



Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

RWS ONGECLASSIFICEERD

Handboek Security

Deel I Achtergronden, uitgangspunten en randvoorwaarden

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

Rol	IPM rolhouders, projectadviseurs integrale veiligheid, assetmanagers
benodigde kennis	Coördineren, initiëren, uitvoeren, communiceren, monitoren
	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.



Inhoud

0	Introductie 8
1	Inleiding 9
2	Definities en afbakeningen 10
2.1	Het begrip security 10
2.2	Security middelen zijn maatregelen én -voorzieningen 11
2.3	Afbakening 11
3	Nut en noodzaak van security 12
4	Doel en gebruik handboek security 14
5	Context van de security bij Rijkswaterstaat 16
5.1	Wet- en regelgevend kader algemeen 16
5.2	Specifieke regelgeving 17
5.3	Stakeholders en hun belangen 17
5.3.1	Op basis van wettelijke voorschriften 18
5.3.2	Op basis van eigen bedrijfscontinuïteit Rijkswaterstaat 18
5.3.3	Op basis van het gebruik van (vaar)wegen en hoofdwatersystemen 18
5.3.4	Vanuit hun eigen belangen 18
6	De security bij Rijkswaterstaat 20
6.1	De security-aandachtsgebieden 20
6.2	Hoe gaat Rijkswaterstaat met de securityrisico's om? 21
6.3	De opbouw van de security bij Rijkswaterstaat 22
7	Algemene uitgangspunten, prestatie-eisen en doelstellingen security 24
7.1	Algemene uitgangspunten 24
7.2	Algemene prestatie-eisen 25
7.3	Algemene doelstellingen 25
8	Securityrandvoorwaarden en –kaders bij Rijkswaterstaat 28
8.1	Rol en positionering Rijkswaterstaat m.b.t. security 28
8.2	Vormgeving Security Rijkswaterstaat 28
8.3	Organisatorische en procesmatige inrichting van de security 30
8.4	De algemene securitybeheersingsdoelen 31
8.5	De algemene securitymiddelen: maatregelen én voorzieningen 32
8.6	De aard en inzet van de securitymiddelen 34
9	De organisatorische en procedurele securitymaatregelen 38
9.1	De doelen van de securitymaatregelen 38
9.1.1	Security-awareness 38
9.1.2	Securitygedragsregels 38
9.1.3	Algemene securityprocedures 38
9.1.4	Kaderstellende securityprocedures 39
9.1.5	Alarmopvolging 39
9.2	Functionele eisen securitymaatregelen 39
9.2.1	Security-awareness 39
9.2.2	Securitygedragsregels 39
9.2.3	Algemene securityprocedures 39

9.2.4	Alarmopvolging	40
9.3	Algemeen geldende securitygedragsregels	40
9.4	Algemeen geldende securityprocedures	40
9.5	Kaderstellende securityprocedures	40
9.6	Securityprotocollen	41
9.7	Locatiespecifieke inrichting en uitwerking	41
10	Securityvoorzieningen	42
10.1	Doelen van de securityvoorzieningen	42
10.1.1	Fysieke afscherming van terreinen	42
10.1.2	Fysieke afscherming van gebouwen	42
10.1.3	Toegangsbeheersing	42
10.1.4	Cameratoezicht en -registratie	42
10.1.5	Detectie en alarmering	42
10.2	Algemene functionele eisen securityvoorzieningen	43
10.3	Inrichting van de securityvoorzieningen	43
10.4	Technische specificaties van de securityvoorzieningen	43
11	De categorisering van de infrastructurele locaties	44
11.1	De opzet van de categoriseringsmethodiek	44
11.2	De infrastructurele type Rijkswaterstaat-locaties	45
11.3	De bedrijfsprocesfactoren van Rijkswaterstaat-locaties	46
11.4	Motiveringen subverdelingen bedrijfsprocesfactoren	46
11.4.1	Bestuurlijke bedrijfsprocesfactoren	46
11.4.2	Bedrijfsmatige bedrijfsprocesfactoren	47
11.5	De attractiviteitsfactoren van de RWS-locaties	48
11.6	Motiveringen subverdelingen attractiviteitsfactoren	48
11.6.1	Omgeving gerelateerde factoren	48
11.6.2	Locatie gerelateerde factoren	50
11.6.3	Infra gerelateerde factoren	53
11.7	Waardering criteria risicogene factoren	54
11.8	Waarderingsmatrix	54
12	De Basis Security Niveau's (BSN's)	55
12.1	Relevante securityrisico's	55
12.2	Relevante incidentscenario's	55
12.3	Daderprofielen	56
12.4	Opbouw van de Basis Security Niveau's (BSN)	57
12.4.1	Algemeen	57
12.4.2	Indeling in Basis Security Niveaus (BSN)	58
12.5	Programma Regie op Industriële Automatisering (PRIA)	59
12.6	Hoe wordt de risicobeheersing bereikt?	59
12.7	BSN als onderdeel totaal securitypakket	60



Wijzigingenoverzicht

Datum	Versie	Wijziging
December 2013	1.1	Typefouten hersteld en arceringen verwijderd
Maart 2014	1.2	Waardering wegcategorieën aangepast
Mei 2014	1.3.1	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, de samenhang met Cybersecurity aangebracht en handleidingen vaststelling security vereenvoudigd
Maart 2015	2.1	Versienummer gewijzigd
Juni 2015	3.0	Aanpassingen o.b.v. de ervaringen vanuit het project IMPAKT in de BSN-opbouw.
December 2015	3.1	Aanvullingen relevanties van weggerelateerde objecttypen Verplaatsing van relevantie-overzichten naar Deel V.
Juni 2017	3.2	Paragraaf 11.2 aangevuld Colofon aangepast naar aanleiding van wijzigingen in deel II en III (objecttypen toegevoegd)

0 Introductie

Dit eerste deel van het handboek security omvat de achtergronden, uitgangspunten en randvoorwaarden voor de inrichting van security binnen Rijkswaterstaat. Dit eerste deel omvat het beleid en de kaders op Directieniveau binnen Rijkswaterstaat. Waar mogelijk zijn verwijzingen naar bestaande beleidsmemo's opgenomen.

Dit eerste deel heeft mede als doelstelling deze beleidsmemo's te integreren zodat op één plaats en in één document een algeheel overzicht geboden kan worden voor de inrichting van de fysieke security binnen Rijkswaterstaat. In de opbouw is het beleidsmatige deel weergegeven in de hoofdtekst, de referenties en onderbouwing zijn opgenomen in de bijlagen.

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, op het handboek gebaseerde, pakket aan securitymaatregelen en -voorzieningen wordt vastgesteld. Daarnaast wordt de locatie op basis van de cybersecurity ingedeeld, waarna het geïntegreerde locatiespecifieke pakket aan securitymaatregelen en -voorzieningen wordt vastgesteld en vertaald in specificaties voor realisatie in nieuwbouw, verbouw of bestaande objecten.

Het vierde deel omvat de beschrijving van de implementatie waarmee de realisatie van de in het derde deel beschreven securitymaatregelen en -voorzieningen wordt vormgegeven.

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 totaalpakket is geborgd dat beleidsmatige keuzen operationeel vertaald kunnen worden en dat de operationele realisatie gebaseerd is op de binnen Rijkswaterstaat gevalideerde uitgangspunten en beleidskeuzen t.a.v. security.



1 Inleiding

Het ministerie van Infrastructuur en Milieu staat nationaal en internationaal voor belangrijke taken die burgers en bedrijven in het dagelijks leven raken. Vlot, Veilig en Leefbaar is daarvoor de missie.

“Het ministerie van Infrastructuur en Milieu investeert in veiligheid, leefbaarheid en bereikbaarheid van Nederland. We maken ruimte: ruimte voor de samenleving, maar ook ruimte voor de organisatie en haar medewerkers. Daarbij moeten we omgaan met de spanning tussen verschillende belangen en invalshoeken en dilemma’s die het werken in ons departement met zich meebrengt. Dit doen we op basis van vertrouwen, vertrouwen op de nakoming van afspraken en de naleving van wet- en regelgeving. Het vertrouwen wordt geborgd door goede afspraken en risicoanalyses.

Goede afspraken over de inrichting van het integrale beveiligingsbeleid zijn onmisbaar. Want beveiligingsrisico’s, integriteit- en privacy-schendingen maken de IenM organisatie kwetsbaar, zowel politiek als bedrijfsmatig.”¹

Rijkswaterstaat streeft in het verlengde daarvan naar de inrichting van een managementsysteem voor de beheersing van haar security risico’s in normale omstandigheden alsmede in tijden van verhoogde dreiging.

De beveiliging van de belangen van Rijkswaterstaat² moet daarom zijn ingericht voor zowel de normale omstandigheden als voor bijzondere dreiging voor zover de beheersing hiervan aan Rijkswaterstaat kan worden toegerekend. Om die redenen is de security bij Rijkswaterstaat systematisch, structureel en transparant opgezet.

Dit handboek is bestemd voor diegenen, die bij Rijkswaterstaat op enigerlei wijze betrokken of verantwoordelijk zijn voor de realisatie en instandhouding van security van de Rijkswaterstaat-locaties.

De uitwerking in dit handboek past in het Rijksbeleid (BIR/Zoneringsmodel), IenM beleid (baseline IenM) en het RWS Integrale beveiligingsbeleid.

Daar waar het Corporate Beveiligings Model (CBM) zich specifiek richt op de uitwerking voor kantoren biedt dit handboek een kader voor alle type locaties van Rijkswaterstaat. De in het CBM voorgeschreven methoden en principes worden op een andere wijze toegepast bij de opbouw en opzet van de in dit handboek beschreven methoden.

¹ Bron: Integraal Beveiligingsbeleid IenM 2013, Voorwoord

²Binnen het spraakgebruik van Rijkswaterstaat wordt onder de term locatie veelal een primair proces bedoeld. Voor fysieke locaties wordt de term TBB, het te beschermen belang, gebruikt. Met in dit document gehanteerde begrip ‘locatietype’ wordt de fysieke locatie bedoeld.

2 Definities en afbakeningen

2.1 Het begrip security

Security is gericht op de beveiliging van locatie tegen inbreuken door menselijk gedrag. Security binnen Rijkswaterstaat richt zich op te beschermen belangen. Alles waartegen ongewenst gedrag zich richt is een te beschermen belang.

Security richt zich daarmee op de bescherming van Rijkswaterstaat-locaties (hierna RWS-locaties) zoals gebouwen, kunstwerken en terreinen ter voorkoming van aantasting van de locaties zelf of de functionaliteit ervan. Voor security is alles waartegen dat ongewenst gedrag gericht kan zijn een aandachtspunt en omvat dus gebouwen, terreinen, middelen, goederen, processen maar óók beleid, bedrijfsinformatie, bedrijfsgegevens en personen.

De RWS-locaties zijn onderhevig aan inbreukrisico's en dienen daartegen te worden beschermd. Security is het stelsel van maatregelen en voorzieningen om de gewenste bescherming (aard en omvang) te bieden tegen onderkende dreigingen en de manier waarop deze risico's zich zouden kunnen manifesteren (incidentscenario's).

Het ongewenste menselijk gedrag waartegen moet worden beschermd betreft het gehele scala van onopzettelijk – niet wederrechtelijk gedrag (bijvoorbeeld van kinderen) tot opzettelijk en wederrechtelijk gedrag (criminelen). Ook onverschilligheid of onachtzaamheid kan leiden tot inbreuken. Het maakt dus niet uit vanuit welke oorzaak of bron het gedrag voortvloeit. Dat gedrag kan gewild en ongewild, bewust of onbewust, bedoeld of onbedoeld, opzettelijk of onopzettelijk zijn. Het gaat om het effect van dat gedrag en dat is de verstoring van de normale gewenste situatie van de RWS-locatie. Inbreuken op de locatie worden doorgaans aangeduid met de aard van de inbreuk (inbraak, vernieling, terrorisme etc.).

Voor Rijkswaterstaat wordt de security daarom inhoudelijk afgebakend tot: "het geheel van maatregelen en voorzieningen ter bescherming van RWS-locaties tegen onderkende dreigingen en incidentscenario's door menselijk gedrag (bewust en onbewust, bedoeld en onbedoeld, gewild en ongewild) die de staat, aard en functionaliteit van de RWS-locaties, bedrijfsprocessen, bedrijfsbeleid, bedrijfsinformatie en de integriteit van de medewerkers kunnen aantasten."



2.2 Securitymiddelen zijn maatregelen én -voorzieningen

Security komt niet vanzelf, daarvoor zijn acties en middelen nodig.

De maatregelen zijn met name gericht op het goed laten functioneren van de security en omvatten voornamelijk de uitvoering van de security door mensen.

De voorzieningen zijn gericht op het voorkomen van beveiligingsinbreuken door het fysiek te bemoeilijken of onmogelijk te maken, het vroegtijdig signaleren van inbreuken en het faciliteren van incidentaanpak en –afhandeling. Je zou kunnen zeggen, dat de voorzieningen de “hardware” van de beveiliging omvat en de maatregelen de ‘software en uitvoeringshandleiding’.

Bij Rijkswaterstaat wordt daarom onder securitymaatregelen begrepen: “de werkwijzen, gedragsregels, instructies, procedures en protocollen ter voorkoming van het optreden van beveiligingsincidenten en ter realisering van een adequate reactie op een beveiligingsinbreuk op Rijkswaterstaat, de bedrijfsprocessen en de daarin werkzame personen.”

Bij Rijkswaterstaat wordt daarom onder securityvoorzieningen begrepen: “de bouwkundige en elektronische inrichting de locaties ter voorkoming van beveiligingsinbreuken bij de RWS-locatie en ter realisering van vroegtijdige signalering van een beveiligingsinbreuk alsmede verificatie en registratie van de inbreuk teneinde een adequate reactie mogelijk te maken.”

2.3 Afbakening

Dit handboek richt zich op de fysieke beveiliging van de te beschermen belangen van Rijkswaterstaat. Buiten beschouwing zijn gebleven de:

- Dienstwoningen van RWS;
- Informatiebeveiliging;
- Integriteit van de medewerkers;
- Achtergrond checks bij de aanname van personeel;
- Privacy;
- Beveiliging van bewindspersonen;
- De daadwerkelijke implementatie van het CBM bij alle diensten en de financiële baten en lasten hiervan.

3 Nut en noodzaak van security

Risicomanagement wordt steeds belangrijker. Het past in de lijn van werken in vertrouwen en van bewust (= verantwoorde) risico's nemen in plaats van onbewust risico lopen.³

Veiligheids- en schade-incidenten kosten ook Rijkswaterstaat jaarlijks veel geld. Deels in de vorm van materiële schade, deels als gevolgschade van incidenten, deels als kosten voor beveiligingen risicomanagement en in toenemende mate ook in de vorm van schadevergoedingen. De omvang van de veiligheids- en schade-incidenten en de daarmee gepaard gaande kosten varieert. Er zijn geen aanwijzingen dat de aard van de risico's afneemt, maar wel dat de attractiviteit voor bepaalde vormen van criminaliteit meer afhankelijk is van economische factoren zoals bijvoorbeeld de prijs van metalen en materialen.

Security is erop gericht het ongewenst gedrag van mensen te voorkomen of minstens zoveel mogelijk te beheersen ter voorkoming en beperking van schade.

Door het onderkennen van de relevante veiligheids- en schaderisico's en incidentscenario's draagt security bij in het borgen/verhogen van zowel veiligheids- als ook kwaliteitsstandaarden. Tevens worden verstoringen die zich wel manifesteren door vastgestelde securityprocedures op de meest efficiënte wijze tot een minimum beperkt. Security levert daardoor een bijdrage aan het minimaliseren en/of vermijden van (faal)kosten van de bedrijfsprocessen en daarmee dus een bijdrage aan de continuïteit van Rijkswaterstaat en de maatschappelijke processen.

Met het integraal veiligheidsbeleid heeft Rijkswaterstaat de toekomstvastheid van de security verankerd in haar strategie. Door bewust te zijn van haar maatschappelijke verantwoordelijkheid handelt Rijkswaterstaat ook in deze lijn van denken. Het is dus van groot belang om een positief imago te behouden. Security draagt bij in het beheersen van risico's die van negatieve invloed zijn op Rijkswaterstaat in het algemeen en het imago van Rijkswaterstaat als waterweg- en wegbeheerder en werkgever in het bijzonder.

Ook bij de realisatie van security bij Rijkswaterstaat dienen de kosten te worden beheerst. Dat is minder goed mogelijk indien de inrichting van de security wordt overgelaten aan individuele inzichten en beoordelingen van medewerkers. Vanuit een uitgekristalliseerde securitybenadering en gestandaardiseerde inrichting van de security bij Rijkswaterstaat worden alleen de beveiligingsvoorzieningen aangeschaft, aangebracht en geïmplementeerd die de gewenste beheersing in voldoende mate kunnen realiseren. Daardoor worden onnodig dure, ineffectieve en inefficiënte securityvoorzieningen voorkomen.

³ Bron: Integraal Beveiligingsbeleid IenM 2013, 18 april 2013 1.0



Aantasting van de bedrijfsvoering door veiligheidsincidenten betekent dat eigen bedrijfsprocessen tot stilstand komen of vertragingen oplopen. Dit leidt niet alleen tot improductieve uren van personeel, maar ook tot extra kosten van zowel herstel als aanpassing van de uitvoering van de betrokken bedrijfsprocessen. De directe schade van een inbreuk (bijvoorbeeld diefstal van materialen) mag dan gering zijn, de kosten, waaronder ook de mogelijke maatschappelijke kosten, die eruit voortvloeien zijn dat niet. Security draagt direct en indirect bij aan het beschermen van de bedrijfsprocessen tegen deze inbreuken en levert daardoor een bijdrage aan de beperking van deze extra kosten.

4 Doel en gebruik handboek security

Vanuit de behoefte om voor de bescherming van de RWS-locaties vanuit een structurele en conceptuele benadering invulling te geven aan de inzet van beheersingsmaatregelen is dit eerste deel van het handboek ontworpen. De inhoud beperkt zich daarom tot de conceptuele achtergronden en uitgangspunten, de gevolgde systematiek voor de bepaling van het vereiste securityniveau en de inrichting van de security op locatie.

Dit handboek heeft daarom tot doel om de betrokkenen bij de security bij Rijkswaterstaat:

- a. Te informeren over de achtergronden, uitgangspunten en uitwerkingen van de security bij Rijkswaterstaat;
- b. De systematiek van de totstandkoming van security op locatie aan te reiken;
- c. De toepassing van de uitwerkingen van de security op locatie zoveel mogelijk te standaardiseren;
- d. Te ondersteunen bij de realisatie van de security op locatie.

Dit handboek heeft daarom voor de betrokkenen zowel de functie van:

- Documentatiebron over de achtergronden van security;
- Documentatiebron over de uitgangspunten en randvoorwaarden voor de security bij Rijkswaterstaat;
- Informatiebron voor de inrichting van de security;
- Hulpmiddel voor de uitwerking van de security op locatie.



5 Context van de security bij Rijkswaterstaat

Rijkswaterstaat is geen eiland in de Nederlandse maatschappij maar is daarvan een onlosmakelijk en niet onbelangrijk onderdeel. Dat betekent, dat Rijkswaterstaat net als alle ondernemingen in Nederland onderhevig is aan de wetgeving, die aan Rijkswaterstaat als werkgever verplichtingen oplegt in de bescherming van haar locaties.

Daarnaast functioneert Rijkswaterstaat in relatie tot anderen, die al dan niet uit eigen belang of wettelijke verplichting eisen en wensen kunnen hebben ten aanzien van de security bij Rijkswaterstaat.

5.1 Wet- en regelgevend kader algemeen

Werkgevers hebben te maken met een veelheid aan wetgeving, waarin verplichtingen zijn opgenomen voor de inrichting en werkwijze van hun bedrijf(svoering). Niet alle wetgeving is echter even duidelijk en afgebakend. Er is dus ook een behoorlijk grijs gebied als het gaat om ordeningswetgeving. Dat neemt echter niet weg, dat de werkgever op basis van deze wetgeving (helder en afgebakend of niet) aansprakelijk gesteld kan worden indien zich incidenten hebben voorgedaan of controle van de overheid heeft plaatsgehad.

Hieronder volgt een summier 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:	Gezonde werkomgeving, veiligheid op de werkplek, veiligheid in en om de gebouwen, veiligheid tijdens calamiteiten
CPR-richtlijnen:	Opslag chemische stoffen, brandpreventie en bestrijdingsmaatregelen, opvang verontreinigd bluswater
Woningwet:	Grondslag voor brandveiligheid gebouwen
WBDBO:	Wet op Brand doorslag en brand overslag
Bouwbesluit:	Brandveiligheid, ontvluchtingmogelijkheden, aanwezigheid blusmiddelen, aanwezigheid noodverlichting en vluchtwegaanduiding
WBP:	Wet Bescherming Persoonsgegevens
Burgerlijk wetboek:	Aansprakelijkheid, schadeverhaal, ordehandhaving, huisregels en sancties, visitatie
Gebruikersvergunning:	
Wet Beheer Rijkswaterstaatswerken:	In deze wet en de daarop berustende bepalingen wordt verstaan onder waterstaatswerken: bij het Rijk in beheer zijnde wegen alsmede, voor zover in beheer bij het Rijk, de daarin gelegen kunstwerken en hetgeen verder naar zijn aard daartoe behoort. Het is verboden zonder vergunning van Onze Minister van Verkeer en Waterstaat gebruik te



Waterwet:

maken van een waterstaatswerk door anders dan waartoe het is bestemd: a. daarin, daarop, daaronder of daarover werken te maken of te behouden; b. daarin, daaronder of daarop vaste stoffen of voorwerpen te storten, te plaatsen of neer te leggen, of deze te laten staan of liggen. Een vergunning kan onder beperkingen worden verleend. Aan een vergunning kunnen voorschriften worden verbonden Voorkomen en waar nodig beperken van overstromingen, wateroverlast en waterschaarste, in samenhang met bescherming en verbeteren van de chemische en ecologische kwaliteit Rijkswaterstaat en het ministerie van Infrastructuur en Milieu van watersystemen en vervulling van maatschappelijke functies door watersystemen

5.2 Specifieke 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 baselines⁴

5.3 Stakeholders en hun belangen

In de beheersing van de veiligheids- en schaderisico's zijn er diverse belanghebbenden met elk hun eigen wensen en soms eisen voor een effectieve risicobeheersing. Deze belangen met de daaraan verbonden eisen en wensen zullen op elkaar moeten zijn afgestemd. Er moet niet alleen een werkbare en betaalbare risicobeheersing worden gerealiseerd. De belanghebbenden moeten zich ook kunnen vinden in de invulling van hun belangen in relatie tot die van anderen.

⁴Bron: Integraal Beveiligingsbeleid IenM 2013, 18 april 2013 1.0

Wie zijn de belanghebbenden en wat zijn hun eisen en wensen?

In de groep belanghebbenden zijn vier categorieën te onderscheiden, te weten op basis van:

- wettelijke voorschriften
- de eigen bedrijfscontinuïteit van Rijkswaterstaat
- het gebruik van (vaar)wegen en hoofdwatersystemen
- hun eigen belangen

5.3.1 Op basis van wettelijke voorschriften

Deze groep betreft alle overheidsinstanties of uitvoeringsorganen die aan een bedrijf maatregelen kunnen opleggen binnen het kader van daartoe geldende wetgeving.

De meest voorkomende zijn de volgende:

- Provinciale en gemeentelijke overheden
- Arbeidsinspectie m.b.t. de veiligheid van het werken in de bedrijfsvoering
- Brandweer m.b.t. de veiligheid van de gebouwen en terreinen
- Milieudienst m.b.t. de veiligheid van de omgeving

5.3.2 Op basis van eigen bedrijfscontinuïteit Rijkswaterstaat

Deze groep betreft degenen, die een eigen belang hebben bij een ongestoord functioneren van Rijkswaterstaat. Tot deze groep behoren voor in elk geval:

- De politiek verantwoordelijken
- De werknemers
- Contractpartijen en aannemers

5.3.3 Op basis van het gebruik van (vaar)wegen en hoofdwatersystemen

Deze groep betreft voor:

- de hoofdwegen: de goederentransportbedrijven, de personenvervoerbedrijven, buurlanden en de individuele verkeersdeelnemers;
- de hoofdwaterwegen: de havendiensten, de scheepvaart en binnenvaart, transport- en veerdiensten, (beroeps)visserij, buurlanden en pleziervaart;
- de hoofdwatersystemen: (lagere) overheden, waterschappen, buurlanden en burgers

5.3.4 Vanuit hun eigen belangen

Deze groep betreft:

- de in de rechtshandhaving werkzame diensten zoals politie en Openbaar Ministerie. Criminaliteit dient zoveel mogelijk te worden voorkomen en waar mogelijk te worden bestraft. Aan politie en justitie de taak om aan



de security bij Rijkswaterstaat het gewenste vervolg te geven. Vanuit dat belang dient Rijkswaterstaat rekening te houden met de eisen en wensen die vanuit de rechtshandhaving worden gesteld.

- daarnaast hebben alle voor RWS werkzame bedrijven en personen zoals de contractaannemers, architectenbureaus etc., belang bij een veilige en ongestoorde bedrijfsvoering bij RWS.
- tenslotte is het belang van omwonenden voor een veilige en rustige woonomgeving niet weg te denken.

6 De security bij Rijkswaterstaat

6.1 De security-aandachtsgebieden

De maatschappelijke verhoudingen zijn in de loop van de jaren veranderd, het gedrag van mensen daardoor ook. Dit uit zich in o.a. de aard en omvang van ongewenste gedragingen van (mede)mensen en angst voor omstandigheden waaraan mensen het ontstaan van dergelijke gedragingen verbinden. Of, en zo ja in hoeverre een causaal verband aanwezig is tussen omstandigheden en het ongewenste gedrag is voor velen niet relevant. In de beleving is er sprake van een ongewenste (lees: onveilige) situatie. Deze veiligheidsbeleving is van invloed op de waardering van (water)wegen als vervoersmodaliteit en de beheerder ervan. Deze zogenoemde sociale veiligheid heeft in de loop der jaren sterk aan betekenis gewonnen.

De ontwikkeling van de inrichting van de bedrijfsprocessen en de enorme rol van de ICT daarin heeft ertoe geleid, dat bepaalde vormen van ongewenst gedrag zoals bijvoorbeeld hacking, binnen de systeemontwerpen van de automatisering moeten worden geweerd. Dat heeft ertoe geleid, dat binnen het gehele veld van de security deelgebieden zo'n specialistische aangelegenheid zijn geworden, dat de beheersing van de inbreukrisico's ook binnen die vakgebieden is/moet worden georganiseerd vanwege de daarvoor vereiste specifieke deskundigheid. Binnen Rijkswaterstaat is de CIO verantwoordelijk. ICT als zodanig valt buiten de scope van dit handboek. De vanuit Cybersecurity geformuleerde eisen voor de fysieke security van objecten met Informatie Automatisering gerelateerde (IA-gerelateerde) ruimten zijn binnen de scope van dit handboek gebracht.

De fysieke en operationele bescherming van de RWS-locaties zoals gebouwen, terreinen, kunstwerken, infrastructuur en materieel is in de loop der jaren eveneens in een andere context komen te verkeren. Was het in een ver verleden nog normaal, dat men het terrein van Rijkswaterstaat niet betrad omdat de verboden toegang met een bord was aangeduid, tegenwoordig zijn andere middelen nodig om ongewenste betreding van de gebouwen en terreinen te voorkomen. Niet alleen de inrichting van de RWS-locatie zelf en de omgeving ervan worden mede vanuit veiligheidsaspecten bepaald, ook het toegangsbeheer krijgt een steeds nadrukkelijker rol in het geheel.

Voorgaande opsomming van security-aandachtsgebieden is lang niet volledig, maar toont wel aan, dat de security bij Rijkswaterstaat op meerdere pijlers rust en tevens dat maatschappelijke veranderingen van invloed zijn op de aard en inhoud van beschermingsmaatregelen.

De in dit handboek beschreven invulling van de zorgplicht voor de fysieke en operationele bescherming van de locaties van Rijkswaterstaat is dus slechts één van die pijlers om inbreuken op de continuïteit van de bedrijfsprocessen en de functionaliteit te kunnen beheersen.



6.2 Hoe gaat Rijkswaterstaat met de securityrisico's om?

Van Rijkswaterstaat kan en mag niet verwacht worden, dat het zich wapent tegen alle mogelijke inbreuken op de integriteit van personen en de infrastructuur. Wel mag van Rijkswaterstaat worden verwacht, dat in alle redelijkheid en in overeenstemming met haar positie en maatschappelijke rol die maatregelen worden genomen, die voor een veilig weg- en waterverkeer en waterbeheer en de informatievoorziening aan de weg- en vaarweggebruiker in Nederland gewenst zijn.

Dat betekent, dat Rijkswaterstaat zich primair richt op de voor haar verantwoordelijkheid relevant te achten risico's, incidentscenario's en daderprofielen. Het is immers niet tot de taak van Rijkswaterstaat te rekenen om alle vormen van criminaliteit te bestrijden. Dat houdt in, dat Rijkswaterstaat accepteert, dat zich binnen haar verantwoordelijkheidsdomein incidenten kunnen voordoen waarvoor geen preventieve maatregelen zijn getroffen zoals bijvoorbeeld moord- en doodslag. Dat is immers inherent aan het gegeven, dat zich op en nabij rijkswegen, waterwegen en watersystemen mensen bevinden. Wel mag van Rijkswaterstaat in dit soort situaties worden verwacht, dat bij constatering van dergelijke incidenten adequaat wordt gereageerd.

Datzelfde geldt voor bedreigingen die het belang van Rijkswaterstaat overstijgen zoals politiek activisme en in zekere zin terrorisme. Voor zover uitingen daarvan als niet direct aan Rijkswaterstaat zijn te relateren, is de bestrijding of beheersing van dergelijke bedreigingen niet aan Rijkswaterstaat toe te rekenen. Ook hiervoor geldt, dat van Rijkswaterstaat wel verwacht mag worden, dat zij haar bijdrage levert aan de diensten en instellingen die voor de bestrijding ervan worden ingezet. Daar waar dit Rijkswaterstaat als organisatie overstijgt wordt het Departementaal Crisis en Coördinatiecentrum (DCC) of de Nationaal Coördinator Terrorismen en Veiligheid (NCTV) ingeschakeld.

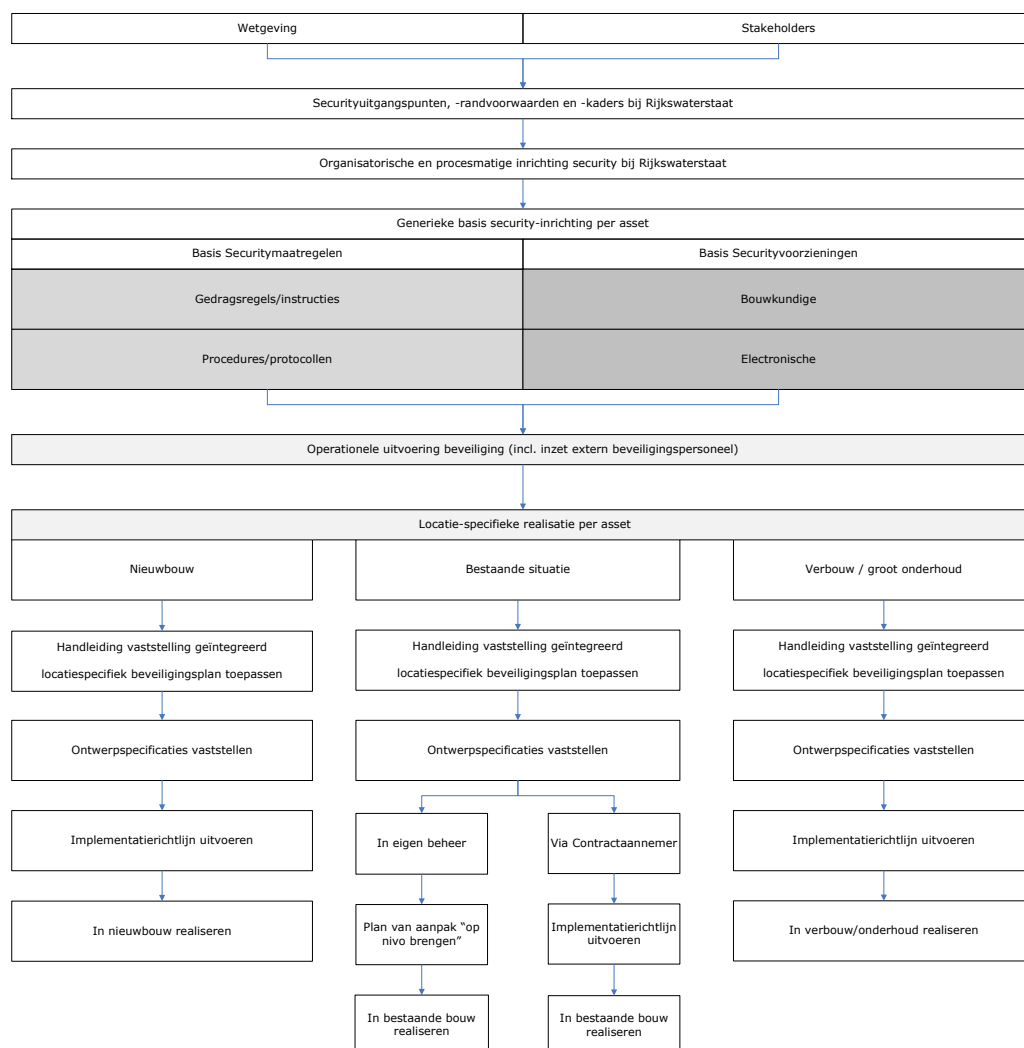
Rijkswaterstaat beperkt zich dus tot de voor haar relevante bedreigingen naar soort, aard en verschijningsvorm. Rijkswaterstaat streeft daarbij naar een duurzame beheersing door een tijd- en plaats onafhankelijke inrichting van de beheersingsmaatregelen en een integrale uitvoering waardoor de effectiviteit van elke beheersingsmaatregel afzonderlijk maximaal wordt uitgenut en de beheersingskosten tot een minimum worden gereduceerd.

Dat wordt in eerste instantie bereikt door de security in het denken en doen van medewerkers te integreren. Zij bepalen immers in grote mate de effectiviteit van alle security-inspanningen. Met een continue en actuele security-awareness is de basis gelegd voor de realisatie van het gewenste securityniveau. Essentieel voor de risicobeheersing is de volledige inrichting en uitvoering van de securitymaatregelen zoals de gedragsregels, instructies, procedures en protocollen. Die bepalen in hoge mate de effectiviteit van de risicobeheersing. Daarnaast wordt het gewenste securityniveau bereikt door de bouwkundige en elektronische voorzieningen, die om efficiencyredenen zoveel mogelijk worden gestandaardiseerd met behoud van de maatwerkinrichting op locatie.

Binnen de security-organisatie van Rijkswaterstaat zal de inrichting en uitvoering van de security bovendien aan alle eisen voldoen waaraan kwaliteitssystemen dienen te voldoen, hetgeen betekent dat de security niet alleen wordt gemonitord, maar ook voortdurend wordt geactualiseerd om het gewenste securityniveau te bereiken en vast te houden. De zogeheten Plan-Do-Check-Act cyclus wordt binnen Rijkswaterstaat hiervoor gevolgd.

6.3 De opbouw van de security bij Rijkswaterstaat

De opbouw en inrichting van de security bij Rijkswaterstaat is voor alle locaties vanuit dezelfde conceptuele benadering en maximale standaardisatie samengesteld. E.e.a. is in onderstaand schema samengevat.



Figuur 1: opbouw security Rijkswaterstaat



Afhankelijk van de locatie en de situatie van de locatie, zal de realisatie in overleg met andere belanghebbenden gestalte moeten krijgen. Denk daarbij bijvoorbeeld aan kruising met andere vitale infrastructuren (bijv. spoorweg, gasleiding), gemeentelijke en provinciale (water)wegen etc.

De Basis Security Niveaus zijn de invullingen van de zorgplicht van Rijkswaterstaat t.a.v. het locatietype. Elk niveau per locatie geeft aan wat de zorgplicht t.a.v. security van het locatietype voor dat niveau inhoudt. Elk Basis Security Niveau is immers toegesneden op de bij dat niveau behorend risicoprofiel t.a.v. de continuïteitsbelangen en locatiekarakteristieken. Het bij dat niveau behorende securitypakket is daarmee een vertaling van de wel geaccepteerde en niet geaccepteerde risico's en incidentscenario's. De samenstelling van de securityvoorzieningen voor dat niveau zijn daarom niet anders te beschouwen als de noodzakelijke voorzieningen om het locatietype als goed huisvader te beschermen en – waar gespecificeerd – te voldoen aan de wettelijke verplichtingen.

Ten behoeve van een systematische en efficiënte realisatie worden de securityvoorzieningen opgenomen in de planstudies en zijn de technische specificaties van de securityvoorzieningen opgenomen in de ontwerpvoorschriften van Rijkswaterstaat.

De opbouw en systematiek van de security bij Rijkswaterstaat biedt tevens de mogelijkheid om bij een combinatie de locaties op één locatie - bijvoorbeeld een brug met aansluitend een sluizencomplex - de security vanuit een overallvisie in te richten om de samenstelling van de maatregelen en voorzieningen, alsmede de operationele uitvoering efficiënt te realiseren.

De Basis Security Niveau's zijn voor ieder onderkend objecttype of combinatie van objecttype uitgewerkt in deel II van het Handboek Security RWS. In deel III zijn de handleidingen uitgewerkt die voor iedere locatie een onderbouwd beveiligingsplan oplevert en tevens de basis vormt voor de specificatie t.b.v. ontwerp, installatie en acceptatie.

7 Algemene uitgangspunten, prestatie-eisen en doelstellingen security

7.1 Algemene uitgangspunten

De algemene uitgangspunten bij de securitymaatregelen en –voorzieningen bij Rijkswaterstaat zijn:

- Zij vinden hun oorsprong in gemeten, geanalyseerde en gewaardeerde risico's, die voor Rijkswaterstaat relevant moeten worden geacht;
- Zij zijn gericht op de bij die risico's voor Rijkswaterstaat relevant te achten incidentscenario's;
- Zij dragen herkenbaar en meetbaar bij aan de beheersing van de risico's waarop de maatregel betrekking heeft;
- Zij zijn ingericht op de voor die risico's vastgestelde beheersingsniveaus;
- Zij zijn samengesteld uit één geïntegreerd stelsel van securitycomponenten;
- Zij worden periodiek geijkt op effectiviteit.

Daarmee wordt door Rijkswaterstaat principieel gekozen voor een risico gerelateerde en niet voor een incident gestuurde benadering.

Een risico gerelateerde benadering gaat uit van de mogelijke risico's die zich met betrekking tot de locatie kunnen manifesteren en de wijze waarop die manifestatie normaliter gestalte zou kunnen krijgen. Daarmee wordt bereikt, dat alle soorten risico's en incidentscenario's worden geïnventariseerd en beoordeeld op relevantie voor die locatie. Daarmee wordt ook bereikt, dat de security van de locatie een meer toekomstvast karakter kan verkrijgen omdat nóch de aard en soort van de relevant te achten risico's snel zal veranderen, nóch de incidentscenario's significant zullen veranderen. Deze benadering biedt bovendien de mogelijkheid om vanuit relevante incidentscenario's na te gaan welke aanpassingen aan de infrastructuur of gebouwen de incidentscenario's structureel kunnen wegnemen en daarmee het risico kunnen elimineren. Denk bijvoorbeeld aan het aanbrengen van graffiti-werende materialen voor gebouwen en bruggen/viaducten en/of ontwerp en inrichting waardoor bepaalde vormen van criminaliteit onmogelijk worden zoals onbrandbaar materiaalgebruik waardoor brandstichting onmogelijk wordt.

Een incident gestuurde benadering is beperkter en van vele factoren afhankelijk en daardoor minder betrouwbaar, noch toekomstvast. De beperktheid schuilt in het feit, dat alleen de plaatsgevonden geconstateerde incidenten in ogenschouw worden genomen op de wijze zoals die zich hebben gemanifesteerd. Daarbij is het dan de vraag of alle daarbij aan de orde geweest zijnde omstandigheden kunnen worden meegewogen.

Aard en omvang van incidenten is mede afhankelijk van de mate waaraan er aandacht aan wordt besteed. Hoe meer toezicht, hoe meer incidenten worden waargenomen en hoe omvangrijker de registratie van incidenten. Dat zegt echter niets over het veiligheidsniveau, wel over de kwaliteit van de waarnemingen.



De aandacht voor incidenten is mede afhankelijk van de media-aandacht en/of politieke aandacht die op dat moment om welke reden dan ook aan dat soort incidenten wordt besteed.

Een incident gestuurde benadering loopt daardoor een groot risico te reageren op de waan van de dag en daarmee het doel van een duurzame security voorbij te schieten.

Aan de risico gestuurde benadering kleef het nadeel, dat geen data kunnen worden overlegd waaruit het bewijs van de noodzaak tot het nemen van securitymaatregelen en –voorzieningen zou moeten blijken. Daartegenover staat, dat de inrichting van de registratie exact kan opleveren welke Key Performance Indicators aan de securitymaatregelen en –voorzieningen dienen te worden verbonden.

Dit betekent niet dat niet op incidenten gereageerd moet worden. Bij het beheersen van incidenten moet echter niet alleen dat type incident in ogenschouw worden genomen maar tevens alle andere mogelijke security incidenten.

7.2 Algemene prestatie-eisen

De Rijkswaterstaat-locaties worden voorzien van een integraal pakket van securitymaatregelen en –voorzieningen, dat aan de volgende kenmerken voldoet:

- Voorzien in een effectieve bescherming tegen de risico's van diefstal, vernieling en beschadiging (graffiti) van RWS-locaties;
- Voorzien in een effectieve bescherming tegen het betreden door ongewenste personen;
- Voorzien in de persoonlijke en collectieve beveiliging tegen inbreuk op de persoonlijke integriteit;
- Biedt de mogelijkheden tot flexibele aanpassing en uitbreiding indien de omstandigheden daartoe aanleiding geven zoals bijvoorbeeld bij verhoogde dreiging in het kader van het Alerteringssysteem Terrorismebestrijding (ATb);
- Bestaat uit alle relevante securitymaatregelen en –voorzieningen en is zodanig samengesteld, dat de securitymaatregelen en –voorzieningen naadloos op elkaar aansluiten en elkaars werking versterken;
- Belemmert de uitvoering van de bedrijfsprocessen van Rijkswaterstaat niet.

7.3 Algemene doelstellingen

Security is gericht op het leveren van die bijdrage die nodig is om de bedrijfscontinuïteit van Rijkswaterstaat en het behalen van haar doelstellingen mogelijk te maken. Voor Rijkswaterstaat is dat, naast het voldoen aan de wetgeving, het leveren van een bijdrage aan:

1. in het algemeen:
 - het welzijn van personen bij Rijkswaterstaat;
 - de continuïteit van het bedrijf en haar bedrijfsprocessen;
 - de continuïteit van de vervoersprocessen op de (water)wegen;
 - de continuïteit van de beheersing en monitoring van waterpeil, waterverdeling en waterkwaliteit;

- het vertrouwen van alle relevante stakeholders;
- het verhogen van het imago;
- het beheersen van de (organisatie)kosten.

2. in het bijzonder:

- de bedrijfszekerheid (systeemzekerheid);
- schadebeperking Rijkswaterstaat en gebruikers;
- ARBO-veiligheid;
- klanttevredenheid;
- verhoging veiligheidsgevoel.



Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

8 Securityrandvoorwaarden en –kaders bij Rijkswaterstaat

8.1 Rol en positionering Rijkswaterstaat m.b.t. security

Het ministerie van Infrastructuur en Milieu staat nationaal en internationaal voor belangrijke taken. Het is de zorg van RWS dat alle RWS-processen die voor de missie van het departement nodig zijn goed functioneren en dat de continuïteit van die processen wordt gewaarborgd. Een adequaat integraal beveiligingsbeleid is hiervoor een belangrijke voorwaarde.

Het Beveiligingsbeleid IenM is een geïntegreerd beleid waarbij samenhang, onderlinge verbanden en ordening is aangebracht binnen de deelaspecten: beveiliging van medewerkers, goederen, gebouwen en terreinen, locatie, bouwwerken, kunstwerken en installaties, informatiebeveiliging, bescherming van persoonsgegevens, en integriteit en ongewenste omgangsvormen.

Het beleidsdocument deelt voorts verantwoordelijkheden, taken en bevoegdheden toe aan het lijnmanagement in hun rol van verantwoordelijke voor de processen, als eigenaar van informatiesystemen, beheerder van persoonsgegevens, hoeder van de veiligheid van personen et cetera.

Het beleidsdocument verwijst tenslotte naar de Baseline Informatiebeveiliging Rijksdienst (BIR), waaraan voldaan moet worden.

Het Beveiligingsbeleid IenM geeft de organisatie en de door de Secretaris-Generaal (SG) vastgestelde kaders van het beveiligingsbeleid van het ministerie van IenM weer.

8.2 Vormgeving Security Rijkswaterstaat

Integrale beveiliging binnen RWS gaat over de samenhang en onderlinge verbanden tussen de deelaspecten:

- informatiebeveiliging (IB);
- fysieke beveiliging (F);
- privacy (P);
- integriteit (I).

Het beleid schrijft voor dat elke dienst een Beveiligingsplan opstelt. De kaders hiervoor worden meegegeven door de aanpak die IenM voorstaat, zijnde het maken van risicoanalyses, rekening houdend met 'te beschermen of cruciale belangen.

Werken aan beveiliging is een dynamisch en continu proces. Om te kunnen waarborgen dat een adequaat niveau van beveiliging binnen IenM blijft gehandhaafd, dient de beveiligingscyclus(plan-do-check-act) steeds weer te worden doorlopen. Hierdoor komt beveiliging steeds op een hoger kwaliteitsniveau terecht.

Van belang is ook dat de nodige aandacht blijft worden geschonken aan een goede, structurele verankering van de beveiligingsorganisatie. Het op



niveau brengen van de beveiligingsorganisatiemoet niet worden geïnterpreteerd als een éénmalige projectinspanning, maar als een continu onderdeel van de kwaliteitshandhaving van de bedrijfsvoering.

Beveiliging heeft alles te maken met het bewust nemen van risico's in plaats van het onbewust lopen ervan. Het moet in het dagelijkse werk van iedere medewerker worden meegenomen en in het gedrag tot uiting komen.

Het beveiligingsplan geeft daar richting aan.

Om te komen tot een goede beveiliging hanteert IenM de volgende aanpak.

1. Het opstellen en invoeren van minimumeisen (ME);
Het invoeren en naleven van de minimumeisen (het minimumpakket) geldt voor alle organisatieonderdelen van IenM.
2. Het uitvoeren van risicoanalyses;
Naast de minimumeisen is het aan de organisatieonderdelen om te bepalen of er aanvullende eisen en maatregelen noodzakelijk zijn. De organisatieonderdelen zullen dit moeten bepalen met risicoanalyses.

ad 1

De SG heeft, overeenkomstig het bepaalde in onderliggende wet- en regelgeving, op centraal niveau zogenaamde minimumeisen opgesteld. Hierin is sprake van een aantal samenhangende eisen en daaruit voortvloeiende minimaal verplicht te treffen maatregelen die een goeduitgangspunt bieden voor het invoeren van (informatie)beveiliging. Het opstellen van de minimumeisen gebeurt op centraal niveau en in samenspraak met de organisatieonderdelen. Het hanteren van minimumeisen voorkomt dat verschillende managers dezelfde afwegingen moeten maken bij het kiezen van maatregelen. Hiermee is voor alle betrokkenen inzichtelijk, consistent en duidelijk wat minimaal wordt verlangd op het gebied van beveiliging. De uitvoering is vervolgens decentraal belegd.

ad 2

IenM kent vier "verplichte" vormen van risicoanalyses, te weten voor o.a. de beveiliging van locaties (dat wil zeggen gebouwen en locaties); Dit omvat het treffen en het onderhouden van een samenhangend pakket van maatregelen om te bemoeilijken of te verhinderen dat schade aan locaties, goederen, installaties, informatie(systemen) en personen wordt toegebracht en om te voorkomen dat ongewenste personen locaties van IenM binnendringen.

Onder locaties wordt verstaan: alle kantoor- en bedrijfsgebouwen en terreinen van IenM met inbegrip van alle roerende zaken (in de ruimste zin van het woord) die in gebruik zijn in de gebouwen, bouwwerken, locatie, locaties, kunstwerken en terreinen.

Bescherming vitale infrastructuren

Sommige sectoren en delen van de infrastructuur zijn zo vitaal voor de Nederlandse samenleving dat uitval of ernstige verstoring ervan grote schade tot gevolg kan hebben. In Nederland heeft het

kabinet daarom besloten om de weerbaarheid van de Nederlandse samenleving te verhogen en te komen tot een samenhangend pakket van maatregelen ter bescherming van de beschikbaarheid en betrouwbaarheid van vitale producten en diensten van overheid en bedrijfsleven. Vanuit risicoanalyse zijn de belangrijkste locatie geïdentificeerd. Deze locatie zijn aangesloten op het Alerteringssysteem Terrorismebestrijding. Bij opschaling van dit alerteringssysteem worden vooraf gedefinieerde organisatorische maatregelen getroffen, lopend tot aan de afsluiting van de betreffende infrastructuur. Inlichtingen zijn verkrijgbaar bij het Departementaal Coördinatiecentrum Crisisbeheersing.⁵

Beveiligingsbeleid RWS

Het Beveiligingsbeleid RWS wordt geconcretiseerd met de zogenaamde Baseline RWS. Dit zijn generieke RWS-beveiligingsmaatregelen, beschreven per RWS-domein.

Het Beveiligingsbeleid RWS wordt daarnaast nader uitgewerkt in de Beveiligingsorganisatie RWS.

Beveiligingsplan

In 2006 is het eerste Beveiligingsplan RWS door de CFO van RWS vastgesteld, waarin de beveiligingsorganisatie van RWS is beschreven met de rollen en procedures (het meer statische en beschrijvende deel) en op welke wijze RWS de verplichtingen en maatregelen die voortkomen uit de opgelegde regelgeving, de Baseline RWS, de risico-analyses maatschappelijk vitale processen, de normenkaders ICT en het Beveiligingsbeleid RWS gaan implementeren (het jaarlijkse operationele deel).

Baseline RWS

De Baseline bestaat uit voor heel RWS geldende beveiligingsmaatregelen verdeeld in verschillende domeinen, zoals onder andere fysieke beveiliging en bewaking.

8.3 Organisatorische en procesmatige inrichting van de security

Het lijnmanagement (van I&M) is verantwoordelijk voor de uitvoering van het integraal beveiligingsbeleid. In het algemeen volgt de inbedding en aansturing van het integraal beveiligingsbeleid de inrichting en sturing van het departement. De beveiligingsorganisatie, de onderlinge afstemming en de control- en toezichttaken zijn als volgt ingericht:

Organisatie op concernniveau

- Er is een directeur Integriteit en Beveiliging (tevens Beveiligingsambtenaar volgens het Beveiligingsvoorschrift Rijksdienst 2005) die de SG ondersteunt in de ontwikkeling en uitvoering van het beveiligings- en integriteitsbeleid.
- Er is een Functionaris Gegevensbescherming (FG) die volgens de wet Bescherming persoonsgegevens namens de Minister toeziet op de toepassing en naleving van de Wbp,

Organisatie op dienstniveau

⁵Bron: RWS Beveiligingsplan 2.4.2 en 2.8.3



- Alle dienstonderdelen (waaronder RWS) hebben coördinatoren om hun management c.q. directieteam te ondersteunen bij het uitvoeren van het integrale beveiligingsbeleid.
- Er zijn bij alle diensten één of meer vertrouwenspersonen integriteit/ongewenste omgangsvormen die een eventuele melder van een integriteitschending ondersteunen en indien nodig de weg wijzen.

Belangrijkste taak van de coördinatoren is het management te ondersteunen bij het voeren van een adequaat risicomanagement: het onderkennen van risico's en het aanreiken van passende maatregelen om deze in te dammen. Daarbij kan bij de bepaling van het ambitieniveau boven de baseline een afweging plaatsvinden tussen de risicozwaarte (kans x impact) en de kosten om maatregelen te treffen.

Afstemming op dienstniveau

De verschillende organisatieonderdelen van IenM kiezen een vorm van interne afstemming die past bij de organisatie.

Beveiligingsplannen

De integrale beveiligingsplannen die door elke dienst worden opgesteld geven een gestructureerd inzicht in de risicovolle processen en de getroffen/te nemen maatregelen. Speerpunten voor het komende jaar worden benoemd.

Control en toezicht

Integrale beveiliging is onderdeel van de departementale bedrijfsvoering. Het is daarmee onderdeel van de management-/sturingscyclus.

Integraal beveiligingsbeleid

Toezicht op procesniveau vindt jaarlijks plaats door het laten uitvoeren van operationele audits. Hierover vindt overleg plaats met de Auditdienst Rijk en de dienst. Het Auditcommittee stelt de definitieve planning vast. De voortgang wordt periodiek met de Auditdienst Rijk besproken. Waar nodig wordt integrale beveiliging opgenomen in de toezichtagenda's van de Directie Financiën, Management en Control van het Ministerie van IenM.⁶

8.4 De algemene securitybeheersingsdoelen

Om de beheersingsdoelen van de security bij Rijkswaterstaat te kunnen bereiken, zal de security moeten voldoen aan de algemene randvoorwaarden voor een effectieve en efficiënte security. Dit betekent, dat duidelijk moet zijn, wat de maatregelen en voorzieningen moeten bewerkstelligen. De belangrijkste zijn:

- te voorkomen, dat inbreuken ontstaan;
- de uitvoering van inbreuken te bemoeilijken;
- de kans op ontdekking/betrapping te vergroten;
- de afvoer van goederen te bemoeilijken;
- de schade bij inbreuken te beperken.

⁶Bron: Integraal Beveiligingsbeleid IenM 2013

8.5 De algemene securitymiddelen: maatregelen én voorzieningen

Om deze algemene securitybeheersingsdoelen te kunnen bereiken, moeten de daarvoor geëigende securitymiddelen worden ingezet. Daartoe behoren:

- Security-awareness programma's;
- Organisatorische maatregelen zoals een taakverdeling m.b.t. security;
- Procedurele maatregelen zoals veiligheidsinstructies, protocollen en gedragsregels;
- Bouwkundige voorzieningen zoals hang- en sluitwerk en hekwerk;
- Technische voorzieningen zoals inbraakdetectie;
- Personele voorzieningen zoals de inzet van bewakers van gebouwen en terreinen.

Niet alle veiligheids- en schaderisico's zijn voor een organisatie even relevant. Daarom kunnen bepaalde risico's die weliswaar niet helemaal zijn uit te sluiten, doch uitermate onwaarschijnlijk zijn, worden geaccepteerd. Daarnaast zijn er veiligheids- en schaderisico's, die amper effect hebben op de continuïteit van de bedrijfsvoering van Rijkswaterstaat. Ook deze risico's kunnen normaliter worden geaccepteerd. Rest de wel relevante veiligheids- en schaderisico's. Deze dienen te worden voorzien van beheersingsmaatregelen. Daarbij dient dan onderscheid gemaakt te worden in de beschermingsmaatregelen en –voorzieningen, die de kans op het ontstaan van het risico kunnen reduceren (kansvermindering) en die welke het gevolg van het optreden van het risico verlagen (ernstreductie).

De effectiviteit, ofwel de mate waarin risico's kunnen worden gereduceerd wordt voor een groot deel bepaald door de mensen die aan het securityregiem onderworpen zijn en degenen, die voor de effectiviteit van de securityvoorzieningen moeten zorgdragen. Hoe groter het bewustzijn van de eigen rol in het realiseren van een veilige werkomgeving en bescherming van de bedrijfsmiddelen, hoe hoger de effectiviteit van de securitymaatregelen en –voorzieningen. De effectiviteit van de bescherming is het grootst bij de zogenaamde organisatorische en procedurele maatregelen.

Immers, zij bepalen hoe onveilige situaties worden voorkomen door gewenst gedrag van zowel medewerkers als derden. Fysieke maatregelen en voorzieningen zijn slechts de hulpmiddelen om het gewenste beschermingsniveau buiten de aanwezigheid van mensen te realiseren. De securityvoorzieningen missen echter elk effect indien de mensen die de effectiviteit ervan moeten realiseren dat achterwege laten. Met andere woorden: een slot op de deur heeft alleen effect, als het ook wordt gebruikt.

Het is daarom van groot belang om te beginnen met de aanpak van de risico's door een aanpassing van de werkwijze kunnen worden geëlimineerd of minstens aanzienlijk kunnen worden verminderd.

Vervolgens kunnen die risico's in ogenschouw worden genomen, die met behulp van gerichte instructies, procedures en gedragsregels kunnen worden verminderd. Een volledig pakket van deze procedurele maatregelen



draagt aanzienlijk bij aan de risicoreductie mits de kennis over de procedures actueel wordt gehouden en de naleving voortdurend aandacht krijgt.

In mindere mate, maar nog altijd met een aanzienlijke reductiebijdrage leveren de bouwkundige voorzieningen. Deugdelijk hang- en sluitwerk en hekwerk bemoeilijken het binnendringen.

Elektrotechnische securityvoorzieningen hebben op zich een beperkte risicoreductie als zodanig. De aanwezigheid ervan verhoogt wel de drempel voor onbevoegden vanwege een hogere pakkans. De voornaamste bijdrage aan de risicobeheersing bestaat echter uit het feit, dat snel en adequaat kan worden gereageerd indien onbevoegden zich van het terrein of gebouw meester trachten te maken.

De inzet van securitypersoneel is qua effect eveneens beperkt. Alleen op de plek van aanwezigheid en alleen gedurende de tijd van aanwezigheid. Bovendien is de herkenbare aanwezigheid van een beveiligingsbeambte alleen effectvol indien die aanwezigheid het gedrag van mensen direct beïnvloed. Met andere woorden, de inzet van een beveiligingsbeambte voor bewaking van een gebouw of terrein is weinig effectvol, inzet voor ordehandhaving bij evenementen is dat wel door directe beïnvloeding van het gedrag van mensen.

Hoe goed de beheersingsmaatregelen en -voorzieningen ook zijn en hoe perfect de security binnen een bedrijf wordt uitgevoerd, het zal altijd onmogelijk zijn om alle risico's tot 100% te beheersen. Niet alleen omdat bepaalde risico's zo specifiek zijn, dat ze niet of niet volledig met de gangbare securitymiddelen kunnen worden beheerst, maar ook omdat de inzet van securitymiddelen niet alle omstandigheden kan omvatten. Deze niet of onvoldoende beïnvloedbare risico's dienen daarom als restrisico's te worden beschouwd. De financiële gevolgen daarvan kunnen worden opgevangen via een verzekering.

Samengevat:

Het risicovolume (het risico) wordt bepaald door de kans, dat een incident zich (kan) manifesteren (K) en het effect van dat incident op de bedrijfsvoering van Rijkswaterstaat (E).

Een binnen het securityvakgebied gehanteerde formule is:

$$K(\text{ans}) \times E(\text{ffect}) = \text{Risico}$$

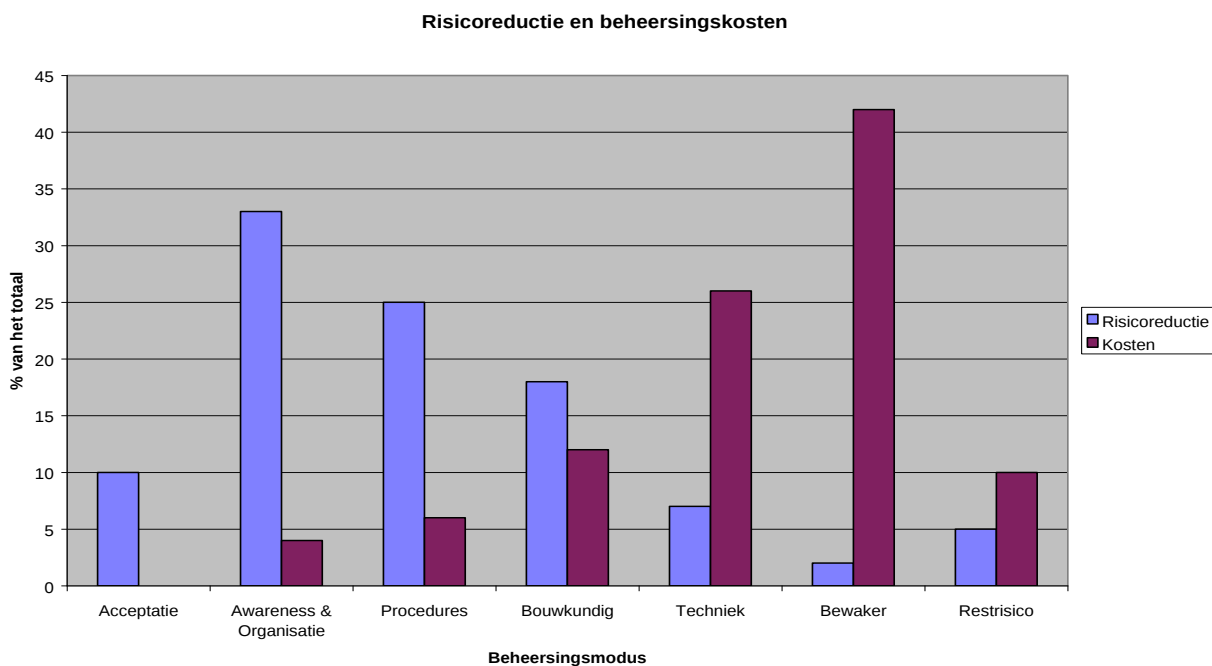
Een deel van de risico's kan worden geaccepteerd, een ander deel is normaliter niet te beheersen en zal als restrisico dienen te worden geaccepteerd. De rest zal met de beheersingsmaatregelen moeten worden bestreden.

De methodiek om de verschillende risico's adequaat te beheersen is het fasegewijs toewerken naar een steeds verdergaande reductie van het risicovolume, is als volgt weer te geven:

Risicovolume		Effect op te beheersen risicovolume
Niet beheersen	Beheersen door	
Acceptatie risico's		↓
	Awareness	↓
	Organisatorische maatregelen	↓
	Procedurele maatregelen	↓
	Bouwkundige maatregelen	↓
	Technische maatregelen	↓
	Inzet beveiligingspersoneel	↓
Acceptatie Restrisiko's		

Figuur 2: beheersing risicovolume

Kostentechnisch is het bovendien wenselijk om deze volgorde aan te houden, zoals uit onderstaand schema mag blijken. De mate van risicoreductie en kostenverdelingen zijn gebaseerd op ervaringscijfers bij een tiental grote ondernemingen.



Figuur 3: risicoreductie en beheersingskosten

8.6 De aard en inzet van de securitymiddelen

De aard van de inzet van securitymiddelen is nauw verbonden met de soort risico's waartegen moet worden beschermd en de beheersingsdoelen die men met de security voor ogen heeft. De securitymiddelen kunnen naar aard van de inzet worden onderscheiden in:



- preventieve inzet: maatregelen om te voorkómen dat zich incidenten voordoen;
- pro-actieve inzet: de voorbereiding van maatregelen die genomen moeten worden indien zich incidenten voordoen;
- reactieve inzet: maatregelen om incidenten te doen beëindigen;
- repressieve inzet: maatregelen ter opsporing van de dader(s) t.b.v. vervolging en schadeverhaal.

aangevuld met gerichte en regelmatig herhaalde security-awareness programma's.

De Rijkswaterstaat-manier om de inbreukrisico's te beheersen is het bewerkstelligen van een samenhangend securitypakket, dat:

- alle relevante security- en schaderisico's bereikt;
- alle securitybeheersingsdoelen bestrijkt;
- alle relevante beheersingsmaatregelen en -middelen omvat;
- alle facetten van de securitymiddeleninzet hanteert;
- de beheersing vanuit één conceptuele benadering realiseert en
- zowel intern als extern als één keten opereert.

Het voorgaande is samengevat in onderstaand schema

Rijkswaterstaat security basisbenadering			
Risico's	Doelen	Middelen	Aard inzet
criminaliteit zaakschade systeemschade persoonlijke veiligheid procesverstoring	voorkomen bemoeilijken betrappen beperken	awareness organisatorische procedurele bouwkundige elektronische Personele	preventief pro-actief reactief repressief
↓	↓	↓	↓
Geïntegreerd in één securityconcept			
↓			
Geïntegreerd met omgeving en externe belanghebbenden			

Figuur 4: security basisbenadering

Résumé

Het voorgaande samenvattend, kan de "handling" van de securityrisico's door Rijkswaterstaat als volgt worden samengevat:

Actie	Aard risico	Reactie	Hoe
Accepteren	Uitermate onwaarschijnlijk	geen	
	Verwaarloosbaar effect	geen	
	Buiten verantwoordelijkheid Rijkswaterstaat	Gedeeltelijk via beheersing	Algemeen preventief Reactief
Beheersen	Relevant	Preventief	Ontwerp nieuwbouw
			Ontwerp verbouw
			Materiaalgebruik
			Securityvoorzieningen
		Pro-actief	Securitymaatregelen
		Reactief	Securitymaatregelen
Restrisico	Noodzakelijk te accepteren	Repressief	Via overheid
		Verzekeren	
	Niet te accepteren	Schade beperken	Pro-actief Reactief
		Activiteiten staken	

Figuur 5: overzicht aanpak securityrisico's



9 De organisatorische en procedurele securitymaatregelen

De inhoudelijke organisatorische en procedurele securitymaatregelen dienen de randvoorwaarden te realiseren waardoor de resultaatdoelstellingen van de securitymaatregelen en –voorzieningen kunnen worden gehaald, de maximale efficiency in de uitvoering van de security kan worden gerealiseerd en de kwaliteit van de uitvoering van de security als geheel kan worden geborgd.

Randvoorwaardelijk daarvoor is, dat de security-awareness van de medewerkers (inclusief inhuurkrachten) een effectieve uitvoering van de organisatorische en procedurele securitymaatregelen ondersteunt. Bij de organisatorische en procedurele securitymaatregelen is onderscheid gemaakt in algemeen geldende gedragsregels, procedures en kaderstellende procedures. De laatste beogen het kader aan te geven waarbinnen de procedures binnen een onderdeel of op locatie te worden geformuleerd en geconcretiseerd.

9.1 De doelen van de securitymaatregelen

De doelen voor security van de RWS-locaties dienen te worden vertaald in doelen, die door de in te voeren securitymaatregelen moeten worden behaald. Per categorie worden hieronder de doelen van de (belangrijkste) organisatorische en procedurele securitymaatregelen opgesomd.

9.1.1 *Security-awareness*

- Permanente aandacht voor de security in de uitvoering van de eigen werkzaamheden;
- Permanente aandacht voor de security in de eigen werkomgeving.

9.1.2 *Securitygedragsregels*

- Voorkomen, dat situaties of omstandigheden ontstaan die incidenten kunnen uitlokken of bevorderen;
- Bescherming van de eigendommen en bedrijfsinformatie van Rijkswaterstaat.

9.1.3 *Algemene securityprocedures*

- Voorkomen, dat situaties of omstandigheden ontstaan die incidenten kunnen uitlokken of bevorderen;
- Bescherming van de eigendommen en bedrijfsinformatie van Rijkswaterstaat;
- Beperking van schade door regulering bevoegde aanwezigheid op terreinen en in gebouwen van Rijkswaterstaat.



9.1.4 *Kaderstellende securityprocedures*

- Voorkomen, dat onbevoegde en/of ondeskundige uitvoering van securitywerkzaamheden door derden worden uitgevoerd;
- Zeker stellen van de kwaliteit van de uitvoering van securitywerkzaamheden door derden.

9.1.5 *Alarmopvolging*

- Beperking van de schade door onderkende risico's door ongewenste activiteiten zo spoedig mogelijk te doen beëindigen en zo snel mogelijk aan te vangen met het nemen van schadebeperkende maatregelen;
- Verhogen van de preventie door verkleining van de kans op voltooiing van de opzet en vergroting van de pakkans.

9.2 **Functionele eisen securitymaatregelen**

Om de securitydoelstellingen te bereiken én om de werking van de securitymaatregelen te kunnen toetsen, dienen de securitymaatregelen te voldoen aan functionele eisen. Per categorie worden hieronder functionele eisen beschreven.

9.2.1 *Security-awareness*

- Gericht op de uitvoering van de eigen werkzaamheden;
- Gericht op de werkplekomgeving;
- Gericht op de positie en rol van Rijkswaterstaat;
- Regelmatig herhaald en geactualiseerd.

9.2.2 *Securitygedragsregels*

- Kort en in begrijpelijke taal;
- Per aandachtsgebied;
- Slechts voor één uitleg vatbaar;
- Controleerbaar.

9.2.3 *Algemene securityprocedures*

- Kort en in begrijpelijke taal;
- Dirigerend en direct;
- Per aandachtsgebied;
- Slechts voor één uitleg vatbaar;
- Controleerbaar.

9.2.3.1. Kaderstellende securityprocedures

- Alle facetten van de uitbesteding omvattend;
- Controleerbaar.

9.2.4 *Alarmopvolging*

- Gegarandeerde response binnen vastgesteld tijd;
- Response door personen met bevoegdheid en bekendheid ten aanzien van de RWS-omgeving.

9.3 **Algemeen geldende securitygedragsregels**

Algemeen geldende gedragsregels geven de normen aan waaraan een ieder in de gebouwen en op de terreinen van Rijkswaterstaat zich dient te houden. Aan deze regels kan niet worden getornd, noch regionaal of lokaal worden afgeweken. De algemene gedragsregels zijn opgenomen in het medewerkersprotocol. Daarnaast gelden de volgende algemene gedragsregels ter bescherming van Rijkswaterstaatinformatie en Rijkswaterstaateigendommen.

9.4 **Algemeen geldende securityprocedures**

Algemeen geldende securityprocedures schrijven voor op welke wijze securityaandachtswelden dienen te worden behandeld in de gebouwen en op de terreinen van Rijkswaterstaat. Aan deze procedures kan niet worden getornd, noch regionaal of lokaal worden afgeweken.

9.5 **Kaderstellende securityprocedures**

Kaderstellende securityprocedures schrijven voor binnen welke randvoorwaarden en kaders decentraal securityprocedures dienen te worden geformuleerd en geconcretiseerd. Deze procedures hebben met name betrekking op de inzet van externe beveiligingsdienstverleners zoals een alarmcentrale, toezichtcentrale en bewakingsdienst.

Vanuit de functionele eis dat response gegarandeerd en binnen de gestelde tijd dient te geschieden, is invulling hiervan met behulp van eigen personeel niet aannemelijk. Dit zou tevens maatregelen vergen om deze response op zodanige wijze te laten geschieden, dat aan de ARBO-wet wordt voldaan. Alarmopvolging door de politie zal op grond van de laatste wetswijziging pas dan worden ingezet als het alarm op enigerlei wijze is geverifieerd. Dergelijke verificatie kan zijn door persoonlijke waarneming, detectie door meerdere afzonderlijke detectoren of met behulp van camerabeelden. Daarbij zal de politie haar response altijd moeten afwegen tegen andere taken en incidenten.

De meest gecontroleerde response kan verkregen worden door met een beveiligingsdienst een overeenkomst met gegarandeerde responsetijd aan te gaan.



De inzet van de beveiligingsdienst dient aansluiting te hebben met opsporing en vervolging van plegers van onbevoegd handelen.

De uitvoering van bewakingswerkzaamheden door een beveiligingsdienst geschiedt bij Rijkswaterstaat onder strikte condities ten aanzien van de organisatie en bedrijfsvoering van de beveiligingsdienst, de gestelde uitvoeringseisen t.a.v. alarmopvolging, sleutelservice, brand-, sluit- en controleronden en receptiediensten, de klachtbehandeling, geheimhouding en overleg over de uitvoering van de werkzaamheden.

9.6 Securityprotocollen

Algemene securityprotocollen schrijven voor op welke wijze securityincidenten afgehandeld dienen te worden. De afhandeling van security-incidenten bij Rijkswaterstaat heeft betrekking op de interne en externe alarmontvangers en de interne en externe alarmopvolgers. Per RWS-locatie kan de uitvoering van zowel de alarmontvangst als de alarmopvolging verschillen. De kernprotocollen alarmafhandeling security-incidenten gelden voor geheel Rijkswaterstaat tenzij op locatie niet van toepassing.

De protocollen bij alarmafhandeling dienen ervoor te zorgen, dat een alarm effectief en efficiënt wordt afgehandeld. Om die redenen zijn voor Rijkswaterstaat t.a.v. de meest relevante alarmsituaties kernprotocollen opgesteld. Voor een juiste effectiviteit dienen deze per Rijkswaterstaatlocatie te worden geconcretiseerd.

De securitygedragsregels, -procedures, -instructies en -protocollen zijn uitgewerkt in deel II van dit handboek.

9.7 Locatiespecifieke inrichting en uitwerking

Per RWS-locatie zullen de organisatorische en procedurele securitymaatregelen specifiek moeten worden gemaakt, geconcretiseerd en zo nodig aangevuld.

10 Securityvoorzieningen

10.1 Doelen van de securityvoorzieningen

De doelen voor security van RWS-locaties dienen te worden vertaald in doelen, die door de aan te brengen voorzieningen moeten worden behaald. Per categorie worden hieronder de doelen van de securityvoorzieningen opgesomd.

10.1.1 *Fysieke afscherming van terreinen*

- voldoen aan wettelijke verplichtingen door onbevoegde betreding van het RWS-gebied voldoende te belemmeren;
- bescherming tegen onderkende risico's door de bereikbaarheid van het RWS-gebied voor onbevoegden en de vluchtmogelijkheden te beperken.

10.1.2 *Fysieke afscherming van gebouwen*

- bescherming tegen onderkende risico's door belemmeren van binnendringen van gebouwen of gebouwdelen door onbevoegden;
- bescherming tegen onderkende risico's door belemmeren van betreding van gebouwen of gebouwdelen door onbevoegden.

10.1.3 *Toegangsbeheersing*

- voldoen aan wettelijke verplichtingen door onbedoelde/onbevoegde betreding het RWS-gebied voldoende te belemmeren;
- bescherming tegen onderkende risico's door belemmeren van betreding van terrein, gebouwen of gebouwdelen door onbevoegden.

10.1.4 *Cameratoezicht en -registratie*

- bescherming tegen onderkende risico's door observeren en registreren van ongewenste aanwezigheid en/of activiteiten op het terrein en rond/in gebouwen als basis voor repressieve maatregelen;
- bieden van herkenbare voorziening ter realisatie van veiligheidsgevoelens van personen.

10.1.5 *Detectie en alarmering*

- signaleren van ongewenste betreding/aanwezigheid op het terrein of in de gebouwen/gebouwdelen;
- mogelijk maken van effectieve en efficiënte alarmverificatie;
- mogelijk maken van effectieve en efficiënte alarmopvolging.



10.2 Algemene functionele eisen securityvoorzieningen

Om de securitydoelstellingen te bereiken én de werking van de securityvoorzieningen te kunnen toetsen, dienen de securityvoorzieningen te voldoen aan functionele eisen. Per categorie voorzieningen zijn de functionele eisen beschreven in Deel V, bijlage 1.

10.3 Inrichting van de securityvoorzieningen

De inzet van securityvoorzieningen bij de inrichting van de security kan op basis van velerlei uitgangspunten en overwegingen. Rijkswaterstaat heeft ervoor gekozen om op basis van de aan de voorzieningen te stellen beheersingsdoelen en de daaraan gekoppelde functionele eisen per soort securityvoorzieningen waar mogelijk te standaardiseren en vanuit het marktaanbod aan uitvoeringen die uitvoeringen te kiezen die het beste bij de uitgangspunten en eisen passen. Een opsomming van deze keuzen per soort securityvoorziening alsmede de daarbij gehanteerde overwegingen zijn opgenomen in Deel V, bijlage 2.

De concretisering van de voorzieningen zijn nader uitgewerkt per soort RWS-locatie en opgenomen in deel II van dit handboek.

10.4 Technische specificaties van de securityvoorzieningen

De aan de securityvoorzieningen gekoppelde functionele eisen dienen te worden vertaald naar technische specificaties. Deze specificaties zijn opgenomen in deel IV.

11 De categorisering van de infrastructurele locaties

De infrastructurele locaties van Rijkswaterstaat verschillen per soort onderling van elkaar. Binnen dezelfde soort locatie zijn ze evenmin gelijk. Een toekomstvaste security van deze locaties vereist echter, dat deze aansluit op het risicoprofiel van het type RWS-locatie. Dat risicoprofiel wordt gevormd door de zogenaamde attractiviteit voor inbreuken en het effect van die inbreuken.

Met attractiviteit wordt bijvoorbeeld bedoeld op de aantrekkingskracht op criminelen en vandalen, de ontdekkingskans bij inbreuken of als gevolg van de aard van de directe omgeving.

Met effect wordt bedoeld op de aard en omvang van de schade, zowel materieel als immaterieel, zowel voor de bedrijfsvoering(en) als voor de bezoekers, personeel en gebruikers en zelfs voor het imago van Rijkswaterstaat en andere belanghebbenden.

11.1 De opzet van de categoriseringsmethodiek

De methodiek heeft alle aspecten, die het risicoprofiel (mede) bepalen, ondergebracht in een tweetal hoofdgroepen, zijnde de risicogene factoren⁷⁾ die het bestuurlijke en bedrijfsmatige belang van het type RWS-locatie vertegenwoordigen (bedrijfsprocesfactoren) en daarnaast de risicogene factoren die de attractiviteitswaarde (attractiviteitsfactoren) van het type RWS-locatie bepalen.

Het gaat hier om de factoren die, vanuit het daderperspectief geredeneerd, van invloed zijn op een keuze om juist op die locatie een moedwillige verstoring te veroorzaken. Waardoor kan een potentiële dader getriggerd worden.

Ten behoeve van een zo groot mogelijke eenvormigheid en maximale effectiviteit van de security bij Rijkswaterstaat zijn in de gehanteerde methodiek de infrastructurele locaties allereerst gezamenlijk voorzien van de van belang zijnde risicogene factoren. Vervolgens is elke risicogene factor voorzien van die criteria die in staat moeten worden geacht om het type RWS-locatie ten opzichte van elkaar te kunnen onderscheiden. Aan de criteria zijn waarden toegekend om binnen dezelfde groep locaties onderscheid te kunnen maken naar zwaarte van het belang voor Rijkswaterstaat. Daarna is per factor de relevantie per locatie bepaald.

Op basis van de aan elke locatie te koppelen risicogene factoren en de daarbij behorende waarderingen zijn per locatie de zwaartecategorieën vastgesteld.

Security richt zich op het beheersen van risico's om verstoring van de bedrijfsvoering te voorkomen of beperken. Het is noodzakelijk om te weten welke inbreukrisico's als relevant moeten worden beschouwd. De security van het type RWS-locatie moet deze risico's kunnen beheersen.

⁷⁾ Risicogene factoren zijn situaties en omstandigheden, de incidenten kunnen doen ontstaan of bevorderen.



In principe hebben locaties te maken met dezelfde scope van securityrisico's. Daarom is vastgesteld welke risico's per locatie als relevant gelden. Deze risicosamenstelling is van invloed op het samen te stellen pakket aan securitymaatregelen en -voorzieningen.

Een effectieve security vereist bovendien, dat de securitymaatregelen en -voorzieningen zodanig zijn ingericht, dat ze gericht zijn op de meest waarschijnlijke scenario's waarop inbreuken kunnen worden uitgevoerd. Daarom is per soort locatie ten behoeve van de opzet en inrichting van de Basis Security Niveau's uitgegaan van de voor die soort algemeen relevant geachte securityrisico's en incidentscenario's en dadertypen. Met inachtneming van de relevante risico's en incidentscenario's zijn per locatie per zwaartecategorie de basissecuritymaatregelen en -voorzieningen samengesteld.

11.2 De infrastructurele type Rijkswaterstaat-locaties

De voor de security bij Rijkswaterstaat te onderscheiden type locaties en combinaties van typen objecten op één locatie zijn:

1. Verkeerscentrales
2. Nautische Verkeersposten
3. Bruggen
4. Tunnels
5. Waterkeringen
6. Schutsluizen
7. Stuwcomplexen
8. Gemalen
9. Spuisluizen
10. Kantoren en overige gebouwen
11. Rijkswegen
12. Vaarwegen
13. Meetsystemen Landelijk Meetnet Water
14. Veerhavens
15. Centrale VICNET Ruimten
16. Brug-schutsluis combinatie
17. Brug-schutsluis-spuisluis combinatie
18. Brug-schutsluis-kering combinatie
19. Brug-schutsluis-gemaal combinatie
20. Schutsluis-spuisluis combinatie
21. Schutsluis-spuisluis-gemaal combinatie
22. Schutsluis-gemaal combinatie
23. Schutsluis-gemaal-kering combinatie
24. Spuisluis-gemaal combinatie
25. Aquaducten
26. Via- en ecoducten
27. Verzorgingsplaatsen
28. Weggebonden DVM

De uitwerking voor de waterwegen volgt op een later moment. De overige objecttypen zijn gereed.

11.3 De bedrijfsprocesfactoren van Rijkswaterstaat-locaties

Het belang van een locatie voor de bedrijfsprocessen van Rijkswaterstaat en dus van Rijkswaterstaat als organisatie wordt voornamelijk bepaald door de aard en omvang van de bedrijfsvoering per type locatie. Het is voor de bepaling van de aard en omvang van de security noodzakelijk om te weten wat het effect is bij gehele of gedeeltelijke uitval van de functionaliteit van de bedrijfsvoorzieningen en bedrijfsprocessen. De methodiek inventariseert daarom de meest van invloed zijnde risicogene factoren van de bedrijfsvoeringaspecten (bedrijfsprocesfactoren) en voorziet deze van een waardering.

De vaststelling van de bedrijfsprocesfactoren is in samenspraak met Rijkswaterstaat uitgevoerd.

11.4 Motiveringen subverdelingen bedrijfsprocesfactoren

11.4.1 Bestuurlijke bedrijfsprocesfactoren

Het bestuur en management van Rijkswaterstaat inclusief de daaraan verbonden ondersteuning (secretariaten en staven) kenmerkt zich door hoogwaardige en bedrijf kritische informatie en hoge beslisniveaus. Aantasting van de integriteit van de uitvoerders, dan wel ontvreemding van de informatie zou tot grote problemen in de continuïteit van de bedrijfsvoering van de Maatschappelijk Vitale Processen, voortgang van infrastructurele projecten of planontwikkeling, grote imagoproblemen voor Rijkswaterstaat alsmede tot problemen in de continuïteit van de bedrijfsvoering van de vervoerders op het hoofd(vaar)wegennet kunnen leiden.

Bestuurlijke & juridische processen

Om onderscheid in de zwaarte van deze bedrijfsprocesfactor te kunnen maken is onderscheid gemaakt in de reikwijdte van de functie in:

- *Nationaal*
- *Regionaal*

Inkoop & Contractmanagement

Om onderscheid in de zwaarte van deze bedrijfsprocesfactor te kunnen maken is onderscheid gemaakt in de omvang van de gevolgen in:

- *Nationaal*
- *Regionaal*

Assetmanagement

Om onderscheid in de zwaarte van deze bedrijfsprocesfactor te kunnen maken is onderscheid gemaakt in de omvang van de gevolgen in:

- *Nationaal*
- *Regionaal*



11.4.2 Bedrijfsmatige bedrijfsprocesfactoren

Operationeel verkeers-/watermanagement

De ongestoorde uitvoering van het operationeel verkeers-/watermanagement is van cruciale invloed op de voortgang van het weg- en waterverkeer. Om onderscheid in de zwaarte van deze bedrijfsprocesfactor te kunnen maken is onderscheid gemaakt in de effecten bij uitval van het aansturingsproces in:

de omvang van de gevolgen in:

- *Internationaal*
- *Nationaal*
- *Regionaal*

Proces gebonden voorzieningen

De permanente beschikbaarheid en ongestuurd functioneren van proces gebonden voorzieningen is cruciaal voor de continuïteit van de bedrijfsvoeringen binnen Rijkswaterstaat. Om onderscheid in de zwaarte van deze bedrijfsprocesfactor te kunnen maken is onderscheid gemaakt in:

- *MVP (Maatschappelijk Vitaal Proces) gebonden voorzieningen zonder alternatieven*
- *MVP gebonden voorzieningen met alternatieven*
- *Overige procesvoorzieningen (inclusief gebouw gebonden voorzieningen).*

Er is sprake van een alternatieve procesvoorzieningen indien op locatie of in de omgeving eenzelfde proces kan worden uitgevoerd zoals bijv. in een sluiscomplex met 2 kolken als er één uitvalt.

Wegvakwaarde

Niet alle wegen zijn voor de uitvoering van het Maatschappelijk Vitaal Verkeersproces van even groot belang. Om onderscheid in de zwaarte van deze bedrijfsprocesfactor van de wegvak gerelateerde locaties te kunnen maken is de wegvakwaarde als basis genomen. Hoe hoger de wegvakwaarde, hoe groter het belang van het wegvak voor de continuïteit van het hoofdwegennet. De wegvakken zijn in de volgende zwaartegroepen ingedeeld, van laag naar hoog:

- *Categorie A (Basisnet)*
- *Categorie B (Hoofdverbindingen tussen regionale netwerken)*
- *Categorie C (Hoofdverbindingen tussen economische en stedelijke netwerken)*
- *Categorie D (Ringen en schakels in nationale en stedelijke netwerken)*

Watervakwaarde

Niet alle vaarwegen zijn voor de uitvoering van het Maatschappelijk Vitaal Scheepvaartproces van even groot belang. Om onderscheid in de zwaarte van deze bedrijfsprocesfactor van de watervak gerelateerde locaties te kunnen maken is de watervakwaarde als basis genomen. Hoe hoger de watervakwaarde, hoe groter het belang van het watervak voor de continuïteit van het hoofdvaarwegennet. De watervakken zijn in de volgende zwaartegroepen ingedeeld:

- *Zeehaventoegangen*
- *Hoofdtransportassen*
- *Hoofdvaarwegennet*
- *Overige vaarwegen*

Watersysteemwaarde

Niet al het waterbeheer is voor het Maatschappelijk Vitaal Waterbeheersingsproces van even groot belang. Om onderscheid in de zwaarte van deze bedrijfsprocesfactor te kunnen maken is de watersysteemwaarde als basis genomen. Hoe hoger deze watersysteemwaarde, hoe groter het belang van het waterbeheer voor de continuïteit van de waterbeheersing in Nederland. De watersysteemwaarde zijn in de volgende zwaartegroepen ingedeeld:

- *Noordzee gebonden*
- *Rivier gebonden*
- *Regionaal*

Het overzicht van de bedrijfsprocesfactoren en de relevantie ervan per type locatie is opgenomen in Deel V, Bijlage 3.

11.5 De attractiviteitsfactoren⁸ van de RWS-locaties

Een RWS-locatie is geen eiland in de maatschappij, maar maakt deel uit van een omgeving. Die omgeving is van invloed op het risicoprofiel. Datzelfde geldt ook voor de locatie zelf en het gebruik ervan. De attractiviteit van een gebouw of terrein voor onrechtmatige inbreuken wordt bepaald door het gebouw of terrein zelf (gevelopeningen, verlichting etc.), de karakteristieken van de bedrijfsvoering (openingstijden, bezettingen etc.) en de omgevingsbijzonderheden. Zij bepalen gezamenlijk de mate van kwetsbaarheid voor criminaliteit en andere onrechtmatige inbreuken. De methodiek inventariseert daarom de meest van invloed zijnde risicogene factoren van de locatieaspecten (attractiviteitsfactoren) en voorziet deze van een waardering.

11.6 Motiveringen subverdelingen attractiviteitsfactoren

11.6.1 Omgeving gerelateerde factoren

Aard omgeving

De aard van de omgeving bepaalt de mate waarin de feitelijke situatie kan bijdragen aan het ontstaan of bevorderen van incidenten. Het betreft hier het overwegend karakter van het gebied in een straal van een kilometer om het object. Om onderscheid te kunnen maken in de zwaarte van deze attractiviteitsfactor is onderscheid gemaakt in:

- *woongebied*

De situering van een locatie in een woongebied impliceert dat de attractiviteit van een woongebied voor allerlei vormen van overlast en criminaliteit zich tot deze locatie uitstrekt. De locatie maakt er immers deel

⁸De attractiviteitsfactoren zijn door het bureau PSCT (Probabilistisch Solution Consult & Training) statistisch onderzocht. De uitkomst van het onderzoek gaf aan dat er een correlatie is tussen incidenten en het totaal aan genoemde factoren van meer dan 80%. De conclusie daarbij is dat de genoemde attractiviteitsfactoren daadwerkelijk bijdragen aan het ontstaan – en bij beheersing – het voorkomen van incidenten.



van uit. Er is sprake van een woongebied indien naast woningen ook scholen en winkels aanwezig zijn

- *landelijk*

De situering van een locatie in een landelijk gebied staat onder invloed van de aard en omvang van landelijke criminaliteit en overlast en is over het algemeen beperkter naar aard en soort criminaliteit en overlast dan de woongebied omgeving. Er is sprake van een landelijk gebied indien noch woonconcentraties, noch bedrijvenconcentraties in de nabije omgeving aanwezig zijn.

- *industrieel*

De situering van een locatie in een industrieel gebied staat onder invloed van de aard en omvang van de criminaliteit en overlast op bedrijventerreinen en is over het algemeen beperkt naar aard en soort criminaliteit en overlast. Er is sprake van een industrieel gebied indien in de nabije omgeving wel bedrijvenconcentraties, maar geen woningconcentraties aanwezig zijn.

Bijzonderheden directe omgeving

De inrichting van de directe en nabije omgeving (op minder dan 1 kilometer van de locatie) is van invloed op de mate waarin de omgevingslocatie personen met de daarbij behorende kenmerken en risico's aantrekken. Om onderscheid te kunnen maken in de zwaarte van deze attractiviteitsfactor is onderscheid gemaakt in:

- *kantoren*

Kantoren beïnvloeden de securityrisico's in de omgeving doordat kantoorpersoneel en bezoekers potentieel slachtoffer kunnen zijn van criminelen die het op geld en goed gemunt hebben. Als zodanig hebben kantoren een aantrekkende werking op bepaalde vormen van vermogenscriminaliteit met meer of minder uitstraling naar de locatie.

- *winkelcentrum*

Winkelcentra trekken tijdens de openingstijden van de winkels bepaalde groepen criminelen (veel voorkomende criminaliteit) aan, terwijl buiten die tijden juist de overlast (junks, zwervers) manifester is. Die uitstraling zal zich tot de locatie uitstrekken.

- *uitgaanscentrum*

Als zodanig hebben uitgaanscentra een aantrekkende werking op bepaalde vormen van criminaliteit (vernieling, graffiti etc.). Afhankelijk van de aard van het uitgaanscentrum zal het effect ervan op de locatie groter of kleiner zijn.

- *sportaccommodaties*

Het publiek van sportaccommodaties zal in het eigen gedrag geen onderscheid maken naar locatie. Het effect zal heel afhankelijk zijn van de soort accommodatie (groot verschil tussen voetbal of zaalsport). De uitstraling van sportaccommodaties zal meer overlast- en vandalisme gerelateerd dan crimineel gerelateerd zijn.

- *scholen*

De aard, omvang en ligging van de scholen is bepalend voor de mate waarin overlast op een locatie gegenereerd wordt. De uitstraling van scholen zal meer overlast- en vandalisme gerelateerd dan crimineel gerelateerd zijn.

- *bedrijven*

De aanwezigheid van bedrijven biedt tijdens werktijd enige sociale controle op de omgeving van de locatie. Buiten werktijd kan de voor bedrijven relevante criminaliteit zich beperkt uitstrekken tot de locatie.

- *woningen*

De aanwezigheid van woningen biedt enige vorm van sociale controle op de directe omgeving van de locatie.

Invloed omgeving

De aard van de directe omgeving van een locatie bepaalt mede de mate waarin wordt overgegaan tot onrechtmatigheden. De mate waarin de locatie in de omgeving van de locaties schoon en heel zijn bepaalt de aantrekkelijkheid voor verloedering en vervuiling. Hoe schoner en heler, hoe hoger de drempel om te vervuilen. De aanwezigheid van junks en zwervers bepaalt in grote mate het gevoel van veiligheid m.b.t. de locatie. Om onderscheid in de zwaarte van deze attractiviteitsfactor te kunnen maken is onderscheid gemaakt in:

- *Positieve invloed (geen zichtbare verloedering, geen junks/zwervers)*
- *Neutrale invloed*
- *Negatieve invloed (veel zichtbare verloedering, zwervers/junks)*

Verlichting

De aard, omvang en werking van de verlichting rondom een locatie is bepalend voor de mate waarin onrechtmatige toegang tot de locatie kan worden ontdekt. Om onderscheid in de zwaarte van deze attractiviteitsfactor te kunnen maken is onderscheid gemaakt in:

- *Goed (omgeving volledig en voldoende verlicht)*
- *Matig (omgeving onvolledig en/of onvoldoende verlicht)*
- *Slecht (omgeving niet of onvolledig en onvoldoende verlicht)*

11.6.2 Locatie gerelateerde factoren

Situering locatie

De ligging van het gebouw is bepalend voor de mate en het gemak waarin onrechtmatige toegang tot het gebouw kan worden verkregen. Om onderscheid in de zwaarte van deze attractiviteitsfactor te kunnen maken is onderscheid gemaakt in:

- *vrijstaand (veel mogelijkheden op inbreuken)*
- *aangebouwd (enige mogelijkheden op inbreuken)*
- *in pandig (geringe mogelijkheden op inbreuken)*



Aantal toegangen

Het aantal reguliere toegangen tot een locatie is bepalend voor de mate waarin onrechtmatige toegang tot de locatie kan worden verkregen. Om onderscheid in de zwaarte van deze attractiviteitsfactor te kunnen maken is onderscheid gemaakt in:

- *< 3 (beperkte mogelijkheid onbevoegd betreden)*
- *3-8 (gerede mogelijkheid onbevoegd betreden)*
- *8> (veel mogelijkheden onbevoegd betreden)*

Aard bezetting

De aard van de bezetting bepaalt in hoge mate de betrokkenheid van de aanwezigen bij de belangen van Rijkswaterstaat. Om onderscheid in de zwaarte van deze attractiviteitsfactor te kunnen maken is onderscheid gemaakt in:

- *eigen personeel Rijkswaterstaat*

Van het eigen Rijkswaterstaatspersoneel mag van een hoge betrokkenheid bij de belangen van Rijkswaterstaat worden uitgegaan en daarmee van een zekere mate van sociale controle. Tot het eigen personeel wordt ook gerekend het personeel van aan Rijkswaterstaat gelieerde instituten en bedrijven die in gebouwen of op terreinen van Rijkswaterstaat zijn gehuisvest.

- *personeel contractpartner*

Verondersteld wordt, dat personeel van contractpartners(contractaannemers) een zekere betrokkenheid heeft met Maatschappelijk Vitaal Proces en daarmee tevens (indirect) bij de belangen van Rijkswaterstaat.

- *inhuurpersoneel*

De betrokkenheid van inhuurpersoneel bij de belangen van Rijkswaterstaat is beperkt. Sociale controle door dit personeel mag niet als standaard worden aangenomen.

- *derden*

Verondersteld wordt, dat personeel van derden (bijv. schoonmaak) een ruime betrokkenheid heeft met de eigen onderneming, doch geen betrokkenheid heeft met de belangen van Rijkswaterstaat.

Omvang bezetting

De omvang van de bezetting op het object is van invloed op de mate van sociale controle en toegangsdiscipline. Om onderscheid in de zwaarte van deze attractiviteitsfactor te kunnen maken is onderscheid gemaakt in:

- *geen (geen mogelijkheden tot toezicht)*
- *< 10 (geringe mogelijkheden tot toezicht)*
- *10 – 50 (enige mogelijkheden tot toezicht)*
- *50 – 100 (gerede mogelijkheden tot toezicht)*
- *100 > (veel mogelijkheden tot toezicht)*

Aanwezigheid bezetting

De openingstijden zijn van invloed op de mate van eigen toezicht op de locatie door werknemers op het object. Om onderscheid in de zwaarte van deze attractiviteitsfactor te kunnen maken is onderscheid gemaakt in:

- *incidentele bezetting (geringe mogelijkheden tot toezicht)*
- *dagbezetting (enige mogelijkheden tot toezicht)*
- *vroeg-laag bezetting (gerede mogelijkheden tot toezicht)*
- *een volcontinue bezetting (veel mogelijkheden tot toezicht)*

Bezoekers/derden per dag

De mate waarin niet medewerkers in het gebouw vertoeven is van invloed op de mate waarin ongecontroleerd in het gebouw kan worden "gezworven" en daardoor bepalend voor de noodzaak tot compartimentering. Om onderscheid in de zwaarte van deze attractiviteitsfactor te kunnen maken is onderscheid gemaakt in:

- *< 10 (weinig mogelijkheden tot zwerfgedrag)*
- *10 – 50 (gerede mogelijkheden tot zwerfgedrag)*
- *50 > (veel mogelijkheden tot zwerfgedrag)*

Parkeren

De plaats waar het parkeren is gesitueerd, bepaalt de mate waarin gebouw gebonden inbreuken kunnen plaatsvinden. De aard van de parkeervoorziening voor auto's is bepalend voor de attractiviteit voor met name diefstal en vernieling. Onder een bewaakte parkeervoorziening wordt verstaan een parkeervoorziening waarbij alle in- en uitgangen volledig zijn afgesloten en alleen toegankelijk zijn voor personen met een geldig parkeerbewijs. Parkeerplaatsen waar wel voor moet worden betaald, maar die vrij toegankelijk zijn voor personen worden gekwalificeerd als onbewaakt.

Om onderscheid in de zwaarte van deze attractiviteitsfactor te kunnen maken is onderscheid gemaakt in:

- | | |
|---------------------------------------|---|
| • <i>uitpandig onbewaakt parkeren</i> | <i>hoge kans op auto gerelateerde incidenten</i> |
| • <i>inpandig onbewaakt parkeren</i> | <i>lage kans auto gerelateerde incidenten, gerede kans op gebouw gebonden inbreuken</i> |
| • <i>uitpandig bewaakt parkeren</i> | <i>lage kans op auto gerelateerde incidenten</i> |
| • <i>inpandig bewaakt parkeren</i> | <i>lage kans op auto gerelateerde incidenten en gebouw gebonden inbreuken</i> |



11.6.3 *Infra gerelateerde factoren*

Kruisingen

Met kruisingen wordt bedoeld op de kruising van de hoofdweg met andere vervoersinfrastructuren. De aard van de kruisende infrastructuur biedt meer of minder mogelijkheden om via de kruisende infrastructuur incidenten op de hoofdweg te veroorzaken. Om onderscheid in de zwaarte van deze attractiviteitsfactor te kunnen maken is onderscheid gemaakt in:

- *Openbare (regionale/lokale) weg: zowel toegankelijk voor motorvoertuigen als (brom)fietzers en voetgangers.*
- *Spoorweg: infrastructuur voor railvervoer (trein, metro, tram).*
- *Bevaarbaar water (geen hoofdvaarweg)*

Aard kruising

Niet elke soort kruising geeft een even grote kans op het ontstaan van incidenten. De positie van de hoofdweg op de kruising biedt meer of minder mogelijkheden om incidenten op de hoofdweg te veroorzaken (bijvoorbeeld het werpen van voorwerpen op de hoofdweg). Om onderscheid in de zwaarte van deze attractiviteitsfactor te kunnen maken is onderscheid gemaakt in:

- *Boven kruisend: het (Rijks)wegverkeer kruist over de andere vervoersinfrastructuur.*
- *Onder kruisend: het (Rijks)wegverkeer kruist onder de andere vervoersinfrastructuur.*

Aard kunstwerk

Met de aard van een kunstwerk wordt de mogelijkheid voor obstructie van de functionaliteit van het kunstwerk aangegeven. Dit element is alleen relevant voor bruggen. Om onderscheid in de zwaarte van deze attractiviteitsfactor te kunnen maken is onderscheid gemaakt in:

- *beweegbaar*
- *vast*

Aantal motorvoertuigen per etmaal

De intensiteit van het wegverkeer bepaalt de mate waarin preventief toezicht kan worden uitgevoerd of incidenten kunnen worden gesignaleerd. Om onderscheid in de zwaarte van deze attractiviteitsfactor te kunnen maken is onderscheid gemaakt in:

- *<50.000*
- *50.000 – 100.000*
- *100.000 >*

Waterverkeersbewegingen/dag

De intensiteit van het waterverkeer bepaalt de mate waarin preventief toezicht kan worden uitgevoerd of incidenten kunnen worden gesignaleerd. Om onderscheid in de zwaarte van deze attractiviteitsfactor te kunnen maken is onderscheid gemaakt in:

- *< 25*
- *25 - 75*
- *75 >*

Het overzicht van de attractiviteitsfactoren en de relevantie ervan per type locatie is opgenomen in Deel V, Bijlage 3.

11.7 Waardering criteria risicogene factoren

Om tot een waarderingsmodel te kunnen komen, is gewerkt volgens een systematische benadering van de waardebeoordeling van de risicogene factoren. Deze waardebeoordeling is in samenwerking met de in de uitwerking betrokken medewerkers van Rijkswaterstaat vastgesteld. Per groep van locaties zijn de relevante onderscheidende factoren geselecteerd en van een relatieve waarde ten opzicht van elkaar voorzien. Daarna zijn de onderscheidende factoren binnen een voor elke locatie gezamenlijk vastgesteld totaal gewaardeerd. Het eindresultaat is vervolgens binnen Rijkswaterstaat getoetst, waarbij geen onevenwichtigheden aan het licht zijn gekomen.

De uitwerking van de waarderingsmethodiek is opgenomen in Deel V, bijlage 4.

11.8 Waarderingsmatrix

Na vaststelling van de relatieve verhoudingen van de diverse groepen, subgroepen en criteria van de risicogene factoren is het mogelijk om deze verhoudingen om te zetten in voor een inventarisatie bruikbare vorm. Om de risicogene factoren te kunnen inventariseren is het noodzakelijk om daaraan concrete waarden te koppelen. Daartoe is het voor het totaal van alle risicogenen factoren een getal gekozen, dat in de uitwerkingen tot bruikbare waarden leidt. Voor Rijkswaterstaat is daarbij uitgekomen op een totaal van 2000 punten. Het is niet belangrijk welk totaalgetal wordt gekozen voor de bruikbaarheid van de methodiek. De onderlinge verhoudingen staan immers vast. Op basis van de procentuele zwaartewegingen is het aantal punten per risicogene factor bepaald.

Omwille van de homogeniteit van de waarderingsmatrix is de waarderingsmatrix opgezet voor alle infrastructurele locaties gezamenlijk. Per soort locatie worden de daarvoor relevante onderdelen van de matrix gebruikt voor de categorisering van de individuele locaties binnen de soort.

De uitwerking van de waarderingsmatrix van de risicogene factoren van Rijkswaterstaat is opgenomen in Deel V, bijlage 5.



12 De Basis Security Niveau's (BSN's)

12.1 Relevante securityrisico's

Security richt zich op het beheersen van risico's om verstoring van de bedrijfsvoering te voorkomen of beperken. Het is noodzakelijk om te weten welke inbreukrisico's als relevant moeten worden beschouwd. De security van gebouwen en locatie moet deze risico's kunnen beheersen. In principe hebben locaties te maken met dezelfde scope van securityrisico's. Daarom is vastgesteld welke risico's per locatie als relevant gelden. Deze risicosamenstelling is van invloed op het samen te stellen securityniveau als standaard.

Het overzicht van de relevantie per type locatie is opgenomen in Deel V, Bijlage 6.

Van alle denkbare risico's en strafbare feiten wordt bovenstaande selectie als meest waarschijnlijke en daarom relevante groep risico's beschouwd. De positie van het hoofdwegennet, hoofdvaarwegennet en het hoofdwatersysteem in Nederland betekent, dat rekening dient te worden gehouden met inbreukrisico's onder normale omstandigheden en voor de gehele maatschappij geldende dreigingen.

De zorgplicht van Rijkswaterstaat ten aanzien van de bescherming van de infrastructuur voor het hoofd(vaar)wegennet en het hoofdwatersysteem strekt zich normaliter uit tot datgene, wat vanuit de aard en omvang van de weg- en scheepvaartverkeer, de algemene bedrijfsrisico's, de specifieke aan het weg- en waterverkeer en watersystemen verbonden risico's en de maatschappelijke positie van Rijkswaterstaat verwacht zou mogen worden. Daartoe behoort niet de bescherming tegen uitzonderlijke vormen van criminaliteit, voor zover deze niet behoren tot een algemeen dreigingsbeeld t.a.v. de Nederlandse maatschappij.

Wel zal Rijkswaterstaat in geval van het optreden van uitzonderlijke vormen van criminaliteit binnen haar verantwoordelijkheidsdomein in samenwerking met de daarvoor primair aangewezen instanties en vanuit de rol van Rijkswaterstaat en de eigen mogelijkheden een bijdrage in de bestrijding ervan moeten kunnen leveren. Dit kenmerkt zich echter als incidenteel en tijdelijk, terwijl de inrichting van de security gericht is op permanente bescherming.

12.2 Relevante incidentscenario's

Een effectieve security vereist, dat de beheersingsmaatregelen en voorzieningen in staat moeten worden geacht de onderkende securityrisico's te kunnen voorkomen of minimaal in voldoende mate kunnen beheersen om de schade bij inbreuken te beperken.

Een effectieve security vereist tevens, dat de securitymaatregelen en -voorzieningen zodanig zijn ingericht en dat ze gericht zijn op de meest waarschijnlijke scenario's waarop inbreuken kunnen worden uitgevoerd.

De voor Rijkswaterstaat als relevant geachte incidentscenario's zijn opgenomen in Deel V, bijlage 7.

12.3 Daderprofielen

De aanwezigheid van personen op niet voor publiek toegankelijke terreinen van Rijkswaterstaat kan worden onderscheiden in:

- a. Aanwezigheid uit argeloosheid en/of onoplettendheid
Deze aanwezigheid veronderstelt geen bedoeling om de infrastructuur, noch de bedrijfsvoering aan te tasten. De aanwezigheid kan echter wel de bedrijfsvoering verstoren. Als zodanig zijn deze onbevoegd aanwezige personen wel als veroorzakers, doch niet als daders aan te merken.
- b. Opzettelijke, doch niet wederrechtelijke aanwezigheid
Deze aanwezigheid veronderstelt wel de opzet om op terrein aanwezig te zijn. De aanwezigheid in de niet voor publiek toegankelijke gebouwen en dito terreinen veronderstelt niet de opzet voor aantasting van het verkeerssysteem of bedrijfsvoering, hoewel de aanwezigheid die wel kan verstoren. Zij zijn als zodanig als veroorzakers, maar ook als daders aan te merken.
- c. Opzettelijke wederrechtelijke aanwezigheid.
Tot deze categorie worden personen gerekend, die om welke reden dan ook het niet voor publiek toegankelijke RWS-terrein of RWS-gebouw betreden om wederrechtelijke handelingen te verrichten. Zij kunnen uitsluitend als dader worden aangemerkt.

Op grond van de aard van de aanwezigheid van personen op de niet voor publiek bestemde terreinen en gebouwen of gebouwdelen moeten daders dus vooral worden gezocht in de personen, die het RWS-gebied gebruiken voor de uitvoering van hun wederrechtelijk handelen.

Om het daderprofiel te kunnen completeren, is eveneens van belang om onderscheid te maken in de mogelijke gerichtheid van daders.

Het overzicht van de voor Rijkswaterstaat relevant geachte dadergerichtheid is opgenomen in Deel V, bijlage 6.

De dadergerichtheid op de aantasting van de informatie- en communicatiesystemen door de systemen te manipuleren wordt voor de security van de infrastructurele locaties van Rijkswaterstaat buiten beschouwing gelaten om reden dat dit binnen de ICT-beveiliging is opgenomen.

T.a.v. de daders is voor de security van de infrastructurele locaties van Rijkswaterstaat geen onderscheid gemaakt tussen buitenstaanders en eigen (ex-)personeel van Rijkswaterstaat of contractpartners etc..

Tenslotte is het van belang om onderscheid te maken in het dadertype, waarvoor de security van de infrastructurele locaties bescherming dient te bieden.



Het overzicht van de voor Rijkswaterstaat relevant geachte dadertypen is opgenomen in Deel V, bijlage 8.

Permanente georganiseerde misdaad wordt niet geacht relevant te zijn voor de infrastructurele locaties van Rijkswaterstaat vanwege de beperktheid van de omvang van de criminele profits.

12.4 Opbouw van de Basis Security Niveau's (BSN)

12.4.1 Algemeen

Op basis van de gegevens uit de categorisering en risicovaststelling kunnen de gebouwen en locatie per zwaartecategorie worden voorzien van een basissecurityniveau. Dit basissecurityniveau "voorziet" in een generiek basispakket securitymaatregelen en –voorzieningen. Het dient als startpunt voor de uitwerking naar het definitieve pakket van securitymaatregelen en –voorzieningen per gebouw en locatie (het locatie specifieke pakket).

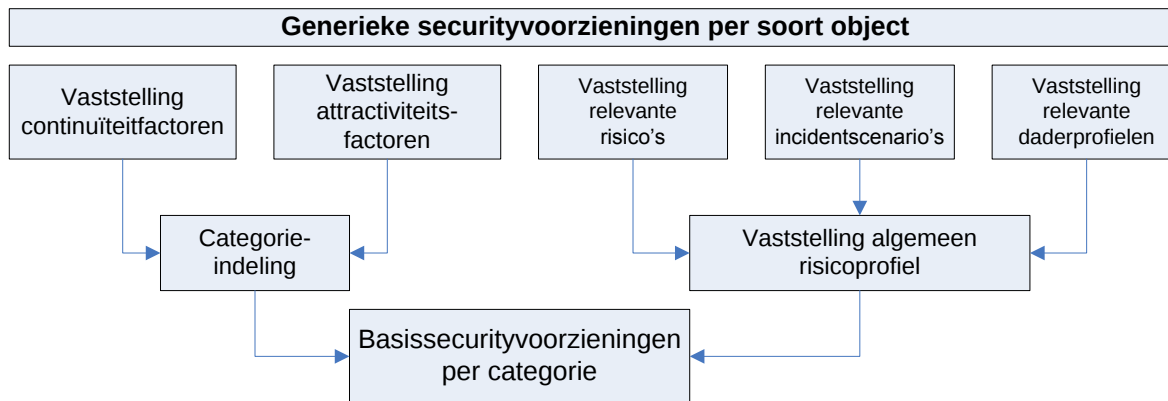
De methodiek beoogt de security van de type RWS-locaties structureel, effectief en efficiënt aan te pakken. Per type locatie is per categorie het voor die categorie geldende basisniveau samengesteld. Dit niveau dient als minimaal noodzakelijk, maar wel voldoende te worden gekenmerkt.

Voor alle Basis Security Niveaus geldt, dat de opbouw en inrichting vanuit dezelfde conceptuele benadering en maximale standaardisatie is samengesteld. De opbouwvolgorde van de BSN's is altijd: bouwkundige voorzieningen (weren), detectie (signaleren), inzet camera's (observeren en verifiëren).

Alle basisniveaus zijn voorzien van bouwkundige voorzieningen. De zwaardere categorieën in meer of mindere mate van de technische voorzieningen (detectie, toegangsbeheersing, camera's). Voor zover toepasbaar zijn daarbij de minimumgrenzen aangegeven conform ENV 1627: 2011.

Indien er detectie is toegepast, dan is er ook alarmopvolging. Hierbij is het minimum alarmtransmissieniveau aangegeven conform NEN EN 50136. Bij alle voorzieningen gelden tevens de daarop betrekking hebbende procedures. Een Basis Security Niveau is te beschouwen als een gestandaardiseerd voorontwerp.

De inrichting van de Basis Security Niveaus in schema:



Figuur 6: inrichting Basis Security Niveaus

12.4.2 Indeling in Basis Security Niveaus (BSN)

Op basis van de beide bovenstaande inventarisaties kunnen de gebouwen, terreinen en locatie in zwaarte worden ingedeeld per soort gebouw/locatie. Deze zwaarte geeft het belang van het gebouw/locatie aan voor de continuïteit van Rijkswaterstaat en/of haar bedrijfsprocessen. De categorisering is daardoor een continuïteitsrisico-indeling per soort gebouw/locatie.

Rijkswaterstaat heeft ervoor gekozen om type locaties in maximaal drie categorieën in te delen. Daarbij worden de volgende uitgangspunten gehanteerd:

Basis Security Niveau 0	Locaties die voor het totaal van de geïnventariseerde risicogene factoren niet boven het totaal van de gemiddelde scores per onderdeel van de waarderingsmatrix van het type locatie uitkomen.
Basis Security Niveau 1	Locaties die voor het totaal van de geïnventariseerde risicogene factoren boven het totaal van de gemiddelde scores per onderdeel van de waarderingsmatrix van de soort locatie uitkomen, doch niet op of boven het totaal van de hoogste scores per onderdeel van de waarderingsmatrix van het type locatie.
Basis Security Niveau 2	Locaties die voor het totaal van de geïnventariseerde risicogene factoren op of boven het totaal van de hoogste scores per onderdeel van de waarderingsmatrix van het type locatie uitkomen.

Bij die soorten locaties, waar deze indeling tot onwerkbaar indelingen zou gaan leiden, is gekozen voor een indeling in 2 Basis Security niveau's volgens de onderstaande criteria.

Basis Security Niveau 0	Locaties die voor het totaal van de geïnventariseerde risicogene factoren niet boven het gemiddelde van het totaal van de gemiddelde scores per onderdeel en van het totaal van de hoogste scores per onderdeel van de waarderingsmatrix van het type locatie uitkomen.
Basis Security Niveau 1	Locaties die voor het totaal van de geïnventariseerde risicogene factoren boven het gemiddelde van het totaal van de gemiddelde scores per onderdeel en van het totaal van de hoogste scores per onderdeel van de waarderingsmatrix van het type locatie uitkomen.



Zie voor een uitgewerkt voorbeeld Deel V, bijlage 9.

De maatregelen en voorzieningen zijn in elk Basis Security Niveau afgestemd op de met dat niveau corresponderende zorgplicht. Hoe hoger het securityniveau, hoe zwaarder en uitgebreider de maatregelen en voorzieningen om aan de zorgplicht te voldoen.

12.5 Programma Regie op Industriële Automatisering (PRIA)

Parallel aan de ontwikkeling van dit handboek Security heeft het Project Industriële Automatisering (PRIA) een set beveiligingseisen van IA-gerelateerde RWS-objecten uitgewerkt.

Ten behoeve van de integratie met het Project industriële Automatisering geldt voor alle objecten die deel uitmaken van de scope van PRIA een set met normen voor de fysieke beveiliging van de IA-gerelateerde ruimten. Voor deze objecten gelden de eisen voor de fysieke beveiliging volgens de handboekmethodiek én de Cybersecurity Richtlijn Objecten RWS.

In deel I is, waar mogelijk de samenhang aangebracht met de uitwerkingen van de aanpak van PRIA.

In deel III is de handleiding ter realisatie van het locatiespecifieke pakket aan fysieke securitymaatregelen en –voorzieningen aangevuld met de cybersecurity uitwerking. Hierdoor ontstaat een overzicht van de resultaten van beide uitwerkingen en kan op basis van de aangegeven criteria het locatiespecifieke geïntegreerde pakket securitymaatregelen en –voorzieningen worden vastgesteld ten behoeve van de specificaties voor nieuwbouw, of aanpassingen bij verbouw of bestaande objecten.

12.6 Hoe wordt de risicobeheersing bereikt?

Met de securityvoorzieningen van de Basis Security Niveaus en de organisatorische en procedurele securitymaatregelen introduceert Rijkswaterstaat een volledige, risico gebaseerde, effectieve en maatwerkgerichte invulling van de security van al haar locaties tegen de relevant geacht securityrisico's.

Om daartoe te kunnen komen, zijn de diverse bouwkundige en elektrotechnische voorzieningen en organisatorische en procedurele securitymaatregelen op toepassing bij Rijkswaterstaat beoordeeld en geselecteerd. Daarnaast zijn zowel de voor Rijkswaterstaat als relevant te achten risico's vastgesteld alsmede de wijze waarop deze risico's zich kunnen manifesteren (incidentscenario's) en de achtergronden van de plegers van inbreuken (daderprofielen). Voor een goed begrip en toepassing van de methodiek is het noodzakelijk om inzicht te hebben in het nut en te verwachten effect van de inzet van de securityvoorzieningen en –maatregelen. Met andere woorden: welke maatregelen zijn bedoeld en geschikt voor de beheersing van welke risico's en incidentscenario's?

De inzet van de securitymaatregelen en –voorzieningen voor de beheersing van de relevant geachte securityrisico's heeft echter ook een effect op de niet relevant geachte securityrisico's. De preventie van de voorzieningen is immers algemeen en zal daarom ook drempels opwerpen voor het plegen van niet verkeer of scheepvaart gerelateerde criminaliteit. Daarnaast zullen de pro-actieve en reactieve maatregelen ook hun werking niet missen bij constatering van niet voor de basissecurity relevant geachte incidenten. Met andere woorden: de basissecurity bij Rijkswaterstaat richt zich op en is ingericht voor de beheersing van de relevant geachte risico's, scenario's en daderprofielen, maar bereikt qua effect een breder spectrum.

12.7 BSN als onderdeel totaal securitypakket

De centrale opzet en opbouw van de securitymaatregelen en –voorzieningen bij Rijkswaterstaat biedt de mogelijkheid tot een pakket zonder hiaten, doublures en tegenstrijdigheden. Het schept bovendien het kader om juist de nadruk te leggen op de zowel goedkope als de meest effectieve securityvoorzieningen en deze uit te nutten.

Daartoe wordt bij de inrichting van de securityvoorzieningen bij Rijkswaterstaat uitgegaan van maximale standaardisatie en waar mogelijk multifunctioneel gebruik van voorzieningen.

Technische securityvoorzieningen (de BSN's) ontberen de gewenste effectiviteit indien niet gelijktijdig de kernvaardigheden voor het gebruik van de voorzieningen (bedieningsinstructies) zijn gerealiseerd. Daarom wordt bij Rijkswaterstaat als randvoorwaarde gehanteerd, dat de bij de securityvoorziening behorende kernvaardigheden minimaal gelijktijdig met de technische voorziening dienen te zijn geïmplementeerd. Indien deze kernvaardigheden niet kunnen worden gegarandeerd bij derden ter uitvoering, dan zal de voorziening in eigen beheer dienen te worden gerealiseerd (bijvoorbeeld cameraverificatie).

Het totale securitypakket wordt gecombineerd met de algemene en specifieke securitygedragsregels, -procedures en –protocollen.

0-0-0-0-0

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