

Handboek Security

Nummer: 1364

Algemene informatie

Soort:	Kader
Status:	In beheer
Ingangsdatum:	21-06-2017
Versievervaldatum:	31-12-2023
Vertrouwelijkheidsniveau:	RWS Informatie
Inhoudelijk beheer:	Bosse Loosveld
Verantwoordelijke afdeling:	Afd. Control en Informatie

Documenten

Naam	Versie
Handboek Security RWS Deel I versie 3.2	
Handboek Security RWS Deel II versie 3.2	
Handboek Security RWS Deel III versie 3.2	
Handboek Security RWS Deel IV versie 3.2	
Handboek Security RWS Deel V versie 3.2	
Handboek Security RWS Deel VI versie 3.2	
handboek Toegang VC 2.0 25 jan 2016	
Managementsamenvatting Handboek security	

Beschrijving

Labels

Objecttype Tunnel

Het kader (deel I) voorziet in uniformering van de fysieke beveiliging van objecten van Rijkswaterstaat. Het gaat hierbij onder andere om security procedures en security voorzieningen. De security voorzieningen worden vastgelegd in een locatiebeveiligingsplan dat met behulp van het handboek kan worden opgesteld. Dit geldt zowel voor nieuwe situaties als bij renovaties. De procedures voor toegang van droge verkeerscentrales staan in een apart document.

Het kader Handboek Security geeft aan hoe projectteams en beheerders op een uniforme wijze een locatiebeveiligingsplan dienen op te stellen. In locatiebeveiligingsplannen staat hoe de objecten dienen te worden beveiligd. Hierin staan onder andere de organisatorische en procedurele RWS-securitymaatregelen, de fysieke security voorzieningen voor deze RWS-locatie en de eisen vanuit het Cybersecurity weerstandsniveau. Door een gestandaardiseerde aanpak worden onnodig dure en inefficiënte securitymaatregelen en -voorzieningen voorkomen. Er zijn sjablonen voor locatiebeveiligingsplannen beschikbaar die bij de beheerder van het handboek security kunnen worden opgevraagd.

In deze grafiek staan de methodes om risico's te beheersen, op volgorde van efficiëntie (risicoreductie / euro). Bij toepassing is het wenselijk deze volgorde aan te houden.

Met het verschijnen van het Handboek Security zijn eerdere modellen en methodieken komen te vervallen (zoals het Corporate BeveiligingsModel (CBM), de Haagse Methode en het normenkader beveiliging Rijksoverheid (NKBR). Voor het Handboek Security zijn de beste onderdelen van de eerdere modellen gebruikt en gecombineerd met inzichten van CEPTED (zie werkveld sociale veiligheid). In de nieuwe versie van het handboek zijn alle ervaringen vanuit het programma IMPAKT verwerkt.

Vanuit Cybersecurity zijn ook eisen geformuleerd voor de fysieke security van objecten. Het gaat hier om de IA- (industriële automatisering) gerelateerde ruimten. Deze eisen zijn in overeenstemming gebracht met het handboek.

De doelgroep van het handboek is iedereen die betrokken of verantwoordelijk is voor de realisatie en instandhouding van security binnen RWS. In de praktijk betekent dit dat verschillende organisatieonderdelen met het handboek security te maken hebben: GPO en PPO bij de aanleg- en onderhoudsprojecten, objectbeheerders in de regio, CD, VWM.

In de praktijk zullen de locatiebeveiligingsplannen vaak worden opgesteld door de objectbeheerders, die verantwoordelijk zijn dat hun objecten blijven functioneren en presteren. De projectteams van GPO en PPO dienen vervolgens uit de locatiebeveiligingsplannen contracteisen te destilleren en in hun contracten op te nemen.

Het kader was voorheen geclassificeerd als "RWS bedrijfsinformatie". De classificering is herzien en het kader is nu "RWS ongeclassificeerd" is. Het is dus geen probleem meer als het document buiten RWS terecht komt. Locatiebeveiligingsplannen bevatten wel vertrouwelijke informatie en zijn dus minimaal geclassificeerd als "RWS bedrijfsinformatie". Deze mogen dus niet buiten RWS terecht komen.

Het handboek security 3.2 is direct van kracht en is van toepassing op alle projecten waarvan de aanbesteding nog plaats moet vinden. Projecten die al zijn aanbesteed, kunnen gewoon de oude versie blijven hanteren. Het handboek security 3.2 onderscheidt zich ten opzichte van versie 3.1 door de toevoeging van twee typen objecten, waarvoor nu ook een locatiebeveiligingsplan kan worden opgesteld. Het gaat om:

- Veerhavens;
- Centrale VICNET ruimtes.

Voor vragen en nadere informatie kunt u contact opnemen met dirkjan.molenaar@rws.nl.

Bedoeling

Kennisdeling: Voorkomen of beperken van kennisverlies.

Toepassingsinformatie

Rol	Netwerken	Fase	Hoofdkennisveld
IV manager Technisch Manager	Hoofdvaarwegennet Hoofdwatersysteem Hoofdwegennet	Onderhoud Planuitwerking Realisatie	Veiligheid en Crisis

Wordt gebruikt in

Aanleg en Onderhoud	> Ontwerp, Effecten en Techniek	> Veiligheid	> Actualiseren integraal veiligheidsplan planuitwerkingsfase
Aanleg en Onderhoud	> Ontwerp, Effecten en Techniek	> Veiligheid	> Actualiseren integraal veiligheidsplan realisatiefase
Aanleg en Onderhoud	> Ontwerp, Effecten en Techniek	> Systeemontwikkeling en specificeren	> Baseline Projectbeslissing: Systeem ontwikkelen en actualiseren systeemspecificatie
Aanleg en Onderhoud	> Ontwerp, Effecten en Techniek	> Systeemontwikkeling en specificeren	> Baseline Contractvoorbereiding: Systeem ontwikkelen en actualiseren systeemspecificatie