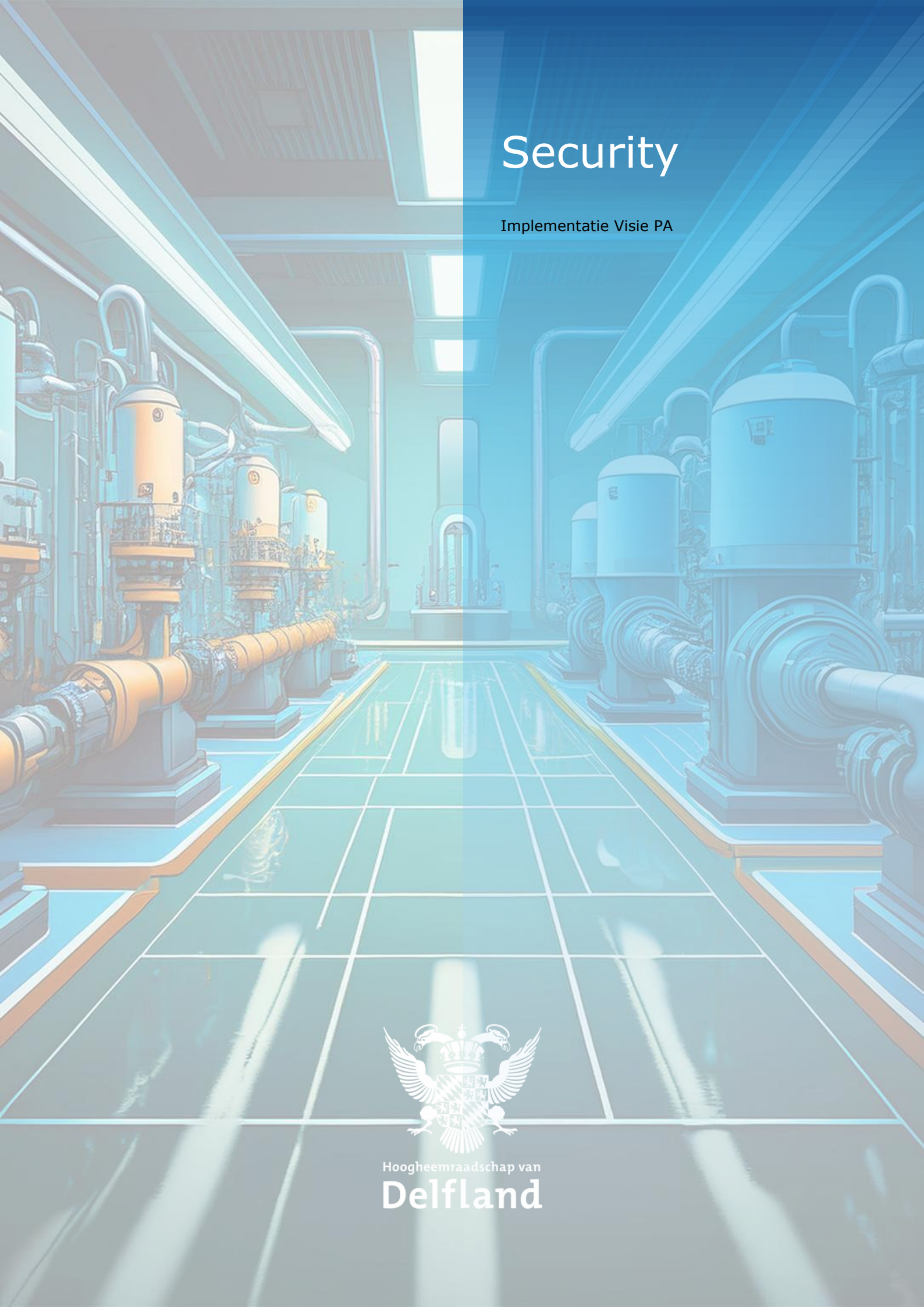


Security

Implementatie Visie PA

Hoogheemraadschap van
Delfland

Documentnaam

GE.SE.001 PA cybersecurity

Eigenaar en beheerder document

Documenteigenaar	
Functie: Manager PA	Naam: Casper Braamse
Documentbeheerder	
Functie: PA-adviseur	Naam: Hidde Schouten, Edwin van Velzen

Versiebeheer

Versie	**Datum**	**Omschrijving**
0.9	10-2-2025	Eerste versie, afgestemd met: Edwin van Velzen (PA-adviseur), Hidde Schouten (PA-adviseur), Boris van den Berg (ISO PA), Ben Bruinink (functioneel beheerder PA), Johan Witkam (specialist PA). Gereed voor stuurgroep op 18 februari 2025.
1.0	18-2-2025	Vastgesteld door Stuurgroep PA

Vaststelling en periodieke validatie

Vastgestelde versie	**Datum vaststelling**	**Wie**	**Functie**
1.0	18-2-2025	Stuurgroep PA	Stuurgroep
Volgende validatie	Q3 2025		
Classificatie	Intern		

Registratie

DMS-nummer: 2405025

Foto voorblad: AI

Hoogheemraadschap van Delfland

Inhoud

1 Implementatie Visie PA

Met het opstellen van de Visie PA is HH Delfland (HHD) in 2021 gestart op standaardisatie binnen de procesautomatisering. Met project Implementatie Visie PA geven wij handen en voeten aan deze standaardisatie. Dit document, PA cybersecurity, is onderdeel van deze standaard.

1.1 Scope document

Security definiëren wij als het samenhangend stelsel van maatregelen dat zich richt op het blijvend realiseren van een optimaal niveau van beschikbaarheid, integriteit en vertrouwelijkheid van onze PA-processen en systemen. Dit document is tijdloos opgesteld en beschrijft de gewenste situatie, alsof deze reeds de dagelijkse realiteit is.

Het doel van dit document is om de lezer, intern en extern, een totaaloverzicht te geven van de gewenste PA security situatie binnen HHD. Dit document is niet geschikt om als contractdocument of ontwerpdocument te dienen. Daarvoor moet de lezer de actuele security-richtlijnen en -procedures opvragen bij de security-functionarissen van HHD.

De impact van cybersecuritymaatregelen op de techniek, de architectuur, beschrijven we niet in dit document, daarvoor verwijzen we naar de PA Architectuur.

1.2 Doelstelling security in PA-standaard

Door security mee te nemen in de PA standaard, borgen we bij vernieuwing of uitbreiding van PA-systemen het behoud van het juiste securityniveau. Daarnaast zorgt deze borging voor een verkleining van het aanvalsoppervlak door kwaadwillende en komt dat ten goede aan de bedrijfscontinuïteit en het behalen van onze bedrijfsdoelstellingen. Daarnaast is het voor HHD van groot belang dat wij blijvend voldoen aan de wet- en regelgeving op landelijk en Europees niveau.

1.3 Samenhang met algemeen securitybeleid

HHD heeft een overkoepelend informatiebeveiligingsbeleid, afgepeld naar richtlijnen en maatregelen. Dit beleid is van toepassing op de hele HHD-organisatie en in algemene zin beschreven met als doel het voldoen aan de van toepassing zijnde nationale en Europese security wetgeving, te weten NIS2.

Voor de implementatie van de securitymaatregelen is besloten om voor PA-systemen de “Cyber Security Implementatie Richtlijn (CSIR) 3.4 voor waterschappen” toe te passen. De CSIR is een vertaalslag en specifieke invulling van de relevante beheer doelen/controls en maatregelen uit de BIO en de IEC 62443, waarmee aan de security doelstellingen voldaan wordt.

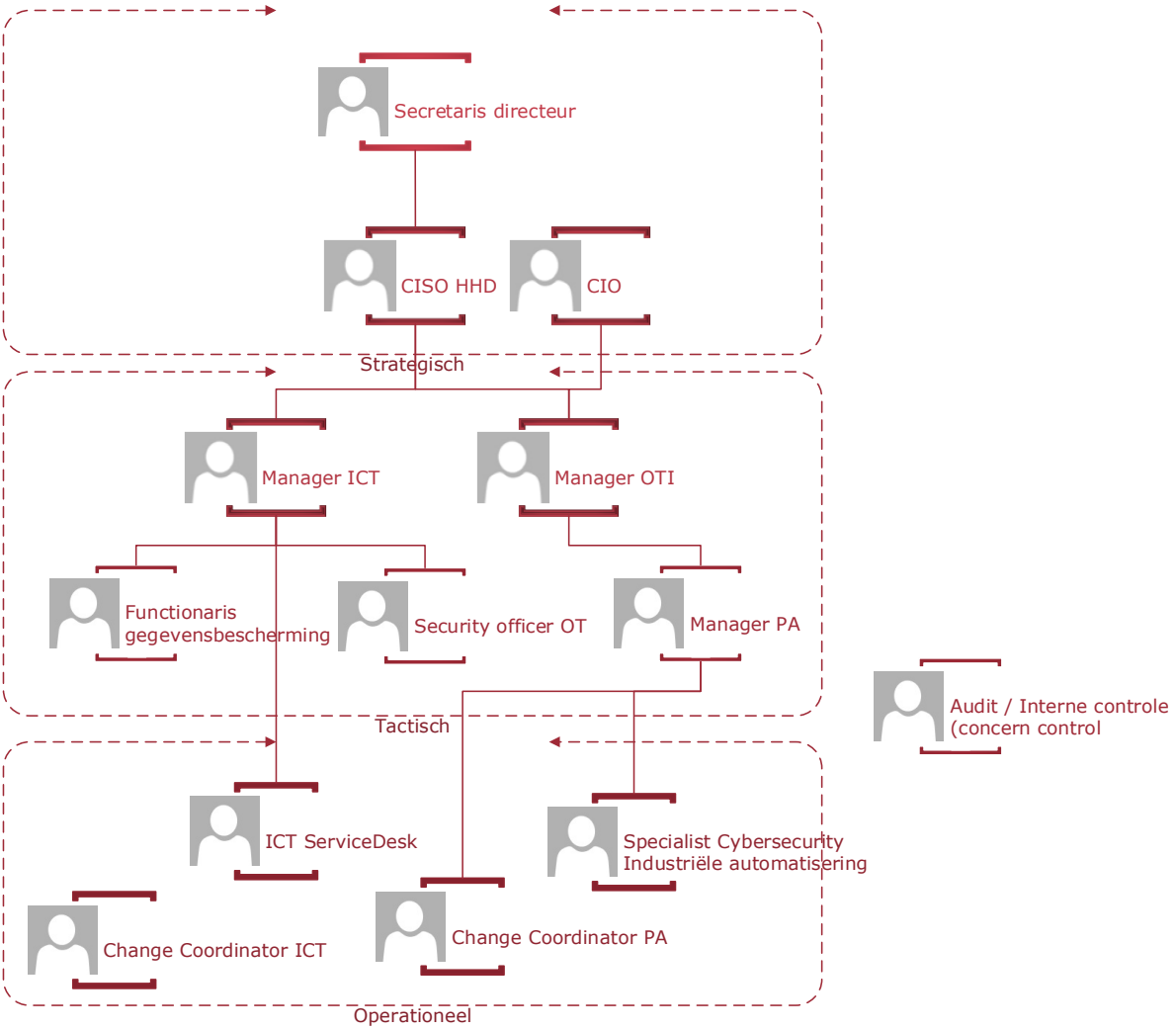
1.4 Samenhang tussen risicomanagement en CSIR-maatregelen

Risicomanagement richt zich op het analyseren en beheersen van risico’s waaraan de PA van Delfland staat blootgesteld. Deze risico’s kunnen op velerlei terreinen betrekking hebben, zoals financiële risico’s en de beschikbaarheid van objecten zoals waterzuiveringen en gemalen, beschikbaarheid van informatiesystemen en inzet van personeel.
Op basis van de ingeschatte risico’s en gevolgen zijn de objecten voorzien van een weerstandsniveau. Dit weerstandsniveau is gekoppeld aan de maatregelen die worden genomen.

2 Organisatie

Bij het behalen en behouden van het gewenste securityniveau hoort een organisatie die dit ondersteunt. Onderstaand organogram schetst de securityorganisatie van HHD.

Rol	Besluit-vormingsniveau	Waarvoor te benaderen
Bestuur	Strategisch	Met het ingaan van de NIS2 draagt het bestuur volgens de wet eindverantwoordelijkheid voor de cybersecurity. Het bestuur moet daar actief op sturen.
Secretaris-Directeur	Strategisch	Eindverantwoordelijk voor cybersecuritybeleid en goedkeuring van strategische besluiten.
CISO	Strategisch	Ontwikkeling van cybersecuritybeleid, risicomanagement en strategische advisering aan de directie.
CIO	Strategisch	Integratie van cybersecurity in ICT-strategiën en governance.
Manager ICT	Tactisch	Coördinatie van cybersecuritymaatregelen binnen ICT en toezicht op de uitvoering.
Manager OTI	Tactisch	Beheer en beveiliging van de PA-omgevingen.
Functionaris gegevensbescherming	Tactisch	Vragen omtrent AVG-compliance en gegevensbescherming.
Security Officer	Tactisch	Implementatie en naleving van securitybeleid binnen afdelingen.
Manager PA	Tactisch	Beveiliging en continuïteit van PA-systemen en -processen.
ICT ServiceDesk	Operationeel	Technische ondersteuning bij cybersecurityproblemen en -incidenten.
Change coordinator ICT	Operationeel	Begeleiding van wijzigingen binnen ICT-systemen en waarborging van security tijdens change management.
Specialist Cybersecurity PA	Operationeel	Advies over en uitvoering van cybersecuritymaatregelen in de PA.
Change coordinator PA	Operationeel	Begeleiding van wijzigingen binnen PA-systemen en waarborging van security tijdens change management.
Audit / Interne controle	Overkoepelend	Onafhankelijke (periodieke) toetsing van securitymaatregelen en naleving van beleidskaders.


Secretaris directeur
CISO HHD
CIO
Strategisch
Manager ICT
Manager OTI
Functionaris gegevensbescherming
Security officer OT
Manager PA
Tactisch
Audit / Interne controle (concern control
ICT ServiceDesk
Specialist Cybersecurity Industriële automatisering
Change Coordinator ICT
Change Coordinator PA
Operationeel

3 PA-Processen en procedures

Over het algemeen zal het overkoepelende cybersecuritybeleid van HHD worden aangehouden. Daarnaast kent PA enkele specifieke processen en procedures. De onderstaande paragrafen geven weer voor welke onderwerpen we overkoepelend cybersecuritybeleid volgen en voor welke onderwerpen we specifieke procedures volgen.

3.1 Overkoepelend cybersecuritybeleid

Tabel 1 bevat een overzicht van cybersecuritybeleidsdocumenten die voor zowel de PA als breder binnen HHD gelden. De tabel bevat enkel titels van de documenten, omdat ze geregeld geactualiseerd worden. Door op de titels te zoeken op de sharepoint van HHD, vind je de laatste versie.

Tabel 1 Documenten ten behoeve van HDD-breed cybersecuritybeleid.

Document	Toelichting
Richtlijn voor wachtwoorden	Tactisch document dat de eisen die de BIO aan decentrale overheden stelt, vertaalt naar een richtlijn.
Wachtwoordbeleid Delfland	Uitwerking van de richtlijn voor wachtwoorden tot een soort werkinstructie.
Standaard beveiligingseisen Delfland voor leveranciers	Vertaling van eisen, beleid en richtlijnen naar standaard beveiligingseisen van leveranciers van kritieke systemen.
Richtlijn bepalen BIV-classificatie en kritieke informatiesystemen	Richtlijn om te bepalen of een leverancier kritiek is waardoor eventueel de standaard beveiligingseisen Delfland voor leveranciers van toepassing is.
Richtlijn voor beveiliging van netwerksegmenten	Overkoepelend document die beschrijft hoe netwerksegmenten afgedwongen en beveiligd dienen te worden oid.
Zones- en conduitmodel	Model dat de netwerkarchitectuur, -segmentatie en zonering van HDD beschrijft. Valt onder de richtlijn voor beveiliging van netwerksegmenten.
Richtlijn patchmanagement	Richtlijn voor patchmanagement op basis van de BIO. Middels patches worden aanpassingen doorgevoerd om fouten op te lossen of verbeteringen aan te brengen in bestaande programmatuur en/of hardware.
Richtlijn hardening	Algemene richtlijn voor hardening van de assets van Delfland. De 'Hardening richtlijnen PA-domein' is hier een afgeleide van.
Uitvoeringskader beleidsnotitie risicomanagement	Beschrijving van de werkwijze, verantwoordelijkheden en uitvoering van risicomanagement binnen Delfland.
Beleid inzake het gebruik van cryptografische beheersmaatregelen	Beschrijving van het beleid voor het gebruik van cryptografische beheersmaatregelen op basis van de eisen die de BIO en de CSIR stellen.

3.2 Uitgewerkt PA-cybersecuritybeleid

Tabel 2 bevat een overzicht van documenten die specifiek voor de PA zijn opgesteld en een uitwerking zijn van het cybersecuritybeleid.

Tabel 2 Specifieke documenten PA met betrekking tot cybersecurity

Document	Toelichting
Procesbeschrijving PA configuratie management	Beschrijving van hoe configuratiemanagement binnen de PA is ingericht.
Procesbeschrijving PA contract- en leveranciersmanagement	Beschrijving van proces en activiteiten rondom contract- en leveranciersmanagement voor de PA van HHD.
Change management PA Procedure	Beschrijving van hoe we bij HDD omgaan met change management binnen de PA.
CSIR eisenlijst contractmanagement	Hulpmiddel om op basis van weerstandsniveau object en het soort contract te bepalen welke CSIR-eisen van toepassing zijn.
Procedure inbellen door derden	Beschrijving van de procedure voor een leverancier om in te bellen in het netwerk van HDD voor het oplossen van fouten.
PA security incident response procedure	Document dat beschrijft hoe HDD omgaat met de response op security incidenten en kwetsbaarheden in de PA-omgeving.
Hardening richtlijnen PA-domein	Beschrijving van de methoden voor hardening van PA-componenten bij HDD.
Back-up en restore plan PA	Document dat de structuur beschrijft voor het maken van back-ups en restore plannen nodig zijn om de PA functioneel te houden.
Driemaandelijkse beoordeling speciale toegangsrechten	Beschrijving van de activiteiten die nodig zijn om toegangsrechten van gebruikers periodiek te beoordelen.
Procedure verwijderen of hergebruik van PA-apparatuur	Beschrijving van de procedure om vertrouwelijke informatie van apparatuur te verwijderen, wanneer apparatuur einde levensduur heeft bereikt.
Finale gap analyse fysieke beveiliging	Lijst met (toekomstige) maatregelen ten behoeve van het fysiek beveiligen van PA-componenten.

4 Impact security op de dagelijkse praktijk

In dit hoofdstuk staan de functionele en technische maatregelen uitgeschreven die van toepassing zijn op onze PA-systemen. De paragrafen bevatten een beschrijving vanuit het PA-perspectief. Voor nauwkeurigere specificaties verwijzen we naar de beleidsdocumenten en richtlijnen.

De eerstvolgende tien paragrafen zijn thema's die als zodanig zijn geclusterd in de CSIR. Daarna volgen drie paragrafen die de voorgaande tien aanvullen op basis van de NIS2-wetgeving.

4.1 Fysieke toegangsbeveiliging

Onder fysieke toegangsbeveiliging scharen wij de toegang tot de ruimtes die ICT of PA gerelateerd zijn. Alleen geautoriseerd personeel heeft toegang tot deze ruimtes of gebouwen. Een deel van de toegang is elektronisch en een deel via sleutels. De managers van de diverse afdelingen bepalen de autorisaties.

Het document 'finale gap analyse fysieke beveiliging' gaat in op de fysieke toegangsbeveiliging van de (individuele) objecten met PA-componenten.

4.2 Logische toegang

Standaard staan MMI-applicaties niet ingelogd. Het is dan niet mogelijk om een bedienhandeling of engineering uit te voeren. Geautoriseerd personeel heeft een eigen account voorzien van een uniek wachtwoord op basis van RBAC (Role base Access control). Deze gegevens worden versleuteld uitgewisseld en opgeslagen. Waar mogelijk is het aantal gelijktijdige sessies te beperken en instelbaar. Na een instelbare hoeveelheid foutieve inlogpogingen wordt de toegang voor een instelbare tijd geblokkeerd.

De complexiteit en vernieuwing van het wachtwoord voldoen aan de algemene wachtwoordeisen van HHD. Periodiek worden de toegangsrechten opnieuw beoordeeld en aangepast.

Voor het veilig opslaan van gebruikersnamen en wachtwoorden wordt er een wachtwoordkluis beschikbaar gesteld door HHD. Het gebruik hiervan is verplicht voor iedereen die toegang heeft tot de PA-systemen.

De volgende documenten gaan specifieker in op het onderwerp logische toegang:

- *Richtlijn voor wachtwoorden*
- *Wachtwoordbeleid Delfland*
- *Procedure inbellen door derden*

4.3 Beveiligingsincidenten en incidentrespons

Waarschuwingen die het PA-systeem genereert, komen als pop-up op de bedienschermen en worden gemeld aan de systeembeheerder. Na een interpretatie wordt besloten of een incident gemeld moet worden. De systemen schakelen automatisch naar een gedefinieerde veilige situatie in het geval het systeem niet meer normaal functioneert.

Kritische PA-systemen zitten achter een noodstroominstallatie, die schakelt automatisch in het geval de netspanning wegvalt. Het schakelen van en naar de noodstroomvoorziening heeft geen invloed op de beveiligingsstatus van het systeem.

De verbinding tussen de PA en KA omgeving kan in het geval van een incident worden verbroken. In dat geval houden de systemen de laatste instellingen die verstuurd werden vanuit de KA vast, en is mogelijk om in "eilandbedrijf" de PA te bedienen.

Het document 'PA security incident response procedure' beschrijft de procedure die we specifiek voor de PA doorlopen na het plaatsvinden van een incident.

4.4 Netwerkkoppelingen en cryptografie

Toegang tot de systemen in de PA-omgeving verkrijg je, mits toegestaan, via de KAPA-werkplek. Hiervandaan kan worden ingelogd op de jumpserver en kan men toegang krijgen tot systemen in de PA-omgeving van HHD. Externen krijgen toegang door het gebruik van de 'procedure inbellen door derden' (zie bronnen in paragraaf 3.2) te gebruiken. Rechtstreekse (vaste of draadloze) toegang tot het systeem vanuit niet HHD-netwerken, of visa versa, is niet toegestaan.

De systemen mogen uitsluitend over veilige protocollen communiceren.

Om ervoor te zorgen dat de verschillende PA-systemen dezelfde tijdinformatie hebben wordt er gebruik gemaakt van kloksynchronisatie via NTP. Dat is vooral belangrijk voor systemen waarin de timing van gebeurtenissen en processen essentieel is.

Om de verbindingen tussen PA-systemen of externe systemen met de PA-systemen extra te beveiligen maken we gebruik van digitale certificaten. De certificaten zorgen ervoor dat er encryptie wordt toegepast op de data die over de verbindingen gaat waardoor de data niet leesbaar is voor onbevoegden.

Om een veilig netwerk te houden monitort een tool wijdverspreid binnen HHD. Dit geldt voor de centrale PA-bediensystemen (level-2). Lokale en besturingssystemen binnen de PA (level-1) vallen buiten de scope van de tool die het netwerk van HHD monitort. Monitoring vindt plaats op kwetsbaarheden en afwijkend gedrag. Het SOK van HHD analyseert en rapporteert de uitkomst.

Zie voor meer informatie over het aansluiten van de systemen op het HHD-netwerk en de bepaling in welke zone systemen geplaats zijn, het zone- en conduitsmodel.

Voor cryptografie is er binnen Delfland een algemene richtlijn en een beleidsdocument (beleid inzake het gebruik van cryptografische beheersmaatregelen) aanwezig.

4.5 Bescherming tegen kwetsbaarheden

Elk PA-bediensysteem (MMI) is voorzien van een werkende en up-to-date virusscanner, die zo is ingesteld dat geen hinder ondervonden wordt op de werking en functionaliteit van de PA systemen. De virusscanner logt alle bevindingen en meldt actief de afwijken aan de beheerder of operator.

Om de beveiliging, stabiliteit en functionaliteit van de PA te waarborgen voeren we periodiek patches en updates door. De patches en updates worden door onze leveranciers aangeboden en actief gemeld. Het installeren en doorvoeren hiervan doen we gecontroleerd via het PA-change managementproces.

Hardening van de systemen wordt bij de installatie geregeld via de hardenigsprocedure, hierin wordt beschreven wat we verwachten van de hardening van systemen. Je moet hierbij denken aan het dichtzetten van ongebruikte netwerkpoorten en het verwijderen van software die niet wordt gebruikt of onderhouden of het uitzetten van ongewenste Windows services.

Bij het verwijderen of afvoeren van systemen is het van belang te voorkomen dat gevoelige informatie in handen komt van onbevoegden. In de "Procedure verwijderen of hergebruiken van PA-apparatuur" staat beschreven hoe we dat op een eenduidige manier aanpakken.

De richtlijnen 'hardening (PA-domein)' en 'patchmanagement' beschrijven specifieke procedures om onze PA te beschermen tegen kwetsbaarheden.

4.6 Logging en monitoring

Afdeling ICT voert logging- en monitoringactiviteiten uit. Alle maatregelen om het SOC te kunnen koppelen zijn genomen, daar waar het SOC nog verdere koppelingen in de toekomst wil gaan maken, is afgesproken dat het SOC dit eerst aan de PA-beheersorganisatie voorlegt, om verstoringen te voorkomen. Er is ook een PA-monitoring tool die automatisch alerts verstuurt naar het SOC.

De handelingen van medewerkers, beheerders, operators, meldingen vanuit systemen en eventlogs worden vastgelegd in audit-logbestanden. Deze logbestanden worden opgeslagen op een goedgekeurd platform. Ongeautoriseerde pogingen tot wijzigingen in software en opgeslagen gegevens worden automatisch gedetecteerd, gerapporteerd en voorkomen.

4.7 Bewustwording en training

De medewerkers worden gefaciliteerd en gestimuleerd in het volgen van opleidingen op het gebied van security.

4.8 Gecontroleerd wijzigen

Wijzigingen worden gecontroleerd middels het PA-changemanagementproces doorgevoerd. De gebruiker dient de gewenste wijziging in via TopDesk. De change board besluit, samen met de risico-eigenaar, of de wijziging wordt doorgevoerd. Afhankelijk van de risico's, complexiteit en impact bepalen zij het te doorlopen wijzigingsproces en nemen zij maatregelen om de risico's te beperken.

Om snel te kunnen reageren op een bedreiging of een incident hebben wij een overzichtelijk en actueel overzicht van alle PA-systemen. Dat overzicht is aanwezig in de Configuratie Management DataBase (CMDB). Het bijwerken van deze CMDB en bijbehorende tekeningen zijn onderdeel van het wijzigingsproces. Als controle op bijwerkingen en actualiteit van de CMDB wordt ook de procedure PA Configuratiemanagement gevolgd.

Om het gecontroleerd wijzigen voor de PA meer invulling te geven, zijn zowel changemanagement- en configuratiemanagementprocessen ingericht. Deze zijn beschreven in resp. 'change management PA Procedure' en 'procesbeschrijving PA configuratie management'.

4.9 Beheer en onderhoud

Om goed en veilig onderhoud aan de PA uit te voeren is ervoor gekozen om PA-laptops beschikbaar te stellen. Deze laptops worden enkel gebruikt om werkzaamheden binnen de PA-omgeving uit te voeren. Het gebruik en inrichting is beschreven in de "Procedure inrichting en gebruik PA-laptop". Voordat gegevensdragers (bijv. USB-harddrives, geheugenkaart), beheer- en onderhoudsapparatuur gekoppeld worden met de PA-systemen, controleren we of ze vrij zijn van malware.

Gedurende FAT, SAT en onderhoud houden we zicht op de werking van de cybersecurityfuncties in de systemen.

Onder beheer en onderhoud valt ook de 'procedure verwijderen of hergebruik van PA-apparatuur'.

4.10 Back-ups

Om na een verstoring of onbeschikbaarheid van de systemen, zo snel mogelijk weer naar een werkende situatie te komen is een proces ingericht rondom het maken van back-ups. Voor ieder PA-systeem is helder wie verantwoordelijk is voor de back-up, wat de frequentie is, hoe deze back-up wordt gemaakt en waar deze wordt opgeslagen. De precieze details zijn vastgelegd in het PA back-up en restore beleid.

Herstelprocedures zijn beschreven en worden jaarlijks getest volgens een afgestemd regime. Niet alles wordt ieder jaar even gedetailleerd getest, afhankelijk van een risicobeoordeling en een belangenbeoordeling wordt de interval en detail van de test vastgelegd en uitgevoerd.

Het beleid voor de PA hebben we vastgelegd in 'back-up en restore plan PA'.

4.11 Leveranciersmanagement

HDD is niet alleen verantwoordelijk voor het identificeren en beperken cyberrisico's binnen HDD, maar binnen de gehele toeleveringsketen. Daarvoor moeten we samenwerken met leveranciers om de gezamenlijke risico's te beheersen. Voor de PA betekent dit dat we afspraken maken met leveranciers over beveiligingsstandaarden, incidentrespons en monitoring. Door bijvoorbeeld het opnemen van eisen in contracten, zetten we stuur op het afdwingen van de beveiliging.

Voor leveranciersmanagement hanteren we de volgende documenten voor de PA bij HHD:

- *Standaard beveiligingseisen Delfland voor leveranciers*
- *Procesbeschrijving PA contract- en leveranciersmanagement*
- *Driemaandelijkse beoordeling speciale toegangsrechten*

De 'CSIR eisenlijst contractmanagement' is een hulpmiddel (Excel) dat we gebruiken om te bepalen welke CSIR-eisen binnen de scope van een leverancier vallen en welke eisen binnen de scope van HHD.

4.12 Risicomanagement

HHD dient een systematische aanpak te hanteren voor het identificeren, analyseren en beheersen van risico's. De PA lift mee op algemene initiatieven binnen HHD op het gebied van risicomanagement.

Voor de PA van HHD geldt het 'algemene risicobeleid'.

4.13 Continuïteitsmanagement

De NIS2-richtlijn benadrukt het belang van continuïteitsmanagement als onderdeel van onze cybersecurity. HHD is verplicht om maatregelen te implementeren die de continuïteit van onze primaire processen waarborgen, zelfs bij cyberincidenten. Voor de PA valt dit bijvoorbeeld onder 'beveiligingsincidenten en incidentrespons' (zie paragraaf 4.3) en 'back-ups en herstelprocedures' (zie paragraaf 4.10). Het 'eilandbedrijf' is een mooi voorbeeld van de continuïteitsmaatregelen die we