

## Regeling beheer en toezicht Basisregistratie Personen (BRP) en reis- en waardedocumenten (PNIK)

Burgemeester en wethouders van de gemeente Elburg,  
Gelet op: de Wet Basisregistratie Personen (Wet BRP), de Algemene Verordening Gegevensbescherming (AVG), de Paspoortuitvoeringsregeling Nederland 2001 (PUN 2001), het Reglement rijbewijzen en de Baseline Informatiebeveiliging Overheid (BIO);  
Besluiten vast te stellen: De Regeling beheer en toezicht Basisregistratie Personen en reis- en waardedocumenten.

### Hoofdstuk 1: Aanwijzen functionarissen

#### Artikel 1

Het college van burgemeester en wethouders wijst functionarissen aan die belast worden met:

- het gegevensbeheerder;
- het applicatiebeheer;
- het systeembeheer;
- het privacybeheer;
- de controle op informatiebeveiliging (CISO).

#### Artikel 2

Daarnaast worden aangewezen de functionarissen belast met:

- het houden van toezicht;
- de gegevensverwerking;
- het namens het college van burgemeester en wethouders afnemen van de in artikel 2.8, lid 2, onder sub e, van de wet bedoelde verklaring.

#### Artikel 3

De burgemeester wijst de volgende functionarissen aan voor de verantwoordelijkheden en taken met betrekking tot reis- en waardedocumenten:

- de autorisatiebevoegde;
- de beveiligingsfunctionaris reis- en waardedocumenten

### Hoofdstuk 2: Het gegevensbeheer

#### Artikel 4

1. De gegevensbeheerder BRP heeft, in samenspraak met de CISO, rechtstreekse verantwoordelijkheid naar het college van burgemeester en wethouders zonder tussenkomst van leidinggevenden in de lijn.

2. De Gegevensbeheerder BRP beheert de gemeentelijke voorziening en het gegevensmagazijn en is verantwoordelijk voor:

- a. de juistheid, actualiteit en betrouwbaarheid van de gegevens die opgenomen zijn of worden, in de gemeentelijke voorziening voor de BRP;
- b. het beheer van documentatie op het gebied van de overige wet- en regelgeving op het gebied van de BRP;
- c. de communicatie met de overheidsorganen aan wie gegevens worden verstrekt uit de BRP en andere houders van voorzieningen voor de BRP omtrent gegevensverwerking;
- d. het verwerken van complexe mutaties en correcties met betrekking tot de BRP;
- e. het uitzetten van richtlijnen met betrekking tot het actualiseren en corrigeren van persoonsgegevens, binnen de gemeentelijke voorziening voor de BRP.

De gegevensbeheerder beslist binnen 5 werkdagen over het in behandeling nemen van meldingen van een overheidsorganen, waarbij gereede twijfel bestaat over de juistheid van een in de gemeentelijke

voorziening van de BRP opgenomen (authentieke) gegevens en stelt het overheidsorgaan in kennis van de genomen beslissing.

#### **Artikel 5**

De Gegevensbeheerder BRP voorziet in:

- a. de jaarlijkse planning van beheeractiviteiten;
- b. de behandeling van wijzigingsverzoeken als bedoeld in artikel 2.57, 2.58 en 2.60 van de Wet BRP;
- c. de controlewerkzaamheden ter waarborging van de kwaliteit van de BRP;
- d. De administratieve beheerprocedures, voor zover hier niet door of bij wet in is voorzien;
- e. het bekend laten maken en toelichten van (nieuwe/gewijzigde) (beveiligings) procedures bij medewerkers;
- f. het laten verzorgen van de beveiligingsonderwerpen tijdens het werkoverleg;
- g. het aanspreken van medewerkers in het geval van (bijna) incidenten of gevaarlijk gedrag;
- h. het laten verzorgen van periodieke voorlichting (tenminste 1 x per jaar) op het gebied van beveiliging om het risicobewustzijn op peil te houden/te verhogen;
- i. het bijstellen van het jaarlijkse beveiligingsplan, in overleg met de CISO, op basis van de gehouden zelfevaluatie;
- j. overleg binnen de eigen organisatie of met derden indien de te behandelen beveiligingsaspecten raakvlakken vertonen met de beveiliging van de BRP.

#### **Artikel 6**

De Gegevensbeheerder BRP is bevoegd vanuit de in artikel 4 bedoelde verantwoordelijkheid de gegevensverwerkers aanwijzingen te geven betreffende de opname en bijhouding van gegevens in de gemeentelijke voorziening voor de BRP.

#### **Artikel 7**

De Gegevensbeheerder BRP is verantwoordelijk voor:

- a. het toezicht op het beheer en de ontwikkeling van beveiligingsprocessen BRP;
- b. het toetsen van de uitvoering van regelgeving en procedures ten aanzien van het BRP;
- c. de evaluatie van de beveiligingsprocessen en het verzorgen van een managementrapportage aan de opdrachtgever BRP (het college).
- d. de periodieke aanlevering met betrekking tot de inhoudelijke kwaliteit van het bestand van persoonslijsten in de BRP, onderworpen aan een inhoudelijke controle door de minister van Binnenlandse Zaken en Koninkrijksrelaties.
- e. een doorlopende kwaliteitssteekproef en de uitvoering van de daarmee samenhangende verbetermaatregelen, gericht op de handhaving van de kwaliteitsnorm van het ministerie van Binnenlandse Zaken.
- f. de uitvoering van het periodiek onderzoek op grond van artikel 4.3 van de Wet BRP, voor wat betreft de verwerking van persoonsgegevens in de gemeentelijke voorziening.

#### **Artikel 8**

De Gegevensbeheerder BRP maakt melding van ieder incident aan de CISO en privacybeheerder.

### **Hoofdstuk 3: Het applicatiebeheer**

#### **Artikel 9**

De Applicatiebeheerder BRP voorziet in:

- a. de communicatie bij storingen in hard- en software;
- b. de verzorging een logboek waarin bijzondere gebeurtenissen worden bijgehouden;
- c. de toekenning van de autorisatieniveaus voor de toepassing van actualiseringen, aan de gegevensverwerkers, de gegevensbeheerder en de applicatiebeheerder BRP;
- d. de bijhouding van een dossier omtrent de autorisaties;
- e. het testen en evalueren van nieuwe versies van het toepassingssysteem, alsmede het testen en evalueren van nieuwe apparatuur;
- f. het plannen van de installatie van nieuwe of gewijzigde versies van het toepassingssysteem voor de gemeentelijke voorziening in overleg met de systeembeheerder;

- g. de beoordeling van de gevolgen van de installatie van nieuwe en of gewijzigde versies van het toepassingssysteem;
- h. de bijhouding van een verzameling van alle problemen en klachten, die bij het gebruik van het toepassingssysteem ontstaan;
- i. een oplossing, eventueel door inschakeling van de systeembeheerder of een derde, voor onstane problemen en klachten;
- j. de voorlichting aan de gegevensverwerkers en gegevensbeheerder, met betrekking tot de gevolgen van een nieuwe of gewijzigde versie van het toepassingssysteem;
- k. de coördinatie van werkzaamheden, in geval van uitwijk in overleg met de systeembeheerder;
- l. de vormgeving en inhoud van documenten, die rechtstreeks aan de BRP worden ontleend;
- m. de afhandeling van verzoeken omtrent managementgegevens;
- n. een zo spoedig mogelijke oplossing in geval van storingen binnen het toepassingssysteem, zo nodig door inschakeling van een derde.

#### **Artikel 10**

De Applicatiebeheerder BRP is verantwoordelijk voor:

- a. de communicatie aan de gebruikers van het toepassingssysteem van de installatie van nieuwe of gewijzigde versies van het systeem en de gevolgen van deze installatie;
- b. de ondersteuning bij het gebruik van het toepassingssysteem;
- c. het tijdig opschonen van de relevante bestanden in de database;
- d. het beheer van de tabellen van de BRP;
- e. het beheer van de gebruikersdocumentatie.

#### **Artikel 11**

De Applicatiebeheerder BRP is bevoegd:

- a. gegevensverwerkers en het personeel van externe afdelingen/diensten die direct toegang hebben tot de BRP, aanwijzingen te geven over het gebruik van het toepassingssysteem;
- b. gedragsregels op te stellen omtrent het gebruik van de BRP.

#### **Artikel 12**

De Applicatiebeheerder BRP is verantwoordelijk voor de gehele of gedeeltelijke uitvoering van de uitwijkprocessen zoals beschreven in de procedure uitwijk van het Informatiebeveiligingsplan.

#### **Artikel 13**

De Applicatiebeheerder BRP ziet erop toe dat voorgeschreven procedures uit het Informatiebeveiligingsplan worden nageleefd.

#### **Artikel 14**

De Applicatiebeheerder BRP:

- a. maakt melding van ieder incident aan de CISO en privacybeheerder;
- b. neemt deel aan het externe gebruikersoverleg.

### **Hoofdstuk 4: Het systeembeheer**

#### **Artikel 15**

De systeembeheerder is verantwoordelijk voor de uitvoer van het technisch onderhoud van de gemeentelijke voorziening voor de BRP (hierna toepassingssysteem genoemd).

#### **Artikel 16**

De systeembeheerder voorziet in:

- a. de fysieke beveiliging van het toepassingssysteem;
- b. een dagelijkse back-up die wordt ondergebracht in een daartoe uitgeruste en beveiligde ruimte, die zich op een andere locatie bevindt, dan de ruimte waarin de apparatuur voor de gemeentelijke voorziening van de BRP is opgesteld;

- c. de technische installatie van gewijzigde of nieuwe versies van het toepassingsstelsel;
- d. de beschikbaarheid van het toepassingsstelsel overeenkomstig hetgeen daarover intern en met derden is overeengekomen.

#### **Artikel 17**

De systeembeheerder is bevoegd:

1. Direct maatregelen te treffen op het moment dat de continuïteit van het toepassingsstelsel of de daarin opgeslagen informatie, acuut in het geding is. Hij is verplicht achteraf ter zake te rapporteren aan de CISO.
2. Aanwijzingen te geven over:
  - het beheer van het toepassingsstelsel;
  - het beheer van bestanden;
  - toe te passen reconstructiemaatregelen.

#### **Artikel 18**

De systeembeheerder maakt melding van ieder incident aan de CISO en privacybeheerder.

### **Hoofdstuk 5: Het privacybeheer**

#### **Artikel 19**

De privacybeheerder (PO/FG) heeft rechtstreekse verantwoordelijkheid naar de Autoriteit Persoonsgegevens zonder tussenkomst van leidinggevend in de lijn. De privacybeheerder adviseert de gegevensbeheerder, de gegevensverwerkers en het college van burgemeester en wethouders over de privacyaspecten die voortvloeien uit de uitvoering van de AVG, de Wet BRP en Verordening BRP.

#### **Artikel 20**

De privacybeheerder is verantwoordelijk voor het beheer van de autorisatiebesluiten;

#### **Artikel 21**

De privacybeheerder adviseert over:

- a. de afhandeling van de verzoeken om inzage in de BRP overeenkomstig artikel 2.55 van de Wet BRP respectievelijk artikel 15 van de AVG (inzage);
- b. de behandeling van alle verzoeken om verstrekking beperking die op basis van artikel 2.59 van de Wet BRP ingediend worden en de eventuele privacytoets als bedoeld in artikel 3.21 lid 2 van de wet BRP;
- c. de afhandeling van verzoeken ingevolge de artikelen 17 en 21 van de AVG;
- d. de kennisgeving ingevolge artikel 19 van de AVG;
- e. de afhandeling van verzoeken om inzage in verstrekkingen uit de BRP aan overheidsorganen en derden.

#### **Artikel 22**

De privacybeheerder beslist:

- a. op verzoeken van organen van de gemeente tot het verkrijgen van gegevens uit de BRP;
- b. op verzoeken van derden, als genoemd in artikel 3.6 van de Wet BRP en als genoemd in de bij Verordening BRP genoemde derden tot het verkrijgen van gegevens uit de Basisregistratie Personen;
- c. over de wijze van de verstrekking van gegevens met betrekking tot het bepaalde in dit artikel onder a en b.

#### **Artikel 23**

De privacybeheerder is bevoegd:

- a. alle gebruikers van gegevens uit de BRP aanwijzingen te geven;
- b. ongevraagd advies uit te brengen over alle procedures en producten die betrekking hebben op de BRP, waarbij sprake is van het in geding zijn van de persoonlijke levenssfeer.

#### **Artikel 24**

De privacybeheerder:

- a. onderkent en reageert op datalekken en adviseert over de maatregelen die nodig zijn om de gevolgen van een incident te beperken en om herhaling te voorkomen;
- b. stelt passende normen en controlemaatregelen op;
- c. implementeert maatregelen;
- d. coördineert en handhaaft de uitvoering van de maatregelen als genoemd onder c.

#### **Artikel 25**

De privacybeheerder is betrokken bij alle bezwaarschriftenprocedures die voortvloeien uit genomen beslissingen op grond van de Wet BRP en daarbij behorende regelingen en de AVG voor zover hierbij privacyaspecten aan de orde zijn.

#### **Artikel 26**

De privacybeheerder is het aanspreekpunt op het gebied van privacybeveiliging en bevordert het beveiligingsbewustzijn bij management en medewerkers.

### **Hoofdstuk 6: De controle op informatiebeveiliging (CISO)**

#### **Artikel 27**

De CISO is verantwoordelijk voor het opstellen en de controle op de uitvoering van het informatiebeveiligingsbeleid waaronder het Informatiebeveiligingsplan voor de GV en GM waarmee de organisatie uitvoering geeft aan de Wet BRP. De CISO adviseert het college van burgemeester en wethouders rechtstreeks over beveiligingsaspecten die uit het Informatiebeveiligingsplan voortvloeien.

#### **Artikel 28**

De CISO ondersteunt en adviseert de organisatie op het gebied van informatiebeveiliging op dusdanige wijze, dat medewerkers diens verantwoordelijkheid op grond van dit reglement op deugdelijke wijze kunnen invullen met inachtneming van de Baseline Informatiebeveiliging Overheid (BIO). De CISO controleert de uitvoering van de beveiligingsmaatregelen van het Informatiebeveiligingsplan en kan dwingende adviezen geven, ten aanzien van de naleving van beveiligingsvoorschriften, die voortvloeien uit de Wet BRP en het Informatiebeveiligingsplan.

#### **Artikel 29**

De CISO is bevoegd:

- a. uit hoofde van diens verantwoordelijkheid als bedoeld in artikel 27, alle gebruikers van gegevens uit de BRP aanwijzingen te geven;
- b. ongevraagd advies uit te brengen over alle procedures en producten die betrekking hebben op de BRP, waarbij de beveiliging in het geding is.

#### **Artikel 30**

De CISO:

- a. onderkent en reageert op incidenten en adviseert over de maatregelen die nodig zijn om de gevolgen van een incident te beperken en om herhaling te voorkomen;
- b. stelt passende normen en controlemaatregelen op;
- c. implementeert beveiligingsmaatregelen;
- d. coördineert en handhaaft de uitvoering van de maatregelen als genoemd onder c.

#### **Artikel 31**

De CISO is het gemeentebrede aanspreekpunt op het gebied van informatiebeveiliging en bevordert het beveiligingsbewustzijn bij management en medewerkers.

### **Artikel 32**

De CISO participeert in de ontwikkeling en formulering van het gemeentebrede informatiebeveiligingsbeleid.

### **Artikel 33**

De CISO voorziet in:

- a. de jaarlijkse rapportage aan het college van burgemeester en wethouders over de bij a. bedoelde planning, waarbij tevens inzicht wordt gegeven in de kengetallen van de bijhoudings- en beheerprocedures;
- b. een jaarlijkse rapportage over de resultaten die voortvloeien uit de zelfevaluatie BRP/PNIK.

### **Artikel 34**

De CISO is verantwoordelijk voor de coördinatie van:

- a. de uitvoering van het periodieke onderzoek op grond van artikel 4.3 van de Wet naar de inrichting, werking en beveiliging van de BRP (zelfevaluatie kwaliteitsmonitor), alsmede naar de verwerking van gegevens in de BRP;
- b. de periodieke toezending van een uittreksel van de resultaten van het onderzoek aan het college bescherming persoonsgegevens en aan de minister van Binnenlandse Zaken en Koninkrijksrelaties.

### **Artikel 35**

De CISO adviseert het college van burgemeester en wethouders over de navolgende aspecten die voortvloeien uit de BRP (collegeverklaring) te weten:

- a. persoonsinformatievoorziening;
- b. beveiliging;
- c. gegevenskwaliteit;
- d. personeelsaangelegenheden.

### **Artikel 36**

De CISO ziet erop toe, door middel van aangeleverde rapportages (PNIK), dat:

- a. de in deze regeling opgenomen bepalingen worden nageleefd;
- b. de bij of krachtens de wet opgelegde verplichtingen ten aanzien van inrichting en bijhouding, evenals de beveiliging van de gemeentelijke voorziening voor de BRP worden nageleefd;
- c. de beveiligingsvoorschriften en -procedures die voortvloeien uit de Wet BRP en het Informatiebeveiligingsplan worden nageleefd.

## **Hoofdstuk 7: De gegevensverwerking**

### **Artikel 37**

De gegevensverwerkers voorzien in:

- a. het verwerken van de gegevens in de BRP overeenkomstig de voorschriften van de krachtens de wet voorgeschreven systeembeschrijving (Logisch Ontwerp GBA) en de handleiding uitvoeringsprocedures, voor zover daartoe door de applicatiebeheerder geautoriseerd;
- b. het verzamelen van de daarvoor bestemde gegevens;
- c. de archivering van de brondocumenten op grond waarvan de gegevens zijn verwerkt;
- d. de behandeling van mutaties;
- e. de behandeling van het netwerkverkeer;
- f. de behandeling van de foutverslagen, voortvloeiend uit de inkomende netwerk- berichten;
- g. de toetsing van de waarde die aan overgelegde brondocumenten kan worden toegekend aan de hand van artikel 2.8 van de Wet BRP en ziet erop toe dat geen gegevens worden verwerkt uit documenten waaraan bij of krachtens de wet geen ontleningstatus is gegeven;
- h. de dagelijkse controle van de in de BRP aangebrachte actualiseringen;
- i. de kennisgeving aan de ingeschrevene voor wat betreft de verwerking van:
  - wijziging van het naamgebruik;
  - vervolgschrijving voor zover het een adreswijziging betreft die leidt tot opname in de BRP;

- j. de toezending van de complete persoonslijst aan de ingeschrevene ingeval van een inschrijving in de BRP;
- k. de afhandeling van de verzoeken om inzage in de BRP overeenkomstig artikel 2.55 van de wet BRP (inzage) in overleg met de privacybeheerder;
- l. de behandeling van alle verzoeken om verstrekingsbeperking die op basis van artikel 2.59 van de wet BRP ingediend worden en de eventuele privacytoets als bedoeld in artikel 3.21 lid 2 van de wet BRP in overleg met de privacybeheerder;
- m. de afhandeling van verzoeken om inzage in verstrekkingen uit de BRP aan overheidsorganen en derden in overleg met de privacybeheerder.

### **Artikel 38**

De gegevensverwerkers:

- a. beslissen op aangiften en verzoekschriften die op grond van de wet worden gedaan met inachtneming van het gestelde in artikel 26 en voor zover hier niet op andere wijze in is voorzien;
- b. beslissen over het verwerken van resultaten van onderzoeken die zijn ingesteld naar aanleiding van een melding van een overheidsorgaan;
- c. stellen overheidsorganen in kennis van de beslissing ingevolge sub b van dit artikel;
- d. maakt melding van ieder incident aan de CISO en privacybeheerder.

## **Hoofdstuk 8: De toezichthouder**

### **Artikel 39**

De toezichthouder als bedoeld in artikel 4.2 van de Wet BRP, is verantwoordelijk voor het toezicht op de naleving van de verplichtingen van de burger ingevolge hoofdstuk 2, afdeling 1, paragraaf 5 van de Wet BRP.

### **Artikel 40**

De toezichthouder controleert of de burger voldoet aan zijn verplichtingen met betrekking tot de inschrijving in de BRP (artikel 2.38), de wijziging van diens adres (2.39), het rechtmatig gebruik van een briefadres (2.40 t/m 2.42), zijn vertrek uit Nederland (2.43), de verstrekking van alle inlichtingen die nodig zijn voor de bijhouding van de BRP.

### **Artikel 41**

De toezichthouder ziet erop toe dat, indien de burger niet zelf aan zijn verplichtingen voldoet of kan voldoen, de verplichtingen worden vervuld door degene die daartoe bevoegd is op grond van de artikelen 2.49 en 2.50 van de Wet BRP.

### **Artikel 42**

De toezichthouder ontleent de hierna toegekende bevoegdheden aan hoofdstuk 5 van de Algemene Wet Bestuursrecht. De toezichthouder is in verband met de uitvoering van de taken als genoemd in artikel 40, bevoegd:

- a. met uitzondering van het zonder toestemming van een bewoner betreden van een woning, elke plaats te betreden met inbeslagname van apparatuur (zoals laptop, fotocamera);
- b. zich zo nodig toegang verschaffen met behulp van de sterke arm;
- c. zich te laten vergezellen door personen die door hem zijn aangewezen;
- d. inlichtingen te vorderen;
- e. inzage te vorderen van een identiteitsbewijs;
- f. zakelijke gegevens te vorderen, kopieën te maken of documenten mee te nemen om te kopiëren;
- g. onderzoek te doen;
- h. rapport op te maken ter zake een geconstateerde overtreding van de bepalingen van de Wet BRP, als genoemd in artikel 40.

### **Artikel 43**

De toezichthouder voert zijn werkzaamheden uit in samenspraak met de gegevensbeheerder en koppelt het resultaat van zijn werkzaamheden terug aan de gegevensbeheerder.

#### **Artikel 44**

1. De toezichthouder is bevoegd om namens burgemeester en wethouders een bestuurlijke boete op te leggen. Voor zover de gemeente van die bevoegdheid gebruik wil maken.
2. De toezichthouder neemt bij gebruik van de bevoegdheid als bedoeld in lid 1 van dit artikel binnen de Gemeente Elburg ter zake geldende beleidsregels in acht.

#### **Artikel 45**

De toezichthouder legt het resultaat van zijn werkzaamheden vast in een onderzoeksrapportage en draagt zorg voor dossiervorming.

### **Hoofdstuk 9: De autorisatiebevoegde**

#### **Artikel 46**

De autorisatiebevoegde is in samenspraak met de CISO rechtstreeks verantwoording verschuldigd aan de burgemeester (zonder tussenkomst van de leidinggevenden in de lijn).

#### **Artikel 47**

De autorisatiebevoegde wordt conform de PUN-2001 en het Reglement rijbewijzen door de burgemeester aangewezen. De aard en het volume van de werkzaamheden maken het mogelijk dat de functie wordt gecombineerd met andere werkzaamheden. Een afschrift van het aanwijzingsbesluit is als bijlage 2 aan deze regeling toegevoegd.

#### **Artikel 48**

De autorisatiebevoegde heeft de volgende verantwoordelijkheden:

- a. Het autorisatiebeheer (onder andere: aanvraag, uitgifte en intrekking) van identificatiekaarten en de registratie van de personen aan wie hij gedurende een bepaald tijdvak een identificatiekaart verstrekt en daarmee hem de bevoegdheid verleend tot het verrichten van handelingen binnen het RAAS of het rijbewijssysteem.
- b. Het in bewaring houden en het gebruik van de USB ten behoeve van de aanvraagstations.
- c. Het houden van toezicht op het zorgvuldige en stipt uitvoeren van de regelgeving en procedures geldend voor de omgang met het RAAS en het rijbewijssysteem.

#### **Artikel 49**

De taken van de autorisatiebevoegde omvatten ten minste:

- a. het dagelijks (laten) controleren of de gegevens op de back-up tapes goed zijn weggeschreven, door het controleren van de logbestanden;
- b. het indien nodig afhandelen van systeemsignalen;
- c. het dagelijks (laten) opstarten van de aanvraagstations;
- d. het na gebruik onmiddellijk (laten) opslaan van de USB in de kluis in de kluisruimte;
- e. het onderhouden van contact met de leverancier van de systemen;
- f. het bekend maken van en toelichting geven over nieuwe of gewijzigde procedures binnen het RAAS of het rijbewijssysteem, in de richting van de betrokken medewerkers;
- g. het toekennen, wijzigen en intrekken van autorisaties na opdracht van de domeinmanager;
- h. het bijhouden van een registratie van uitgereikte autorisaties en het afleggen van verantwoording hierover;
- i. het aan de leverancier melden van diefstal, verlies of onzorgvuldig gebruik van identificatiekaarten;
- j. het bijhouden van de registratie van ontvangen identificatiekaarten;
- k. het aan de leverancier melden van een defecte of verloren identificatiekaarten;
- l. het opsturen van defecte USB + identificatiekaarten naar de leverancier;
- m. het op juiste wijze laten archiveren van brondocumenten;
- n. het periodiek uitvoeren van controles op het gebied van autorisaties, functioneel gebruik en correcte verslaglegging van handelingen.



## Artikel 50

Functietypering:

- De functionaris heeft kennis van de werkprocessen rondom waardedocumenten.
- De functionaris is bekend met geldende beveiligingseisen en -procedures en heeft het vermogen om corrigerend op te treden.
- De functionaris beschikt over goede contactuele, redactionele en communicatieve vaardigheden.
- De functionaris beschikt over een goed ontwikkeld probleemoplossend vermogen

## Hoofdstuk 10: De beveiligingsfunctionaris reis- en waardedocumenten

### Artikel 51

De beveiligingsfunctionaris reis- en waardedocumenten heeft, in samenspraak met de CISO, rechtstreekse verantwoordelijkheid naar de burgemeester zonder tussenkomst van leidinggevenden in de lijn.

### Artikel 52

1. De beveiligingsfunctionaris reis en waardedocumenten is bij afzonderlijk besluit aangewezen.
2. De beveiligingsfunctionaris reis en waardedocumenten heeft geen uitvoerende taken met betrekking tot de waardedocumenten en heeft daartoe ook geen bevoegdheden tenzij de formatie geen mogelijkheden biedt tot scheiding van taken.
3. De aanwijzing wordt schriftelijk kenbaar gemaakt aan de minister van Binnenlandse Zaken en Koninkrijksrelaties (RvI/G).
4. De aard en het volume van de werkzaamheden maken het mogelijk dat de functie wordt gecombineerd met andere werkzaamheden.

### Artikel 53

De beveiligingsfunctionaris reis en waardedocumenten is verantwoordelijk voor:

- a. het toezicht op het beheer en de ontwikkeling van beveiligingsprocessen waardedocumenten;
- b. het toetsen van de uitvoering van regelgeving en procedures ten aanzien van het waardedocumentenproces;
- c. de evaluatie van de beveiligingsprocessen en het verzorgen van een managementrapportage aan de opdrachtgever waardedocumenten (de burgemeester).

### Artikel 54

De werkzaamheden omvatten ten minste:

- a. het bekend laten maken en toelichten van (nieuwe/gewijzigde) (beveiligings) procedures bij medewerkers;
- b. het laten verzorgen van de beveiligingsonderwerpen tijdens het werkoverleg;
- c. het aanspreken van medewerkers in het geval van (bijna) incidenten of gevaarlijk gedrag;
- d. het laten verzorgen van periodieke voorlichting (tenminste 1 x per jaar) op het gebied van beveiliging om het risicobewustzijn op peil te houden/te verhogen;
- e. overleg binnen de eigen organisatie of met derden indien de te behandelen beveiligingsaspecten raakvlakken vertonen met de beveiliging van de reisdocumenten en rijbewijzen;
- f. het steekproefsgewijs laten uitvoeren van tussentijdse controles op het gebied van voorraadadministratie, de status van fysieke en financiële voorraden, de toepassing van functiescheiding en de kwaliteit van de uitvoering van procedures;
- g. het laten verrichten van onderzoek bij afwijkingen in de levering en/of voorraden;
- h. het bijstellen van het jaarlijkse beveiligingsplan, in overleg met de CISO, op basis van de gehouden zelfevaluatie;
- i. het onderzoeken of de betreffende inspanningen en uitgaven in de onderzochte periode daadwerkelijk hebben bijgedragen aan de realisatie van het beoogde doel (effectiviteit) en het nagaan of de kosten in verhouding staan tot de opbrengsten (doelmatigheid).

### Artikel 55

In de jaarlijkse rapportages worden, in overleg met de CISO, de resultaten gepresenteerd aan het college en aan de burgemeester. De rapportage bevat minimaal informatie over:

- a. de uitkomsten of verrichtingen van de uit te voeren/uitgevoerde onderzoeken;

- b. geconstateerde afwijkingen bij de levering van documenten;
- c. geconstateerde afwijkingen in de fysieke/administratieve/financiële voorraad;
- d. gevaarlijk gedrag van medewerkers of het niet opvolgen van procedures;
- e. geconstateerde tekortkomingen in de beveiligingsvoorzieningen;
- f. het verrichte accountantsonderzoek;
- g. de wijziging van procedures/afspraken of de naleving hiervan;
- h. het zoekraken of in buiten gebruik van sleutels/sluitcodes /badges;
- i. handelingen die afwijken van de voorgeschreven functiescheidingsprocedure.

#### **Artikel 56**

1. De functionaris heeft kennis van de werkprocessen reis- en waardedocumenten.
2. De functionaris heeft bekendheid met geldende beveiligingseisen en -procedures.
3. De functionaris beschikt over goede contactuele, redactionele en communicatieve vaardigheden.
4. De functionaris heeft bedrijfsmatig inzicht en beschikt over probleemoplossend vermogen.
5. De functionaris onderhoudt contacten met collega's binnen en buiten de eigen afdeling.

### **Hoofdstuk 11: Slotbepalingen**

#### **Artikel 57**

De in deze regeling opgenomen bepalingen gelden voor de GV als bedoeld artikel 1.2 juncto 1.4 van de Wet BRP, evenals voor de in de GV genoemde aangehaakte gegevens en voor de basisgegevens uit de BRP die zich in het GM bevinden.

#### **Artikel 52**

Deze regeling treedt in werking op de eerste dag na bekendmaking.

#### **Artikel 53**

Deze regeling wordt aangehaald als Regeling beheer en toezicht BRP en PNIK.

*Aldus besloten in de vergadering van het college van burgemeester en wethouders van 17 december 2019,*

*Burgemeester en wethouders van Gemeente Elburg*

*De burgemeester, ir. J.N. Rozendaal*

*De secretaris, P.W. Wanrooij*