Algemeen

Voor de invulling van de Cybersecurity eisen voor de i-VRI's volgt Provincie Noord-Holland de aanpak van Rijkswaterstaat zoals uitgewerkt in de Cybersecurity Implementatie Richtlijn (CSIR).

Voor de i-VRI's hanteert provincie Noord-Holland weerstandsniveau 1. Hieronder zijn de maatregelen verzameld per thema voor weerstandsniveau 1 uit de CSIR versie 1.04 (PNH versie 2016).

Deze maatregelen worden als eisen toegevoegd aan de ERBI voor i-VRI's, waarbij de volgende uitganspunten gelden:

- 'ICS/SCADA' moet gelezen worden als de TLC, de RIS, C-ITS applicatie en het WIFI-p modem.
- 'lokale objectdatanetwerk' moet gelezen worden als het netwerk in (en om) de iVRI kast, dat de verschillende componenten binnen de i-VRI met elkaar verbindt. Daarnaast is de i-VRI verbonden met het PNH netwerk voor communicatie met de verkeerscentrale en TLEX en via Wifi-P met passerende voertuigen.
- 'ondersteunde ICT systemen', hiermee worden alle ICT middelen die worden ingezet voor de ontwikkeling en/of het beheer van de i-VRI's.
- 'Hulppersonen' zijn alle medewerkers (in- en extern) die vanuit hun taken fysieke of logische toegang hebben tot de i-VRI's.

De eisen uit de CSIR voor weerstandsniveau 1 die Noord-Holland als niet van toepassing verklaart voor de i-VRI's zijn doorgehaald.

Fysieke toegangsbeveiliging

Aspect	**Eisen (uit CSIR – versie 2016/PNH)**
Toegangsbeheer	Toegang middels een fysieke sleutel (voor normering zie Bouwkundige maatregelen/sluitwerk)[1]
Toegangsproces	Uitgangspunt is dat alleen toegang wordt verleend aan personen (internen / externen incl. bezoekers) die in de IA-gerelateerde ruimten moeten zijn vanwege het verrichten van werkzaamheden of het houden van toezicht.
Organisatorische maatregelen	O1 Standaard maatregelen + voorlichting over preventie + uitleg over het systeem.
~~Bouwkundige maatregelen~~	~~B1 Hang- en sluitwerk met een inbraakwerendheid van 3 minuten volgens BRL3104 of klasse 2 NEN5096.~~
~~Compartimentering / Meeneem beperkende maatregelen~~	~~C/M1 Inbraakwerende kast/safe volgens VGW kwalificaties. Of M1 door verankeren, verplaatsen. Of bouwkundig compartiment C1. Alles met inbraakvertraging van 3 minuten.~~
~~Inbraak installatie~~	~~E1 Inbraakalarminstallatie. Grade 2 /NCP 2~~

[1] Half-cylindrische sloten en het driekantslot worden ter beschikking gesteld (zie standaard bepalingen VRI, versie 5.28).

~~Alarmering~~	~~AL0 Optische en/of akoestische alarmgever en/ of alarmtransmissie naar (mobiele) telefoon~~
~~Reactie (alarmopvolging)~~	~~R0 Alarmopvolging door sleutelhouder na melding naar (mobiele) telefoon.~~

Logische toegang

ID	**Eisen (uit CSIR – versie 2016/PNH)**
LTPO1	De Opdrachtgever heeft het recht om controles uit te voeren op de naleving van het logische toegangsproces door de Opdrachtnemer.
LTPO2	Er dient erop toe te worden gezien dat: • de toegang voor de bestuurders tot het ICS/SCADA en overige ondersteunende ICT-systemen uitsluitend op basis van het 'need to have' principe plaatsvindt; • de toewijzing en het gebruik van privileges van administrators en systeembeheerders beperkt dienen te blijven tot het noodzakelijke; • fysieke toegang tot objecten en ruimten waar zich informatie, software en andere bedrijfsmiddelen (o.a. apparatuur) bevinden, alsmede de logische toegang tot systemen, uitsluitend toegestaan wordt voor personen die hiertoe geautoriseerd zijn; • bij misbruik van accounts en autorisaties dienen disciplinaire maatregelen te worden genomen.
LTPO3	De toegangsrechten van Hulppersonen dient jaarlijks beoordeelt en geactualiseerd te worden in een formeel proces.
LTPO4	De lokale logische toegang voor medewerkers tot Infrastructuur van PNH, ICT, ICS/SCADA systemen en de centrale en locale objectnetwerken dient bij de hiertoe verantwoordelijk verantwoordelijk gestelde en gemandateerde functionaris aangevraagd en goedgekeurd te worden.
LTPO5	Bij remote toegang om beheeractiviteiten uit te voeren dient gebruik gemaakt te worden van de diensten die PNH hiervoor beschikbaar stelt.
LTPO6	De logische toegang dient afhankelijk van de classificatie van het object als volgt te worden ingevuld: · Lokaal bediening en beheer – minimaal een user-id en wachtwoord combinatie met navolging van de wachtwoordrichtlijn · Remote toegang voor bediening en beheer - 'two factor' authenticatie en uitsluitend via de beveiligde voorzieningen van de provincie.
LTT1	De logische toegang tot informatiesystemen en netwerk dient plaats te vinden na het succesvol doorlopen van het identificatie, authenticatie en autorisatieproces (IAA), waarbij de IAA- gegevens voor zover haalbaar in versleutelde vorm worden uitgewisseld en opgeslagen.
LTT2	De toegang tot ICS/SCADA en overige ondersteunende ICT-systemen is geblokkeerd, tenzij het expliciet is toegestaan.
LTT3	Voor bedienaars en beheerders en systemen worden unieke ID's gehanteerd zodat uitgevoerde handelingen terug te leiden zijn tot een persoon of systeem.

Maatregelen Beveiligingsincidenten en incident Response Plan

ID	Eisen (uit CSIR – versie 2016/PNH)
BIRPO1	Er dient een geborgde procedure te bestaan die regelt dat Hulppersonen security incidenten en zwakke plekken in de beveiliging zo snel mogelijk melden bij de daartoe ingerichte meldpunten. Van Hulppersonen moet worden geëist dat zij alle security incidenten, verdachte of zwakke plekken in systemen of diensten registreren en rapporteren.
BIRPO2	Bij Opdrachtnemer is een Incident Manager benoemd en bijbehorende verantwoordelijkheden voor cybersecurity zijn vastgesteld.
BIRPO3	Er is 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 het betrouwbaarheidsniveau en de ernst van de storing. Welke rolhouders aanspreekbaar zijn inzake storingen, security incidenten en zwakke plekken. De verantwoordelijkheden en incidentenprocedure moet gecommuniceerd worden naar de Hulppersonen van Opdrachtnemer.
BIRPO5	Voor het afhandelen van urgente en niet-standaard security incidenten (bijv. bij computervirusinfecties en aanvallen via publieke netwerken zoals internet) wordt de Incidentmanager van PNH ingeschakeld.
BIRPT1	De ingebouwde beveiligingsfuncties, controlemechanismen en waarschuwingen die systemen genereren dienen geactiveerd en benut te worden voor registratie en rapportage van beveiligingsincidenten.

Maatregelen Netwerkkoppelingen

ID	Eisen (uit CSIR – versie 2016/PNH)
NKPO1	Opdrachtnemer draagt zorg voor en ziet erop toe dat alle netwerkkoppelingen met het lokale objectnetwerk strikt en uitsluitend plaatsvinden via de beveiligde centrale netwerkvoorzieningen en koppelpunten van PNH. Rechtstreekse toegang tot ICS/SCADA-systemen vanuit een publiek netwerk - waaronder het gebruik van internet en e-mail - is verboden.
NKPO2	Opdrachtnemer draagt zorg voor en ziet erop toe dat bij netwerkkoppelingen tussen het object en de centrale netwerken van PNH de aansluitvoorwaarden/beveiliging in acht wordt genomen. Voor remote logische toegang van personeel tot de aan het object gekoppelde systemen moet de procedure "Toegang Derden" van PNH worden gevolgd waarbij de Objectverantwoordelijke/-beheer de aanvraag verzorgt.
NKPO4	Opdrachtnemer dient zorg te dragen dat het aantal data netwerkkoppelingen tussen ICS/SCADA systemen en andere datanetwerken beperkt blijft tot alleen de functioneel noodzakelijke, waarbij de koppeling een passende vorm van beveiliging kent en geen onacceptabele risico's oplevert voor het object en de centrale netwerkdienstverlening. Voor elke koppeling is een risicoanalyse en afweging gemaakt.
NKPO5	Opdrachtnemer draagt zorg voor en ziet erop toe dat het lokale objectdatanetwerk gehardend is door niet noodzakelijke netwerkservices uit te zetten (voor hardening zie 'Maatregelen bescherming tegen malware, hardening en patching').
NKPO6	Het koppelen van mobiele apparatuur van derden of removable media aan lokale ICS/SCADA systemen, lokale objectdatanetwerken of het datanetwerk van PNH dient plaats te vinden na autorisatie van de hiertoe aangewezen en gemandateerde functionaris aan de kant van Opdrachtnemer.
NKPO8	Opdrachtnemer draagt zorg voor een geborgde procedure die aanhaakt en opvolging geeft aan geregistreerde datacommunicatienetwerk incidentmeldingen vanuit de provincie.
NKT1	Wanneer configuratie van ICS/SCADA-systemen op afstand plaatsvindt, dient dit altijd over beveiligde verbindingen plaats te vinden. Het gebruik van onveilige communicatieprotocollen zoals FTP, Telnet, VNC en RDP dient vermeden te worden. Indien dit niet haalbaar is, mogen deze enkel gemotiveerd worden ingezet wanneer een additioneel encryptiekanaal wordt toegepast (zoals SSL, TLS of IPSEC).
NKT2	ICS/SCADA en de ondersteunende systemen en besloten (lokale) objectnetwerken mogen geen directe verbindingen hebben met kantoornetwerken.

Maatregelen bescherming tegen malware, hardening en patching

ID	Eisen (uit CSIR – versie 2016/PNH)
MHPPO1	Opdrachtnemer dient over een geborgde procedure en voorzieningen te beschikken voor detectie van en preventie tegen malware waarbij de anti-malware software en signature updates dagelijks dienen plaats te vinden.

MHPPO2	Opdrachtnemer dient over een geborgde procedure te beschikken voor het (laten) hardenen van de bediening- en besturingssystemen en overige ondersteunde ICT-systemen en datanetwerkelementen door: • niet noodzakelijke datanetwerkservices uit te zetten; • het verwijderen (patchen) van bekende kwetsbaarheden; • alle poorten die niet nodig zijn te deactiveren/blokkeren; • alle default "access points" te verwijderen; • De default accounts uit te schakelen conform het wachtwoord policy; • Indien beschikbaar gebruik te maken van de security opties van leveranciers.
MHPPO3	De Opdrachtnemer dient zorg te dragen dat zijn ICT systemen, die gekoppeld worden aan de ICT en IA van Opdrachtgever voorzien zijn van alle recente beveiligingsupdates en patches.
MHPPO4	De Opdrachtnemer dient over een geborgde procedure te beschikken waarmee tijdig gereageerd kan worden op technische kwetsbaarheden van de in gebruik zijnde ICS/SCADA en ondersteunende ICT-systemen en netwerken.
MHPPO5	Opdrachtnemer dient over een geborgde procedure te beschikken voor patching waarin taken, bevoegdheden en verantwoordelijkheden van de betrokken rolhouders zijn beschreven inclusief de van toepassing zijn doorlooptijden.
MHPPO8	Opdrachtnemer dient te beschikken over een herstelplan na een besmetting met malware, waaronder alle nodige voorzieningen voor back-up, kopieën van gegevens en programmatuur evenals herstelmaatregelen.
MHPPO10	Opdrachtnemer draagt zorg voor en ziet erop toe dat gegevensdragers, beheer- en onderhoudsapparatuur altijd vooraf op malware gecontroleerd worden voordat deze worden gekoppeld aan de ICS/SCADA of overige ondersteunende ICT-systemen en lokale objectdatanetwerken.
MHPT1	Indien mogelijk dienen ICS/SCADA-systemen zodanig (her)geconfigureerd te worden dat auto-run van USB-tokens, USB harde schijven, mounted network shares of andere removable media niet wordt toegestaan.
MHPT2	Antimalware voorzieningen moeten in afstemming met PNH ingezet worden.

Maatregelen Logging en Monitoring

ID	**Eisen (uit CSIR – versie 2016/PNH)**
LMPO1	De handelingen van medewerkers, beheerders, meldingen vanuit systemen en eventlogs dienen te worden vastgelegd in auditlogbestanden waarbij een logregel minimaal de volgende gegevens bevat: • de gebeurtenis zelf; • een tot een natuurlijk persoon herleidbare gebruikersnaam of een (systeem)-ID • het object waarop de handeling werd uitgevoerd • het resultaat van de handeling • de datum en het tijdstip van de gebeurtenis • optioneel de identiteit van het werkstation of de locatie • een doorlopende en unieke nummering per logregel
LMPO2	Opdrachtnemer draagt zorg voor en ziet er op toe dat: • de loggegevens in een apart bestand worden weggeschreven en opgeslagen die alleen toegankelijk is voor speciaal hiertoe geautoriseerd personeel; • de logbestanden van bediening- en besturingssystemen, beveiliging en ondersteunende ICT-systemen en –netwerkelementen beschermd worden voor verlies of wijziging; • van systemen met logvoorzieningen de logbestanden drie maanden bewaard worden; • loggegevens die gebruikt zijn voor incidentonderzoeken conform de bewaartermijnen die de (feiten)onderzoekers aangeven langer worden bewaard.
LMPO3	Voor de levering van logbestanden aan derden dient de Objectverantwoordelijke/-beheerder van PNH expliciet toestemming te verlenen.

LMPO4	Opdrachtnemer draagt zorg voor een geborgde procedure die opvolging geeft aan meldingen uit de centrale logging en monitoringsvoorzieningen en proces vanuit PNH.
LMT1	Logfiles van ICS/SCADA, beveiliging en ondersteunende ICT-systemen en-netwerkelementen dienen in CSV-formaat opgeleverd te kunnen worden.
LMT2	In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden zoals wachtwoorden, inbelnummers, e.d.
LMT3	Het overschrijven of verwijderen van logregels- en bestanden wordt gelogd in een nieuw aangelegde log.
LMT4	De loginstellingen en -bestanden worden zodanig beschermd dat deze niet gewijzigd of gewist kunnen worden door ongeautoriseerden.

Maatregelen Bewustwording en Training

Voor alle betrokken medewerkers van opdrachtnemer:

ID	**Eisen (uit CSIR – versie 2016/PNH)**
BTME1	Hulppersonen van Opdrachtnemer zijn verplicht om de door Opdrachtnemer aangegeven en beschikbaar gestelde periodieke cybersecurity cursussen, trainingen, E-Learning modulen te volgen en hiernaar te handelen.
BTME2	Ieder Hulppersoon is zich bewust van de voor hem/haar van toepassing zijnde taken, bevoegdheden en verantwoordelijkheden voor beveiliging en weet dat gebruikers- en systeemactiviteiten worden gelogd.
BTME3	Hulppersonen nemen de cybersecurity beveiligingsinstructies strikt in acht en zijn verantwoordelijk voor hun aandeel in de beveiliging van het object.
BTME4	Hulppersonen doen aan sociale controle, spreken elkaar aan op ontoelaatbaar en risicovol gedrag en bespreken geconstateerde onregelmatigheden in het periodieke werkoverleg met het eigen management/Objectbeheerder.
BTME5	Bij het constateren van een security incident dienen Hulppersonen dit direct als een security incident te melden bij de verantwoordelijke objecteigenaar/ -beheerder. Er is sprake van een security incident bij het manifest worden van een (dreigend of reeds opgetreden) security risico als gevolg van een (mogelijke) overtreding van het cybersecurity beleid of onregelmatigheid. Voorbeelden van security incidenten zijn: - verlies van dienst, apparatuur of voorzieningen; - systeemstoringen of overbelasting; - menselijke fouten die leiden tot functionele verstoring of uitval van systemen; - inbreuk op fysieke en logische beveiligingsvoorzieningen van het object; - inbreuk op de bediening en beheer; - ongeautoriseerde systeemwijzingen; - niet-naleving van beleid of gedragsregels; - virusmeldingen; - verlies of diefstal van bedrijfsmiddelen; - oneigenlijk gebruik van bevoegdheden; - vandalisme, moedwillige beschadiging.
BTME6	Afwijkend systeemgedrag kan een aanwijzing zijn voor een aanval op de beveiliging of voor een daadwerkelijk beveiligingslek en behoort daarom altijd direct te worden gerapporteerd als een beveiligingsincident en gemeld.
BTME7	Hulppersonen moeten bij het constateren van eventuele onregelmatigheden dan wel onveilige situaties die handelingen verrichten of maatregelen treffen die verdere uitbreiding van het incident kunnen voorkomen dan wel de schade beperken.
BTME8	Hulppersonen gaan zorgvuldig om met de verstrekte persoonsgebonden fysieke toegangmiddelen voor het object en de (systeem, bedien, technische) ruimten hierbinnen en delen deze niet met collega's.
BTME9	Hulppersonen creëren geen eigen netwerkkoppelingen op het object en melden dit als een beveiligingsincident als er een zelf aangelegde netwerkkoppeling wordt geconstateerd.
BTME10	Hulppersonen nemen de wachtwoordrichtlijn voor de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen in acht.

BTME11	Hulppersonen koppelen geen mobiele apparatuur of removable media aan de ICS/SCADA, overige ondersteunende ICT-systemen en object netwerken. Uitgezonderd zijn de beheerders die dit alleen na autorisatie van de hiertoe gemandateerde functionaris en uitgevoerde actuele malwarecontrole van apparatuur/media mogen doen.
BTME12	Voor Hulppersonen is toegang tot internet en het gebruik van email vanaf ICS/SCADA en overige daaraan ondersteunende ICT-systemen strikt verboden.
BTME13	Hulppersonen mogen de beschikbaar gestelde toegangsmiddelen (tokens, pasjes) tot ICS/SCADA en ondersteunende systemen en –netwerken alleen gebruiken voor het doel waarvoor ze ontworpen zijn. Hierbij mogen de getroffen beveiligingsmaatregelen niet omzeild worden.
BTME14	Hulppersonen houden hun accountgegevens strikt geheim; zij gebruiken hun account en uitgegeven autorisaties alleen zelf en staan niet toe dat anderen onder hun account kunnen inloggen. Handelingen zijn altijd te herleiden naar de voor dat account geautoriseerde persoon.
BTME15	Hulpersonen dienen op ICS/SCADA en de overige ondersteunende ICT systemen en –netwerken de standaard/default/fabrieks accounts en/of wachtwoorden bij ingebruikname te wijzigen conform de wachtwoordrichtlijn.
BTME16	Bij het constateren van onregelmatigheden in de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen dient Opdrachtnemer dit onverwijld als een beveiligingsincident te melden bij de hiervoor aangewezen functionaris.
BTME17	Ongeautoriseerd aan- of afkoppelen van removable apparatuur of usb-sticks aan het netwerk of ICS/SCADA systemen is strikt verboden.
BTME18	Alleen geautoriseerde Hulppersonen mogen systemen die voorzien zijn van de laatste security updates, patches en actuele viruscontroleprogrammatuur koppelen aan objectdatanetwerken of ICS/SCADA systemen.
BTME19	Gegevensdragers worden altijd vooraf op malware gecontroleerd voordat deze worden gekoppeld aan ICS/SCADA of overige ondersteunende ICT-systemen en netwerken.
BTME20	Incidenten die zich voordoen binnen het wijzigingsproces en afwijkingen van het wijzigingsproces moeten worden gemeld bij de hiervoor aangewezen functionaris.
BTME21	Onregelmatigheden, incidenten en storingen binnen het back-up en recovery proces moeten worden gemeld bij de hiervoor aangewezen functionaris.
BTME22	Hulppersonen van Opdrachtnemer zorgen ervoor dat onbeheerde ICS/SCADA-systemen en overige ICT-apparatuur – zo mogelijk - wordt gelocked.

Voor verantwoordelijke managers van opdrachtnemer:

ID	**Eisen (uit CSIR – versie 2016/PNH)**
BTMA1	Er dient bewerkstelligd te worden dat Hulppersonen continu bewust worden gemaakt door Opdrachtnemer en geschikte training en regelmatige bijscholing krijgen met betrekking tot het beveiligingsbeleid en procedures, voor zover relevant voor hun functie.
BTMA2	Opdrachtnemer draagt zorg voor en ziet erop toe dat: • Hulppersonen de periodieke Cybersecurity cursussen, trainingen en E-Learningmodulen volgen en een actuele administratie hiervan aanwezig is; • Hulppersonen de beschikking hebben over actuele (technische) beheerdocumentatie, gebruikers- en/of installatiehandleidingen voor de ICS/SCADA en overige ondersteunende ICT-systemen en bedrijfsmiddelen; • dat werkzaamheden door gescreende (achtgrond verificatie) Hulppersonen wordt uitgevoerd en dat geheimhouding is overeengekomen; • dat Hulppersonen alle bedrijfsmiddelen, ICS/SCADA en overige ondersteunende ICT-systeemdocumentatie van PNH die ze in hun bezit hebben retourneren bij beëindiging van hun dienstverband, contract of overeenkomst; • dat de toegangsrechten van Hulppersonen direct worden geblokkeerd bij beëindiging van het dienstverband, het contract of na wijziging van de overeenkomst worden aangepast; • dat calamiteitenplannen worden betrokken in de bewustwordingstrainingen, trainingen en testactiviteiten; • gebruik van de centraal beschikbaar gestelde technische middelen voor fysieke en logische toegang op medewerkers niveau wordt bijgehouden.

BTMA5	Opdrachtnemer besteedt en bespreekt cybersecurity in de functioneringsgesprekken met Hulppersonen en maakt hiertoe opleidingsplannen waarbij wordt toegezien op uitvoering.
BTMA6	Opdrachtnemer dient bij het constateren van onregelmatigheden in de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen uit voorzorg in dergelijke situaties het betreffende account en wachtwoord altijd te laten wijzigen.
BTMA7	De Opdrachtnemer dient zijn Hulppersonen nadrukkelijk te informeren over het feit dat het doorgeven van informatie over de werking, inrichting, organisatie rondom de objecten in welke vorm dan ook NIET zal geschieden dan na uitdrukkelijke toestemming van de Opdrachtgever.

Maatregelen gecontroleerd wijzigen

ID	**Eisen (uit CSIR – versie 2016/PNH)**
GWPO1	Opdrachtnemer dient over een geborgde procedure te beschikken voor het (laten) inventariseren en registreren van alle Configuration Items (CI's) met bijbehorende settings/configuraties in een Configuration Management Database (CMDB) die actueel wordt gehouden.
GWPO2	Opdrachtnemer dient over een geborgde wijzigingsprocedure te beschikken voor het doorvoeren van wijzigingen aan ICS/SCADA en ondersteunende ICT systemen, beveiliging- en netwerkomgeving. Alle wijzigingen worden conform de wijzigingsprocedure geregistreerd. Updates en patches dienen via de reguliere wijzigingsprocedure te verlopen.
GWPO3	Wijzigingen mogen alleen door geautoriseerde beheerders worden aangevraagd en uitgevoerd.
GWPO5	De wijzigingen worden bijgewerkt in de CMDB en jaarlijks worden de settings/configuraties van ICS/SCADA en overige ondersteunende ICT-systemen in de CMDB vergeleken met de daadwerkelijke en de CMDB indien nodig bijgewerkt.
GWPO7	Opdrachtnemer draagt zorg voor en ziet erop toe dat noodwijzigingen die buiten het reguliere wijzigingsproces om zijn aangebrachte als gevolg van incidenten met een bijzonder (urgent) karakter achteraf alsnog de gebruikelijke procedures volgen en de CMDB administratie wordt bijgewerkt.
GWPO9	Opdrachtnemer ziet erop toe dat naar aanleiding van een wijziging uitgeschakelde beveiligingsmaatregelen weer zijn geactiveerd alvorens de wijziging te sluiten.
GWT1	Alle CI's met bijbehorende settings/configuraties en de wijzigingen hierop worden geregistreerd in een CMDB.
GWT2	Voor zover beschikbaar wordt gebruik gemaakt van testvoorzieningen.

Maatregelen beheer en onderhoud

ID	**Eisen (uit CSIR – versie 2016/PNH)**
BOPO1	Opdrachtnemer draagt zorg voor het evalueren van risico's en effectieve werking van de getroffen cybersecurity beheersmaatregelen voor beveiliging in het kader van life-cycle management.
BOPO2	Opdrachtnemer draagt zorg voor en ziet erop toe dat waar nodig in de beheer en onderhoudscontracten met onderaannemers: • Geheimhouding opgenomen is; • Training- en opleidingsvereisten alsmede overige benodigde certificeringen beschreven zijn; • Welke screening (verificatie achtergrond) van personeel nodig is; • Beschreven is dat de gedragsregels voor beveiliging en communicatie strikt in acht moeten worden genomen; • Een concrete procedure bekend is en is vastgelegd met betrekking tot incidentresponse en voor escalatieprocedures met de leverancier (7*24) • De procedures voor fysieke toegang tot objecten en ruimten en de logische toegang tot systemen vastgelegd zijn; • De registratie en rapportage van beveiligingsincidenten geregeld is;

	• Beschreven is dat handelingen van medewerkers en systemen gelogd en gemonitord worden; • Beschreven is dat loggegevens van PNH beschermd moeten worden tegen verlies en wijziging en niet voor andere doeleinden gebruikt mogen worden; • De bewaartermijnen van back-ups en logbestanden geregeld is; • De procedures voor aan- en afkoppeling van apparatuur beschreven zijn; • De procedure "Toegang Derden" van de PNH gevolgd moet worden voor de logische toegang tot netwerken en systemen. De tijdelijke toegang tot de systemen ten behoeve van ondersteuning dient geautoriseerd te zijn en handelingen dienen te worden gelogd. • Beschreven is dat onderhoud en wijzigingen op ICS/SCADA systemen alleen uitgevoerd mogen worden vanaf systemen die voorzien zijn van de laatste security update's en patches en actuele viruscontroleprogrammatuur; • Beschreven is dat netwerkkoppelingen op objectnetwerken altijd en strikt via de beveiligde centrale voorzieningen van PNH verlopen; • Welke netwerkkoppelingen er toegestaan zijn; • Beschreven is dat logging en monitoring van netwerkverkeer plaatsvindt via de centrale voorzieningen van PNH; • Beschreven is dat wijzigingen conform het wijzigingsproces uitgevoerd mogen worden; • Beschreven is dat patchen strikt conform de Patchrichtlijnen en doorlooptijden uitgevoerd moeten worden; • Beschreven is dat het ongeautoriseerd koppelen van removable media en usb sticks aan (object)datanetwerken strikt verboden is.
BOPO3	Opdrachtnemer draagt waar nodig zorg voor en ziet erop toe dat in de SLA/DAP afspraken met Opdrachtgever en onderaannemers worden gemaakt over: • De dienstverlening en functionaliteit; • Tijd van openstelling, bereikbaarheid en reactietijd, incident melding en afhandeling; • Wat wordt verstaan onder een storing, beveiligingsincident en zwakke plek; • Het classificeren van incidenten en de geldende maximale oplossingsduur; • Escalatieprocedures (horizontaal en verticaal) bij overschrijding van de overeengekomen normtijden inclusief namen en telefoonnummers. • Het indienen en afhandelen van wijzigingsverzoeken; • Directe melding van beveiligingsincidenten; • Noodprocedures met zowel interne als externe leveranciers voor ICT en ICS/SCADA systemen; • Ondersteuning bij calamiteiten en beschikbaarheid van reserve onderdelen en apparatuur; • De communicatielijnen (wie, wanneer en waarover); • Hoe de fysieke en logische toegang tot systemen en ruimten geregeld is; • De bewaartermijn van back-ups en logbestanden; • Rapportages die verplicht zijn zoals die voor beveiligingsincidenten en welke frequentie daarvoor geldt; • Het signaleren van nieuwe kwetsbaarheden en tijdig uitbrengen van patches door de leverancier; • Het testen van software-updates alvorens deze in productie gaan; • Evaluatie en actualisatie;
BOPO4	Opdrachtnemer draagt zorg voor de beschikbaarheid en onderhoud van (technische) beheerdocumentatie, gebruikers- en/of installatiehandleidingen voor de ICT en IA systemen alsmede procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen.
BOPO6	Opdrachtnemer houdt toezicht op de operationele uitvoering en naleving van: • de uitvoering van wijzigingen conform de wijzigingen procedure; • de procedure voor fysieke toegang; • de procedure voor logische toegang; • patching, de back-up procedure en bewaartermijnen; • incidentmanagement, log- en incidentrapportages en de analyse hiervan.
BOT1	Voor de fysieke toegang (ICT-deel) van bedienaars, beheerders en overig ondersteunend personeel zowel van PNH als die van Opdrachtnemer tot objecten en de ruimten hierbinnen wordt gebruikt gemaakt van de producten en diensten van PNH.

BOT2	Voor (remote) logische toegang van bedienaars en beheerders tot het netwerk en ICS/SCADA systemen wordt gebruikt gemaakt van de producten en diensten van PNH.

Maatregelen Back-Ups

ID	**Eisen (uit CSIR – versie 2016/PNH)**
BUPO1	Dagelijks dient automatisch een back-up gemaakt te worden van alle in het systeem aanwezige dynamische en configuratiegegevens welke back-up op het systeem zelf of op de hoofdlocatie van het systeem mag worden opgeslagen. De juiste verwerking van de back-up wordt bewaakt op basis van het back-up log. Deze back-ups worden een week bewaard.
BUPO2	De integriteit en beschikbaarheid van de laatste drie versies van de ICS/SCADA systemen, programmatuur en besturingssystemen dient gewaarborgd te worden door het maken en testen van systeemimages/back-ups, conform een geborgde procedure: • systeemimages/back-ups worden gemaakt vooraf en na iedere (functionele) systeemwijziging en wanneer wijzigingen uitblijven wordt de systeemimage/back-up van de laatste versie op jaarbasis vernieuwd, met deze back-up moet men in staat zijn een volledige roll-back naar de werkende situatie terug te kunnen gaan; • Deze back-ups worden opgeslagen op een locatie die zich op zodanige afstand bevindt dat geen schade aan de back-up kan worden aangericht als een calamiteit zich voordoet op de locatie waar het systeem zich bevind; • Back-ups en de ruimte waarin ze zijn opgeslagen behoren fysiek goed te worden beschermd volgens dezelfde normen die gelden voor de hoofdlocatie en zijn alleen toegankelijk voor bevoegden; • Back-ups worden bewaard tot het moment van uitdienstname van betreffend systeem; • Ingeval de back-up terug wordt gezet, dient eventueel ook rekening te worden gehouden met ook het terugzetten van de dynamische gegevens over de systeemstatus.
BUPO3	Er bestaan gedocumenteerde herstelprocedures en volledige en actuele registers van back-up kopieën.
BUT1	Benodigde voorzieningen voor het back-up en restoreproces worden in overleg met de Opdrachtgever ingevuld.