteund wordt door de leverancier en dat aanbevolen (security) updates regelmatig geïnstalleerd worden - Alle niet-noodzakelijke diensten of applicaties op het systeem worden uitgeschakeld of verwijderd - Systemen die geen verbinding hebben met internet / AV server (virus patronen) dienen jaarlijks handmatig, offline via USB software, gescand te worden.	Componenten / apparatuur, offline	Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Netwerk	0-1-2	Technische controle	TC 7	Tijdsynchronisatie: Alle apparaten binnen het OT-netwerk moeten synchroon lopen via een beveiligde tijdbron (zoals een beveiligde NTP-server).		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Kennis en kunde	KEN 1	Toelichting: van belang om de exacte volgorde van gebeurtenissen te reconstrueren bij een Incident. Opleiding en Vaardigheden: Bedienaars, beheerders en overig ondersteunend personeel dienen aantoonbaar over de benodigde (technische) vaardigheden te beschikken om systemen op een veilige manier te beheren. Hiervoor dienen periodieke cybersecurity trainingen gevolgd te worden, (bijv. awarenesscursussen, trainingen en E-Learning) en worden passende opleidingsmogelijkheden geboden voor functie-specifieke kennis. Wanneer uit evaluatie blijkt dat beheerwerkzaamheden niet op een veilige manier plaatsvinden wegens gebrek aan kennis bij personeel, wordt dit als beveiligingsincident gezien.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Kennis en kunde	KEN 2	Verantwoordelijkheden: Bedienaars, beheerders en overig ondersteunend personeel zijn zich bewust van zijn of haar verantwoordelijkheden rondom Cybersecurity. Het personeel handelt proactief en kaart afwijkingen, problemen, (potentiële) risico's en incidenten tijdig aan zodat deze onderzocht en/of verholpen kunnen worden.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Kennis en kunde	KEN 3	Veilig Beheer: Er wordt zorg gedragen voor de risico's die het uitvoeren van beheerswerkzaamheden met zich meebrengt. Bedienaars, beheerders en overig ondersteunend personeel dienen zich bewust te zijn van beleidsregels, gemaakte afspraken en beheerprocedures die relevant zijn voor het (veilige) beheer van een installatie. Dit wordt behandeld bij indiensttreding en bij significante wijzigingen wordt bestaand personeel geïnformeerd. In deze werkspraken dienen de volgende maatregelen in acht genomen te worden: - Bij beheerwerkzaamheden wordt alleen apparatuur gebruikt die geschikt is voor dat doel. Laptops of smartphones die gebruikt worden voor beheerwerkzaamheden dienen beschermd te worden tegen malware. Er worden geen apparaten voor persoonlijk gebruik gekoppeld aan systemen van de gemeente (met uitzondering van systemen voor publiek gebruik). - Bij de uitvoering van werkzaamheden worden beveiligingsmaatregelen niet omzeild of tijdelijk uitgeschakeld. Dit betekent ook dat er geen netwerkkoppelingen opgezet worden die beveiligde koppelingen omzeilen.		Actief				Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Kennis en kunde	KEN 4	Toegangsmiddelen: Bedienaars, beheerders en overig ondersteunend personeel dragen zorg voor het gedegen beheer van verleende toegangsmiddelen (bijv. wachtwoorden, sleutels, keycards, pincodes). Dit omvat ten minste de volgende maatregelen: - Personeel is verplicht en wordt expliciet geïnstrueerd om geen wachtwoorden te gebruiken die zij ook elders gebruik(t)en. Personeel wordt daarbij gewezen op hulpmiddelen voor wachtwoordbeheer. - Personeel is verplicht hun toegangsmiddelen niet met anderen te delen en niet op een voor anderen toegankelijke wijze te bewaren. Dit betekent ook dat er, voor zover mogelijk, geen gebruik wordt gemaakt van gedeelde accounts. - Voor accounts worden, waar mogelijk, altijd minstens 12 tekens gebruikt voor wachtwoorden en wordt gebruik gemaakt van een vorm van Multi-Factor Authenticatie (MFA/2FA). - Na het afronden van werkzaamheden dient de (fysieke) toegang opnieuw afgesloten te worden. Zie paswoord beleid van de Gemeente Haarlem-Zandvoort (zie CSIR voor installaties - bijlage 7).		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Incident Response & Disaster Recovery	IPP 1	Er dient een geborgde procedure te bestaan die regelt dat bedienaars, beheerders en overig ondersteunend personeel (zowel van Gemeente als die van externe partijen) beveiligingsincidenten en zwakke plekken in de beveiliging in systemen en diensten zo snel mogelijk melden bij de Installatie verantwoordelijke/-beheerder die de registratie bijhoudt en rapporteert.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26	21-jul-26	Beheer	0-1-2	Incident Response & Disaster Recovery	IPP 2	Opdrachtnemer stelt een Incident / Cyber Security Manager aan met bijbehorende verantwoordelijkheden voor Cybersecurity en informatiebeveiliging in het project en/of in Beheer & Onderhouds organisatie.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Incident Response & Disaster Recovery	IPP 3	Er bestaat een geborgde procedure voor de reactie op en eventuele escalatie van security incidenten. De security incidenten worden vastgelegd, gerapporteerd, gerouteerd, geanalyseerd, gekwantificeerd en afgewikkeld in relatie tot de ernst van het incident.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Incident Response & Disaster Recovery	IPP 4	De Opdrachtnemer draagt zorg voor aansluiting en borging van het eigen incidentmanagementproces op dat van de Gemeente.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Incident Response & Disaster Recovery	IPP 5	Er dient een operationeel incident response plan te bestaan voor reactie op en afhandeling van incidenten en calamiteiten.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Incident Response & Disaster Recovery	IPP 6	Er dient een operationeel recovery plan te bestaan voor recovery na incidenten of calamiteiten.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Incident Response & Disaster Recovery	IPP 7	Jaarlijks dienen de incident response en recovery te worden beproefd aan de hand van een actueel oefenplan om te bewerkstelligen dat ze doeltreffend blijven. Onderdeel van de jaarlijkse oefening is het testen van de noodbediening indien deze aanwezig is.	kritisch - jaarlijks niet kritisch - 2 jaarlijks risico profiel is belangrijk.	Actief	in SLA opnemen			Beheer & Onderhoud	V1.0

24-jun-26		Beheer	0-1-2	Incident Response & Disaster Recovery	IPP 8	Meldingsplicht: Bedienaars, beheerders en overig ondersteunend personeel dienen beveiligingsincidenten, storingen, verdachte situaties of zwakke plekken in systemen aan te kaarten bij het relevante meldpunt of persoon. Significante risico's moeten ook aan het verantwoordelijke management of bestuur worden gecommuniceerd.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Incident Response & Disaster Recovery	IPP 9	Incident Response: Cybersecurity incidenten dienen geregistreerd te worden en op een traceerbare en zorgvuldige wijze afgehandeld te worden. Er dient een escalatie procedure opgesteld te worden, waarin een overzicht beschikbaar is met verantwoordelijkheden en contactgegevens.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Incident Response & Disaster Recovery	IPP 10	Disaster Recovery: Voor alle installatietypes onder het beheer van de beheerorganisatie dient in overleg te worden bepaald voor welke periode uitval acceptabel is in een zogenaamde Recovery Time Objective (RTO). De bepaling van de RTO houdt rekening met de impact op de organisatie en de omgeving. Op basis van de vastgestelde RTO's stelt de beheerorganisatie een Disaster Recovery Plan op voor de verschillende installatietypes. In dit plan wordt aangegeven welke middelen en gegevens nodig zijn voor herstel (bijvoorbeeld backups en personeel) en welke stappen vereist zijn om het herstel uit te voeren.	RTO tijden dienen bepaald te worden door de Gemeente. Indelen in gradaties mbt respons tijden. RTO voor VRI bestaan. Respons tijden is anders dan hersteltijd (functioneel herstel)	Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Incident Response & Disaster Recovery	IPP 11	Incident Evaluatie: Er dient periodiek, of na een significant incident, een evaluatie te zijn van (bijna) incidenten in het verleden om te bepalen: Wat de oorzaak van het incident was, of de incident respons effectief was en of er relevante verbeteringen/lessons learned zijn.		Actief	in SLA opnemen			Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Incident Response & Disaster Recovery	IR-DR 12	Oefening: Er dient jaarlijks een oefening plaats te vinden waarbij de beschikbare respons- en herstelplannen getoetst worden. Als onderdeel van dit proces dienen de verantwoordelijkheden benadrukt te worden en de documentatie bijgewerkt te worden.		Actief	in SLA opnemen	Baseline +		Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Incident Response & Disaster Recovery	IR-DR 12	Oefening: Er dient twee jaarlijks een oefening plaats te vinden waarbij de beschikbare respons- en herstelplannen getoetst worden. Als onderdeel van dit proces dienen de verantwoordelijkheden benadrukt te worden en de documentatie bijgewerkt te worden.		Actief	in SLA opnemen			Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Technisch beheer	TB 1	Opdrachtnemer beschikt over een geborgde wijzigingsprocedure voor het doorvoeren van wijzigingen aan de installatie, ondersteunende ICT-systemen, beveiligings- en netwerkomgeving. Alle wijzigingen worden conform de wijzigingsprocedure geregistreerd. Updates en patches dienen via de reguliere wijzigingsprocedure te verlopen. Wijzigingen mogen alleen worden aangevraagd en uitgevoerd door geautoriseerden.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Technisch beheer	TB 2	Opdrachtnemer houdt toezicht op de operationele uitvoering en naleving van: a. het doorvoeren van wijzigingen conform de wijzigingen procedure; b. de procedure voor fysieke toegang; c. de procedure voor logische toegang; d. patching, back-up procedure en bewaartermijnen; e. incidentmanagement, log- en incidentrapportages en de analyse daarvan.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Technisch beheer	TB 3	Documentatie en Asset Management: De beheerorganisatie dient ervoor te zorgen dat voor beheerde systemen relevante beheerdocumentatie actueel is, beschikbaar is en bewaard blijft. Dit omvat bijvoorbeeld een offerte, contract, lijst met acceptatiecriteria, netwerkdiagram, Service Level Agreement (SLA), Dossier Afspraken en Procedures (DAP) of een gebruikers-en/of installatiehandleiding. Daarvoor dient de beheerorganisatie een actueel overzicht te hebben van de assets onder haar beheer. Dit overzicht dient per asset de volgende informatie te bevatten: 1. Functie of type systeem (bijv. VRI, waterbeheerobject, firewall, camera) 2. Locatie (logisch en fysiek) 3. Verantwoordelijke afdeling, specifieke eigenaar of externe partij 4. Merk, model en serienummer 5. Installatiedatum (waar van toepassing) 6. Verwijzing naar bijbehorend contract(en) voor beheerwerkzaamheden (bijv. SLA, DAP)		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Technisch beheer	TB 4	Patching: Systemen onder de beheerorganisatie worden regelmatig gepatcht om bekende kwetsbaarheden in de software te verhelpen. Hiervoor dient een standaard werkwijze te zijn, welke een regelmatige herhaling garandeert. Wanneer een kritieke kwetsbaarheid opgemerkt wordt dient er zo snel mogelijk een patch uitgevoerd te worden om deze te verhelpen en dienen mitigerende maatregelen overwogen te worden. De voorkeurs prioritering en frequentie van patching is als volgt: Hoge prioriteit (bijv. wekelijks): Alle systemen die direct vanaf het internet benaderbaar zijn Gemiddelde prioriteit (bijv. iedere 3 maanden): IT systemen en netwerkkaparaatuur Lage prioriteit (bijv. alleen bij onderhoud): OT systemen (installaties)	zie onderdeel patchen of gaat dit om de procedure	Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Technisch beheer	TB 5	Accountbeheer: Bij het installeren en beheren van systemen wordt het principe van least privilege gehanteerd, waarbij toegangsrechten alleen worden verleend wanneer deze noodzakelijk zijn voor het uitvoeren van werkzaamheden ('need to have'). Dit betekent dat ten minste de volgende maatregelen doorgevoerd moeten worden: 1. Toegang tot systemen (of de kanalen daarnaartoe) wordt enkel verleend na goedkeuring door de voor het desbetreffende systeem verantwoordelijke beheerder/bestuurder. 2. Het aantal personen met hoog-geprivilegieerde (administrator) toegang tot systemen wordt tot een minimum beperkt. 3. Er wordt een actueel overzicht bijgehouden van gebruikers en de daaraan toebedeelde toegangsrechten. Gebruikers (en toegangsrechten) die niet noodzakelijk zijn worden gedeactiveerd of bij voorkeur verwijderd.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Leveranciersmanagement	LM 1	Overzicht Leveranciers: Er dient een actueel en bijgehouden overzicht te zijn welke leveranciers werkzaamheden uitvoeren op de beheerde systemen namens de beheerorganisatie. Dit overzicht bevat ten minste de volgende informatie: 1. Naam leverancier 2. Type werkzaamheden (bijv. Bediening, Onderhoud (fysiek), Onderhoud (Op Afstand), Levering, Ondersteuning) 3. Betrokken systemen (bijv. VRIs, firewalls, laptops, waterbeheerobjecten) 4. Verwijzing naar bijbehorend contract (bijv. SLA, DAP) 5. Einddatum contract 6. Verantwoordelijk beheerder, bestuurder, project- of accountmanager of andere gemeentelijke medewerker		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Leveranciersmanagement	LM 2	Informatie per installatie: Voor iedere installatie(type) moet ten minste de volgende informatie beschikbaar en hervindbaar zijn: 1. Welke leveranciers werkzaamheden uitvoeren aan- en/of toegang hebben tot de installatie 2. Hoeveel gebruikers van een leverancier toegang hebben tot de installatie. Waar relevant omvat dit ook het aantal gebruikers met bijzonder geprivilegieerde toegangsrechten. 3. Wie eindverantwoordelijk is voor de kwaliteit en veiligheid van geleverde beheerdiensten 4. Wat voor incidenten/klachten rondom de kwaliteit van geleverde diensten of cybersecurity van de installatie hebben plaatsgevonden gedurende de samenwerking met deze leverancier. Waar relevant ook wat daarop de opvolging was.		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Leveranciersmanagement	LM 3	Inkoopbeisen: De beheerorganisatie wordt, bij voorkeur in een vroeg stadium, betrokken voor het aangaan van een contractuele relatie met een leverancier wanneer deze inkoop betrekking heeft tot systemen die door de beheerorganisatie (gaan) worden beheerd. Voordat een contract wordt afgesloten, worden de volgende factoren overwogen en waar relevant opgenomen in het contract of de aanbesteding: 1. De in deze baseline en in andere kaders (bijv. BIO(2), IEC62443) gestelde maatregelen voor informatiebeveiliging. In het bijzonder de verplichting om transparantie te tonen rondom incidenten of kwetsbaarheden met betrekking tot informatiebeveiliging en deze onverwijld aan de opdrachtgever te melden. 2. De afhankelijkheid van de gemeente van de leverancier en een uitwerking van een exit-strategie. 3. De verdeling van verantwoordelijkheden voor informatiebeveiliging en incidentrespons tussen leverancier en beheerorganisatie.	SLA	Actief				Project en Beheer & Onderhoud	V1.0

24-jun-26		Algemeen	0-1-2	CSIR voor Installaties	ALG 1	Naast de eisen uit dit document zijn de eisen van het document "CSIR voor Installaties" incl alle bijlages van toepassing. Inclusief alle bijlages (indien van toepassing): CSR 1 Omgang met vertrouwelijke informatie en documenten CSR 2 Personele toegang (fysiek / logisch) CSR 3 Architectuur Installatie netwerk CSR 4 Het veilig koppelen van beheer- en onderhoudsapparatuur CSR 5 Draadloze netwerken CSR 6 IIoT CSR 7 Wachtwoorden CSR 8 Patchmanagement CS9 Hardening CSR 10 Logging CSR 11 Malware scanning en opschoning middels een USB CSR 12 Continuïteitsplan voor energievoorziening CSR 13 Handelswijze bij SOC incident melding en verhoogde dreiging CSR 14 Incident response CSR 15 Recoveryplan CSR 16 Registratie assets in een configuratiemanagementdatabase (CMDB) CSR 17 Back-up en recovery CSR 18 Camera's en omgang met camerabeelden CSR 19 Uniform aanleveren van incidentrapportages CSR 20 Virtualisatie CSR 21 Verwijdering en vernietiging van informatie en apparatuur	deze tekst ergens in de Bael document opnemen	Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Overig / CMDB	ALG 2	Opdrachtnemer draagt zorg voor de beschikbaarheid van de actuele configuratiegegevens van de OT Installatie d.m.v. een Configuration Management Database (CMDB). Zie CSIR voor Installaties, bijlage "CSR 16 Registratie assets in een configuratiemanagementdatabase (CMDB)"		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Kennis en kunde	ALG 3	Er dient een OT Cyber Security en Informatie beveiliging Dossier opgeleverd te worden en te onderhouden door Opdrachtnemer bestaande uit: - OT Informatie beveiligings- en Cyber Security plan - Risico beoordeling (RiBo) OT Installatie - Incident management (procedure) - Afwijkingsregister m.b.t. de eisen - Business Continuïteit plan / Disaster Recovery plan incl backup / restore document(en)		Actief				Project en Beheer & Onderhoud	V1.0
24-jun-26		Beheer	0-1-2	Leveranciersmanagement	ALG 4	De opdrachtnemer (en onderaannemers) dienen medewerking te verlenen wanneer de Gemeente pentesten / andere testen wil doorvoeren of audits		Actief	Deze eis is specifiek gericht op de verplichtingen van een opdrachtnemer / integrator / serviceprovider, deze eis valt onder IEC 62443-2-4: Requirements for IACS service providers.			Project en Beheer & Onderhoud	V1.0