



Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

RWS BEDRIJFSINFORMATIE

Handboek Security

Managementsamenvatting

Datum	29 juni 2015
Status	definitief



Colofon

Metagegevens

Proces:	Aanleg & Onderhoud
Proceseigenaar:	Jean-Luc Beguin
Netwerk:	Droog, Nat
Hoofdkennisveld:	Veiligheid en Crisis
Kennisveld:	Security
Soort document:	Informatie (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:	21-06-2017
Vastgesteld door:	Proceseigenaar
Van kracht vanaf:	21-06-2017
Overgangsregeling:	
Beveiliging:	RWS bedrijfsinformatie
Beheerder:	GPO, afdeling Advies Technisch Management, Dirk-Jan Molenaar
Informatie:	Kaderadviseurs GPO/PPO
Verbetervoorstellen:	Dirk-Jan Molenaar
Toepassingsgebied:	Projecten voor aanleg en onderhoud
Versienummer:	3.0.0
Houdbaar tot:	December 2017
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 Coördineren, initiëren, uitvoeren, communiceren, monitoren
benodigde kennis	Basiscursus integrale veiligheid in projecten

Hoofdproces

Aanleg & Onderhoud

Relatie met andere RWS standaarden

Wettelijk	Zie deel IV, hoofdstuk 2, Van kracht zijnde voorschriften en normen voor de securityvoorzieningen
Bovenliggend	Kader Veiligheidsmanagement RWS, 14 september 2011, WVL
Nevenliggend	Kader Integrale Veiligheid in Projecten 3.0

Toepassingsbereik

- Intern RWS, bij:
- Aanlegprojecten, van contractvoorbereiding tot oplevering;
 - Onderhoudsprojecten, van contractvoorbereiding tot einde contract.

- Afwijken van kader** Conform de regels van de WWA0 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.



Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

Inleiding

Beveiliging tegen schade en beheersing van veiligheidsrisico's komt niet vanzelf, daarvoor zijn acties en hulpmiddelen nodig. Er zijn vele manieren om de beveiliging binnen een organisatie in te richten. Vele daarvan blijken na verloop van tijd toch niet aan de verwachtingen te voldoen. Vaak is daarvan de oorzaak een te beperkte of te eenzijdige opzet van de beveiliging.

Het securityhandboek van RWS is ontwikkeld om een duurzame en werkbare security te realiseren. Het begrip security is daartoe in het handboek afgebakend ter onderscheid met safety.

Ook bij de realisatie van security 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 voor geheel RWS geldende securitybenadering en gestandaardiseerde security-inrichting worden alleen die beveiligingsmaatregelen en -voorzieningen aangeschaft, aangebracht en geïmplementeerd die de gewenste beheersing in voldoende mate kunnen realiseren. Daardoor worden onnodig dure, ineffectieve en inefficiënte securitymaatregelen en -voorzieningen voorkomen.

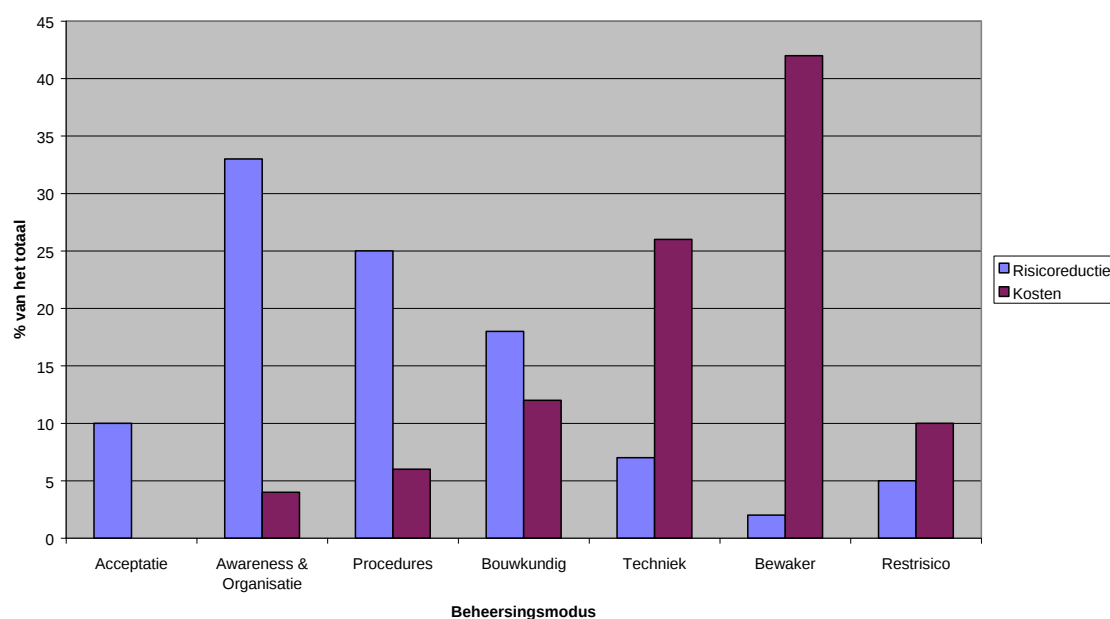
De methodiek om de verschillende risico's adequaat te beheersen is het fasegewijs toewerken naar een steeds verdergaande reductie van het risicovolume, is als volgt weer te geven:

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		

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.



Risicoreductie en beheersingskosten



Waaruit is het securityhandboek RWS opgebouwd?

Het handboek is bedoeld voor diegenen, die bij op enigerlei wijze betrokken of verantwoordelijk zijn voor de realisatie en instandhouding van security binnen RWS.

De gehanteerde methodiek is risk-based en concretiseert het framework van de randvoorwaarden en kaders, de scope, de vormgeving via een procesmatige inrichting naar de aard en inzet van de middelen voor de inrichting van een effectieve en efficiënte security per object.

De risico-objecten bij RWS verschillen per soort onderling van elkaar. Binnen dezelfde soort zijn ze evenmin gelijk. Een toekomstvast security van deze objecten vereist, dat de security aansluit op het risicoprofiel van het object. Dat risicoprofiel wordt gevormd door de zogenaamde attractiviteit voor inbreuken (kans) en het effect van die inbreuken. Een maatwerkinrichting is daarom van groot belang voor de effectiviteit van de beveiliging.

Daartoe zijn generieke (basis) securitymaatregelen en securityvoorzieningen uitgewerkt.

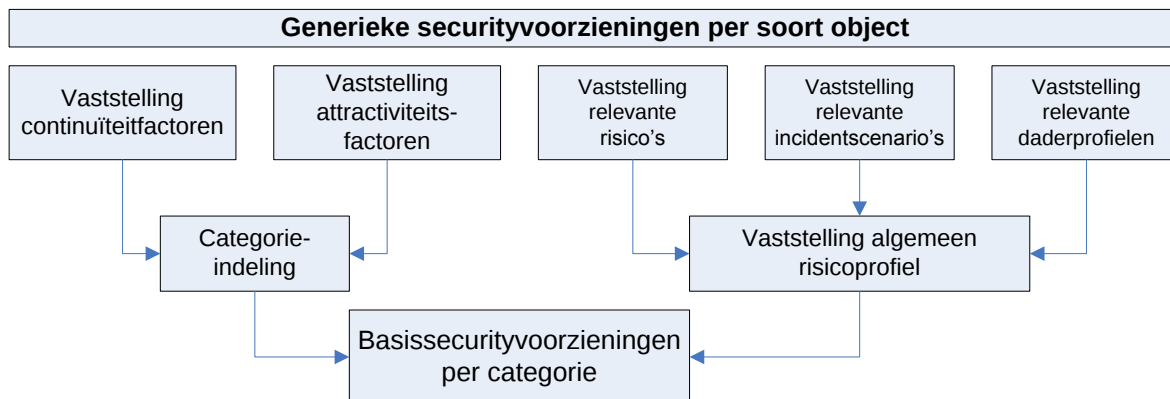
De basis securitymaatregelen bestaan uit gedragsregels, beveiligingsprocedures en protocollen alsmede kaderstellende procedures voor de uitbesteding van beveiligingstaken aan derden.

Voor de generieke (bouwkundige en elektronische) securityvoorzieningen is een methodiek ontwikkeld om elk risico-object te kunnen voorzien van de voor dat specifieke object noodzakelijke maatwerk aan securityvoorzieningen. Deze methodiek heeft alle aspecten, die het risicoprofiel (mede) bepalen, ondergebracht in een tweetal hoofdgroepen, zijnde factoren die het continuïteitsbelang van het object

vertegenwoordigen (continuïteitsfactoren) en de factoren die de attractiviteitswaarde (attractiviteitsfactoren) bepalen.

Op basis van de aan elk soort object te koppelen factoren en de daarbij behorende waarderingen worden per soort object de zwaartecategorieën vastgesteld, de zogeheten objectcategorisering. Deze categoriseringsmethodiek is wetenschappelijk getoetst. Per objectcategorie en per zwaarteniveau is een basis securitypakket voorzieningen ontworpen, de zogenoemde Basis Security Niveaus. Deze niveaus zijn de invullingen van de zorgplicht van RWS t.a.v. de objecten. Elk BSN-niveau is toegesneden op de bij dat niveau behorend risicoprofiel, continuïteitsbelangen en locatiekarakteristieken en Cybersecurityspecificaties voor de fysieke beveiliging van de IA-gerelateerde ruimten. De samenstelling van de securityvoorzieningen voor dat niveau zijn daarom niet anders te beschouwen als de noodzakelijke voorzieningen om het object als goed huisvader te beschermen. Per soort object is t. b. v. de opzet en inrichting van de Basis Security Niveaus uitgegaan van de voor die soort relevant geachte securityrisico's en incidentscenario's en dadertypen.

In schema:



De realisatie

Het doel van de beveiliging is het voorkomen van onveilige situaties en/of ongewenste handelingen t.a.v. objecten en adequaat te reageren indien zich toch incidenten voordoen. De invoering van de generieke securitymaatregelen en -voorzieningen is daartoe niet voldoende. Generieke maatregelen en -voorzieningen kunnen immers niet zijn afgestemd op de locatiespecifieke omstandigheden. Voor een effectieve security is maatwerk vereist. Een efficiënte security daarentegen vereist maximale standaardisatie waar mogelijk.

Om dat te bereiken hanteert het handboek een systematische en transparante werkwijze om per object tot een afgewogen, uitgekristalliseerde, maar toekomstvast maatwerkinrichting te kunnen komen. Deze werkwijze is per soort object in een voor dat type object uitgewerkte handleiding vastgelegd.

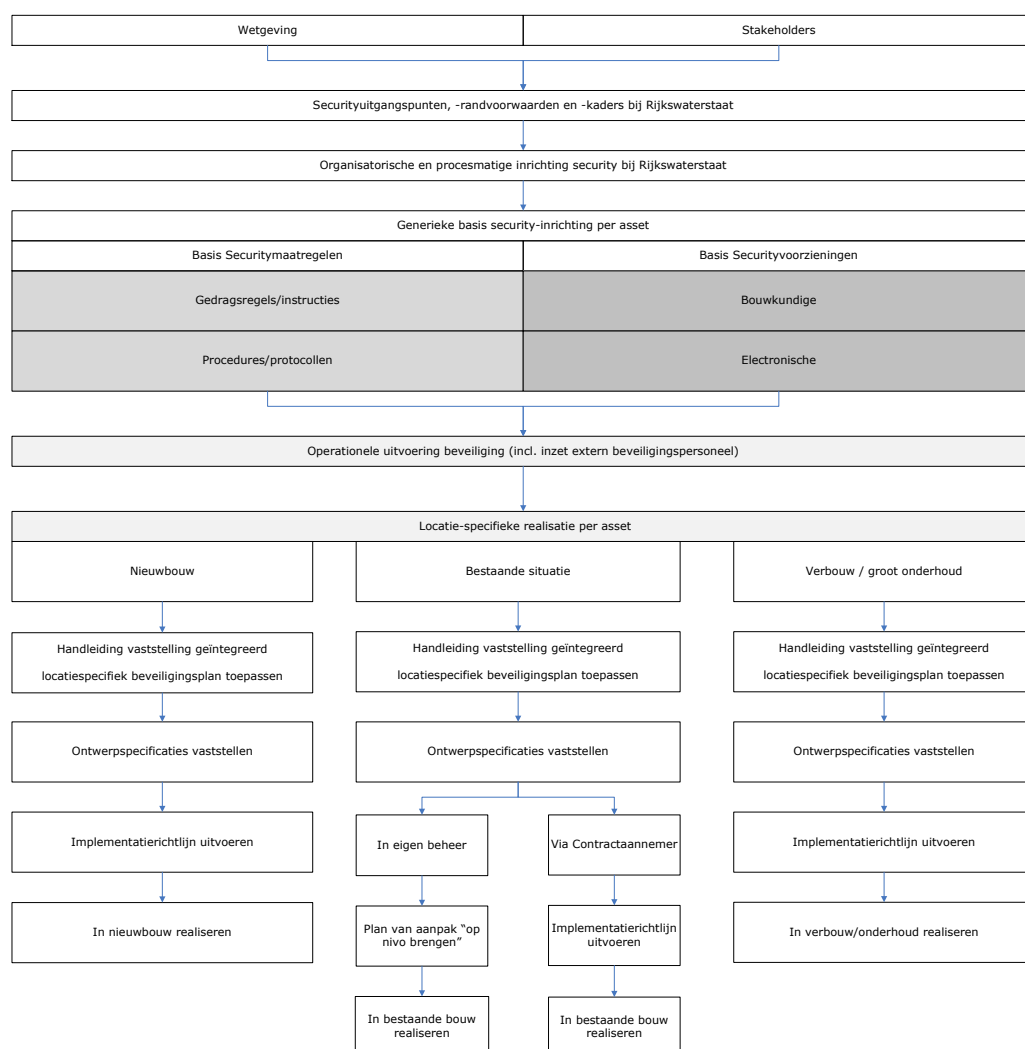


Die handleiding bevat het stelsel van regels en voorschriften om tijdens het ontwerpproces de analyses t.a.v. gedragsregels, procedures, protocollen, omgevingsfactoren, risico's, incidentscenario's en daderprofielen uit te voeren en de resultaten te vertalen in de voor de locatie benodigde beveiligingsmaatregelen en -voorzieningen.

De handleiding bevat bovendien de stappen naar de gehele of gedeeltelijke inpassing van de op de locatie bestaande securitymaatregelen en -voorzieningen.

De integratie met het Project Industriële automatisering is in het handboek vormgegeven door de uit de verschillende weerstandsniveau's voortvloeiende eisen voor de cyber gerelateerde ruimten op te nemen na de omschrijvingen van de Basis Security Niveau's voor de -combinatie van- objecttypen. In de handleidingen worden de security maatregelen en voorzieningen aangevuld met de uitwerkingen uit cyber. Hierdoor ontstaat één overzicht voor een geïntegreerd pakket voor nieuwbouw, verbouw en bestaande objecten.

Samengevat



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