



RWS INFORMATIE

**Richtlijnen informatiebeveiliging bij RWS IV-
contracteisen**

Proces- en systeemrichtlijnen voor informatiebeveiliging bij IV-contracten

Datum	21 februari 2017
Status	Definitief

Colofon

Uitgegeven door	RWS/CIV/Security Centre
Informatie	
Telefoon	
Fax	
Uitgevoerd door	P. van den Berg
Opmaak	
Datum	21 februari 2017
Status	Definitief
Versienummer	1.0

Inhoud

1	Inleiding—6
1.1	Baseline Informatiebeveiliging Rijksdienst—6
1.2	Informatiebeveiliging in IV-inkoopcontracten—6
1.3	Structuur—6
2	IBR-1: Beleid voor gegevensclassificatie—7
2.1	Doelgroep—7
2.2	Doel—7
2.3	Scenario's—7
2.4	Stappen bij informatieclassificaties—7
2.4.1	Stap 1: Vaststellen vertrouwelijkheid en informatieklassie—7
2.4.1.1.	Classificatiewijzer informatie—8
2.4.1.2.	Classificatiewijzer persoonsgegevens—9
2.4.2	Stap 2: Vaststellen herzieningsdatum vertrouwelijkheid—11
2.4.3	Stap 3: Het aanbrengen van vertrouwelijkheidskenmerk—11
2.4.3.1.	Metadata—12
2.4.4	Stap 4: Verwerken volgens vastgestelde informatieklassie—12
2.4.5	Stap 5: Vertrouwelijkheid en informatieklassie wijzigen—13
3	IBR-2: Beleid voor logische toegangsbeveiliging—14
3.1	Doelgroep—14
3.2	Doel—14
3.3	Scenario's—14
3.4	Richtlijnen—14
4	IBR-3: Beleid voor wachtwoordgebruik—16
4.1	Doelgroep—16
4.2	Doel—16
4.3	Scenario's—16
4.4	Richtlijnen—16
4.5	Tips bij gebruik van wachtwoorden—17
5	IBR-4: Richtlijnen voor beveiligen bij ontwikkelen—19
5.1	Doelgroep—19
5.2	Doel—19
5.3	Scenario's—19
5.4	Richtlijnen—19
5.5	Bronnen bij IBR-4—20
6	IBR-5: Richtlijnen voor informatiebeveiligingsincidenten—21
6.1	Doelgroep—21
6.2	Doel—21
6.3	Scenario's—21
6.4	Richtlijnen—21
7	IBR-6: Richtlijnen voor fysieke beveiliging—22
7.1	Doelgroep—22
7.2	Doel—22
7.3	Scenario's—22

- 7.4 Richtlijnen—22
- 7.5 Bronnen bij IBR-5—23

8 IBR-7: Richtlijnen voor logging—24

- 8.1 Doelgroep—24
- 8.2 Doel—24
- 8.3 Scenario's—24
- 8.4 Richtlijnen—24

1 Inleiding

Dit document bevat richtlijnen op het gebied van informatiebeveiliging waar naar verwezen wordt vanuit contacteisen in *Informatievoorziening (IV)* inkoopcontracten van Rijkswaterstaat (RWS). Deze richtlijnen dragen bij aan de beschikbaarheid, de integriteit, de vertrouwelijkheid en de controleerbaarheid van de IV van RWS.

1.1 Baseline Informatiebeveiliging Rijksdienst

De *Baseline Informatiebeveiliging Rijksdienst* (BIR) is een tactisch normenkader waarin het basisniveau voor informatiebeveiliging staat beschreven voor alle rijksdiensten. De BIR biedt één normenkader voor de beveiliging van de IV van de verschillende rijksdiensten. Dit maakt het mogelijk om veilig samen te werken en onderling gegevens uit te wisselen. De BIR zorgt voor één heldere set afspraken zodat een bedrijfsonderdeel weet dat de gegevens die verstuurd worden naar een ander onderdeel van de rijksdienst op het juiste beveiligingsniveau (vertrouwelijkheid, integriteit en beschikbaarheid) worden behandeld.

1.2 Informatiebeveiliging in IV-inkoopcontracten

RWS moet aan de BIR voldoen, wat impliceert dat door RWS aangekochte producten en uitbestede dienstverlening dat ook moeten doen. Om deze reden moeten eisen voor informatiebeveiliging een standaard onderdeel zijn van alle IV-inkoopcontracten van RWS. Sommige eisen zijn echter te specifiek om op te nemen in contractteksten. Om deze reden wordt vanuit de IV-inkoopcontracten soms verwezen naar de richtlijnen voor informatiebeveiliging bij RWS waarin verschillende aspecten van de informatiebeveiliging verder worden uitgediept. Dit document beschrijft deze richtlijnen.

1.3 Structuur

Richtlijnen zijn gedefinieerd op verschillende deelgebieden van de informatiebeveiliging, en kunnen betrekking hebben op beleid, processen, dan wel systemen. Vooralsnog beschikt RWS over de onderstaande richtlijnen waar naar verwezen kan worden vanuit IV-inkoopcontracten:

- IBR-1: Beleid voor gegevensclassificatie;
- IBR-2: Beleid voor logische toegangsbeveiliging;
- IBR-2: Beleid voor wachtwoordgebruik;
- IBR-3: Richtlijnen voor beveiligen bij ontwikkelen;
- IBR-4: Richtlijnen voor informatiebeveiligingsincidenten;
- IBR-5: Richtlijnen voor fysieke beveiliging;
- IBR-6: Richtlijnen voor logging.

Elk volgend hoofdstuk beschrijft één van deze richtlijnen.

2 IBR-1: Beleid voor gegevensclassificatie

2.1 Doelgroep

Personeel met een rol in het leveren van de Prestatie en die contractueel gebonden zijn aan het RWS beleid voor gegevensclassificatie.

2.2 Doel

Dit beleid heeft als doel:

1. Richtlijnen te bieden in hoe informatie geclassificeerd moet worden;
2. Richtlijnen te bieden over hoe moet worden omgegaan met geclassificeerde informatie.

2.3 Scenario's

De richtlijnen hieronder beschreven moeten worden verwerkt in procedures, systeemeisen en bewustwordingstrajecten op het gebied van de informatiebeveiliging.

2.4 Stappen bij informatieclassificaties

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

1. Vaststellen vertrouwelijkheid en informatieklaas van de informatie;
2. Vaststellen herzieningsdatum vertrouwelijkheid (alleen bij Departementaal VERTROUWELIJK);
3. Aanbrengen van een passende markering op het document;
4. Vaststellen hoe de informatie moet worden verwerkt;
5. Het beoordelen van het classificatieniveau en eventueel wijzigen van de informatieklaas.

2.4.1 Stap 1: Vaststellen vertrouwelijkheid en informatieklaas

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 informatieklaas. De informatieklaas bepaalt hoe je met de informatie om moet gaan. Hierbij een overzicht van de relatie tussen classificatieniveaus en informatieklassen.

Classificatieniveaus van informatie	Informatieklaas
Departementaal VERTROUWELIJK	RWS-II
RWS Bedrijfsvertrouwelijk	RWS-I
RWS Informatie	RWS-0
Classificatieniveaus van persoonsgegevens	Informatieklaas
Persoonsgegevens ZEER VERTROUWELIJK	RWS-II
Persoonsvertrouwelijk	RWS-I

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 bestuursstukken 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.

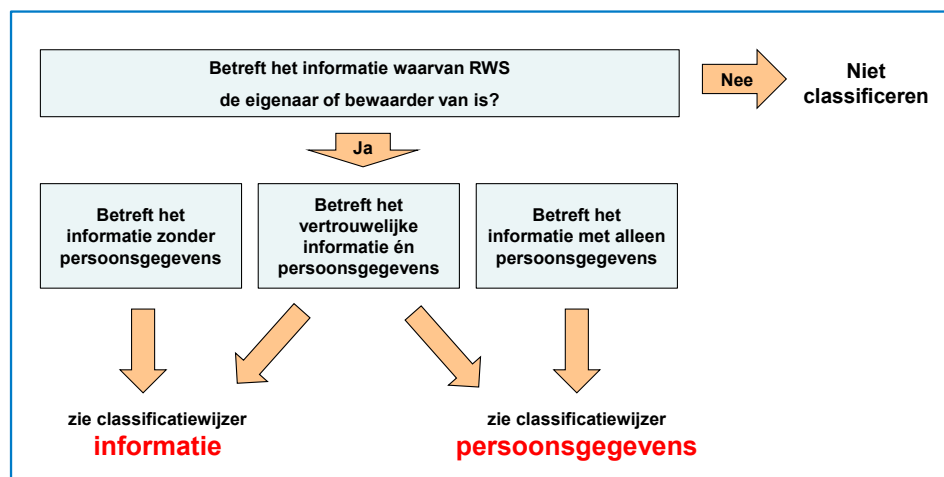
Voorbeelden waar RWS niet de eigenaar of beheerder van is zijn:

- publieke informatie op Internet;
- persoonsgegevens ten behoeve van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden (zie Wbp, artikel 2.2.a).

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.

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



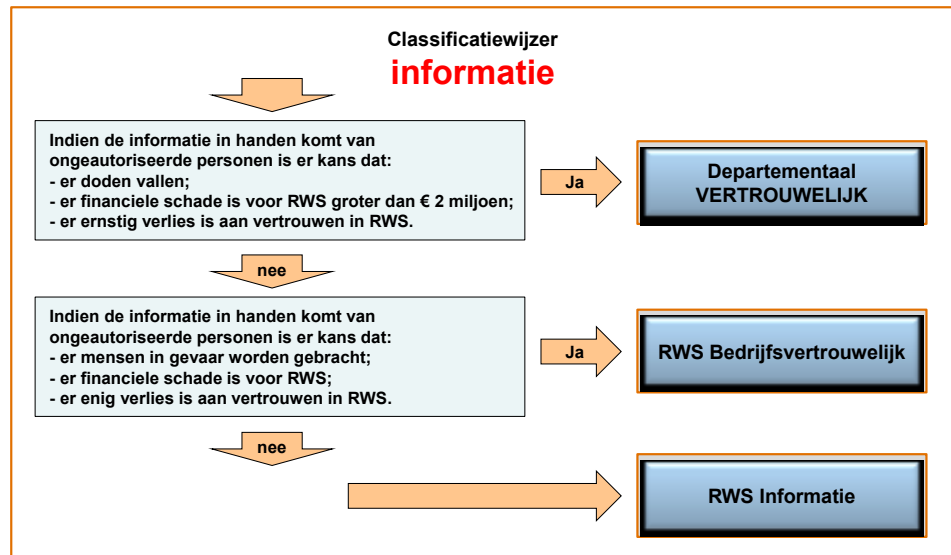
Figuur 1: Classificatiewijzer

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

1. Classificatiewijzer informatie
2. Classificatiewijzer persoonsgegevens

2.4.1.1. 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.



Figuur 2: Classificatiewijzer informatie

Voorbeelden Departementaal VERTROUWELIJK

- Afstemming van interdepartementale vertrouwelijke bestuursstukken.
- 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.

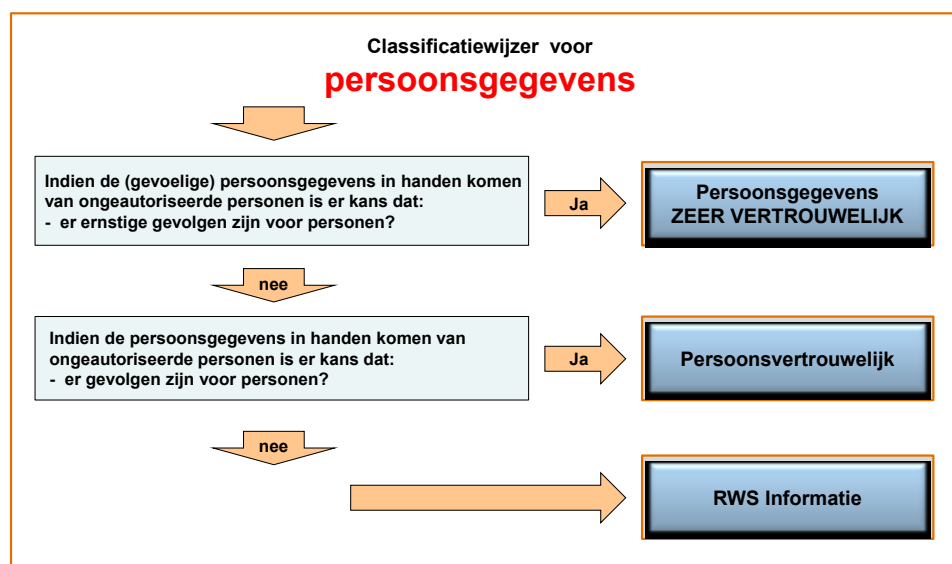
Belangrijk: Volgens de VIR-BI dient Departementaal VERTROUWELIJK informatie door een lijnmanager (gedelegeerde rubriceringsambtenaar) te worden vastgesteld. Indien de lijnmanager onzeker is over het classificatieniveau dient advies te worden gevraagd aan de RWS beveiligingscoördinator van Centrale Coördinatie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

2.4.1.2. 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 Wet bescherming persoonsgegevens. 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 Wet bescherming persoonsgegevens.

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



Figuur 3: classificatiewijzer persoonsgegevens

Hieronder enkele voorbeelden van geclassificeerde persoonsgegevens.

Voorbeelden Persoonsgegevens ZEER VERTROUWELIJK:

- Medische gegevens
- Financiële gegevens van personen
- Stigmatiserende gegevens zoals geloof, etniciteit, strafbaar verleden, ..
- Inloggegevens van bijvoorbeeld IT diensten, bank, overheid, ..
- Identiteitsgegevens zoals BSN, ID kaart, paspoort, ...
- Integriteitsonderzoeken naar een persoon

Voorbeelden van Persoonsvertrouwelijk:

- Sollicitatiebrieven
- Personeelsadministratie
- Salarisadministratie

Voorbeelden van RWS Informatie met niet gevoelige persoonsgegevens:

- Zakelijk e-mailadres
- Zakelijk telefoonnummer
- Zakelijk werklocatie

Opmerkingen:

- (bijzondere) Persoonsgegevens dienen te worden verwerkt door informatie-systemen die voldoen aan de vereiste beveiligingsnormen (o.b.v. Privacy Impact Assessment) waarbij passende beveiligingsmaatregelen genomen zijn.
- Systemen die (bijzondere) persoonsgegevens verwerken dienen te zijn ge-meld aan de privacy coördinatoren.

- Gebruikers worden in staat gesteld om (bijzondere) persoonsgegevens te classificeren en overeenkomstige markering aanbrengen op de bestanden.

2.4.2

Stap 2: Vaststellen herzieningsdatum vertrouwelijkheid

OPMERKING: (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.

Vertrouwelijkheidskenmerk	Herzieningsdatum
Departementaal VERTROUWELIJK	na 5 jaar heroverwegen
RWS Bedrijfsvertrouwelij	geen
RWS Informatie	geen
Persoonsgegevens ZEER VERTROUWELIJK	nog nader te bepalen*
Persoonsvertrouwelij	nog nader te bepalen*

Opmerking*: De herzieningsdatum van persoonsgegevens is op voorhand moeilijk te bepalen. Deze is onder andere afhankelijk van de gevoeligheid en de aard van de gegevens. In veel gevallen zal er geen herzieningsdatum voor persoonsgegevens zijn. Het kan echter voorkomen dat (naar aanleiding van gebeurtenissen) persoonsgegevens in de loop der tijd meer of minder gevoelig worden en dat deze opnieuw dienen te worden geclassificeerd. In het geval een persoon overlijdt is het ook niet op voorhand te bepalen of openbaarmaking van de persoonsgegevens er (ernstige) gevolgen zijn voor bijvoorbeeld familieleden.

2.4.3

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!):

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:

Overige vertrouwelijke documenten:

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

Auteur: Datum: Vertrouwelijkheid:

2.4.3.1.

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.

2.4.4

Stap 4: Verwerken volgens vastgestelde informatieklassse

De informatieklassse (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 gecijferd; of het met externe partijen mag worden gedeeld; etc. De wijze van verwerking per informatieklassse 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 white board) 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.

2.4.5

Stap 5: Vertrouwelijkheid en informatieklassie 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.*

3 IBR-2: Beleid voor logische toegangsbeveiliging

3.1 Doelgroep

Personeel dat voor de Prestatie programmatuur of andere soorten informatiesystemen met toegangsbeveiliging ontwikkelt of configureert.

3.2 Doel

Deze richtlijn heeft als doel om inzicht te bieden en richting te geven aan de maatregelen op het gebied van logische toegangsbeveiliging die medewerkers van de opdrachtnemer moeten nemen bij het ontwikkelen en/of configureren van programmatuur of andere soorten informatiesystemen.

3.3 Scenario's

De richtlijnen hieronder beschreven moeten verwerkt zijn in alle op te leveren programmatuur of andere informatiesystemen waarin gebruik wordt gemaakt van logische toegangsbeveiliging.

3.4 Richtlijnen

De richtlijnen te implementeren binnen de ontwikkelprocessen zijn de volgende:

- 9.4.2.1 De inlogprocedure behoort geen systeem- of toepassingsidentificatie te tonen voordat het inlogproces met succes is afgerond.
- 9.4.2.2 De inlogprocedure behoort een algemene waarschuwing te tonen dat gebruik van het informatiesysteem enkel is toegestaan voor expliciet door de organisatie geautoriseerde personen en vastgestelde doeleinden.
- 9.4.2.3 De inlogprocedure behoort tijdens de inlogprocedure geen hulpboodschappen weer te geven waarmee onbevoegde gebruikers hun doel kunnen bereiken.
- 9.4.2.4 De inlogprocedure behoort de inloginformatie pas na invoer van alle gegevens te valideren. Indien zich een fout voordoet, behoort het systeem niet aan te geven welk deel van de gegevens juist of onjuist is.
- 9.4.2.5 De inlogprocedure behoort een account minimaal 10 minuten te blokkeren nadat voor een gebruikersnaam 5 keer achtereenvolgend een foutief wachtwoord is gegeven is. Indien er geen lock-out periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lock-out op te heffen of het wachtwoord te resetten.
- 9.4.2.6 De inlogprocedure behoort niet-succesvolle en succesvolle pogingen te registreren.
- 9.4.2.7 De inlogprocedure behoort een informatiebeveiligingsgebeurtenis te initiëren als een poging tot of een succesvolle schending van de inlogbeheersmaatregelen is vastgesteld.
- 9.4.2.8 De inlogprocedure behoort na een succesvolle login de datum en tijd van de voorgaande login of loginpoging te tonen.
- 9.4.2.9 De inlogprocedure behoort een wachtwoord dat wordt ingevoerd niet weer te geven.
- 9.4.2.10 De inlogprocedure behoort geen ongecodeerde wachtwoorden op te

- slaan of via een netwerk te versturen.
- 9.4.2.11 De inlogprocedure behoort inactieve sessies na 15 minuten van inactiviteit te vergrendelen dan wel te beëindigen.
- 9.4.2.12 De inlogprocedure behoort de maximale verbindingstijd te beperken.
- 9.4.2.SC-1 Toegang tot kritische toepassingen of toepassingen met een hoog belang wordt verleend op basis van twee-factor authenticatie.

4 IBR-3: Beleid voor wachtwoordgebruik

4.1 Doelgroep

Personeel met een rol in het leveren van de Prestatie.

4.2 Doel

Het doel van het beleid voor wachtwoordgebruik is tweeledig:

1. Gebruikers behoren correct om te gaan met geheime authenticatiegegevens;
2. Authenticatiemechanismen, waar gebruik wordt gemaakt van wachtwoorden als authenticatiemiddel, behoren interactief te zijn en sterke wachtwoorden te af te dwingen.

4.3 Scenario's

De richtlijnen hieronder beschreven moeten worden verwerkt in procedures, systeemeisen en bewustwordingstrajecten op het gebied van de informatiebeveiliging. Hierna worden ook nog een aantal tips gegeven die kunnen worden meegenomen in bewustwordingstrajecten.

4.4 Richtlijnen

De richtlijnen voor wachtwoordgebruik zijn opgedeeld in generieke en specifieke richtlijnen. Alle accounts moeten voldoen aan zowel de generieke richtlijnen, als de specifieke richtlijnen die bij het accounttype horen.

De generieke richtlijnen zijn de volgende:

- Wachtwoorden moeten minimaal vier van de volgende 5 soorten karakters bevatten:
 - gewone letters
 - hoofdletters
 - getallen
 - punctuatie (bijvoorbeeld: ";',!)
 - speciale karakters (bijvoorbeeld: "@#\$%^&*<>~+=)
- Hergebruik van hetzelfde wachtwoord op vervangingsmomenten is niet toegestaan.
- Standaard/default accountnamen en wachtwoorden worden uitgeschakeld of na eerste gebruik tijdens installatie gewijzigd; na de initiële installatie van een informatiesysteem mag er dus geen default accountnaam en wachtwoord meer aanwezig zijn in het component.
- Alle standaard fabrieksaccounts moeten worden vervangen door persoonlijke accounts en wachtwoorden. Tevens dient voor de onderkende accounttypen de aangegeven duur voor wachtwoordvervanging alsmede de wachtwoordlengte aangehouden te worden.

Alle accounts dienen in een onderstaande account-type te worden ingedeeld en te voldoen aan de specifieke richtlijnen die aan het betreffende type account gesteld worden. Deze specifieke richtlijnen komen bovenop de generieke richtlijnen.

- **Applicatiebeheeraccount**

- Omschrijving: Een persoonlijk account dat wordt gebruikt om applicaties op systemen te beheren
- Soort: persoonsgebonden (terug te herleiden naar een individu)

- Wachtwoord vervangtermijn: 30 dagen
- Wachtwoordlengte: minimaal 15 tekens
- **Systeemaccount (service/applicatie account)**
 - Omschrijving: Een account dat ervoor zorg draagt dat een applicatie zonder menselijke interventie applicatieopdrachten kan uitvoeren onder speciale rechten.
 - Soort: service
 - Wachtwoord vervangtermijn: 365 dagen
 - Wachtwoordlengte: minimaal 15 tekens
- **Administratoraccount**
 - Omschrijving: Een persoonlijk account dat op de systemen volledig beheer heeft d.m.v. administrator rechten.
 - Soort: persoonsgebonden (terug te herleiden naar een individu)
 - Wachtwoord vervangtermijn: 30 dagen
 - Wachtwoordlengte: minimaal 15 tekens
- **Kantoorautomatiseringsaccount (KA-account)**
 - Omschrijving: Het persoonlijke gebruikers account waarmee men kan werken op een kantoorautomatiseringsomgeving.
 - Soort: persoonsgebonden (terug te herleiden naar een individu)
 - Wachtwoord vervangtermijn: 90 dagen
 - Wachtwoordlengte: minimaal 8 tekens

Bij informatiesystemen waar niet voldaan kan worden aan de generieke en specifieke wachtwoordeisen, moet een risico-inschatting worden gemaakt en compenserende maatregelen worden getroffen. De afwijkingen moeten worden gedocumenteerd en gecommuniceerd.

4.5

Tips bij gebruik van wachtwoorden

De effectiviteit van bovengenoemde richtlijnen vallen of staan bij de manier hoe met wachtwoorden wordt omgegaan. Daarom volgen hier nog een aantal tips over hoe sterke wachtwoorden goed kunnen worden onthouden, beschermd en gewijzigd.

Onthouden van sterke wachtwoorden:

- Maak een wachtwoord dat is gebaseerd op een songtekst of een rijmpje. Zet de eerste letters van ieder woord achterelkaar, en probeer letters door cijfers te vervangen (bijvoorbeeld het rijmpje "Als het regent in mei is april voorbij en leggen alle vogels een ei" wordt "Ahri5i4velavee", waarbij de maanden zijn vervangen door cijfers).
- Maak een zin (een zogenaamde *passphrase*) in plaats van een wachtwoord (*password*). Typ de woorden van een makkelijke zin achterelkaar en vervang woorden of letters door hoofdletters, getallen of leettertekens (bijvoorbeeld: 03KleineKleutertjesdiezatenopeen###).

Beschermen van wachtwoorden:

- Gebruik voor je bedrijfs-account niet hetzelfde wachtwoord als voor je privéaccounts (bijvoorbeeld: persoonlijke Gmail, Facebook, ANWB site, Bol.com, etc.).
- Gebruik binnen het bedrijf niet overal hetzelfde wachtwoord. Gebruik een verschillend wachtwoord voor je gewone desktopomgeving, je bedienplek of je Yammer account.
- Deel je wachtwoord met niemand, tenzij dit is vereist volgens de procedures.

- Wachtwoorden mogen nooit worden opgeschreven of digitaal worden opgeslagen zonder te zijn gecijferd.
- Schrijf nooit een wachtwoord in e-mail, chat of ander communicatiemiddel.
- Praat niet over je wachtwoord, geef geen hints over je wachtwoord aan anderen.
- Als het niet anders kan en wachtwoorden moeten toch worden opgeslagen (bijvoorbeeld omdat dat volgens een veiligheidsprocedure moet), sla een wachtwoord dan op in een fysieke kluis of een speciaal daarvoor ontwikkelde beveiligde applicatie.
- Als een wachtwoord in een kluis wordt opgeslagen, zorg er dan voor dat de sleutel niet eenvoudig te vinden is of dat de kluis op een andere locatie staat.
- Als een wachtwoord in een beveiligde applicatie wordt opgeslagen, dan is er vaak weer een wachtwoord nodig om die applicatie te openen. Daarvoor geldt wederom de wachtwoordrichtlijn.

Wat dus *niet* mag gebeuren:

- Het wachtwoord is opgeschreven en ligt binnen handbereik (en de hacker die fysiek binnendringt, kan het wachtwoord ook gemakkelijk vinden).
- Het wachtwoord van 15 karakters is opgeslagen in een applicatie dat is beveiligd met 8 karakters (en daarmee is de wachtwoordlengte gereduceerd tot 8 karakters, want nu hoeft de hacker alleen nog een wachtwoord van 8 karakters te kraken om bij het wachtwoord van 15 karakters te komen).
- Het wachtwoord is opgeslagen in een document op een gezamenlijke schijf of op Sharepoint (en de hacker kan het op afstand of ter plaatse ook vinden. Op afstand heeft hij alle tijd om rustig op zoek te gaan).

Wijzigen van wachtwoorden:

Als het afdwingen van wijzigen van wachtwoorden niet automatisch wordt afgedwongen, zorg dan dat het procedureel wordt afgedwongen. Dit kan simpelweg door zelf (bijvoorbeeld op de eerste maandag van de maand) het wachtwoord te wijzigen.

5 IBR-4: Richtlijnen voor beveiligen bij ontwikkelen

5.1 Doelgroep

Personeel dat voor de Prestatie programmatuur of andere soorten informatiesystemen ontwikkelt.

5.2 Doel

Deze richtlijn heeft als doel om inzicht te bieden en richting te geven aan de maatregelen die medewerkers van de opdrachtnemer moeten nemen bij het ontwikkelen van programmatuur of andere soorten informatiesystemen.

5.3 Scenario's

De richtlijnen hieronder beschreven moeten worden verwerkt in de processen die worden gehanteerd bij het ontwikkelen van programmatuur of andere informatiesystemen.

5.4 Richtlijnen

De richtlijnen te implementeren binnen de ontwikkelprocessen zijn de volgende:

- 14.2.1 Wederpartij dient voor het ontwikkelen van het Product besteld door Opdrachtgever over een operationeel geborgd ontwikkelproces te beschikken waarin ook informatiebeveiliging is geïntegreerd, en welke in het specifieke geval van Programmatuur ten minste de processen bevat uit één van de onderstaande normenkaders:
 - 1. CIP, "*Grip op Secure Software Development (SSD) – Het proces*" [1];
 - 2. Secure Software Foundation, "*Framework Secure Software*" [2];
 - 3. OWASP, "*Software Assurance Maturity Model (SAMM)*" [3].
- 14.2.5 Wederpartij dient geborgde *engineering principles* voor beveiligde apparatuur en programmatuur te hebben voor de Implementatie van de Prestatie.
- 14.2.6 Wederpartij dient een beveiligde ontwikkelomgeving te hebben en passend te beveiligen voor verrichtingen op het gebied van apparatuur- en programmatuurontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de Prestatie.
- 14.2.7 Door Opdrachtgever uitbestede ontwikkeling van het Product aan Wederpartij staat onder supervisie van Opdrachtgever en dient door hen gemonitord te kunnen worden.
- 14.2.8 Wederpartij dient tijdens alle ontwikkelactiviteiten en -iteraties aantoonbaar te toetsen op alle relevante beveiligingseisen uit de actuele versie van het CIP document *Grip op SSD - Beveiligingseisen voor (web)applicaties* [4], en de door Opdrachtgever bestelde beveiligingsfunctionaliteit [5] te testen.
- 14.2.9 Wederpartij dient voor nieuwe apparatuur en programmatuur, upgrades en nieuwe versies betrokken bij de Prestatie, aantoonbaar programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te hebben vastgesteld. Hierbij moet ook rekening worden gehouden met naastliggende apparatuur en programmatuur in een keten, en onder- en/of bovenliggende programmatuur in een *software stack*.

5.5

Bronnen bij IBR-4

In de eisen in richtlijn IBR-4 wordt verwezen naar de onderstaande bronnen.

Nummer	Bron
[1]	CIP, "Grip op Secure Software Development (SSD): De Methode v2.0 – De Opdrachtgever aan het Stuur", URL: " https://www.cip-overheid.nl/wp-content/uploads/2015/05/Grip-op-SSD-Het-proces-v2.0.pdf "
[2]	Secure Software Foundation, "Framework Secure Software", URL: " https://www.securesoftwarefoundation.org/index.php/framework-secure-software/ "
[3]	OWASP, "OWASP Top 10", URL: " https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project "
[4]	CIP, "Grip op SSD - Beveiligingseisen voor (web)applicaties", URL: " http://www.cip-overheid.nl/wp-content/uploads/2014/10/Grip-op-SSD-Beveiligingseisen-v2_0.pdf "
[5]	Door Opdrachtgever bestelde beveiligingsfunctionaliteit: n.t.b.

6 IBR-5: Richtlijnen voor informatiebeveiligingsincidenten

6.1 Doelgroep

Personeel met een rol in het incidentproces, indien dit contractueel onderdeel uitmaakt van de Prestatie.

6.2 Doel

Deze richtlijn heeft als doel om richting te geven aan de processen die moeten worden ingericht om doeltreffend met informatiebeveiligingsincidenten om te gaan.

6.3 Scenario's

De richtlijnen hieronder beschreven moeten worden verwerkt in de processen die worden gehanteerd als respons op informatiebeveiligingsincidenten.

6.4 Richtlijnen

De richtlijnen te implementeren voor de omgang met informatiebeveiligingsincidenten zijn de volgende:

- 16.1.1 Wederpartij dient voor de Prestatie een operationeel geborgd informatiebeveiligingsincidentproces te hebben waarin ook directieverantwoordelijkheden en –procedures zijn vastgesteld om een snelle, doeltreffende en ordelijke respons te bewerkstelligen.
- 16.1.2 Wederpartij dient informatiebeveiligingsgebeurtenissen relevant voor de Prestatie zo snel mogelijk, maar binnen de limiet gesteld in de SLA en via de hierin beschreven route, te rapporteren aan het *Security Operations Centre* (SOC) van Opdrachtgever.
- 16.1.3 Wederpartij dient van Personeel die gebruikmaken van informatiesystemen en processen betrokken bij de Prestatie te eisen dat zij hierin waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreert en rapporteert aan het *Security Operations Centre* (SOC) van Opdrachtgever.
- 16.1.4 Wederpartij dient een operationeel geborgd proces te hebben voor het beoordelen van informatiebeveiligingsgebeurtenissen bij informatiesystemen betrokken bij de Prestatie, en welke criteria bevat voor het classificeren hiervan als informatiebeveiligingsincidenten. Datalekken behoren hierin de hoogste classificatie te hebben.
- 16.1.5 Wederpartij dient in overeenstemming met de gedocumenteerde procedure te reageren op informatiebeveiligingsincidenten bij informatiesystemen betrokken bij de Prestatie.
- 16.1.6 Wederpartij dient een operationeel geborgd proces te hebben voor het gebruik van de opgedane kennis, die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen, om de waarschijnlijkheid of impact van toekomstige incidenten in de dienstverlening voor Opdrachtgever te verkleinen.
- 16.1.7 Wederpartij dient operationeel geborgde procedures te hebben voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen bij informatiebeveiligingsincidenten gerelateerd aan de Prestatie.
- 16.1.SC-07 Wederpartij dient periodiek, maar ten minste jaarlijks, te oefenen met het inperken van de impact van security incidenten.

7 IBR-6: Richtlijnen voor fysieke beveiliging

7.1 Doelgroep

Personeel met een rol in het fysiek beveiligen van informatieverwerkende faciliteiten betrokken bij de Prestatie.

7.2 Doel

Deze richtlijn heeft als doel om richting te geven aan de processen die moeten worden ingericht om de fysieke beveiliging van informatieverwerkende faciliteiten betrokken bij de Prestatie, doeltreffend in te richten.

7.3 Scenario's

De richtlijnen hieronder beschreven moeten worden verwerkt in de processen die worden gehanteerd voor de fysieke beveiliging van informatieverwerkende faciliteiten.

7.4 Richtlijnen

De richtlijnen te implementeren voor de fysieke beveiliging van informatieverwerkende faciliteiten zijn de volgende:

- 11.1.2 Wederpartij dient operationeel geborgd te hebben dat beveiligde gebieden betrokken bij de Prestatie zijn beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegde Personeel toegang heeft.
- 11.1.3 Wederpartij dient operationeel geborgd te hebben dat voor kantoren, ruimten en faciliteiten waarin wordt gewerkt met informatiesystemen betrokken bij de Prestatie, fysieke beveiliging is toegepast conform ten minste de richtlijnen in norm 11.1.3 uit *ISO/IEC 27002:2013* [1].
- 11.1.4 Wederpartij dient operationeel geborgd te hebben dat fysieke bescherming van apparatuur betrokken bij de Prestatie, tegen natuurrampen, kwaadwillige aanvallen of ongelukken, is ontworpen en wordt toegepast.
- 11.1.6 Wederpartij dient operationeel geborgd te hebben dat de toegang op punten waar onbevoegde personen het terrein van Wederpartij kunnen betreden (zoals laad- en loslocaties), wordt beheerst, en deze punten zo mogelijk zijn afgeschermd van informatieverwerkende faciliteiten.
- 11.2.1 Wederpartij dient operationeel geborgd te hebben dat apparatuur betrokken bij de Prestatie, zo zijn geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, als ook de kans op onbevoegde toegang, zijn verkleind.
- 11.2.2 Wederpartij dient operationeel geborgd te hebben dat apparatuur betrokken bij de Prestatie zijn beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.
- 11.2.3 Wederpartij dient operationeel geborgd te hebben dat voedings- en telecommunicatiekabels betrokken bij de Prestatie beschermd zijn tegen verstoring of schade.
- 11.2.6 Wederpartij dient operationeel geborgd te hebben dat bedrijfsmiddelen betrokken bij de Prestatie en die zich buiten het terrein van Wederpartij bevinden, zijn beveiligd, waarbij rekening is gehouden met de

verschillende risico's van werken buiten het eigen terrein.

7.5

Bronnen bij IBR-5

In de eisen in richtlijn IBR-5 wordt verwezen naar de onderstaande bronnen.

Nummer	Bron
[1]	NEN, "ISO/IEC 27002:2013: IT Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging", URL: " https://www.nen.nl/NEN-Shop/Norm/NENISOIEC-270022013C22015-nl-1.htm "

8 IBR-7: Richtlijnen voor logging

8.1 Doelgroep

Personeel met een rol in het inrichten van informatiesystemen betrokken bij de Prestatie.

8.2 Doel

Deze richtlijn heeft als doel om de minimale eisen te definiëren voor het inrichten van logging op informatiesystemen betrokken bij de Prestatie.

8.3 Scenario's

De richtlijnen hieronder beschreven moeten worden verwerkt in de configuraties van informatiesystemen betrokken bij de Prestatie.

8.4 Richtlijnen

De richtlijnen te implementeren voor logging op informatiesystemen zijn de volgende:

- 12.4.1a Wederpartij dient operationeel geborgd te hebben dat alle informatiesystemen betrokken bij de Prestatie, logdata in logbestanden wegschrijven over ten minste de volgende gebeurtenissen:
- a. Gebruik van technische en functionele beheerfuncties en systeemhulpmiddelen zoals:
 - uitvoeren van een systeemcommando;
 - het wijzigen van een configuratie of instelling;
 - het starten en stoppen van services, applicaties, daemons, etc.;
 - het uitvoering van een back-up of restore;
 - (tijdelijke) toekenning en gebruikmaking van rechten die hoger zijn dan gebruikelijk (inclusief handelingen verricht met geprivilegieerde accounts; zoals *root*, *administrator*, *proddb*, etc.);
 - De release van nieuwe functionaliteit die kan ingrijpen in gegevenssets (waaronder databases).
 - b. Handelingen van beveiligingsbeheer, zoals:
 - het opvoeren en afvoeren van gebruikers;
 - toekennen en intrekken van toegangsrechten;
 - resets van wachtwoorden;
 - uitgifte en intrekken van cryptografische sleutels.
 - c. Beveiligingsovertredingen, zoals:
 - de constatering van *malware*;
 - een *portscan* of *vulnerability scan*;
 - zowel foutieve als succesvolle (deze laatste is geen overtreding, maar wel nuttige informatie) inlogpogingen;
 - overschrijding van autorisatiebevoegdheden;
 - geweigerde pogingen om toegang te krijgen;
 - het gebruik van niet-operationele systeemservices;
 - het starten en stoppen van security- en database services.
 - d. Gebeurtenissen die verstoring in het productieproces veroorzaken of gaan veroorzaken, zoals:
 - systeemfouten en het vollopen van wachtrijen;
 - onverwacht afbreken van programmatuur in uitvoering;

- het niet-beschikbaar zijn van aangeroepen programmaonderdelen of systemen.
 - e. Handelingen van gebruikers, zoals:
 - verleende toegangsrechten;
 - gebruik van *online* transacties;
 - toegang tot gegevensbestanden door systeembeheerders.
 - f. Handelingen die de integriteit van logging aantasten, zoals:
 - Verwijderen van loggegevens;
 - Wijzigingen in logbestanden anders dan door het hiervoor geautoriseerde service account.
- 12.4.1b Wederpartij dient operationeel geborgd te hebben dat alle weggeschreven logregels ten minste de volgende componenten bevatten:
- **Wanneer**
 - Tijd en datum;
 - *Optioneel: Interaction Identifier* (middel om gebeurtenissen aan unieke gebruikers te kunnen koppelen);
 - **Waar**
 - Naam van het informatiesysteem, eventueel aangevuld met de versie;
 - IP adres van het informatiesysteem;
 - *Optioneel: Werkstationnaam, servernaam of DNS-naam;*
 - *Optioneel: Naam van service of protocol, of nummer van TCP/UDP port;*
 - *Optioneel: Gebruikte module, pagina, formulier, method of dialogboxnaam;*
 - *Optioneel: Geografische locatie;*
 - **Wie**
 - Bronadres waar de opdracht vandaan komt (IP adres, telefoonnummer, etc.);
 - *User Identifier* dat gebruikt is om de opdracht uit te voeren;
 - **Wat**
 - Zwaarte van de gebeurtenis (*fatal, error, warning, info, etc.*);
 - Omschrijving van de gebeurtenis;
 - Resultaat (*succes, failure*).
- 12.4.1c Wederpartij dient operationeel geborgd te hebben dat logbestanden ten minste drie maanden worden bewaard. Informatiesystemen die verantwoordelijk zijn voor de opslag van logdata moeten hiertoe zijn voorzien van een alarmering die, ruim voordat de opslagruimte is volgelopen, aangeeft dat ingegrepen moet worden om verlies van logdata tegen te gaan.
- 12.4.1d Wederpartij dient operationeel geborgd te hebben dat passende maatregelen worden genomen om persoonsgegevens of andere gevoelige informatie te verwijderen uit logdata of deze onleesbaar te maken. Het gaat hierbij om de onderstaande typen data:
- Privacygevoelige gegevens die niet noodzakelijk zijn om de taak uit te voeren;
 - Gegevens die de beveiliging van informatiesystemen kunnen aantasten, zoals wachtwoorden, inbelnummers, encryptiesleutels, toegangscode's, etc.;
 - Gegevens die gevoelig zijn voor misbruik, zoals creditcardnummers, bankrekeningnummers, etc.
- 12.4.2a Wederpartij dient operationeel geborgd te hebben dat logbestanden en -faciliteiten op apparatuur betrokken bij de Prestatie beschermd zijn tegen deactivatie, wijziging, wissen en onbevoegde toegang. Uitsluitend service accounts, die bedoeld zijn voor het wegschrijven van logdata, hebben schrijftoegang tot logbestanden. Alleen accounts met daartoe

- geautoriseerde rollen hebben leestoeegang tot de logbestanden.
- 12.4.2b Wederpartij dient operationeel geborgd te hebben dat het *vierogenprincipe* van toepassing is op wijzigingen in configuraties van logfaciliteiten.
- 12.4.3 Wederpartij dient operationeel geborgd te hebben dat activiteiten van systeembeheerders en -operators op informatiesystemen betrokken bij de Prestatie worden vastgelegd in beschermde logbestanden die zij niet zelf kunnen wijzigen, wissen, of deactiveren.
- 12.4.4 Wederpartij dient operationeel geborgd te hebben dat de klokken van alle informatiesystemen betrokken bij de Prestatie zijn gesynchroniseerd met ten minste een *Stratum 3* internet-tijdserver. De tijdzone moet ook correct ingesteld zijn; voor Nederland en West Europa is dit UTC+01:00 (ook CEST genoemd).