

## Informatiebeveiligingsplan BRP en waardedocumenten

### 1. Inleiding

#### 1.1 Vooraf

Dit informatiebeveiligingsplan is een actualisering van het plan dat op 22 januari 2013 door burgemeester en wethouders is vastgesteld onder nummer DV/PBO/2013001739.

Het plan is herschreven, minder beschrijvend en meer toegespitst op het onderkennen van veiligheidsrisico's en het nemen, uitvoeren en onderhouden van passende of verplichte beveiligingsmaatregelen in de uitvoeringspraktijk van de BRP en waardedocumenten. Daarvoor sluit het plan aan op het ISO kwaliteitssysteem van de afdeling.

#### 1.2 Begripsbepalingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BIO	Baseline informatiebeveiliging overheden
BBN 2	Basisbeveiligingsniveau2: bescherming van gegevens en andere te beschermen belangen in de processen van de overheid, waarin o.a. vertrouwelijkheid aan de orde is, omdat het om gevoelige informatie gaat (Zie bijlage B voor alle niveaus)
BRP	Basisregistratie personen
DPIA	Data protectie en Impact Analyse. Betreft informatiebeveiligingsvragen over de inrichting en beveiliging van systemen waarin de persoonsgegevens worden opgeslagen
ENSIA	Eenduidige Normatiek Single Information Audit
Fraude	Door kwaadwillenden worden misleid (externe fraude), of - al dan niet onder druk van chantage, bedreiging of omkoping - misbruik maken van eigen bevoegdheden (interne fraude).
ISO-kwaliteitssysteem	ISO 9001:2015 is een internationale kwaliteitsnorm. In deze norm staan eisen om kwaliteitsmanagementsystemen te standaardiseren, meetbaar en controleerbaar te maken. In 2015 is de norm vernieuwd en gepubliceerd. De afdeling gebruikt deze norm als ijkpunt voor de kwaliteit en continuïteit van de bedrijfsvoering.
KZS	Kwaliteitszorgsysteem
PNIK	Paspoorten en Nederlandse identiteitskaarten
PUN	Paspoort Uitvoeringsregeling Nederland
RR	Reglement Rijbewijzen
RvIG	Rijksdienst voor Identiteitsgegevens
Verantwoordelijke	De informatiebeheerder volgens art. 2 van de beheerregeling basisregistratie personen, tevens afdelingshoofd
Waardedocumenten	Identiteitsdocumenten volgens de Wet op de Identificatieplicht: reisdocumenten (Nederlands paspoort, Nederlandse identiteitskaart, Nederlands Vreemdelingendocument) en Nederlandse rijbewijzen. Voor apart vermelde documenten gelden specifiek wettelijke bepalingen.
Zelfevaluatie BRP	Onderzoek naar de inrichting, verwerking en beveiliging van de Basisregistratie personen

#### 1.3 Wettelijk kader en verantwoordelijken

##### 1.3.1 Toepasselijke wet- en regelgeving

De AVG vormt het algemeen kader voor de verwerking van persoonsgegevens. De verplichting tot beveiliging van persoonsgegevens is geregeld in artikel 5, lid 1 onder f van de AVG.

Naast het algemeen kader van de AVG zijn voor dit plan specifiek de *Wet BRP*, de *Paspoortwet*, de *PUN* en het *RR* van toepassing. De AVG is beperkt van toepassing op de verwerking van persoonsgegevens en gegevens over waardedocumenten in de gemeentelijke onderdelen van de BRP. Zie hiervoor artikel 40 van de beheerregeling BRP.

##### 1.3.2 Beleid

Het te beveiligen object (zie voor nadere uitleg par. 1.4.1) staat als informatievoorziening niet op zichzelf, maar is ingebed in het geheel van de gemeentelijke informatievoorziening en landelijke voorzieningen. Dit plan is een tactische uitwerking van het strategisch gemeentelijk informatiebeveiligingsbeleid en het Privacyreglement Haarlem voor het te beveiligen object.

De BIO beschrijft het basisnormenkader voor informatiebeveiliging van overheden gebaseerd op standaarden en kwaliteitseisen.

### 1.3.3 Verantwoordelijken

De verantwoordelijke bestuursorganen voor de BRP zijn burgemeester en wethouders. De Paspoortwet en het Reglement rijbewijzen vallen onder de verantwoordelijkheid van de burgemeester.

De afdelingsmanager Klantcontactcentrum is door burgemeester en wethouders gemandateerd als beheerder van de BRP en de waardedocumenten, alsmede aangewezen als informatiebeheerder BRP (Beheerregeling BRP) en in die hoedanigheden verantwoordelijke voor de uitvoering van dit plan.

De beveiligingsbeheerder BRP en de beveiligingsfunctionaris waardedocumenten worden door het college van burgemeester en wethouders, respectievelijk de burgemeester van Haarlem aangewezen en zijn belast met het toezicht op de naleving van dit plan. De rol en bevoegdheden van de beveiligingsbeheerder BRP staan beschreven in de artikelen 31 tot en met 35 van de beheerregeling BRP. Voor de beveiligingsfunctionaris waardedocumenten staan taken en bevoegdheden in hoofdstuk 4 van dit plan.

De AP kan de verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens, bij gemeenten het college van B&W of de burgemeester, aanspreken op het niveau van de maatregelen ter beveiliging van de verwerking van persoonsgegevens, en op de wijze waarop het stelsel van maatregelen is geïmplementeerd en wordt nageleefd.

Medewerkers in de taakuitvoering van het te beveiligen object werken volgens de beschreven werkprocessen. Hierin zijn veiligheidsmaatregelen in de vorm van procedures en -instructies vastgelegd. Deze procesbeschrijvingen zijn eenvoudig raadpleegbaar in het KZS ter ondersteuning van de medewerker tijdens de taakuitvoering.

## 1.4 Wat en waarom beveiligen?

### 1.4.1 Te beveiligen object

Het object van beveiliging betreft:

- het samenhangend geheel van middelen, processen, gegevens en logica voor het uitvoeren van de wettelijke taken van de BRP en waardedocumenten;
- Deze taken betreffen het registreren, onderhouden en actualiseren van persoonsgegevens; het verstrekken van persoonsinformatie aan betrokkenen, belanghebbenden met een gerechtvaardigd belang en geautoriseerde in- en externe afnemers; alsmede het vaststellen van identiteit en het afgeven, innemen en registreren van waardedocumenten.

### 1.4.2 Doel van de beveiliging

Het doel van dit plan is om beveiligingsmaatregelen te treffen die mogelijke veiligheidsrisico's voor de continuïteit en het gewenste kwaliteitsniveau van het object van beveiliging terug brengen naar een aanvaardbaar niveau. Beveiligingsmaatregelen richten zich daarvoor op de volgende vier algemene beheersaspecten van de bedrijfsvoering:

1. *Beschikbaarheid en continuïteit:* ervoor zorgen dat informatie en informatie verwerkende bedrijfsmiddelen voor gebruikers beschikbaar zijn op de juiste tijd en plaats.
2. *Integriteit en betrouwbaarheid:* het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en van informatieverwerking.
3. *Vertrouwelijkheid en exclusiviteit:* het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor diegenen die ertoe geautoriseerd zijn.
4. *Controleerbaarheid:* de mate waarin de juistheid en volledigheid van de informatie kunnen worden gecontroleerd. De mate waarin de verwerking van de gegevens kan worden gereconstrueerd.

## 2. Beheersing veiligheidsrisico's

### 2.1 Mogelijke veiligheidsrisico's

Het object van dit plan kent de volgende categorieën van veiligheidsrisico's. De cijfers 1 tot en met 4 corresponderen met de beveiligingsdoelen in paragraaf 1.4.2.

- (1) Verstoringe calamiteiten, zoals door blikseminslag, stroomuitval, brand en explosie
- (1) Verstoringe overlast van stof, vuil en water
- (1) Systeemstoringen en fouten
- (2) Onkundig gebruik, te laag kennisniveau, onvoldoende privacy- en veiligheidsbewustzijn
- (2) Onvoldoende mutatiecontrole, ontbreken vier-ogen-principe
- (2) Ontbrekende of onvolledige beschrijving werkprocessen, veiligheidsprocedures en instructies
- (2) Onvoldoende beschikbaarheid en raadpleegbaarheid van procesbeschrijvingen
- (3) Sabotages, zoals: hacking, gijzeling, afpersing en virussen

- (3) Onbevoegd gebruik van systemen en toegang tot werkruimtes
- (3) Fraude, diefstal, datalekken en phishing
- (4) Ontbreken van backup, uitwijk en logging van mutaties,
- (4) Ontbreken van aanvragen, aangiften, mutatieverslagen en brondocumenten

## 2.2 Risicoanalyse en dreigingsprofiel

De veiligheidsrisico's voor het te beveiligen object brengt het lijnmanagement jaarlijks in kaart door de dreigingscategorieën te kwantificeren. Daarvoor wordt de kans dat een dreiging zich voordoet en de gevolgen daarvan ingeschat volgens de formule:  $Risico = Kans \times Gevolg$ .

Hieruit ontstaat een dreigingsprofiel waarop de verantwoordelijke maatregelen voor verzachting van de veiligheidsrisico's neemt en van prioriteit voorziet. De BIO is te gebruiken als hulpmiddel bij het bepalen van relevante, proportionele beveiligingsmaatregelen.

De risicoanalyse en de daaruit volgende maatregelen zijn onderdeel van de uitvoeringsagenda en acties van het kwaliteitssysteem van de afdeling. Input voor de risicoanalyse komt onder meer uit:

- De status van de risicobeperkende maatregelen (zie bijlage 1);
- De uitkomsten van de jaarlijkse controles (zie hoofdstuk 3.2);
- Verzamelde incidentmeldingen;
- Informatie van de security- en privacyofficieren;
- Landelijke bronnen

## 2.3 Risicobeperkende maatregelen

### 2.3.1 Uitvoering risicobeperkende maatregelen

De risicobeperkende maatregelen leiden ertoe dat medewerkers in de taakuitvoering van het te beveiligen object de voorgeschreven veiligheidsprocedures en -instructies volgen.

- De veiligheidsmaatregelen zijn beschreven en vastgelegd in de procedures, instructies en procesbeschrijvingen binnen het kwaliteitssysteem;
- De in de PUN en het RR voorgeschreven functiescheidingen (zie hoofdstuk 5) zijn eveneens in het kwaliteitssysteem beschreven en vastgelegd;
- Medewerkers kunnen deze procesbeschrijvingen eenvoudig raadplegen ter ondersteuning van de taakuitvoering;
- Actualisering van bestaande veiligheidsmaatregelen geschiedt volgens de jaaragenda van het kwaliteitssysteem van de afdeling;
- Wanneer de uitvoering van een veiligheidsmaatregel niet onder de eigen uitvoeringsverantwoordelijkheid valt stelt de verantwoordelijke deze maatregel als eis aan de daarin faciliterende partij;
- De faciliterende partij moet op verzoek aan verantwoordelijke kunnen aantonen dat de maatregel bestaat en uitgevoerd wordt.

### 2.3.2 Soorten risicobeperkende maatregelen

De risicobeperkende maatregelen vallen uiteen in verschillende soorten:

- Procedures en instructies bij de taakuitvoering voor de BRP
- Procedures en instructies bij de taakuitvoering voor de Waardedocumenten
- Algemene procedures en instructies voor de afdeling Klantcontactcentrum
- Eisen aan procedures en instructies voor faciliterende afdelingen en partijen.

In bijlage 1 van dit plan staat een actueel overzicht van maatregelen per soort en hun status.

## 3. Normenkader en controlesystematiek

### 3.1 Normenkader

Normen voor kwaliteits- en veiligheidsmaatregelen komen uit wet- en regelgeving, het strategisch informatiebeveiligingsbeleid, de BIO en/of de accountantsopdracht.

De BIO formuleert op basis van generieke schades standaard BBN's met bijbehorende beveiligingsnormen en eisen. Per uitvoeringsproces van het te beveiligen object bepaalt verantwoordelijke het BBN (1, 2 of 3). De BIO biedt daarvoor een BBN-toets. Te nemen veiligheidsmaatregelen worden gebaseerd op BBN 2 bij het ontbreken van wettelijke normen.

### 3.2 Controlesystematiek

#### 3.2.1 Zelfevaluatie Basisregistratie Personen (BRP) door gemeenten

Jaarlijks voert verantwoordelijke de verplichte 'Zelfevaluatie BRP' uit. Het onderzoek bestaat uit vragenlijsten, bestandscontrole en inhoudelijke controle waarvan de vragen worden verwerkt in de kwaliteits-

monitor. Grondslag is artikel 4.3 wet BRP. Zie voor meer informatie: <https://www.rvig.nl/brp/zelfevaluatie-brp>

Op basis van te lage of te hoge scores op de verschillende onderdelen van de Zelfevaluatie kan de RvIG besluiten een gemeente te monitoren met als doel de oorzaken daarvan te analyseren en te werken aan verbetering.

### 3.2.2 ENSIA

Jaarlijks verantwoordt het bestuur zich en aan de gemeenteraad over beveiliging van de systemen waarin persoonsgegevens worden opgeslagen. Dit betreft daarmee ook reisdocumenten. Dit gaat volgens de verplichte ENSIA-methodiek. Tegelijk legt de gemeente hiermee verantwoording af aan de rijksoverheid. Zie voor meer informatie: [Wat is ENSIA? - ENSIA](#) en [ENSIA Cybersecurity - Digitale Overheid](#)

### 3.2.3 Zelfevaluatie Reisdocumenten

Jaarlijks voert verantwoordelijke de Zelfevaluatie Reisdocumenten uit. De vragen worden verwerkt in de Kwaliteitsmonitor van de Rijksdienst voor identiteitsgegevens (RvIG). Zie voor meer informatie: <https://www.rvig.nl/reisdocumenten/zelfevaluatie-reisdocumenten>

### 3.2.4 Aanbevelingen Zelfevaluaties

De RvIG analyseert de resultaten van de Zelfevaluaties. Uit deze analyse ontstaat een beeld van de inrichting, de beveiliging en de verwerking van gegevens van de BRP. Op basis van het landelijke beeld bepaalt het ministerie van BZK de acties die het jaar na de evaluatie worden ondernomen om de kwaliteit van de BRP te verbeteren.

### 3.2.5 Accountantscontrole Rijbewijzen

Ook de procedures rond het verstrekken van rijbewijzen zijn onderwerp van controle. Op grond van artikel 128 lid 7 van het Reglement Rijbewijzen moeten de maatregelen zoals genoemd in artikel 128 lid 1 van dit reglement jaarlijks onderdeel uitmaken van de accountantscontrole. De bij de jaarlijkse evaluatie van het beheerproces rond Waardedocumenten (reisdocumenten en rijbewijzen) geconstateerde tekortkomingen worden schriftelijk vastgelegd en de daarop betrekking hebbende rapportages worden 5 jaar bewaard. Op de eventueel geconstateerde tekortkomingen wordt actie ondernomen.

### 3.2.6 Overige instrumenten

Verantwoordelijke kan self-assessments uitvoeren om te bepalen in hoeverre veiligheidsmaatregelen voor het object van dit plan bestaan en voldoen aan het bepaalde in de AVG en de BIO. Dit kan bijvoorbeeld zijn een 'privacy self-assessment' of een DPIA.

Een DPIA is een instrument om (vooraf) de privacyrisico's van een gegevensverwerking in kaart te brengen en om daarna maatregelen te kunnen nemen om de veiligheidsrisico's te verkleinen. De AP heeft een lijst met gegevensverwerkingen opgesteld waarvoor een DPIA verplicht is om uit te voeren, bv voor het grootschalig verwerken van biometrische gegevens voor identificatie van een persoon.

Concerncontrol kan interne controles op essentiële bedrijfsprocessen prioriteit geven om sluimerende bedrijfsrisico's op de continuïteit te detecteren.

### 3.2.7 Planning en acties

De landelijke jaarplanningen voor de zelfevaluaties en accountantscontrole zijn leidend op de jaaragenda van het kwaliteitssysteem. De toepassing van de overige controle-instrumenten plant verantwoordelijke naar behoefte in als daar een noodzaak voor is, blijkend uit bijvoorbeeld de jaarlijkse risicoanalyse of een advies van de beveiligings- of privacyfunctionarissen. Verbeteracties en aanbevelingen voortkomend uit de diverse controles en analyses neemt verantwoordelijke mee als input op de jaarlijkse risicoanalyse en de daaruit voortvloeiende beveiligingsmaatregelen.

## 4. Beveiligingsfunctionaris waardedocumenten

### 4.1 Aanwijzingsbesluit

De aanwijzing van de beveiligingsfunctionaris reisdocumenten en rijbewijzen geschiedt met een aanwijzingsbesluit door de burgemeester en wordt via het standaarddocument B5 gemeld aan de RvIG. (Zie hiervoor: [Toelichting B- en C- formulieren | Reisdocumenten | Rijksdienst voor Identiteitsgegevens \(rvig.nl\)](#))

### 4.2 Taakomschrijving

De beveiligingsfunctionaris waardedocumenten is belast met en verantwoordelijk voor de volgende taken:

- De controle op de naleving van de beveiligingsprocessen, -procedures en instructies betreffende reisdocumenten mede aan de hand van de normeringen uit de zelfevaluatie PNIK;
- De controle op een juiste afhandeling van de zelfevaluatie PNIK;
- Het (laten) verrichten van onderzoek bij beveiligingsincidenten met het doel dergelijke situaties in de toekomst te voorkomen;
- Het naar aanleiding van onderzoek/controles en/of incidenten signaleren van knelpunten en/of tekortkomingen in de beveiligingsvoorzieningen.
- Het bewaken van uit te voeren acties voortkomend uit onderzoek, incidenten of de jaarlijkse risicoanalyse;
- Het toezicht houden op de actualiteit van het Informatiebeveiligingsplan BRP en waardedocumenten, alsmede de uitvoering van de beveiligingsmaatregelen;
- Gevraagd en ongevraagd advies geven aan de burgemeester en het managementteam over verbeteringen ten aanzien van de beveiliging;
- Het adviseren bij het ontwikkelen van nieuwe beveiligingsprocedures en onderhouden/aanpassen van bestaande beveiligingsprocedures;
- Het bevorderen van eenduidigheid, efficiëntie en effectiviteit ten aanzien van beveiligingsaspecten door het ten minste eenmaal per jaar geven van voorlichting en instructie aan medewerkers en het toetsen van de bestaande beveiligingsprocedures en –processen;
- Het toezicht houden of (nieuwe) medewerkers worden geïnstrueerd en bekendgemaakt met de beveiligingsprocedures en –processen met betrekking tot reisdocumenten;
- Toezien op het naleven van de voorschriften over functiescheiding;
- Het registreren van de meldingen van beveiligingsincidenten;
- Het rapporteren aan de burgemeester betreffende de stand van zaken van beveiliging, eventueel naar aanleiding van bijzonderheden/incidenten;
- Het rapporteren van de uitkomsten van controles en onderzoeken aan de burgemeester.

## **5. Functiescheiding**

### **5.1 Waarom functiescheiding?**

Functiescheiding bij het verstrekken van waardedocumenten en het vaststellen of wijzigen van BRP-gegevens verkleint de kans op in- of externe fraude. Functiescheiding staat beschreven of komt tot uiting in de procesbeschrijvingen en besluiten bij de taken waarvoor functiescheiding is bepaald. De uitwerking in de dagelijkse praktijk is onderdeel van de werkverdeling. De mate van naleving blijkt uit de toetsing van processen aan de praktijk.

#### **5.1.1 Functiescheiding in taken reisdocumenten**

Ter uitvoering van het bepaalde in artikel 93 van de PUN over functiescheiding bestaan en werken de volgende functiescheidingen in de taakuitvoering:

- Tussen de beveiligingsfunctionaris reisdocumenten en degenen die belast zijn met uitvoerende en beheertaken met betrekking tot reisdocumenten. De beveiligingsfunctionaris reisdocumenten mag niet betrokken zijn bij, of verantwoordelijkheid dragen voor de procedures rondom reisdocumenten. Dit voorkomt dat de beveiligingsfunctionaris reisdocumenten zijn eigen werk controleert.
- Tussen aanvraag, verstrekking, beheer en uitreiking van reisdocumenten. Het reisdocument moet door een andere medewerker worden uitgereikt dan degene die de beslissing op de aanvraag heeft genomen.

#### **5.1.2 Functiescheiding in taken rijbewijzen**

Ter uitvoering van het bepaalde in artikel 128, lid 1, 2 en 3 van RR bestaat en werkt de volgende functiescheiding in de taakuitvoering:

- Tussen aanvraag en uitreiking van rijbewijzen. Het rijbewijs wordt door een andere medewerker uitgereikt dan degene die de beslissing op de aanvraag heeft genomen.

#### **5.1.3 Functiescheiding in taken BRP**

Bij het uitvoeren van taken voor registratie en actualisatie van persoonsgegevens in de BRP bestaat functiescheiding tussen het uitvoeren van mutaties en het goedkeuren van mutaties in de BRP.

#### **5.1.4 Vastlegging functiescheiding**

De voorgeschreven functiescheidingen zijn beschreven in procedures en instructies van de betreffende uitvoeringsprocessen. Deze liggen vast in het Kwaliteitssysteem van de afdeling.

## **6. Vaststelling**

### **6.1 Evaluatie en actualisering**

De werking van dit plan wordt jaarlijks geëvalueerd door de beveiligingsfunctionarissen BRP en waar-dedocumenten. De evaluatie geeft input op het onderdeel beveiliging van de jaarlijkse risicoanalyse uit paragraaf 2.2. Zo nodig wordt dit plan geactualiseerd.

### **6.2 Ondertekening verantwoordelijke**

Haarlem, (*datum*)

Het afdelingshoofd Klantcontactcentrum,

(*Handtekening*)

### **6.3 Besluit vaststelling door burgemeester en wethouders**

Dit plan wordt per besluit vastgesteld door burgemeester en wethouders van Haarlem.

## Bijlagen

### A. Statusoverzicht risicobeperkende maatregelen

Zie volgende bladzijde.

Procedures, trainingen en besluiten	Geldt voor	Opgenomen KZS	Beschreven in applicatie	Actueel
<b>Procedure algemeen</b>				
Vaststellen identiteit en machtiging	KCC	niet	Word	
Beheren kas	KCC	wel	BPMN	
Verwerken kas en bank	Fin	wel	BPMN	
Calamiteiten (fysieke uitwijk balie en/of productie)	KCC	niet	Word	2019
Rapporteren incidenten	KCC		Excel-regel	2023
Instructie privacyregels	KCC		Word	
Introductie nieuw personeel	KCC		?	
Jaarlijkse risicoanalyse	KCC		Excel bestand	
<b>Procedures BRP</b>				
Beoordelen brondocumenten	KCC	niet	Word	2019
Inschrijven in de gemeente	KCC	niet	Word	2019
Actualiseren gegevens	KCC	niet	Word	2019
Corrigeren gegevens	KCC	niet	Word	2019
Controleren volledigheid, juistheid en actualiteit gegevens	KCC	niet	Word	2019
Verwijderen gegevens	KCC	niet	Word	2019
Toekennen verstrekingsbeperking (geheimhouding)	KCC	niet	Word	2019
Onderzoeken juistheid gegevens	KCC	niet	Word	2019
Protocolleren	KCC	niet	Word	2019
Terugmelden	KCC	niet	Word	2019
Verstrekken gegevens	KCC	niet	Word	2019
Autoriseren koppeling maken met database	KCC	niet	Word	
Herstellen/reconstrueren gegevens na systeemstoring	KCC	niet		
Verklaren geheimhouding gegevens door gebruikers	KCC	niet	Word	
<b>Procedures Waardedocumenten</b>				
Aanvragen reisdocumenten	KCC	wel	Word	2019
Ontvangst en transport reisdocumenten en materialen	KCC	wel	Word	2019
Verzenden aanvragen reisdocumenten	KCC	wel	Word	2019
Uitreiken en vernietigen reisdocumenten	KCC	wel	Word	2019
Vermissing van reisdocumenten	KCC	wel	Word	2019
Van rechtsweg vervalLEN reisdocumenten	KCC	wel	Word	2019
Afwijking in voorraad	KCC	wel	Word	2019
Fysieke beveiliging RAAS en mobiele aanvraagstations	KCC	wel	Word	2019
Registreren afgifte identiteitskaart	KCC	wel	Word	2019
Uitreiken en vernietigen reisdocumenten met koerier	KCC	wel	Word	2019
Overvalinstructie	KCC			
<b>Vereiste procedures faciliterende afdelingen</b>				

Autoriseren gebruikers voor toegang tot systemen	IV	nvt	BPMN	
Autoriseren/Controleren toegang tot applicaties	ID	nvt	BPMN	
Autoriseren toegang tot beveiligde ruimtes	Faza	nvt		
Maken backup database	IV	nvt	BPMN	
Recovery database	IV	nvt	BPMN	
Antecedentenonderzoek	HRM	nvt	BPMN	
Sollicitatieonderzoek aanstelling personeel	HRM	nvt	BPMN	
Integriteitsverklaring	HRM	nvt	BPMN	
Afvoeren computers	IV	nvt	BPMN	
Uitvoeren en goedkeuren updates applicaties	IV	nvt	BPMN	
Ongedaanmaken systematische verstrekkingen	ID	nvt		
Vernietiging verwijderbare media	ID	nvt		
Verstrekken alternatief medium	ID	nvt		
Uitvoeren technische systeemuitwijk	IV	nvt	BPMN	
Uitvoeren terugkeer na systeemuitwijk	IV	nvt	BPMN	
Fysieke uitwijk naar alternatieve locatie bij calamiteiten	Faza	nvt		
Herstart kritische bedrijfsprocessen na calamiteiten	Concerncontrol	nvt		
Incidenten melden	IV	nvt	BPMN	
Incidentenprotocol	HRM	nvt	Pdf	
<b>Trainingen</b>				
Omgaan met agressie	KCC		pdf	2023
Omgaan met documentfraude	KCC		pdf	2023
Bewustzijn informatieveiligheid en privacy	KCC		pdf	2023
Integriteitstraining	KCC		pdf	2023
<b>Benoemingsbesluiten</b>				
Aanwijzingsbesluit beveiligingsfunctionaris BRP	KCC		(2020/1183476)	2022
Aanwijzingsbesluit beveiligingsfunctionaris Waardedocumenten	KCC		Std B5 form RvIG	

## B. Basisbeveiligingsniveaus van de Baseline Informatiebeveiliging Overheden

### Vertrouwelijkheidsniveau hoog (BBN3):

Verlies van informatie heeft een grote impact, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3;

- informatie wordt door derden geleverd met een rubricering (niet zijnde BBN2); of
- aansluiting op een infrastructuur vereist (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen) BBN3 om informatie te kunnen verwerken op deze infrastructuur; of
- weerstand tegen statelijke actoren is noodzakelijk.

### Vertrouwelijkheidsniveau midden (BBN 2):

Bescherming van gegevens en andere te beschermen belangen in de processen van de overheid, waar o.a. vertrouwelijkheid aan de orde is, omdat het om gevoelige informatie gaat.

Het openbaar worden van de gegevens, kan leiden tot:

- politieke schade aan een bestuurder: bestuurder moet zich verantwoorden n.a.v. verantwoordingsvragen; of
- schade te herstellen door ambtelijke opschaling; of



- financiële gevolgen: niet meer op te vangen binnen de begroting van de organisatie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of
- verlies van publiek respect; klachten van burgers of significant verlies van motivatie van medewerkers; of
- bindende aanwijzing van de AP in verband met schending van de privacy; of
- directe imagoschade, bijvoorbeeld door negatieve publiciteit

**Vertrouwelijkheidsniveau laag (BBN1):**

Kennisname van informatie door ongeautoriseerden (buitenstaanders) is niet gewenst, maar leidt niet tot schade van enige omvang. Het gaat hier om ongerubriceerde informatie. Het openbaar worden van deze informatie kan leiden tot:

- financiële gevolgen: op te vangen binnen de begroting van de organisatie of uitvoeringsorganisatie; of
- irritatie en ongemak bij burgers geventileerd in de media; of
- interne negatieve publiciteit (imagoschade).

**Vertrouwelijkheidsniveau openbaar (BBN0):**

verwaarloosbare schade of niet van toepassing.

Het gaat hierbij om openbare gegevens. De gegevens hoeven niet afgeschermd te worden. Geen enkele beveiliging op de gegevens is noodzakelijk. Het is juist zaak dat deze gegevens openbaar worden gemaakt voor publicatie.

- melding in de pers en social media; lokaal protest; diplomatieke schade te herstellen door ambtelijke opschaling
- minimaal verlies van management control; een week vertraging van nieuwe ontwikkelingen
- nauwelijks discussie op internet en social media met minimaal verlies van vertrouwen; minimale negatieve publiciteit (imagoschade)
- minimaal verlies van motivatie van medewerkers; minimale afname van personele capaciteit.