

RWS ONGECLASSIFICEERD

Handboek Security

Deel IV De realisatie

Datum	7 juni 2017
Status	Definitief

Colofon

Metagegevens

Proces:	Aanleg & Onderhoud
Proceseigenaar:	Jean-Luc Beguin
Netwerk:	Droog, Nat
Hoofdkennisveld:	Veiligheid en Crisis
Kennisveld:	Security
Soort document:	Kader (deel I heeft de status van een kader, deel II tot en met IV hebben de status van handreiking, de overige delen zijn informatie)
Datum vaststelling:	
Vastgesteld door:	
Van kracht vanaf:	
Overgangsregeling:	
Beveiliging:	Ongeclassificeerd
Beheerder:	GPO, afdeling Advies Technisch Management, Dirk-Jan Molenaar
Informatie:	Kaderadviseurs GPO/PPO
Verbetervoorstellen:	Dirk-Jan Molenaar
Toepassingsgebied:	Projecten voor aanleg en onderhoud (GPO/PPO) Beheer van objecten (OAM)
Versienummer:	3.2.0
Houdbaar tot:	Juni 2018
Monitoring gebruik:	GPO, afdeling Advies Technisch Management

Context

Procesdoel	uniformering van processen en voorzieningen, nodig voor borging van fysieke beveiliging van objecten
Inhoudelijk doel	Beheersing van alle fysieke beveiligingsaspecten van een object

Gebruikersgroepen

IPM rolhouders, projectadviseurs integrale veiligheid, assetmanagers	
Rol	Coördineren, initiëren, uitvoeren, communiceren, monitoren
benodigde kennis	Basiscursus integrale veiligheid in projecten

Hoofdproces

Aanleg & Onderhoud

Relatie met andere RWS standaarden

Wettelijk	Zie deel IV, hoofdstuk 2, Van kracht zijnde voorschriften en normen voor de securityvoorzieningen
Bovenliggend	Kader Veiligheidsmanagement RWS, 14 september 2011, WVL
Nevenliggend	Kader Integrale Veiligheid in Projecten 3.1

Toepassingsbereik

- Intern RWS, bij:
- Aanlegprojecten, van contractvoorbereiding tot oplevering;

- Onderhoudsprojecten, van contractvoorbereiding tot einde contract.
- Assetmanagement, areaalbeheer

Afwijken van kader

Conform de regels van de Werkwijzer RWS met toestemming vooraf van:

- de interne opdrachtgever;
- (tijdens verkenning en planuitwerking:) het Programmabureau Verkenningen & Planstudies voor het Hoofdwegennet en Hoofdvaarwegennet en het Programmabureau Aanleg Hoofdwatersysteem;
- (tijdens realisatie:) de portfoliomanager.

Leg afwijking met bijbehorende toestemming vast in het projectarchief. Geef de afwijking door aan de Kaderbeheerder (zie hierboven), voor het interne leerproces en verbetering van het Kader.

0	Introductie 8
1	Algemeen 10
2	Van kracht zijnde voorschriften en normen voor de securityvoorzieningen 11
2.1	Wetgeving 11
2.2	Regelgeving 11
2.3	Normen 11
2.4	Definities en afkortingen 12
2.5	Installatieconcretisering securityvoorzieningen 12
3	Algemene systeemeisen security RWS-locaties 13
3.1	Algemene basiseisen 13
3.2	Algemene ontwerpeisen terreinafscherming 13
3.2.1	Hekwerk 15
3.2.2	Hekwerkpoort voertuigen 15
3.2.3	Looppoort personen 15
3.2.4	Vluchtdeur 15
3.2.5	Overklimbelemmering 15
3.2.6	Open beveiligingstourniquet 15
3.3	Fysieke afscherming gebouwen en gebouwdelen 16
3.3.1	Algemene ontwerpeisen afscherming gebouw(delen) 16
3.3.2	Hang- en sluitwerk 16
3.3.3	Gevelopeningen 16
3.3.4	Beveiligingstoegangen 17
3.3.5	Compartimenten 17
3.4	Toegangsbeheersing en registratie 17
3.5	Algemene ontwerpeisen detectiesysteem 18
3.5.1	Terreindetectie 19
3.5.2	Gebouwdetectie 19
3.5.3	Warmtebeeld detectie 19
3.6	Algemene ontwerpeisen camera-observatie en -registratie 20
3.7	Verlichting ten behoeve van securitymaatregelen 21
3.8	Netwerken ten behoeve van security installaties 21
3.9	Video Management Systeem 22
3.10	Security Management Systeem 23
4	De eisen m.b.t. securitymaatregelen 28
4.1	Aanpassing/aanvulling securitygedragsregels 28
4.2	Aanpassing/aanvulling algemene securityprocedures 28
4.3	Aanpassing/aanvulling algemene securityprotocollen 28
4.4	Aanpassing/aanvulling kaderstellende securityprocedures 29

Wijzigingenoverzicht

Datum	Versie	Wijziging
December 2013	1.1	typefouten hersteld en arceringen verwijderd
Maart 2014	1.2	waardering wegcategorieën aangepast
Mei 2014	1.3	consistentie in terminologie aangebracht
December 2014	2.0	actualisering op basis van ervaringen met toepassing in de praktijk (indelingscriteria, weging categoriseringsfactoren), aanvullingen met uitgewerkte objecttypen en combinaties van objecttypen en de samenhang met Cybersecurity
Maart 2015	2.1	Versienummer gewijzigd, dubbel wijzigingenoverzicht verwijderd
Juni 2015	3.0	Aanpassingen o.b.v. de ervaringen vanuit het project IMPAKT in de BSN-opbouw.
December 2015	3.1	Versienummer gewijzigd
Juni 2017	3.2	Colofon aangepast naar aanleiding van wijzigingen in deel II en III (objecttypen toegevoegd)

O Introductie

Dit vierde deel van het handboek beschrijft de inrichting van security binnen Rijkswaterstaat en werkt het stappenplan voor de realisatie van de security bij Rijkswaterstaat uit.

Het eerste deel van het handboek security omvat de achtergronden, uitgangspunten en randvoorwaarden voor de inrichting van security binnen Rijkswaterstaat. Het eerste deel omvat het beleid en de kaders op Directieniveau binnen Rijkswaterstaat.

Het tweede deel van het handboek beschrijft de inrichting van security binnen Rijkswaterstaat en werkt voor de verschillende Rijkswaterstaat-locaties de basis security niveau's uit. Per objecttype is tevens het overzicht van de fysieke beveiliging van de cybersecurity opgenomen.

Het derde deel omvat handleidingen voor de geïdentificeerde Rijkswaterstaat-locaties waarmee het definitieve pakket aan securitymaatregelen en -voorzieningen wordt vastgesteld.

Het vijfde deel omvat de bijlagen waar in de andere delen naar wordt verwezen.

Het zesde deel omvat de bij Rijkswaterstaat geldende basis securitymaatregelen ten behoeve van de implementatie door de contractpartner of beheerder.

De eerste vier delen gezamenlijk omvatten het geheel voor een geïntegreerde aanpak van de security binnen Rijkswaterstaat. Het eerste deel is meer strategisch van aard, het tweede deel meer tactisch en het derde en vierde deel zijn meer operationeel. Door de ontwikkeling van deze afzonderlijke delen als één totaal pakket is geborgd, dat beleidsmatige keuzen operationeel vertaald kunnen worden en dat de operationele realisatie gebaseerd is op de binnen Rijkswaterstaat gebaseerde beleidskeuzen.

In de basisspecificaties van de diverse objecttypen dient middels een verwijzing de relatie naar dit handboek gemaakt te worden.

1 Algemeen

Dit deel van het Handboek Security van Rijkswaterstaat beschrijft het stappenplan voor de realisatie van de security van een object op het gewenste en vastgestelde niveau.

Het vaststellen van de gewenste security niveau voor een object van Rijkswaterstaat vindt plaats aan de hand van de voor dat object geldende handleiding vaststelling security. Per objectsoort is een daarop toegesneden handleiding beschikbaar.

Pas nadat het maatwerk securitypakket is vastgesteld en geautoriseerd, kan de realisatie worden uitgevoerd. Deze bestaat uit de volgende onderdelen:

- A. De vertaling van de onderdelen van de onderdelen van de geïntegreerde locatiespecifieke security in de ontwerpspecificaties voor de securityvoorzieningen. Dit specificatieoverzicht wordt als bijlage bij de Richtlijn Implementatie Security gevoegd.
- B. Realisatie van de implementatie aan de hand van de voor dat object geldende Richtlijn Implementatie Security (DBFM, D&C, PC of eigen beheer).

2 Van kracht zijnde voorschriften en normen voor de securityvoorzieningen

2.1 Wetgeving

Hieronder volgt een summiere opsomming van de wetgeving waar met betrekking tot de veiligheid van de bedrijfslocatie en personen mee te maken kan/zal hebben. Tot de belangrijkste behoren onder andere:

- Arbowet
- CPR-richtlijnen
- Woningwet (inzake brandveiligheid gebouwen)
- Wet op Brand doorslag en brand overslag
- Bouwbesluit
- Wet Bescherming Persoonsgegevens
- Burgerlijk wetboek
- Gebruikersvergunning
- Wet Beheer Rijkswaterstaatswerken
- Waterwet

2.2 Regelgeving

Het management is verantwoordelijk voor de uitvoering van het integraal beveiligingsbeleid (ondersteund door een netwerk van beveiliging- en integriteitscoördinatoren). Het gaat daarbij onder andere om de invulling van:

- Beveiligingsvoorschrift Rijksdienst 2005
- BIR: Baseline Informatiebeveiliging Rijk(2012)
- Voorschrift informatiebeveiliging Rijksdienst - Bijzondere Informatie 2004
- Wet veiligheidsonderzoeken
- Archiefwet (voor zover van toepassing)
- Wet bescherming persoonsgegevens
- Ambtenarenwet en ARAR (integriteit)
- Rijks PDC
- Rijksbeveiligingsbeleid
- In interdepartementaal verband afgesproken baselines
- Handboek Security RWS

2.3 Normen

- NEN 356 Glas in gebouwen – beveiligingsbeglazing.
- NEN 1010 Elektrotechnische norm voor laagspanningsinstallaties
- NEN 1303 Cilinders voor sloten: Eisen en beproevingsmethoden
- ENV 1627: 2011
- NEN 1303 Hang- en sluitwerk – Cilinders voor sloten- Eisen en
- NEN 1906 Deurklinen en knoppen: Eisen en beproevingsmethoden.
- NEN 3140 Bedrijfsvoering van elektrische installaties – Aanvullende Nederlandse bepalingen voor laagspanningsinstallaties.
- NEN 5089 Inbraakwerend hang- en sluitwerk- Classificatie, eisen en beproevingsmethoden.

- NEN 5096 Inbraakwerendheid – Dag- of gevelelementen met deuren, ramen, luiken en vaste vullingen – Eisen, classificatie en beproevingsmethoden.
- NEN 6702 Technische grondslagen voor bouwconstructies – TGB 1990 – Belastingen en vervormingen
- NEN 12209 Hang- en Sluitwerk- Sloten en grendels- Mechanisch bediende sloten, grendels en sluitplaten. Eisen en beproevingsmethoden.
- NEN 50131/ IS 01 Alarmsystemen- Inbraak en overvalsysteem- Deel 1: Systeemeisen

2.4

Definities en afkortingen

MI&M	Ministerie van Infrastructuur en Milieu
RWS	Rijkswaterstaat
CP	Contractpartner
DBFM	Design Built Finance and Maintain
D&C	Design and Construct
PC	Prestatie Contract
CCTV	Closed Circuit TeleVision
CIF	Kwaliteitsmaat van beeldweergave op een scherm.
Fps	Frames per seconde: video beelden per seconde.
Framerate	Het aantal beelden per seconde uitgedrukt in fps
Lux	Maat voor verlichtingssterkte
MTBF	Gemiddelde tijd tussen storingsmeldingen. Uptime
MTTR	Gemiddelde tijd tussen storingsmelding en functieherstel. Downtime.
False Positive	Het onterechte signaleren van terreinbetreding door een mens/groep mensen.
False Negative	Het onterecht niet signaleren van een terreinbetreding door een mens/ groep mensen.
NEN	Nederlandse Norm
SMS	Security Management Systeem
Tripwire	Virtuele lijn op videobeeld binnen intelligente video analyse. Bij overschrijden van deze lijn kan bijvoorbeeld een alarmsignaal gegeven worden.

2.5

Installatieconcretisering van securityvoorzieningen

Voor de installatieconcretisering van de securityvoorzieningen wordt het CPTED-concept toegepast voor de afschermingsvoorzieningen van terrein en gebouwen in onderlinge relatie tot elkaar. Dit houdt onder meer in, dat wanneer om welke reden dan ook een afscherming van de terreingrens met hekwerk niet acceptabel wordt geacht, de afschermingsweerbaarheid gerealiseerd zal moeten worden met natuurlijke middelen. Hiertoe wordt een adviseur Vormgeving en Ruimtelijke Kwaliteit ingeschakeld.

De CPTED-uitwerking wordt vastgelegd in een rapport, waarbij de effecten van de keuzes voor de terreinafscherming concreet worden aangegeven. Zie de Functionele Eisen Sociale Veiligheid voor meer informatie.

3 Algemene systeemeisen security RWS-locaties

3.1 Algemene basiseisen

1. De opstallen dienen afgeschermd te zijn van de openbare weg.
2. Indien de opstallen niet direct grenzen aan de openbare weg dient dit gerealiseerd te worden met hekwerk.
3. Doorgangen in de buitengevel worden afgesloten met deuren, roldeuren, nooddeuren.
Tourniquets worden alleen gebruikt bij personeelsingangen/ doorgangen voor fietsers.
4. Glasopeningen die vanaf de begane grond eenvoudig bereikbaar zijn worden voorzien van een extra afscherming. Deze dienen daarmee over het algemeen te worden aangebracht op de verdiepingen: begane grond, begane grond -1 en begane grond +1.
5. De eisen van de gevel(elementen) en hang en sluitwerk dienen op elkaar afgestemd te zijn.
6. Van nooduitgangen wordt het openen gedetecteerd.
7. Deuren van compartimenten worden voorzien van deurstandsignalering.
8. Binnendeuren voor zover deze een scheiding vormen tussen een hoger en een lager beveiligde ruimte, worden voorzien van deurstandsignalering.
9. In verkeersruimten op de begane grond dient bewegingsdetectie aanwezig te zijn.
10. Nadat een incident is gedetecteerd, vindt alarmverificatie plaats.
11. Bij cameraverificatie is minimaal een persoon voor herkenning in beeld te brengen. Herkenning: persoon is van top tot teen in beeld gebracht waarbij deze minimaal 50% van de beeldhoogte beslaat.
12. Bij cameraobservatie is minimaal een persoon voor observatie in beeld te brengen.
Observatie: persoon is van top tot teen in beeld gebracht waarbij deze minimaal 10% van de beeldhoogte beslaat.
13. Bij cameraobservatie is minimaal de volledige gevellijn van de opstal(len) te observeren.
14. Videobeelden worden opgeslagen zodat het incident achteraf kan worden bekeken.
15. De securitysystemen (afscherming, detectie, observatie, registratie) dienen 24 uur per dag operationeel te zijn.
16. De securitysystemen dienen te werken onder alle in Nederland voorkomende klimaat- en weerscondities.
17. Op een Security Management Systeem zijn alle beveiligingsinstallaties van de opstal(len) aangesloten.
18. De alarmsignalen alsmede de afhandeling ervan worden in het Security Management Systeem opgeslagen en geregistreerd.

3.2 Algemene ontwerpisen terreinafscherming

1. De terreinafscherming dient te voldoen aan de ontwerpspecificaties.
2. Het hekwerk, overklimbelemmering en de doorgang voldoen aan de volgende functionele eisen:

- a. niet onderkruipbaar;
 - b. niet doorkruipbaar;
 - c. niet met doe het zelf gereedschap demonteerbaar;
 - d. niet met doe het zelf gereedschap doorknipbaar;
 - e. niet met (huis- tuin- en keuken-)hulpmiddelen overklimbaar.
 - f. niet zonder de geëigende (elektronische) sleutel te openen.
3. De doorgang in het hekwerk dient zodanig geplaatst te worden, dat deze aansluit bij het hekwerk dat het terrein afsluit.
 4. De doorgang in het hekwerk dient van gelijke hoogte als het hekwerk te zijn.
 5. Indien het hekwerk voorzien is van overklimbelemmering, dan dienen de zich daarin bevindende doorgangen eveneens voorzien te zijn van overklimbelemmering.
 6. De doorgang in het hekwerk en het hekwerk moeten fysiek geheel op elkaar aansluiten ofwel:
tussen de uiteinden van de doorgang en de uiteinden van het hekwerk mag geen ruime zitten.
 7. Het hekwerk en doorgangen worden geplaatst op de perimeter van het terrein.
 8. De ondergrond dient zodanig bewerkt te zijn/worden, dat er geen mogelijkheid is en geen mogelijkheid geschapen kan worden, om onder het hekwerk en doorgangen door te kruipen.
 9. De doorgangen dienen vergrendeld te kunnen worden met een nachtvergrendeling.
 10. Voor elektrisch bediende doorgangen gelden de volgende eisen:
 - a. Ten behoeve van de automatische schuifpoorten zullen de volgende componenten worden aangebracht:
 1. inductielussen voor beveiliging/opensturing;
 2. een afknelbeveiliging;
 3. een infrarood straalset voor doorrijdbeveiliging;
 4. praatpalen voor intercomtoestellen;
 5. verkeerslichten (voor het geven van een stop-respectievelijk oprijdsignaal).
 6. deurstandsignalering.
 - b. Bediening van de doorgang dient plaats te vinden met behulp van paslezers opdat bevoegde personen, die in het bezit zijn van een geldige persoonsgebonden pas, zelf het beveiligde gebied kunnen betreden, respectievelijk verlaten zonder tussenkomst van de centrale bedienplaats.
 - c. De paslezers zijn aangesloten op de toegangscontrole-installatie.
 - d. Voorts is de besturing van de doorgang zodanig, dat de volgende signalen vanuit de bedienplaats van de doorgang kunnen worden gegeven:
 1. 'puls in';
 2. 'puls uit';
 3. blokkeren;
 4. deblokkeren;
 5. 'vrij uit'.
 6. Reset (spanningsloos waarna weer inschakelen)
 - e. Voertuigpoorten zijn voorzien van een uitrijdlus indien geen paslezer voor uitgaand verkeer wordt aangebracht.

3.2.1 *Hekwerk*

1. Als basis wordt draadmathekwerk (8 mm) als terreinafscherming gebruikt.
2. Indien draadmathekwerk in een bebouwde omgeving niet wenselijk of mogelijk is, dan wordt vierkante spijlenhekwerk gebruikt.
3. De hoogte dient waar relevant, gemeten vanaf het hoogste standvlak binnen een afstand van 1,5m aan weerszijden van het hekwerk, eveneens even hoog als het hekwerk te zijn.
4. Bij het plaatsten van het hekwerk dient daarnaast een naadloze aansluiting te worden gemaakt met de op het RWS-gebied aanwezige gebouwen, kunstwerken en geluidsschermen en dergelijke.

3.2.2 *Hekwerkpoort voertuigen*

1. Als basis wordt een vierkante spijlenpoort toegepast.
2. Als basis wordt de schuifpoort toegepast.
3. De paslezer dient bij doorgangen met een elektrische poort waar ook vrachtverkeer passeert zowel voor personenvoertuigen als vrachtvoertuigen geschikt te zijn.

3.2.3 *Looppoort personen*

1. Als basis wordt een vierkante spijlenpoort toegepast.
2. Als basis wordt de draaiport toegepast.
3. De looppoort dient te zijn voorzien van een deurdranger waardoor de looppoort na opening automatisch in het slot valt.

3.2.4 *Vluchtdeur*

1. Als basis wordt een vierkante spijlenpoort toegepast.
2. Als basis wordt de draaideur toegepast.
3. De vluchtdeur moet met één handeling te openen zijn.
4. De vluchtdeur mag uitsluitend van de binnenzijde van het terrein te openen zijn.
5. De vluchtdeur dient te zijn voorzien van een deurdranger waardoor de deur na opening automatisch in het slot valt.

3.2.5 *Overklimbelemmering*

1. Als basis de bij draadmathekwerk standaard aanwezige overklimbelemmering toepassen.
2. Poorten worden in het verlengde hiervan uitgevoerd met puntenkam.
3. Slechts op plaatsen met bijzondere risico's over kleinere afstanden toepassing van rolkammen.

3.2.6 *Open beveiligingstourniquet*

Voor de toegang tot een afgeschermd gebied kan om reden van bijzondere omstandigheden en/of securityrisico's gekozen worden voor een tourniquet in plaats van een looppoort. Met behulp van het tourniquet kunnen personen gecontroleerd worden toegelaten tot het beveiligde gebied zonder dat een directe open verbinding ontstaat tussen beide gebieden. Het tourniquet kan gecombineerd worden toegepast met een lage enkelvleugelige deur voor het doorvoeren van een fiets.

1. Het tourniquet moet zodanig zijn uitgevoerd dat de doorgang over de volledige hoogte en breedte wordt geblokkeerd.
2. Daar waar door het tourniquet de doorgang wordt afgesloten van een evacuatie-/vluchtroute, zal er naast het tourniquet ook een nooddeur worden aangebracht.
3. Bij afsluiting en vergrendeling van het tourniquet dienen de draaivleugels geblokkeerd te worden.
4. Indien geplaatst in een hekwerk dat als erfafscheiding dient, dan dienen het tourniquet en de eventuele nooddeur van gelijke hoogte als het hekwerk te zijn.
5. Indien het hekwerk voorzien is van overklimbelemmering, dan dient het zich daarin bevindende tourniquet (eventueel ook de daarin bevindende nooddeur) voorzien te zijn van overklimbelemmering.
6. Het tourniquet moet geschikt zijn voor zowel in- als uitgaand verkeer.
7. De capaciteit van het tourniquet dient zodanig te zijn dat de maximale wachttijd, gerekend vanaf één zijde, minder dan 15 seconden is.
8. Nadat personen het beveiligde gebied hebben betreden respectievelijk verlaten, moet dit worden doorgegeven aan de toegangscontrole-installatie (registratie aan-/ afwezigheid respectievelijk anti-passback faciliteit).
9. Bij onbevoegd gebruik dient het betreffende tourniquet direct te blokkeren.
10. Indien de spanning wordt onderbroken, moeten de betreffende onderdelen worden vergrendeld.
Het tourniquet moet dan zodanig worden gefixeerd dat uit ieder kwadrant vrij kan worden teruggetreden in het betreffende gebied (personen mogen bij spanningsuitval niet worden opgesloten).

3.3 Fysieke afscherming gebouwen en gebouwdelen

3.3.1 *Algemene ontwerpeisen afscherming gebouw(delen)*

1. De afscherming van gebouw(delen) dient aan de ontwerpspecificaties te voldoen
2. De gehele combinatie van elementen dient te voldoen aan de in de ontwerpspecificatie aangegeven weerstandsklasse gevelementen.

3.3.2 *Hang- en sluitwerk*

1. Een met het slot vergrendelde gevelopening mag in gesloten toestand niet uitneembaar zijn, c.q. verwijderd kunnen worden.
2. Cilinders mogen niet buiten het beslag uitsteken.

3.3.3 *Gevelopeningen*

1. Een gesloten gevelopening mag niet zonder toepassing van de (elektronische) sleutel te openen zijn.
2. Gevelopeningen kunnen worden voorzien van de meest passende en gewenste beschermingsmiddelen zoals inbraakwerend folie, rolluiken etc. om de noodzakelijke weerstandsklasse te realiseren.

3.3.4

Beveiligingstoegangen

Met behulp van beveiligingstoegangen kunnen personen gecontroleerd worden toegelaten tot het beveiligde gebied van een gebouw of gebouwdeel zonder dat een directe open verbinding ontstaat tussen beide gebieden.

1. De beveiligingstoegang kan in een open (beveiligingssluis, doorloopsluis, drie-armig draaikruis etc) of gesloten (beveiligingsdraaideur etc.) uitvoering worden toegepast, afhankelijk van de ontwerpspecificatie.
2. De beveiligingstoegang moet zodanig zijn uitgevoerd dat de doorgang over de volledige breedte van de gebiedsafscheiding wordt geblokkeerd.
3. Daar waar door de beveiligingstoegang de doorgang wordt afgesloten van een evacuatie-/vluchtroute, zal er naast de beveiligingstoegang ook een nooddeur worden aangebracht.
4. Bij afsluiting en vergrendeling van de beveiligingstoegang dienen de vleugels geblokkeerd te worden.
5. Indien geplaatst in een gebouwfafscheiding, dan dienen de beveiligingstoegang en de eventuele nooddeur van gelijke hoogte te zijn.
6. De beveiligingstoegang moet geschikt zijn voor zowel in- als uitgaand personenverkeer.
7. De capaciteit van de beveiligingstoegang dient zodanig te zijn dat de maximale wachttijd, gerekend vanaf één zijde, minder dan 15 seconden is.
8. Er mag in een beveiligingsdraaideur slechts één persoon tegelijk worden doorgelaten.
9. Bij onbevoegd gebruik dient de betreffende beveiligingsdoorgang direct te blokkeren.
10. Indien bij een gesloten beveiligingsdraaideur de spanning wordt onderbroken, moeten de betreffende onderdelen worden vergrendeld. Het tourniquet moet dan zodanig worden gefixeerd dat uit ieder kwadrant vrij kan worden teruggetreden in het betreffende gebied (personen mogen bij spanningsuitval niet worden opgesloten).

3.3.5

Compartimenten

1. De ramen, deuren, wanden, vloer en plafond van de ruimten dienen elk aan het in de ontwerpspecificatie aangegeven weerstandsniveau te voldoen.

3.4

Toegangsbeheersing en registratie

Doel:

Het gecontroleerd toelaten van personen en voertuigen tot beveiligd gebied (terrein/gebouw/gebouwdelen) en de registratie van aanwezigen.

Indien de Rijkspas wordt toegepast, dan dienen alle product- en installatie-eisen van de Rijkspas te worden toegepast.

Indien de Rijkspas niet wordt toegepast, dan gelden onderstaande minimum ontwerpseisen.

1. Het toegangsbeheersingssysteem dient geschikt te zijn voor:
 - a. automatisch toelaten van bevoegde personen tot het complex zonder tussenkomst van beveiligingsbeambten;

- b. legitimatie en identificatie van personen;
 - c. registratie van aan-/afwezigheid
 - d. ontgrendeling van poorten, tourniquets in perimeter door bevoegde personen na autorisatie via de persoonsgebonden pas.
 - e. per pashouder per aangegeven periode een overzicht te kunnen leveren over de, in de betreffende periode, per dag aangehouden aankomst- en vertrektijden.
- 2. De afstand tussen pas en paslezer voor het aanbieden van de toegangsaanvraag dient tenminste 10 tot 15 centimeter te kunnen bedragen.
- 3. Indien een paslezer wordt geactiveerd door het aanbieden van een pas zal binnen een tijdsbestek van 0,5 seconden:
 - a. na goedgekeurde autorisatie het betreffende slot wordt vrijgegeven (inclusief tijd benodigd voor ontgrendeling/vrijgave);
 - b. signalering plaats vinden naar de bedienplaats indien de toegang door het systeem wordt geweigerd.
 - c. de informatie wordt opgeslagen in het geheugen van het systeem en is daarmee beschikbaar voor rapportage.
- 4. Paslezers zullen zijn voorzien van een slagvaste vandaalbestendige behuizing.
- 5. Paslezers zullen zodanig zijn uitgevoerd dat deze volledig geschikt zijn voor de klimatologische omstandigheden waarin deze worden toegepast.
- 6. De persoonsgebonden pas dient voorzien te kunnen worden van een pasfoto van de betreffende pashouder.
- 7. Iedere keer als functie met wachtwoordbescherming wordt uitgevoerd, zal de naam van de gebruiker, die de functie oproept, worden vastgelegd in het systeem en beschikbaar zijn voor rapportage.
- 8. Alle systeemactiviteiten zullen door het systeem worden vastgelegd.
- 9. Uit het registratiebestand zal zowel een selectieve (per paslezer, toegangspas etc.) als een gehele print-out van historische informatie kunnen worden gemaakt.
- 10. Elke pas zal kunnen worden gekoppeld aan meervoudige toegangsniveau-/tijdzone- combinaties.
- 11. Er dient een tijdelijke pas aangemaakt te kunnen worden.
- 12. Bij uitgifte van een tijdelijke pas, als tijdelijke vervanging van een persoonsgebonden pas, wordt de oorspronkelijke pas direct automatisch geblokkeerd.
- 13. In het systeem zullen minimaal alle voor het object noodzakelijke toegangsniveaus kunnen worden toegewezen.
- 14. In het systeem zullen tenminste alle voor het object noodzakelijke tijdzones kunnen worden toegewezen.
- 15. In het systeem zullen tenminste alle op het object noodzakelijke paslezers kunnen worden opgenomen.
- 16. Een persoonsgebonden pas kan niet binnen een instelbare tijd voor een tweede maal worden aangeboden aan dezelfde paslezer. (timed antipass back)

3.5 Algemene ontwerpeisen detectiesysteem

1. Het detectiesysteem dient te voldoen aan de ontwerpspecificaties

2. Tijdens de standaard werkuren dient er geen detectie plaats te vinden bij de ingangen die voorzien zijn van een paslezer (reguliere personeelsingangen).
3. Na beschikbaar komen van het detectiesignaal dient een eventueel alarmsignaal binnen 15 seconden afgegeven te worden.
4. Het detectiesysteem dient in één of meerdere segmenten te kunnen worden opgezet.
5. Het detectiesysteem dient per segment te kunnen detecteren en (indien daartoe aanleiding toe is) per segment detectie/alarm signalen te kunnen genereren.
6. Het detectiesysteem dient per segment te kunnen worden uitgeschakeld cq. spanningsloos gemaakt te kunnen worden.
7. Het detectiesysteem dient in staat te zijn om meerdere (gelijktijdige) detectiesignalen/alarmen te kunnen afhandelen.
8. Detectiesystemen en onderdelen daarvan dienen vandaalbestendig te zijn aangebracht.
9. Het detectiesysteem en onderdelen daarvan dient/dienen zodanig van opzet te zijn dat sabotage (disfunctioneel maken) hiervan niet mogelijk is.

3.5.1 *Terreindetectie*

Voor de detectie op de locatie kan om reden van bijzondere omstandigheden en/of securityrisico's gekozen worden voor detectie op of nabij de terreinafscherming of op het terrein zelf.

Voor terreindetectie gelden de volgende (aanvullende) eisen:

1. Detectie dient plaats te vinden onder alle in Nederland voorkomende weersomstandigheden.
2. De detectieapparatuur op de terreinafscherming is onderverdeeld in afzonderlijk in- en uitschakelbare secties. De secties waar tijdens werktijden geen personen kunnen verblijven blijven tijdens werktijden ingeschakeld.
3. De detectieapparatuur is zodanig opgesteld, dat beschadiging of sabotage ervan van buiten het terrein niet mogelijk is.
4. De detectieapparatuur is zodanig opgesteld, dat de bedrijfsvoering op het terrein niet wordt gehinderd.
5. De detectieapparatuur heeft permanent vrij "zicht", d.w.z. in de detectiezones staan geen obstakels of is geen belemmerende groenvoorziening.
6. Een door de terreindetectie tijdens werktijd gegenereerd alarm wordt onmiddellijk doorgemeld aan de bedienpost.

3.5.2 *Gebouwdetectie*

1. De gebouwdetectie voldoet aan de uitvoeringseisen van de BORG-ontwerpspecificatie.
2. Bewegingsdetectoren zijn altijd anti-mask uitgevoerd.
3. Nooddeuren zijn voorzien van "open deur" signalering.

3.5.3 *Warmtebeeld detectie*

1. Detectiebetrouwbaarheid dient 100% te bedragen.

2. Het detectiesysteem met warmtebeeldcamera's dient in staat te zijn om mensen (één, meerdere en/of groepen) met 100% waarschijnlijkheid te detecteren.
3. Bij detectie van mensen (één, meerdere en/of groepen) in de detectiezone dient het betreffende beeld automatisch getoond te kunnen worden aan de bedienpost.
4. Bij detectie van mensen (één, meerdere en/of groepen) in de detectiezone (en presentatie van de camerabeelden) dient op de bedienpost een akoestisch en optisch attentiesignaal gegeven te worden.
5. Het systeem dient 24 uur per dag operationeel te zijn.
6. Het detectiesysteem dient normaal te blijven functioneren bij het tijdelijk wegvallen van de voedingsspanning.
7. Bij terugkeer van de voedingsspanning (na tijdelijke onderbreking) dient het systeem terug te keren in functionerende modus.

3.6 Algemene ontwerpeisen camera-observatie en -registratie

1. De observatiecamera's dienen op afstand met de hand bestuurd te kunnen worden.
2. De camera's dienen handmatig geactiveerd te kunnen worden vanaf de bedienplek.
3. De camera's kunnen handmatig bediend worden vanaf de bedienplek.
4. De camera's keren na handmatige bediening terug in de voorkeursstand.
5. De camera's dienen een goed beeld in kleur te geven bij zowel daglicht als bij lage lichtsterkten.
6. De camera's dienen bij onvoldoende omgevingslicht automatisch om te schakelen van kleur naar zwart/wit en vice versa.
7. Bij het wegvallen van de voedingsspanning dient het systeem op de normale/correcte manier af te sluiten.
8. Bij het terugkeren van de voedingsspanning (na wegvallen van voedingsspanning) dient het systeem weer in te schakelen in de standaardinstelling.
9. Camera's zijn uitgerust volgens IP technologie.
10. Beelden van de camera's worden opgeslagen.
11. Beelden worden maximaal 28 dagen bewaard en daarna automatisch door het systeem verwijderd.
12. Opgeslagen beelden mogen alleen toegankelijk zijn voor bevoegden.
13. Het systeem dient voorzien te zijn van faciliteit om de authenticiteit en integriteit van de beelden te kunnen waarborgen.
14. Bewerken van opgeslagen beelden is niet toegestaan.
15. Het moet mogelijk zijn een kopie van beelden op te slaan op een extern opslagmedium. De beelden die extern zijn opgeslagen mogen alleen toegankelijk zijn voor bevoegden.

3.7 Verlichting ten behoeve van securitymaatregelen

1. De verlichting is gericht op de observatie- of verificatiezone.
2. Omliggende/naastliggende bebouwing mag door de verlichting niet worden aangestraald.
3. De verlichting mag geen hinder opleveren voor wegverkeer of omwonenden.
4. De verlichting dient zodanig te zijn dat de kleuren van objecten, personen, kleding en signalerende kleding natuurgetrouw worden weergegeven.
5. Ter voorkoming van schaduwvorming is op de observatie- of verificatiezone een gelijkmatige terreinverlichting aanwezig.
6. Het minimale verlichtingsniveau op de observatie- of verificatiezone is 5-9 lux.

3.8 Netwerken ten behoeve van security installaties

1. Het netwerk dient zodanig gedimensioneerd te zijn dat minimaal 20 videostreams (ieder 25 fps) tegelijkertijd op de bedienlocatie gepresenteerd kunnen worden. Dit ongeacht de bron van de videobeelden.
2. Middels FMECA dient aangetoond te worden dat het netwerk de gevraagde beschikbaarheid van de (sub)systemen ondersteund.
3. Het netwerk dient uitval van netwerkapparatuur op te kunnen vangen zonder dat dit gevolgen heeft voor functionaliteit en functioneren van het netwerk als geheel.
4. Enkelvoudige kabelbreuk in het netwerk dient de functionaliteit van het netwerk niet te beïnvloeden.
5. Uitval van elementen in het netwerk mogen geen negatieve invloed hebben op de functionaliteit van het netwerk als geheel.
6. Voor de eventueel benodigde grondwerkzaamheden dienen de richtlijnen van Rijkswaterstaat gevolgd te worden.
7. De transmissie infrastructuur dient eenvoudig uitgebreid te kunnen worden zonder dat de architectuur van het netwerk herzien behoeft te worden.
8. De grenzen van de uitbreidbaarheid van het toegepaste transmissienetwerk dient in het ontwerp aangegeven te worden.
9. Het toegepaste transmissienetwerk dient geschikt te zijn voor transport van signalen uit meerdere systeemfuncties (i.e. video, audio, signalering en besturing)
10. Het netwerk dient een MTBF te hebben van 60.000 uur.
11. Het netwerk dient een MTTR te hebben van 48 uur
12. De gemiddelde reparatietijd van de afzonderlijke delen van het systeem mag niet meer dan 2 uur bedragen.
13. Het systeem dient 24 uur per dag operationeel te zijn.
14. Het systeem dient een beschikbaarheid te hebben van 99,95% per jaar.
15. Het onderhoud dient zodanig plaats te kunnen vinden dat de functionaliteit van het netwerk niet onderbroken dient te worden.

16. De levensduur van componenten en het systeem dient ten minste 10 jaar te bedragen.

3.9 Video Management Systeem

1. Toezicht dient plaats te kunnen vinden in daartoe geëigende bedienpost.
2. Alarmen van de op beveiligd gebieden opgestelde systemen dienen direct automatisch beschikbaar te zijn in de bedienpost.
3. Binnenkomende alarmen dienen middels een signaal kenbaar gemaakt te worden bij de bedienpost. (blackscreen + popup, auditief, visueel)
4. Multibeeld van alle camera's dient mogelijk te zijn.
5. Presentatie van meerdere beelden tegelijk op een scherm is mogelijk.
6. Het systeem dient een 'standaard product' te zijn (geen maatwerk; paswerk is wel toegestaan)
7. Een software development kit (SDK) voor het tonen van real-time camera beelden moet worden geleverd en integreerbaar zijn in WinsowsXP, WindowsVista, Windows7 en Linux omgeving.
8. De SDK moet compliant zijn met/ en geleverd worden voor Windows XP SP2 en SP3, Windows Vista, Windows7 en Linux.
9. Maken van een video still in JPEG formaat uit de realtime stream moet mogelijk zijn.
10. In het systeem dient de mogelijk geactiveerd te kunnen worden dat de Particuliere Alarm Centrale en/of politie op afstand kan meekijken.
11. Beeldtransmissie naar de alarmcentrale en/of politie dient mogelijk te zijn.
12. Aan een detectiealarm dienen de camerabeelden te worden gekoppeld die het dichtst in de buurt van het detectie(segment) staan.
13. De bij een alarm behorende camerabeelden dienen automatisch en direct getoond te worden aan een bedienpost.
14. Het systeem dient de mogelijkheid te bezitten om camerabeelden van incidenten door te sturen naar een PDA van een beveiligder.
15. Ten behoeve van het terugzoeken van beelden dienen deze op datum en/of binnen tijdgrenzen benaderd te kunnen worden.
16. Ten behoeven van het terugzoeken van beelden dienen deze op datum en/of een specifiek tijdstip benaderd te kunnen worden.
17. De opgeslagen videobeelden dienen versneld, vertraagd, beeld voor beeld en op normale snelheid afgedraaid te kunnen worden.
18. Stilstaand beeld van opgenomen beelden dient mogelijk te zijn.
19. Het dient mogelijk te zijn om de videobeelden in diverse bestandsformaten op te slaan en/of om te zetten.
20. Het bekijken van opgenomen camerabeelden mag geen invloed hebben op de realtime werking van het camerasysteem.
21. De bedientafels dienen inricht te worden volgens het ARBO themacahier "Werken in meld- en controle kamers".
22. Het systeem dient een MTBF te hebben van 60.000 uur.
23. Het systeem dient een MTTR te hebben van 48 uur

24. De gemiddelde reparatietijd van de afzonderlijke delen van het systeem mag niet meer dan 2 uur bedragen.
25. Het systeem dient 24 uur per dag operationeel te zijn.
26. Het systeem dient een beschikbaarheid te hebben van 99,95% per jaar.
27. De levensduur van componenten en het systeem dient ten minste 10 jaar te bedragen.

3.10 Security Management Systeem

Het SMS dient de volgende taken te ondersteunen:

1. uitvoeren van bedieningshandelingen voor de volgende installaties:
 - a. de toegangscontrole-installatie;
 - b. de detectie-installatie
 - c. de verificatie-installatie
 - d. de observatie-installatie;
 - e. registratie van (alarm)meldingen;
 - f. het eenduidig afhandelen van (alarm)meldingen vanuit de diverse voorzieningen van het beveiligingssysteem;
2. De centrale apparatuur van de volgende installaties mag geen onderdeel uitmaken van respectievelijk zijn geïntegreerd in het Security Management Systeem:
 - a. de toegangscontrole-installatie.
 - b. de detectie-installatie
 - c. de verificatie-installatie
 - d. de observatie-installatie;
3. Een interactieve werking tussen de volgende installaties mag niet worden gevoerd via het Security Management Systeem.
 - a. de toegangscontrole-installatie.
 - b. de detectie-installatie
 - c. de verificatie-installatie
 - d. de observatie-installatie;
4. Op het systeem zullen diverse werkstations kunnen worden aangesloten. Deze werkstations zijn met de centrale apparatuur verbonden door middel van TCP/IP gebaseerde ethernet netwerken.
5. In het gehele systeem zal met één tijdstandaard worden gewerkt en zal gesynchroniseerd kunnen worden met een atoomklok of vergelijkbare oplossing.
6. Alle registraties zullen volgens één tijdstandaard worden vastgelegd. Afwijkingen in tijden zijn niet toegestaan.
7. Zomer- en wintertijdschakeling zal automatisch plaatsvinden.
8. De beheerder zal zelf de, bij de in- en uitgangscircuits behorende, relevante gegevens (parameters) kunnen toevoegen, verwijderen of herbestemmen door middel van toetsenbordcommando's.
9. De volgende (Alarm)meldingen dienen op het SMS binnen te komen:
 - a. Uit de toegangscontrole-installatie
 - b. Uit de detectie-installatie
 - c. Uit de verificatie-installatie
 - d. Uit de observatie-installatie;
 - e. sabotagemeldingen;
 - f. storingsmeldingen;
 - g. diversen.

10. De functionaliteit van het SMS dient doorgeschakeld te kunnen worden naar een ander beheersysteem. (Zoals bijvoorbeeld gebruikelijk bij dag/nacht schakeling) Op het andere beheersysteem dient de functionaliteit overgenomen te kunnen worden.
11. Meldingen worden wel op het SMS weergegeven als de systemen zijn doorgeschakeld naar een andere beheersysteem. (zoals bijvoorbeeld bij doorschakelen naar alarmcentrale tijdens nachturen)
12. Het gehele systeem is Nederlandstalig. Dit geldt o.a. voor de GUI, bedieningsmeldingen, alarmmeldingen, alarmafhandeling, bedienteksten, handleidingen, print-outs, besturing- en bedienknoppen.
13. Het systeem dient een 'standaard product' te zijn (geen maatwerk; paswerk is wel toegestaan)
14. Alle print-outs en boodschappen zullen in de Nederlandse taal zijn gesteld.
15. Aan de hand van verklarende teksten zullen beveiligingsbeambten worden ondersteund bij het verwerken van (alarm)meldingen en het gebruik van het systeem. Indien de beveiligingsbeambte uit meerdere mogelijkheden kan kiezen, zal het systeem een menu met beschikbare keuzen weergeven.
16. De bedienpost zal met behulp van functietoetsen:
 - a. Procedures voor alarmafhandeling kunnen verrichten;
 - b. statusoverzichten kunnen opvragen en zo nodig kunnen uitprinten.
 - c. Alarmmeldingen dienen chronologisch te worden opgeslagen in het betreffende registratiebestand;
 - d. Alarmmeldingen worden getoond op het betreffende beeldscherm (op basis van weergegeven van teksten/plattegronden). Met behulp van een functietoets (eenmaal klikken met de muis) wordt de alarmmelding geaccepteerd en gepresenteerd op het beeldscherm.
17. Bij acceptatie van de alarmmelding wordt de het tijdstip van de melding geregistreerd.
18. Het akoestisch en optisch attentiesignaal wordt gelijktijdig met acceptatie van de melding afgesteld.
19. Bij meer dan één alarm wordt het oudste alarm met de hoogste prioriteit getoond of kan door de bedienpost zelf de keuze worden bepaald.
20. Nadat de alarmmelding op het scherm is verschenen en de bedienpost de vereiste actie heeft ondernomen, zal een 'functietoets' ter bevestiging worden bediend. Vervolgens zal het alarm van het beeldscherm en uit de 'wachtrij' verdwijnen (reset na alarmmelding).
21. Alarmmeldingen zullen alleen kunnen worden 'ge-reset' nadat de bedienpost heeft aangegeven welke acties zijn genomen en bevindingen zijn vastgesteld (logboekfunctie).
22. Terugkeer naar de 'rustsituatie' worden geregistreerd in het betreffende bestand.
23. Indien meerdere alarmmeldingen worden doorgegeven, kan het akoestische en optische attentiesignaal met een aparte functietoets worden afgesteld.
24. Op het beeldscherm wordt zichtbaar gemaakt welke alarmmeldingen aanwezig zijn welke 'wachten' op verdere afhandeling door de beveiligingsbeambte(n).

25. Middels een functietoets dient een lijst van openstaande alarmmeldingen respectievelijk 'geparkeerde' alarmmeldingen getoond te worden.
26. Middels een functietoets moet een alarmmelding zichtbaar gemaakt kunnen worden.
27. Indien een alarmmelding op een beeldscherm wordt getoond, zullen volgende gegevens getoond moeten worden
 - a. datum en tijd,
 - b. een omschrijving van het systeem (onderdeel) dat de melding veroorzaakt.
 - c. de status waarin het betreffende systeemonderdeel zich bevindt;
 - d. een instructie welke handelingen door beveiligingsbeambten zullen worden verricht (Voor de instructie dienen tenminste 280 karakters en minimaal 5 regels beschikbaar te zijn.);
 - e. een plattegrondtekening van de locatie waar het systeem(onderdeel) zich bevindt, met daarop een aanduiding van de plek waar het systeemonderdeel zich bevindt. Op deze plek is het type (systeem)onderdeel aangegeven.
28. Bij iedere (alarm)melding moet in het logboek een toelichting gegeven kunnen worden door de bedienpost.
29. Het zal mogelijk zijn dat afgehandelde alarmmeldingen van circuits, die niet zijn terug gekeerd in de rustsituatie met een bepaalde periodiciteit opnieuw onder de aandacht van de beveiligingsbeambte te brengen.
30. Aan elk circuit zal een categorie-indeling kunnen worden toegekend.
31. Aan elk circuit zal een prioriteitsniveau kunnen worden toegekend.
32. De prioriteit die aan een alarmcircuit is toegekend, bepaalt de positie in de wachtrij.
33. Het systeem bevat tenminste tien prioriteitsniveaus.
34. Individuele alarmcircuits of groepen alarmcircuits zullen door toetsenbordhandelingen en/of conventionele bedieningselementen buiten werking kunnen worden gesteld. (Overschakelen in een dag-/nachtschakeling)
35. (Alarm)meldingen moeten in tenminste 25 tijdsperioden kunnen worden ingedeeld.
36. Indien een alarmcircuit of groep buiten werking is gesteld mogen statusveranderingen niet meer worden weergegeven op de betreffende beeldschermen en/of verdere acties tot gevolg hebben (interactieve werking met andere installaties).
37. Een alarmcircuit of groep zal buiten werking blijven, totdat het commando is opgeheven door het betreffende commando.
38. Schakelfuncties zullen op de volgende wijze kunnen worden gerealiseerd:
 - a. door middel van toetsenbordcommando's;
 - b. door middel van bediening van functietoetsen;
 - c. volgens vooraf geprogrammeerde condities (kalenderfunctie).
39. Alle schakelhandelingen zullen chronologisch worden opgeslagen in het betreffende registratiebestand.

40. Storingen in circuits worden automatisch in het SMS geregistreerd.
41. Storingen in circuits die buiten werking zijn gesteld worden automatisch in het SMS geregistreerd.
42. Het SMS en de daarbij behorende grafische gebruikers bediening (GUI: graphic user interface) is bruikbaar voor zowel de alarmverwerking als voor de gebruikersfuncties en de systeemfuncties
43. Het presenteren van alarmen, het uitvoeren van systeemfuncties en functies voor beheer van de database zijn tegelijk mogelijk op meerdere posten zonder dat de alarmverwerking en afhandeling verstoord wordt.
44. Alarmen moeten op een vooraf ingestelde post/beeldscherm binnen kunnen komen ter afhandeling.
45. Bevoegdheden voor systeem- en gebruikershandelingen zullen in het SMS met wachtwoorden zijn afgeschermd.
46. In het SMS zullen tenminste vier niveaus voor autorisatie kunnen worden ingevoerd.
47. Elk wachtwoord zal bestaan uit tenminste zeven alfanumerieke tekens.
48. Het systeem dient tenminste 100 wachtwoorden te kunnen beheren.
49. Onder het hoogste wachtwoordniveau zullen wachtwoorden aan elk bevoegdheidsniveau kunnen worden toegewezen.
50. Iedere keer als een wachtwoordbeschermende functie wordt uitgevoerd, zal de naam van de gebruiker, die de functie oproept, worden vastgelegd in het registratiebestand.
51. Alle systeemactiviteiten zullen door het systeem worden vastgelegd in het registratiebestand.
52. De capaciteit van het registratiebestand zodanig dat hierin de gebeurtenissen kunnen worden vastgelegd voor een periode van tenminste 30 dagen.
53. Uit het registratiebestand zal zowel een selectieve (per alarmpunt, per alarmsoort etc.) een printout van volledige historische informatie kunnen worden gemaakt.
54. Alle systeembestanden zullen kunnen worden uitgeprint zonder de alarmverwerking te onderbreken/beïnvloeden.
55. Voor het printen van bestanden zal het mogelijk zijn chronologisch gezien een start- en stoplimiet in te stellen.
56. Het maken van reservekopieën zal de (alarm)verwerking van het risicobeheersysteem niet beïnvloeden;
57. Met behulp van een 'functietoets' zullen statusoverzichten per alarmcategorie op de betreffende
58. beeldschermen worden getoond, waarbij alle uitzonderlijke condities zijn vermeld die op dat moment in de betreffende alarmcategorie bestaan.
59. In de statusoverzichten zullen de gegevens zodanig worden gepresenteerd dat deze door 'leken' kunnen worden beoordeeld zonder technische achtergrondinformatie. Meldingen mogen niet in code worden weergegeven.
60. Fabrikant/ Leverancier dient aan te tonen en te garanderen dat het systeem een 'Open Architectuur' heeft.
61. Fabrikant/ Leverancier dient de open architectuur te ondersteunen door het beschikbaar stellen van een SDK.

- 62. Fabrikant/ Leveranciers levert diensten om apparatuur (eventueel middels de geleverde SDK) aan te sluiten op het SMS.
- 63. Het systeem dient een MTBF te hebben van 60.000 uur.
- 64. Het systeem dient een MTTR te hebben van 48 uur
- 65. De gemiddelde reparatietijd van de afzonderlijke delen van het systeem mag niet meer dan 2 uur bedragen.
- 66. Het systeem dient 24 uur per dag operationeel te zijn.
- 67. Het systeem dient een beschikbaarheid te hebben van 99,95% per jaar.
- 68. De levensduur van componenten en het systeem dient ten minste 10 jaar te bedragen.
- 69. Er kunnen systemen van andere fabrikanten op het SMS worden aangesloten waarbij de functionaliteit van het SMS volledig ondersteund blijft.

4 De eisen m.b.t. securitymaatregelen

4.1 **Aanpassing/aanvulling securitygedragsregels**

- De aanpassing/aanvulling van de securitygedragsregels worden onder verantwoordelijkheid van de objectbeheerder opgesteld, gevalideerd en geautoriseerd voor zover deze reikwijdte van de gedragsregel niet verder reikt dan het object zelf.
- De lokale gedragsregels mogen nimmer strijdig zijn met algemeen geldende gedragsregels voor geheel Rijkswaterstaat.
- Is de reikwijdte van de aangepaste gedragsregel locatie overstijgend, dan geschiedt validatie en autorisatie door de voor het werkingsgebied bevoegde bestuurder.
- De aangepaste securitygedragsregels worden aan de betrokken medewerkers en overige gebruikers van de locatie toegelicht en geïnstrueerd.

4.2 **Aanpassing/aanvulling algemene securityprocedures**

- De aanpassing/aanvulling van de securityprocedures worden onder verantwoordelijkheid van de objectbeheerder opgesteld, gevalideerd en geautoriseerd voor zover deze reikwijdte van de securityprocedures niet verder reikt dan het object zelf.
- De lokale securityprocedures mogen nimmer strijdig zijn met algemeen geldende securityprocedures voor geheel Rijkswaterstaat.
- Is de reikwijdte van de aangepaste securityprocedure locatie overstijgend, dan geschiedt validatie en autorisatie door de voor het werkingsgebied bevoegde bestuurder.
- Voordat de securityprocedures worden ingevoerd, vindt een uitgebreide test op de werking plaats.
- De aangepaste securityprocedures worden na te zijn getest en in orde bevonden aan de betrokken medewerkers en overige gebruikers van de locatie toegelicht en geïnstrueerd.

4.3 **Aanpassing/aanvulling algemene securityprotocollen**

- De aanpassing/aanvulling van de securityprotocollen worden onder verantwoordelijkheid van de objectbeheerder opgesteld, gevalideerd en geautoriseerd voor zover deze reikwijdte van de securityprotocollen niet verder reikt dan het object zelf.
- De lokale securityprotocollen mogen nimmer strijdig zijn met algemeen geldende securityprotocollen voor geheel Rijkswaterstaat.
- De aanpassing van de securityprotocollen geschiedt altijd in overleg met de securitydienstverlener(s), die in het protocol een deel van de werkzaamheden uitvoert.
- Is de reikwijdte van het aangepaste securityprotocol locatie overstijgend, dan geschiedt validatie en autorisatie door de voor het werkingsgebied bevoegde bestuurder.
- Voordat de securityprotocollen worden ingevoerd, vindt met de externe dienstverleners een uitgebreide test op de werking plaats.
- De aangepaste securityprocedures worden na te zijn getest en door zowel de externe dienstverleners als Rijkswaterstaat in orde bevonden,

door de externe dienstverleners in hun uitvoeringsprocedures geïmplementeerd. Nadat bij controle gebleken is, dat deze implementatie correct is uitgevoerd, worden de aangepaste securityprotocollen aan de betrokken medewerkers en overige gebruikers van de locatie toegelicht en geïnstrueerd.

4.4

Aanpassing/aanvulling kaderstellende securityprocedures

De aanpassing/aanvulling van de kaderstellende securityprocedures worden altijd onder verantwoordelijkheid van de contractbeheerder met de externe securitydienstverlener(s) opgesteld, gevalideerd en geautoriseerd.

Handboek Security

Nummer:	1364
Versie:	2.4
Status:	In beheer
Type:	Kader
Inhoudelijk beheerder:	Dirk-Jan Molenaar
Verantwoordelijke afdeling:	Afd. Advies Technisch Management
Netwerken:	Hoofdvaarwegennet, Hoofdwatersysteem, Hoofdwegennet
Rollen:	Technisch Manager
Fase:	Planuitwerking, Realisatie, Onderhoud
Proceseigenaar	Proceseigenaar Aanleg en Onderhoud