



Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

Instructie

Classificeren en omgaan met vertrouwelijke informatie

Uitgegeven door	RWS
Informatie	Hellen Havinga en Dirkjan Joor
Auteur	Hellen Havinga en Dirkjan Joor
Datum	11 September 2018
Vertrouwelijkheid	RWS INFORMATIE
Status	Definitief
Versie	2.4

Revisiegegevens

Wijzigingen t.o.v. versie 1.3

Onderstaande tabellen geven inzicht in wat in het document is veranderd ten opzichte van vorige versies.

Wijzigingen in versie 2.4 ten opzichte van versie 1.3 (november 2014).

Onderdeel	Wijziging
Beslisboom	Beslisboom bijgesteld ter verduidelijking: Classificeren is alleen nodig wanneer RWS eigenaar is.
Overal	Term wijziging van Wet privacy: Van Wet bescherming persoonsgegevens (Wbp) naar Algemene Verordening Gegevensbescherming (AVG) Nieuwe naamgeving classificaties doorgevoerd RWS-O (letter O van Ongeclassificeerd) gewijzigd in RWS-0 (nul).
Stap 3	Schrijfwijze aangepast aan nieuwe naamgeving. Alles in Hoofdletters Documentgegevens aangepast. Informatieclassificatie (RWS-II, etc.) verwijderd uit gegevens.
Bijlage	Blackberry vervangen door RWS Smartphone
Toepassingsgebied classificeren	Binnenkomende documenten hoeven niet geclassificeerd te worden. Dit was bij versie 2.0 t.o.v. versie 1.3 wel zo geformuleerd.
Alle onderdelen	Naar aanleiding van het besluit van de Stuurgroep BWR om het classificeren van informatie aan te passen zijn wijzigingen doorgevoerd ten aanzien markeringsterminologie classificatie-beslisboom, beleid t.a.v. het markeren van documenten en het omgaan met vertrouwelijke informatie. Link gemaakt naar gedragsregeling voor de digitale werkomgeving en metadata in DocGen.

Inhoud

Revisiegegevens—2

Wijzigingen t.o.v. versie 1.3—2

Introductie—4

Stap 1) Vaststellen vertrouwelijkheid en informatieklass—6

Stap 2) Vaststellen herzieningsdatum vertrouwelijkheid—10

Stap 3) Het aanbrengen van vertrouwelijkheidskenmerk—11

Stap 4) Verwerken volgens vastgestelde informatieklass—13

Stap 5) Vertrouwelijkheid en informatieklass wijzigen—14

Bijlage 1 Voorbeelden van geclassificeerd informatie en persoonsgegevens.—15

Bijlage 2 Beslisboom—16

Bijlage 3 Omgaan met gevoelige informatie—18

Bijlage 4 Termijnbepaling vertrouwelijkheid—24

Bijlage 5 Begrippenlijst—25

Introductie

Doelstelling van het classificeren van informatie is dat op basis van een risicoafweging passende beveiligingsmaatregelen worden toegepast om ervoor te zorgen dat ongeautoriseerde personen geen toegang kunnen krijgen tot vertrouwelijke informatie. De informatie over het omgaan met vertrouwelijke, gerubriceerde of privacygevoelige gegevens is opgenomen in de bijlage van dit document en in de gedragsregeling voor de digitale werkomgeving.

Volgens de BIR behoort informatie te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie. Medewerkers van Rijkswaterstaat dienen daarom vertrouwelijke informatie te voorzien van een markering met een passend classificeringsniveau en zodanig met de vertrouwelijke informatie om te gaan dat de vertrouwelijkheid ervan is gewaarborgd.

De opsteller van een document of een communicatiebericht¹ maakt een inschatting van de mogelijke schade die kan worden veroorzaakt als de informatie in verkeerde handen komt en wordt misbruikt. De opsteller beoordeelt in welke mate er maatschappelijke schade, financiële schade of vertrouwensverlies kan ontstaan voor RWS en in welke mate er (ernstige) nadelige gevolgen kunnen optreden voor personen.

Rijkswaterstaat biedt IT-voorzieningen voor kantoorautomatisering waarmee informatie op een beveiligde wijze kan worden verwerkt. De menselijke factoren speelt echter een belangrijke factor in het proces van informatieverwerking. Dit document beschrijft daarom hoe medewerkers een passend classificeringsniveau kunnen bepalen, documenten van een markering kunnen voorzien en hoe zij zorgvuldig om moeten gaan met (vertrouwelijke) informatie.

Vertrouwelijkheid wordt vanuit vier invalshoeken benaderd:

1. Privacy: Algemene Verordening Gegevensbescherming (AVG)

Vanuit de wet- en regelgeving dienen (gevoelige) persoonsgegevens zodanig te worden beschermd dat de privacy is gewaarborgd en dat er geen (ernstige) nadelige gevolgen ontstaan voor personen.

2. VIR-BI 2012

Het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie 2012 (VIR-BI 2012) beschrijft hoe vertrouwelijke informatie op basis van risicoafweging dient te worden geclassificeerd (gerubriceerd). De hoogste rubricering hierin is Staatsgeheim Zeer Geheim (STG ZG). De laagste rubricering is DEPARTEMENTAAL VERTROUWELIJK (Dep. V.). Het omgaan met de hoogste vertrouwelijkheidsklassen (Staatsgeheim Confidentieel of hoger) wordt in dit document niet behandeld, omdat dit voor de meeste RWS'ers niet of nagenoeg niet voorkomt.

¹ Zie "de gedragsregeling voor de digitale werkomgeving", versie 1.0, 23 juni 2016, ministerie van BZK

3. BIR

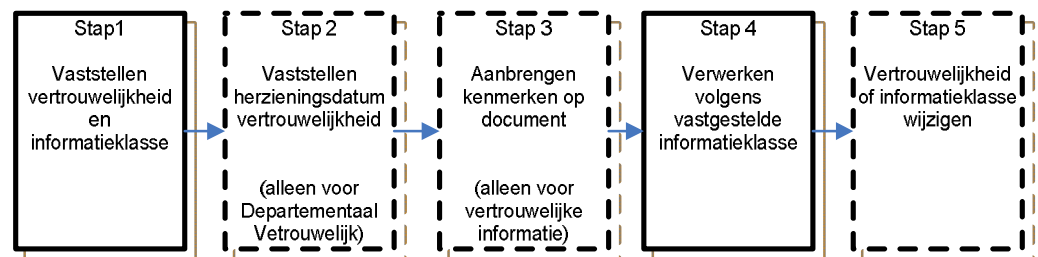
De Baseline Informatiebeveiliging Rijk (BIR) is een beleidsrichtlijn die aangeeft dat informatie dient te worden geclassificeerd en gelabeld, zodat deze een geschikt niveau van bescherming krijgt.

4. Gedragscode 'Bewust Integer 2012 – hoofdstuk 3)

Alle vaste RWS medewerkers dienen bij aanvang van hun aanstelling een 'eed of belofte' af te leggen waarmee zij zich verplichten tot geheimhouding en het zorgvuldig omgaan met vertrouwelijke informatie.

Om de vertrouwelijkheid van de informatie in een document of communicatiebericht (zoals e-mail) vast te stellen dient de opsteller de classificatiewijzer(s) te doorlopen. Het kan voorkomen dat een document vertrouwelijke informatie voor Rijkswaterstaat bevat en tegelijk ook persoonsgevoelige informatie. In dat geval heeft het document tegelijkertijd twee classificaties, één voor informatie en één voor persoonsgegevens.

De volgende stappen moeten worden doorlopen bij het bepalen van de vertrouwelijkheid van informatie in documenten en het verwerken ervan:



Figuur 1: Proces van classificeren en markeren en tenslotte wijzigen van classificatie

Stap 1) vaststellen vertrouwelijkheid en informatieklasse van de informatie

Stap 2) vaststellen herzieningsdatum vertrouwelijkheid (alleen bij DEPARTEMENTAAL VERTROUWELIJK)

Stap 3) aanbrengen van een passende markering op het document.

Stap 4) vaststellen hoe de informatie moet worden verwerkt

De volgende stap komt later in het proces aan de orde (als het DEPARTEMENTAAL VERTROUWELIJK informatie betreft):

Stap 5) Het beoordelen van het classificatieniveau en eventueel wijzigen van de informatieklasse.

Deze instructie beschrijft de processtappen en biedt praktische handvaten om op een passende wijze zorgvuldig om te gaan met vertrouwelijke informatie.

In bijlage 2 is een beslisboom opgenomen voor het classificeren van informatie met een overzicht van alle vragen die moeten worden gesteld om een juiste classificatie te bepalen. Enkele voorbeelden van geclassificeerde informatie en persoonsgegevens zijn onder de classificatiewijzers opgesomd. De voorbeelden zijn niet uitputtend. Zie bijlage 1 voor meer voorbeelden. Bijlage 5 bevat een begrippenlijst.

Stap 1) Vaststellen vertrouwelijkheid en informatieklasse

Bij het vaststellen van een passend vertrouwelijkheidsniveau van informatie wordt op basis van een risicoafweging bepaald in welke mate de informatie schade kan toebrengen als het in verkeerde handen terecht komt. Het kan gaan om maatschappelijke schade, financiële schade, vertrouwensverlies of schending van privacy. Bij elk niveau van vertrouwelijkheid hoort een informatieklasse. De informatieklasse bepaalt hoe je met de informatie om moet gaan. Hierbij een overzicht van de relatie tussen classificatieniveaus en informatieklassen.

Tabel 1: Classificatieniveaus en bijbehorende informatieklasse.

Classificatieniveaus van informatie	Informatieklasse
DEPARTEMENTAAL VERTROUWELIJK	RWS-II
RWS BEDRIJFSVERTROUWELIJK	RWS-I
RWS INFORMATIE	RWS-0
Classificatieniveaus van persoonsgegevens	Informatieklasse
PERSOONSgegevens ZEER VERTROUWELIJK	RWS-II
PERSOONSVERTROUWELIJK	RWS-I

Vaststellen of en hoe informatie dient te worden geclassificeerd:

Met de informatiewijzer wordt vastgesteld of en hoe informatie dient te worden geclassificeerd. Eerst wordt vastgesteld of de informatie moet worden geclassificeerd door na te gaan of RWS de eigenaar is van de informatie. Uitgangspunt is dat alleen informatie waarvan RWS de eigenaar is wordt geclassificeerd. Binnenkomende documenten waar RWS alleen de bewaarder van is, hoeven niet te worden geclassificeerd². Wel moet hier zorgvuldig mee om worden gegaan.

Voorbeelden van informatie waar RWS de eigenaar van is zijn:

- RWS bestuur stukken of RWS projectplannen
- RWS personele administratie

Voorbeelden van informatie van buiten waar RWS de bewaarder van is zijn:

- ontvangen e-mails van externe partijen
- ontvangen offertes van marktpartijen

Voorbeelden waar RWS niet de eigenaar of beheerder van is zijn:

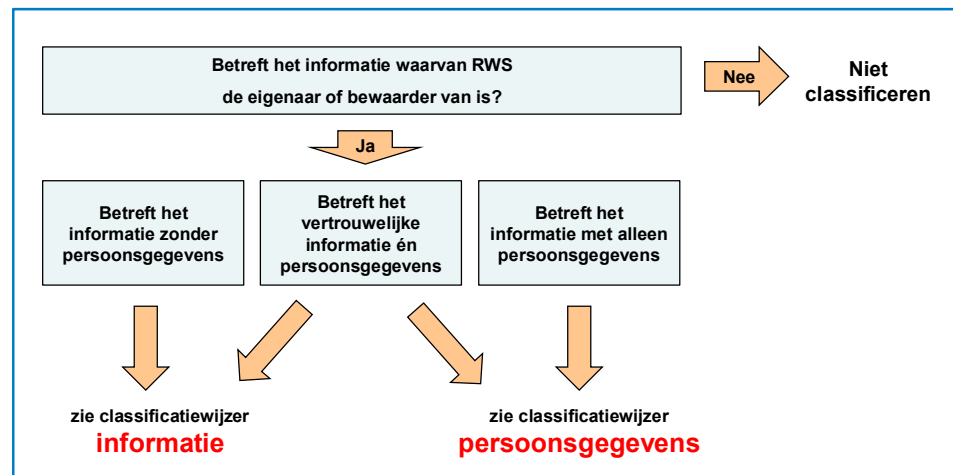
- publieke informatie op Internet
- persoonsgegevens ten behoeve van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden (zie AVG)

Een uitzondering van informatie waar RWS wel de eigenaar van is maar niet hoeft te worden geclassificeerd is "publieke informatie" waarbij officieel door RWS is vastgesteld is dat de informatie bestemd is voor het openbare publiek.

² Externe partijen dienen hun eigen documenten te zien van een voor hen geldende markering. Over de naamgeving en verhouding van deze markeringen tot die van RWS kunnen nadere afspraken worden gemaakt. Het is wenselijk om zoveel mogelijk te uniformeren.

Een hulpmiddel bij het classificeren is de classificatiewijzer in figuur 1. De eerste stap in de classificatiewijzer is vast om onderscheid te maken tussen:

1. informatie zonder persoonsgegevens
2. vertrouwelijke informatie én persoonsgegevens
3. informatie met alleen persoonsgegevens

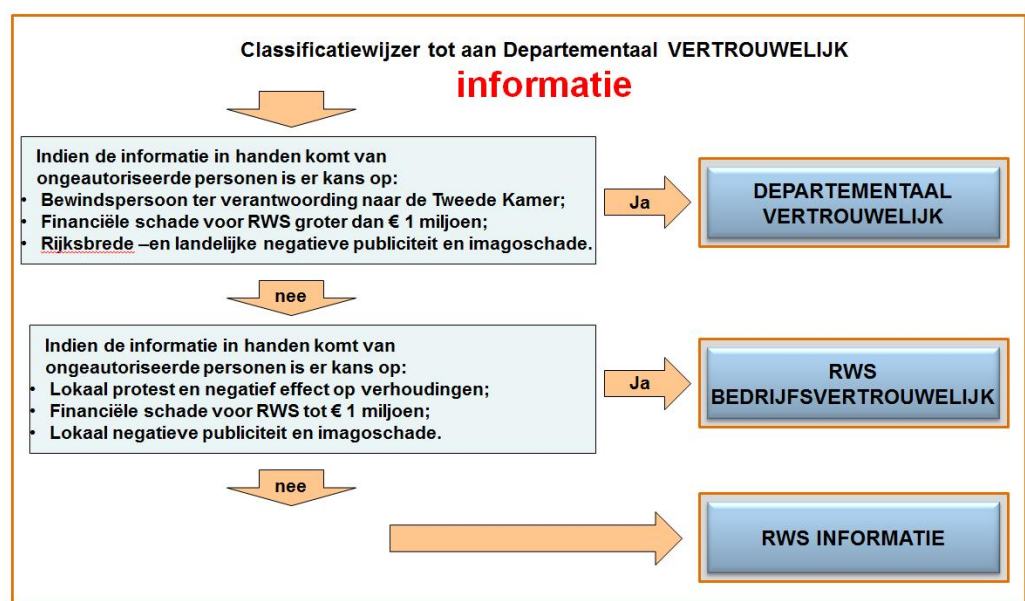


Figuur 1: Classificatiewijzer

Op basis van bovenstaande vaststelling wordt bepaald welke volgende classificatiewijzer(s) dienst te worden toegepast:

1. Classificatiewijzer informatie
2. Classificatiewijzer persoonsgegevens

1. Classificatiewijzer informatie



Figuur 2: Classificatiewijzer informatie

In figuur 2 is de classificatiewijzer te zien om het juiste classificatieniveau van informatie vast te stellen. Hieronder enkele voorbeelden van geclassificeerde informatie.

Voorbeelden DEPARTEMENTAAL VERTROUWELIJK

- Afstemming van interdepartementale vertrouwelijke bestuur stukken.
- Voorbereiding beleidsplannen uitbreiding weg- en waterinfrastructuur.
- IP nummerplannen netwerkinfrastructuur van kritieke systemen.

Voorbeelden RWS BEDRIJFSVERTROUWELIJK

- Rapport achterstallig onderhoud van infrastructuur.
- Verwerking van security incidenten.
- Beschrijving van netwerk architectuur.
- Documentatie van aanbestedingen.

Voorbeelden van RWS INFORMATIE

- Documenten van reguliere projecten, processen.
- E-mail communicatie met betrekking tot operationele taken.
- RWS Intranet publicaties met als doelgroep RWS medewerkers.

Belangrijk

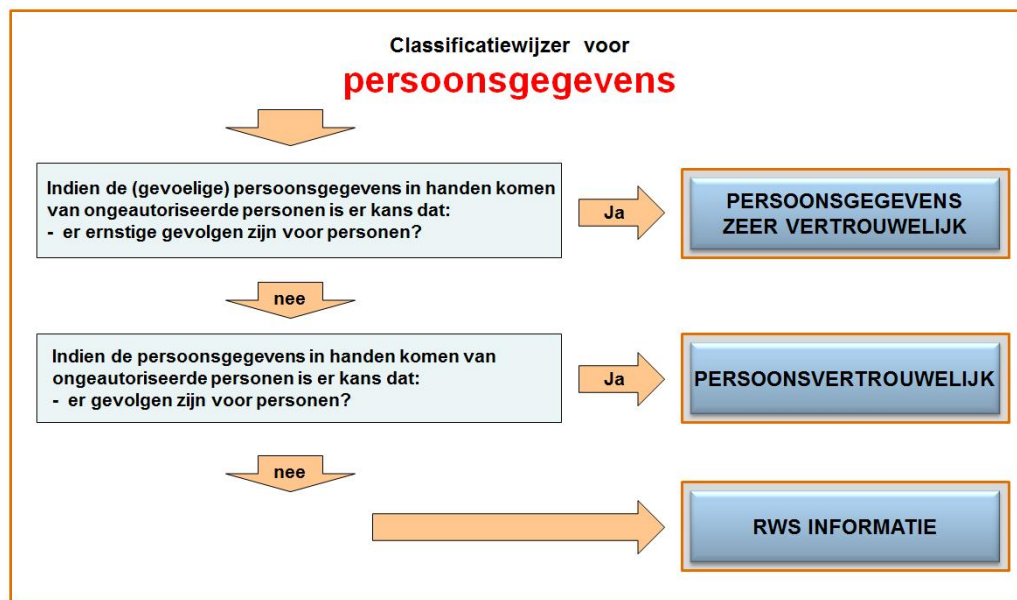
Volgens de VIR-BI dient DEPARTEMENTAAL VERTROUWELIJK informatie door een lijnmanager (gedelegeerde rubriceringsambtenaar) te worden vastgesteld. Indien de lijnmanager onzeker is over het classificatieniveau dient advies te worden gevraagd aan de RWS beveiligingscoördinator van Centrale Coördinatie Integrale Beveiliging.

2. Classificatiewijzer persoonsgegevens

Daar waar persoonsgegevens zijn opgenomen in documenten en/of communicatiemiddelen dient een risico afweging te worden gemaakt met betrekking tot de gevoeligheid van de gegevens voor de personen die het betreffen. Passende beveiligingsmaatregelen, waaronder het zorgvuldig verwerken van de gegevens, dienen te worden genomen op basis van de risico afweging en vaststelling van het classificatieniveau.

Het aanbrengen van markeringen voor persoonsgegevens is geen verplichting vanuit de Algemene Verordening Gegevensbescherming. Het is wel een wettelijke verplichting om passende maatregelen te nemen voor het beschermen van (bijzondere) persoonsgegevens. Het classificeren van persoonsgegevens is een ondersteunende maatregel, zoals die wordt verlangd in de Algemene Verordening Gegevensbescherming.

Hieronder de classificatiewijzer persoonsgegevens om het juiste classificatieniveau van persoonsgegevens vast te stellen.



Figuur 3: classificatiewijzer persoonsgegevens

Voorbeelden van **PERSOONSgegevens ZEER VERTROUWELIJK** / 'bijzondere persoonsgegevens' zijn expliciet genoemd in de Algemene Verordening Gegevensbescherming:

- Politieke opvattingen;
- Religieuze of levensbeschouwelijke overtuigingen;
- Lidmaatschap van een vakbond;
- Genetische gegevens;
- Biometrische gegevens met het oog op de unieke identificatie van een persoon;
- Gezondheid
- Seksueel gedrag of seksuele gerichtheid;
- Inloggegevens van bijvoorbeeld IT diensten, bank, overheid, ..
- Identiteitsgegevens zoals BSN, ID kaart, paspoort, ...

RWS vult deze aan met:

- Integriteitsonderzoeken naar een persoon

Voorbeelden van **PERSOONSVERTROUWELIJK**:

- Sollicitatiebrieven
- Personeelsadministratie
- Salarisadministratie

Voorbeelden van **RWS INFORMATIE** met gewone persoonsgegevens:

- (Zakelijk) e-mailadres
- (Zakelijk) telefoonnummer

Opmerkingen:

- Systemen die (bijzondere) persoonsgegevens verwerken dienen te zijn gemeld aan de privacy coördinatoren.
- Gebruikers worden in staat gesteld om (bijzondere) persoonsgegevens te classificeren en overeenkomstige markering aanbrengen op de bestanden. In Docgen is hiervoor een veld aangemaakt.

Stap 2) Vaststellen herzieningsdatum vertrouwelijkheid

(Alleen nodig voor DEPARTEMENTAAL VERTROUWELIJK informatie)

De vertrouwelijkheid van informatie neemt vaak af in de loop van de tijd. Het VIR-BI schrijft voor dat de rubricering "DEPARTEMENTAAL VERTROUWELIJK" moet zijn gekoppeld aan een maximum tijdsverloop of aan een bepaalde gebeurtenis.

Het is daarom nodig om de herzieningsdatum van de DEPARTEMENTAAL VERTROUWELIJK informatie op voorhand aan te geven in een document. Als deze datum verstrijkt, dan betekent dit dat de opsteller van het document opnieuw de informatie moet beoordelen op vertrouwelijkheid en stap 5 moet doorlopen.

Als er op een eerder tijdstip argumenten zijn om de vertrouwelijkheid van de informatie te verlagen, dan kan dat ook door stap 5 te doorlopen.

De herzieningsdatum van de vertrouwelijkheid van informatie kan afhangen van verschillende factoren. In bijlage 4 zijn een aantal voorbeelden gegeven van situaties waarin de vertrouwelijkheid kan worden herzien. Het is aan de opsteller om goed na te denken of er een tijdstip denkbaar is waarna de vertrouwelijkheid van een document kan worden herzien. Als het niet mogelijk is om op basis van argumenten een herzieningsdatum te bepalen, dan moet onderstaande tabel 3 worden gehanteerd.

Tabel 3: Vertrouwelijkheid en herzieningsdatum

Vertrouwelijkheidskenmerk	Herzieningsdatum
DEPARTEMENTAAL VERTROUWELIJK	na 5 jaar heroverwegen
RWS BEDRIJFSVERTROUWELIJK	geen
RWS INFORMATIE	geen
PERSOONSGEGEVENS ZEER VERTROUWELIJK	nog nader te bepalen*
PERSOONSVERTROUWELIJK	nog nader te bepalen*

Opmerking*

De herzieningsdatum van persoonsgegevens is op voorhand moeilijk te bepalen. Deze is onder andere afhankelijk van de grondslag van persoonsgegevensverwerking, de gevoeligheid en de aard van de gegevens. In het kader van de AVG wordt altijd een bewaartermijn voor het verwerken van persoonsgegevens geëist. Na het verstrijken van de bewaartermijn moeten persoonsgegevens worden vernietigd.

Stap 3) Het aanbrengen van vertrouwelijkheidskenmerk

Op alle pagina's en sheets (inclusief voorblad) moet het vertrouwelijkheidskenmerk worden aangegeven volgens onderstaande richtlijn:

- schrijf onder - of bovenaan de pagina het vertrouwelijkheidskenmerk
- gecentreerd op de pagina
- kleur van de letters is zwart
- tekenstijl is vet
- lettertype Verdana
- puntgrootte 6,5 voor documenten en spreadsheets
- puntgrootte 10 voor presentaties

De volgende schrijfwijze moet worden gehanteerd (let op de hoofdletters!):

DEPARTEMENTAAL VERTROUWELIJK
RWS BEDRIJFSVERTROUWELIJK
RWS INFORMATIE
PERSOONSGEGEVENS ZEER VERTROUWELIJK
PERSOONSVERTROUWELIJK

Als er bijvoorbeeld sprake is van bijzonder vertrouwelijke informatie en persoonsgegevens dan wordt de vertrouwelijkheid als volgt aangebracht: "DEPARTEMENTAAL VERTROUWELIJK en PERSOONSVERTROUWELIJK"

In de documentgegevens moet de volgende informatie worden opgenomen:

Als het document DEPARTEMENTAAL VERTROUWELIJK is:

Auteur: Datum: Vastgesteld door: Vertrouwelijkheid: DEPARTEMENTAAL VERTROUWELIJK Herzieningsdatum vertrouwelijkheid: dd-mm-jjjj Aantal pagina's:

Overige vertrouwelijke documenten:

Auteur: Datum: Vertrouwelijkheid:

Metadata

Naast de markering op het document zelf, dient de rubricering ook in de metadata te zijn opgenomen. De gebruiker mag ervan uitgaan dat de kantoorautomatisering dit automatisch doet bij het aanbrengen van de markering via bijvoorbeeld bij DocGen. Het wordt daarom ook aangeraden om documenten met DocGen aan te maken. Zie onderstaande figuur over de vastlegging van metadata in het document.

Eigenschappen voor Instructie vertrouwelijkheid documenten en g... ? X

Algemeen Samenvatting Statistieken Inhoud Aangepast

Naam:

Afdeling
Beschikking
Bestemming
Bron
Datum voltooid
Divisie

Type: Tekst

Waarde: ☐ Koppelen aan inhoud

Eigenschappen:

Naam	Waarde	Type
Rubricering	RWS Informatie	Tekst

Stap 4) Verwerken volgens vastgestelde informatieklasse

De informatieklasse (RWS-II, RWS-I of RWS-0) bepaalt hoe men de informatie dient te verwerken. Bijvoorbeeld waar het document wel of niet mag worden opgeslagen; of het moet worden versleuteld; of het met externe partijen mag worden gedeeld; etc. De wijze van verwerking per informatieklasse is te vinden in bijlage 3. De bijlage bestaat uit 2 tabellen: fysieke verwerking en digitale verwerking van gegevens.

De verwerking die voor de verschillende informatieklassen is beschreven, is niet beperkt tot alleen het behandelen van documenten. Ook het bespreken, al of niet via social media en het vastleggen op beeld van informatie (bijvoorbeeld: foto van een volgeschreven whiteboard) is in de instructie meegenomen, omdat dit risicovolle manieren zijn waarop informatie ook kan lekken.

Van informatie welke *niet* is voorzien van een markering en waar RWS de eigenaar of bewaarder van is, is het niet vanzelfsprekend dat de informatie niet vertrouwelijk kan zijn. RWS medewerkers dienen op basis van de gedragscode 'Bewust Integer' altijd zelf te beoordelen of de informatie zonder markering alsnog vertrouwelijk is en er zorgvuldig mee omgaan. Indien je als RWS medewerker alsnog een markering wilt aanbrengen, dan is het goed gebruik om het document terug te sturen naar de steller van de informatie met het verzoek om alsnog het document te classificeren.

Op [RWS intranet](#) is een vraag en antwoord pagina geopend, waar aanvullende instructies en tips over het omgaan met vertrouwelijke informatie wordt gegeven. Hier zijn ook hulpmiddelen te vinden om de juiste classificatie te kiezen en af te leiden hoe je met de informatie om moet gaan.

Link:

http://corporate.intranet.rws.nl/Ondersteuning/Kantoorautomatisering_en_Telefonie/Vertrouwelijkheidsniveau_toepassen/?pk_campaign=Docgenwidgetclassif&pk_kwd=intranet

Stap 5) Vertrouwelijkheid en informatieklassering wijzigen

Als de vertrouwelijkheid van de informatie in een document wijzigt, of de herzieningsdatum verstrijkt, dan moeten stap 1 tot en met 4 opnieuw worden doorlopen. De opsteller van het document moet daartoe het initiatief nemen.

Als de opsteller van het document niet (meer) beschikbaar is of niet meer werkzaam is bij RWS, dan wordt het document zonder tussenkomst van de oorspronkelijke opsteller voorgelegd aan diens logische opvolger of zijn lijnmanager. Bij twijfel kan de beveiligingscoördinator adviseren.

Opmerking

Een medewerker die uit dienst treedt dient ervoor te zorgen dat alle documenten waarvan hij/zij de eigenaar was beschikbaar blijven voor verwerking door RWS. Indien documenten versleuteld zijn, dan dient de medewerker het wachtwoord over te dragen aan een opvolger of de documenten (in overleg met lijnmanager) te ontsleutelen. Indien de lijnmanager onzeker is over het ontsleutelen van de documenten dient advies te worden gevraagd aan een beveiligingscoördinator van Centrale Coördinatie Integrale Beveiliging. Wachtwoorden kunnen worden opgeslagen in de applicatie KeePass, beschikbaar als basis programma op de KA omgeving.

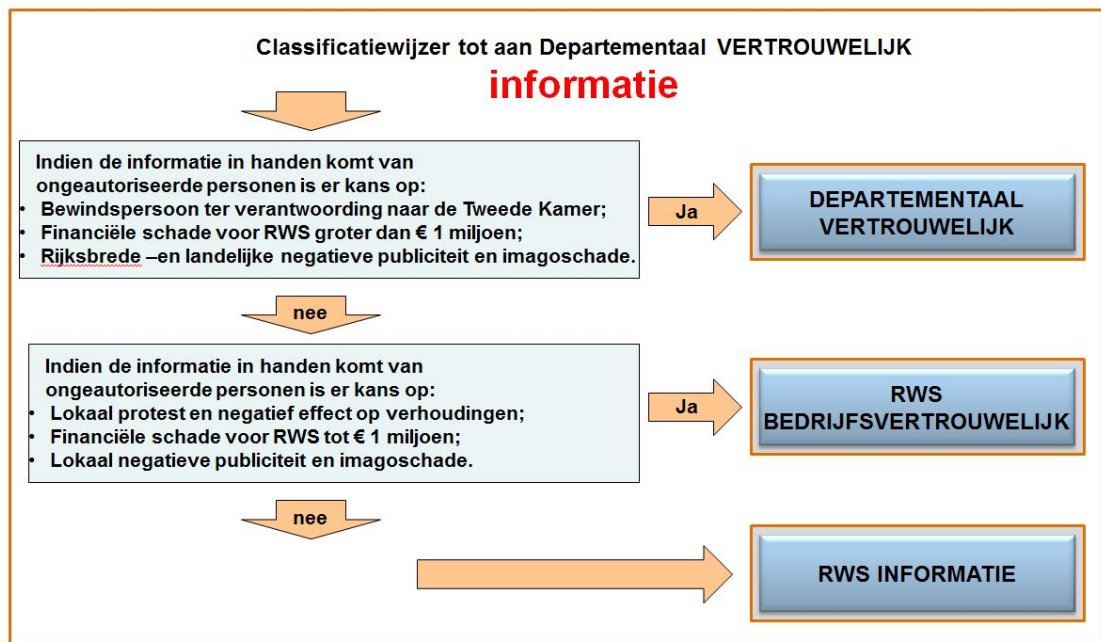
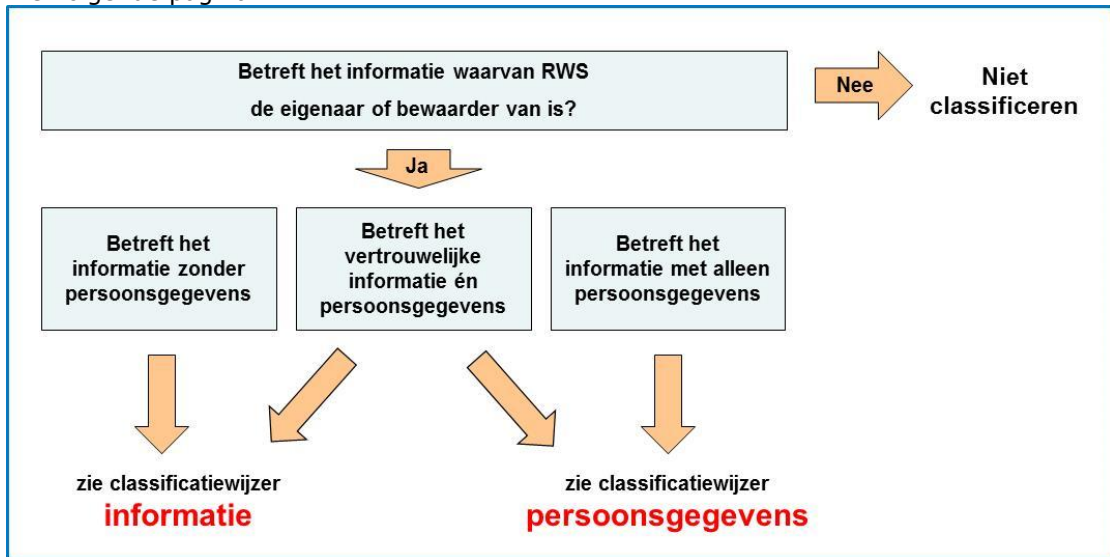
Bijlage 1 Voorbeelden van geclassificeerd informatie en persoonsgegevens.

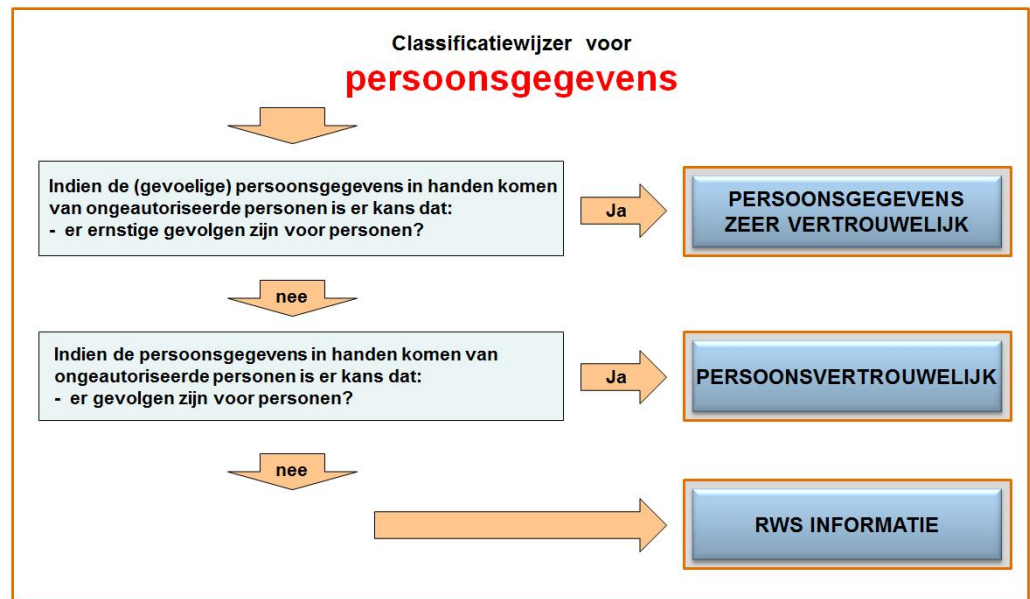
	RWS INFORMATIE	RWS BEDRIJFSVER- TROUWELIJK	DEPARTEMENTAAL VERTROUWELIJK
Maatschap- pelijke scha- de	Luchtfoto Oosterschelde kering	Detail bouwtekening Oosterschelde ke- ring	IA systeemtekening Oos- terschelde kering
Financiële Schade	Kosten van de bouw van de Oosterschelde kering	Plannen voor weg- verbreding	Strategische plannen voor uitbreiding snelweg Documenten die vertrou- welijk moeten worden behandeld volgens de aanbestedingswet
Vertrou- wensverlies	Actuele waterstanden	Rapporten over achterstallig onder- houd op enkele objecten	Rapporten over achter- stallig onderhoud op vele objecten

	RWS INFORMATIE	PERSOONSVERTROU- WELIJK	PERSOONSgegevens ZEER VERTROUWE- LIJK
Persoonlijke schade	Verkeersbeelden met onleesbare kente- kens Document met naam en zakelijk adres en telefoonnummer van een RWS medewer- ker Document met na- men van RWS me- dewerkers die het document geschre- ven en ge-reviewd hebben	Document met naam en privé-adres en privé- telefoon-nummer van een RWS medewerker Document met naam en medische gegevens van een RWS medewerker. CV van sollicitant RWS Gesprekscyclus	Gegevensverzameling P-direct Document waarin van een aantal medewerkers het lidmaatschap van vakbonden is aangege- ven

Bijlage 2 Beslisboom

Zie volgende pagina.





Bijlage 3 Omgaan met gevoelige informatie

Classificatie Informatie	Classificatie Persoonsgegevens	Informatieklasse
DEPARTEMENTAAL VERTROUWELIJK	PERSOONSgegevens ZEER VERTROUWELIJK	RWS-II
RWS BEDRIJFSVERTROUWELIJK	PERSOONSVERTROUWE- LIJK	RWS-I
RWS INFORMATIE		RWS-0

Maatwerk oplossingen voor specifieke (gevoelige) informatie die buiten bovenstaande klassen en rubriceringen vallen zijn buiten beschouwing gelaten.

Informatie moet minimaal worden behandeld volgens de richtlijnen die bij de informatieklasse horen, en mag worden behandeld volgens de richtlijnen van hogere klassen.

Bijvoorbeeld:

- RWS-I informatie mag onversleuteld op Sharepoint worden opgeslagen maar mag ook versleuteld op Sharepoint (eis voor RWS-II) worden opgeslagen.
- RWS-I informatie mag niet onversleuteld in de OpenCloud (bijvoorbeeld Dropbox: RWS-0) worden opgeslagen.

Om de tabel overzichtelijk te houden worden de behandelingswijzen die bij bovenliggende klassen horen, niet bij onderliggende klassen herhaald, tenzij ze hetzelfde zijn.

Bij informatieklasse RWS-0 bestaat het risico dat medewerkers niet voldoende in staat zijn om te beoordelen of informatie vertrouwelijk is of niet en het toch verspreken op publieke of privé media. Daarom mag een medewerker alleen externe opslag gebruiken als vooraf zeker is gesteld, dat de medewerker de informatieclassificatie kent en beheerst.

Fysieke verwerking van gegevens door gebruikers													
Infor- matie- klasse	Posten		Zelf vervoeren van documenten	Fysiek opbergen		Weggooiden		Kopiëren/ Printen/ Scannen		Foto- graferen	Bespreken (voor bespreken via telefoon, lees ook volgende kolom)		Telefoneren (als middel om iets te bespre- ken)
	Interne post RWS	Post naar adres buiten RWS		Binnen RWS gebouw	Buiten RWS gebouw	Binnen RWS gebouw	Buiten RWS gebouw	Multi function- als van RWS	Printers en scanners buiten RWS		Binnen RWS gebouw	Buiten RWS gebouw	
RWS-II	In een dichtge- plakte enveloppe gericht aan de need-to-know ontvanger met de markering “Per- soonlijk”	In een dubbele envelop. Op de binnenste enve- loppe is de classi- ficering aangege- ven, op de buiten- ste envelop de need-to-know ontvanger met de markering “Per- soonlijk”	Alleen als het noodzakelijk is voor de werk- zaamheden. In een ongemar- keerde dichtge- plakte enveloppe. De enveloppe mag niet onbe- heerd worden achtergelaten.	Opbergen in een afgesloten kast die alleen door need-to-know medewerkers te openen is	Opbergen in af- gesloten kast die alleen door de eigenaar van het document te ope- nen is need-to- know medewer- kers in een aan- toonbaar beveilig- de ruimte van Rijksoverheid of privé persoon	Versnipperen met papierver- nietiger of: deponeren in de afgesloten sta- len bakken gemarkeerd met ‘vertrouwelijk’	Versnipperen in een daar- voor aangewe- zen papierver- nietiger bij ander Depar- tement	Printen met prin- ter na aanbieden Rijkspas of na invoeren pincode Printen, kopiëren en scannen terwijl je wacht tot het klaar is	Alleen printen, kopiëren en scannen met daarvoor aan- gemerkte Rijks- overheid Multi functionals Printen, kopiëren en scannen terwijl je wacht tot het klaar is	mag niet	Binnen besloten RWS ruimte	Open ruimte zon- der mensen in de buurt, binnen besloten ruimte Departement of huis van privé persoon	Mobiele telefoon RWS, vaste tele- foon RWS, waar- bij de uit te wisse- len vertrouwelijke informatie tot het strikt noodzakelij- ke wordt beperkt.
RWS-I	In een dichtge- plakte enveloppe gericht aan de need-to-know ontvanger	In een dichtge- plakte enveloppe gericht aan de need-to-know ontvanger	In een ongemar- keerde tas of map De tas of map mag niet onbe- heerd worden achtergelaten.	Opbergen in een afgesloten kast die alleen door need-to-know medewerkers te openen is	Opbergen in een afgesloten kast die alleen door need-to-know medewerkers te openen is in een aantoonbaar beveiligde ruimte	Deponeren in de afgesloten sta- len bakken gemarkeerd met Vertrouwelijk	Versnipperen of deponeren in daarvoor aangewezen hulpmiddelen van leveran- cier, NGO of overheid	Printen, kopiëren en scannen terwijl je wacht tot het klaar is	Alleen printen, kopiëren en scannen met daarvoor aan- gemerkte Multi functionals van leverancier, NGO of overheid Printen, kopiëren en scannen terwijl je wacht tot het klaar is	RWS smartphone	Binnen besloten RWS ruimte	Binnen besloten ruimte van leve- rancier, NGO, overheid of hore- ca/ conferentie- centrum	Mobiele telefoon RWS, vaste tele- foon RWS
RWS-0	In een open enve- loppe of cellofaan	In een open enve- loppe of cellofaan	In een ongemar- keerde tas of map. Liever niet onbeheerd achter- laten.	Op bureau; in open kast; zonder enveloppe in postvak; etc	Op bureau; in open kast; zonder enveloppe in postvak; etc	Deponeren in de papierbakken bij bureau's of blauwe contai- ners	Deponeren als oud papier	Printen, kopiëren en scannen zonder authenti- catie of pincode en zonder er bij te blijven	Printen, kopiëren en scannen zonder authenti- catie of pincode. Er wel bij blijven.	Smartphone; Tablet; Camera	Receptie, bezoe- kerscentra en ruimtes	In de kantine, in de trein, etc.	Skype, Whats- App, andere apps.

Instructies voor het verwerken van digitale informatie									
Informatie-klasse	Bewerken van informatie		Opslaan van informatie op vaste dragers		Opslaan van informatie op mobiele dragers	Digitale communicatie		Agenda	
	RWS KA-omgeving	Externe KA-omgeving	RWS-intern	Externe KA-omgeving	Buiten RWS	RWS-intern naar RWS-intern	RWS-intern naar KA-extern	RWS-intern	RWS-intern naar KA-extern
RWS-II	RWS KA-omgeving ¹ of i-SWF ⁴ . Toegangsbeheer o.b.v. 'need-to-know'.	Rijks KA-omgeving ² . Externe KA-omgeving ³ (die voldoet aan de BIR) of e-SWF ⁵ -omgeving van externe medewerker met geheimhoudingsverklaring en VOG werkzaam bij ketenpartner met bewerkersovereenkomst. Toegangsbeheer o.b.v. 'need-to-know'.	Onversleuteld opslaan op RWS KA-omgeving ¹ of i-SWF ⁴ . Versleuteld opslaan op Sharepoint/VPR. Toegangsbeheer o.b.v. 'need-to-know'.	Onversleuteld opslaan op Rijks KA-omgeving ² . Versleuteld opslaan (7ZIP ⁸) op externe KA-omgeving ³ (die voldoet aan de BIR) of e-SWF ⁵ -omgeving van externe medewerker met geheimhoudingsverklaring en VOG werkzaam bij ketenpartner met bewerkersovereenkomst. Toegangsbeheer o.b.v. 'need-to-know'.	Opslaan op RWS-IronKey of Rijks-IronKey. Opslaan op IronKey van externe medewerker met geheimhoudingsverklaring en VOG werkzaam bij ketenpartner met bewerkersovereenkomst.	Versturen van berichten met interne e-mail. Bijlagen onversleuteld. Delen van informatie m.b.v. i-SWF ⁴ . Interactieve communicatie met VideoTeleCommu-nicatie of Lync. Toegangsbeheer o.b.v. 'need-to-know'.	Versturen van berichten met e-mail naar Rijks-omgeving ² . Bijlagen onversleuteld. Versturen van berichten met e-mail (bijlagen versleuteld met 7ZIP ⁸) naar externe KA-omgeving ³ (die voldoet aan de BIR) of delen van informatie via e-SWF-omgeving van externe medewerkers met geheimhoudingsverklaring en VOG werkzaam bij ketenpartner met bewerkersovereenkomst.	Agenda items moeten ingesteld zijn op 'privé'. Bijlage onversleuteld. Toegangsbeheer o.b.v. 'need-to-know'.	Agenda items moeten ingesteld zijn op 'privé'.. Bijlage versleuteld (7ZIP ⁸). Toegangsbeheer o.b.v. 'need-to-know'.
RWS-I	RWS KA-omgeving ¹ of i-SWF ⁴ . Toegangsbeheer o.b.v. 'need-to-know'.	Rijks KA-omgeving ² . Externe KA-omgeving ³ (die voldoet aan de BIR) of e-SWF ⁵ -omgeving van externe medewerker met geheimhoudingsverklaring op organisatieniveau. Toegangsbeheer o.b.v. 'need-to-know'	Onversleuteld opslaan op RWS KA-omgeving ¹ , i-SWF ⁴ of Sharepoint/VPR. Toegangsbeheer o.b.v. 'need-to-know'.	Onversleuteld opslaan op Rijks KA-omgeving ² . Onversleuteld opslaan op externe KA-omgeving ³ (die voldoet aan de BIR) of e-SWF ⁵ -omgeving van externe medewerker met geheimhoudingsverklaring op organisatieniveau. Toegangsbeheer o.b.v. 'need-to-know'.	Opslaan op RWS-IronKey of Rijks-gecertificeerde USB met AES-256 encryptie. Opslaan op USB met sterke encryptie (AES 256, zoals 7ZIP ⁸) van externe medewerker met geheimhoudingsverklaring op organisatieniveau.	Versturen berichten met interne e-mail. Bijlage onversleuteld. Delen van informatie m.b.v. i-SWF ⁴ . Interactieve communicatie met VideoTeleCommunicatie (VTC), Lync, WhatsApp of FaceTime. Toegangsbeheer o.b.v. 'need-to-know'.	Versturen van berichten met e-mail (bijlage onversleuteld) of delen van informatie m.b.v. e-SWF ⁵ -omgeving naar externe medewerkers met geheimhoudingsverklaring op organisatieniveau. Interactieve communicatie met beveiligde multimedia middelen zoals WhatsApp of FaceTime.	Agenda items moeten ingesteld zijn op 'privé'. Bijlage onversleuteld. Toegangsbeheer o.b.v. 'need-to-know'.	Agenda items moeten ingesteld zijn op 'privé'. Bijlage onversleuteld. Toegangsbeheer o.b.v. 'need-to-know'.
RWS-O	RWS KA-omgeving ¹ of i-SWF ⁴ .	Rijks KA-omgeving ² , e-SWF ⁵ , OpenCloud ⁷ , externe KA-omgeving ³ of prive ICT-middelen.	Onversleuteld opslaan op RWS KA-omgeving ¹ , i-SWF ⁴ of Sharepoint/VPR.	Onversleuteld opslaan op Rijks KA-omgeving ² , e-SWF ⁵ , OpenCloud ⁷ , externe KA-omgeving ³ of prive ICT-middelen.	Onversleuteld opslaan op USB, CD-ROM, DVD of andere mobiele dragers ⁶ .	Versturen van berichten met o.a.: e-mail, RWS Yammer, Chat of SMS. Bijlage onversleuteld. Delen van informatie m.b.v. i-SWF ⁴ . Interactieve communicatie met multimedia middelen zoals VTC, Lync, WhatsApp, Face-time, Skype, ...	Versturen van berichten met o.a.: e-mail, Berichtenbox ⁸ of SMS. Bijlage onversleuteld. Delen van informatie m.b.v. e-SWF ⁵ . Interactieve communicatie met multimedia middelen zoals WhatsApp, FaceTime, Skype, ...	Agenda mag gedeeld worden met collega's. Bijlage onversleuteld.	Agenda mag gedeeld worden met externen. Bijlage onversleuteld.

Gegevens bestaan uit (vertrouwelijke) informatie en (gevoelige) persoonsgegevens.

¹ RWS KA-omgeving bestaat uit RWS Desktop, RWS Laptop, RWS Thuiswerkoplossing, RWS Groepsschijf, RWS Smartphone en RWS Tablet.

² Rijks KA-omgeving bestaan uit alle KA-middelen die door het rijk worden beheerd en ter beschikking worden gesteld aan rijksambtenaren.

³ Externe KA-omgeving zijn ICT-systemen en middelen van externe organisaties die niet worden beheerd door RWS of het Rijk. Externe KA-omgeving met vertrouwelijke informatie dient te voldoen aan de BIR normen (of vergelijkbaar zoals ISO 27001/2).

⁴ i-SWF staat voor interne SamenwerkingsFunctionaliteit en is een online platform voor het delen en bewerken van documenten met RWS medewerkers. Het beveiligingsniveau is RWS II (Dep.V)

⁵ e-SWF staat voor externe SamenwerkingsFunctionaliteit en is een online platform voor het delen en bewerken van documenten met externe partijen. Het beveiligingsniveau is RWS II (Dep.V)

⁶ Mobiele dragers zijn IT middelen voor opslag van gegevens die buiten de fysieke locatie van RWS kunnen worden meegenomen, zoals IronKey, USB sticks, CD-ROM's, DVD's en smartphones. ...

⁷ OpenCloud bestaat uit internet gebaseerde diensten die niet worden beheerd door het Rijk en worden gebruikt door meerdere organisties en/of gebruikers op basis van persoonlijk toegangsbeheer. (b.v.: google docs, dropbox, ...).

⁸ 7ZIP is (opensource) software waarmee bestanden op een sterke wijze versleuteld kunnen worden. Gebruik een sterk wachtwoord en AES-256 encryptie.

Opmerkingen

Het verwerken van RWS INFORMATIE op externe KA-omgevingen of prive IT-middelen dient tot het minimum te worden beperkt om te voorkomen dat vertrouwelijke gegevens alsnog (onbedoeld) worden gelekt. Gegevens die niet zijn gemarkeerd zijn niet vanzelfsprekend RWS-0 (RWS INFORMATIE). Beoordeel ook zelf of de gegevens die je verwerkt eventueel vertrouwelijk zijn. Neem vervolgens passende maatregelen. Ga altijd integer en zorgvuldig met gegevens om zodat vertrouwelijke informatie niet in handen kan komen van onbevoegden. Je bent zelf verantwoordelijk voor de wijze waarop je informatie van RWS verwerkt. Voor het nieuwe werken is het aanbevolen om collega's toegang te geven tot je agenda, dus kan ook iederen bijlagen in de agenda items zien. Daar waar de gegevens vertrouwelijk zijn dient de agenda items op prive te worden ingesteld.

Deze bladzijde is bewust leeg gelaten, zodat de tabel op de volgende pagina op de juiste manier wordt afgedrukt

Bijlage 4 Termijnbepaling vertrouwelijkheid

De volgende oorzaken kunnen bijvoorbeeld tot gevolg hebben dat de vertrouwelijkheid van informatie kan worden verlaagd:

- Tijdstip en locatie van een bezoek van een bepaald persoon aan RWS is als vertrouwelijk aangemerkt, omdat de veiligheid van de persoon in kwestie moet worden gewaarborgd. Als het bezoek heeft plaatsgevonden hoeft deze informatie niet meer vertrouwelijk te zijn, maar kan worden gedeeld. Vaak wordt het zelfs direct openbaar gemaakt in een persbericht.
- Informatie over een vitaal object is als vertrouwelijk aangemerkt. Als de functie van het object verandert en het object niet langer als vitaal wordt aangemerkt, dan kan de vertrouwelijkheid van de objectinformatie worden verlaagd.
- Concept plannen voor een reorganisatie kunnen als vertrouwelijk worden aangemerkt. Als de conceptplannen op een bepaald moment naar de medewerkers worden gecommuniceerd kan de vertrouwelijkheid worden verlaagd.
- Informatie over kwetsbaarheden in de beveiliging is als vertrouwelijk aangemerkt. Als de kwetsbaarheden zijn weggenomen kan de vertrouwelijkheid van de informatie in sommige gevallen worden verminderd om bijvoorbeeld in bewustwordingstrainingen te worden gebruikt.
- Bepaalde aanbestedingsgegevens zijn vertrouwelijk totdat het werk is gegund. Maar sommige aanbestedingsgegevens moeten ook na gunning vertrouwelijk worden behandeld, omdat de aanbiedende partij dit bijvoorbeeld heeft verzocht.

Bijlage 5 Begrippenlijst

AVG	Algemene Verordening Gegevensbescherming
BVA	Beveiligingsambtenaar van Departement
Classificeren	Het vaststellen van een vertrouwelijkheidsniveau van informatie (waaronder persoonsgegevens) op basis van een risicoafweging.
Classificatie	Vertrouwelijkheidsklassen van informatie te weten: RWS BEDRIJFSVERTROUWELIJK, RWS INFORMATIE, PERSOONSgegevens ZEER VERTROUWELIJK, PERSOONSVERTROUWELIJK.
Gedelegeerde rubriceringsambtenaar	De verantwoordelijkheid voor het vaststellen van de rubricering van RWS documenten is door de Beveiligingsambtenaar van het Ministerie van I&M gedelegeerd naar de lijnmanagers van RWS.
Gegevensverzameling	Een gegevensverzameling bevat een business gegevensset; onderliggende gegevenssets en versies; alsmede adequate meta-data.
Informatieklasse	Aanduiding van de wijze waarop de informatie moet worden verwerkt, opgeslagen of gecommuniceerd. Informatieklassen zijn: RWS-II, RWS-I en RWS-0.
Herzieningsdatum	Datum waarop de rubricering DEPARTEMENTAAL VERTROUWELIJK informatie moet worden herzien
Markeren	Het aanbrengen van een classificatiekenmerk op een informatiedrager.
Merken	Het aanbrengen van een Rijksbede rubriceringskenmerk op een informatiedrager.
Need-to-know	Informatie wordt alleen bekend gesteld aan personen die de informatie nodig hebben om de hen opgelegde werkzaamheden uit te kunnen voeren.
Onrechtmatig gebruik	Gebruik door personen die daartoe niet gerechtigd zijn.

Open data	Open data is: - openbare overheidsinformatie; - overheidsinformatie die is verzameld/geproduceerd in het kader; - van een publieke taak en met publieke middelen.; - gratis of tegen maximaal marginale verstrekingskosten; - data in de vorm waarin deze is verzameld in het kader van een publieke taak; - bij voorkeur machine leesbaar; - bij voorkeur open standaarden.
Persoonsgegevens	Informatie waarin gegevens zijn opgenomen over een natuurlijke persoon en waarmee die persoon identificeerbaar of herleidbaar is.
Privacy coördinator	De privacy-coördinator houdt namens de Functionaris Gegevensbescherming binnen Rijkswaterstaat toezicht op de verwerkingen en is het eerste aanspreekpunt voor de contactpersonen.
Rubriceren	Het vaststellen van een vertrouwelijkheidsniveau op basis van Rijksbrede normen (VIR-BI).
Rubricering	Rijksbrede vertrouwelijkheidsklassen te weten: DEPARTEMENTAAL VERTROUWELIJK, Staatsgeheim Confidentieel, Staatsgeheim Geheim en Staatsgeheim Zeer Geheim.
Rubriceringsambtenaar	Ambtenaar bevoegd tot het vaststellen van rubriceringen, hiertoe aangewezen door de secretaris-generaal. Dit is de BVA van I&M.
RWS	Rijkswaterstaat
Schadecategorieën	Indeling van wijzen waarop Rijkswaterstaat schade kan oplopen.
Staatsgeheimen	Alle informatie die valt onder de rubriceringsklassen: Staatsgeheim Confidentieel, Staatsgeheim Geheim en Staatsgeheim Zeer Geheim.
Vaststeller van de rubricering	Minister, staatssecretaris, secretaris-generaal of een door de secretaris-generaal aangewezen rubriceringsambtenaar.

Vertrouwelijkheid	Vertrouwelijkheid is een informatie-eigenschap waardoor alleen gemachtigde personen, entiteiten of processen toegang hebben tot informatie en waardoor informatie alleen kan worden doorgegeven aan gemachtigde personen, entiteiten of processen.
Vertrouwelijkheidsniveau	Mate van vertrouwelijkheid van informatie. Door het rubriceren of classificeren van informatie wordt het vertrouwelijkheidsniveau ingedeeld in drie informatieklassen te weten: RWS-II, RWS-I, RWS-0.
VIR-BI	Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie
Wbp	Wet bescherming persoonsgegevens
WOB	Wet Openbaarheid Bestuur