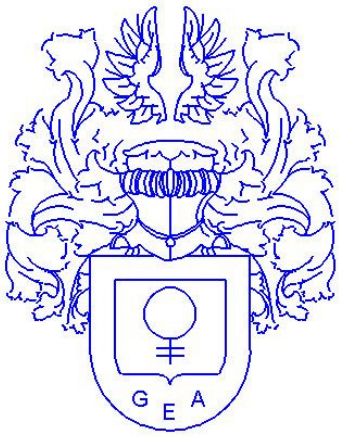
Preview

Handboek Burgerzaken

NEN-ISO/IEC 27002 (CvI / BIG)

*



Gemeentelijk Efficiency Adviesbureau bv
Schoonouwenseweg 10
2821 NX Stolwijk
☎0182-341350
info@gea-bv.nl

---

* Versie: preview
Datum: oktober 2014

INHOUDSOPGAVE

1. Onderwerp en toepassingsgebied

1.1 Inleiding

Om de kwaliteit van de BRP te waarborgen en deze kwaliteit te kunnen garanderen heeft de Algemene Rekenkamer in 1996 geadviseerd om een kwaliteitscontrole in te voeren. Het ministerie van Binnenlandse Zaken heeft dit advies overgenomen.

Met ingang van 6 januari 2014 is de Wet Basisregistratie personen (Brp) in werking getreden. De BRP-audit is vervangen door het Evaluatie-instrument BRP en Reisdocumenten, onderdeel BRP, en is in de vorm van een zelfevaluatie.
De toetsing van het proces- en privacydeel verloopt via een vragenlijst. Deze vragenlijst is beschikbaar en de beantwoording is jaarlijks verplicht vóór 1 oktober, voor 1 november moet de gegenereerde rapportage aan het agentschap BPR worden toegezonden.

De inhoudelijke kwaliteit wordt centraal via de GBA-V gecontroleerd en de resultaten worden aan de gemeente beschikbaar gesteld. De eerste fase van deze controle is afgerond en de tweede fase is operationeel en heeft tot doel om de conversie van het BRP-stelsel naar het BRP-stelsel op termijn mogelijk te maken.

Zolang de BRP nog niet over de volle breedte is gerealiseerd, blijft de opzet van de persoonslijsten ongewijzigd en ook de controle daarop blijft via de programmatuur van de leverancier mogelijk.

De eisen rond de aanvraag, productie en verstrekking van reisdocumenten zijn vastgelegd in de Paspoortwet en de Paspoort uitvoeringsregeling Nederland 2001 (PUN 2001). De gemeente heeft de plicht om vanuit deze wet en regeling te voldoen aan een aantal minimale eisen.

De vragenlijst binnen het Evaluatie-instrument BRP en reisdocumenten, onderdeel Reisdocumenten, is begin 2013 definitief door de minister van BZK vastgesteld en gepubliceerd.
Deze vragenlijst vervangt de jaarlijkse toets via het “Beveiligingsnet” en de driejaarlijkse externe controle. Vóór 1 oktober van elk jaar moet de vragenlijst ingevuld zijn.
Het Evaluatie-instrument genereert een rapportage die beschikbaar is voor de gemeente. De rapportage moet vóór 1 november worden opgestuurd naar het agentschap BPR.

Met ingang van 1 oktober 2006 is er een nieuw rijbewijs gekomen. De eisen en regels voor de aanvraag, de productie en verstrekking (uitreiking) zijn vastgelegd in de Wegenverkeerswet 1994 (WVW), het Reglement rijbewijzen (RR) en de Regeling bestelling, transport en beveiliging rijbewijzen. Op enkele uitzonderingen na, komen deze overeen met de eisen en regels voor de reisdocumenten.

De controle op de naleving van de regels maakt deel uit van de reguliere accountantscontrole.

Het is van essentieel belang dat het Handboek Burgerzaken actueel blijft, de medewerkers op de hoogte zijn van de inhoud ervan en dat de maatregelen en procedures nageleefd worden. In de verschillende hoofdstukken wordt aandacht besteed aan deze aspecten.

1.2 Bewaarplaats handboek

Dit handboek bevat waardevolle en vertrouwelijke informatie die niet in handen mag komen van onbevoegden. Het origineel wordt bewaard in de kluis op de afdeling Burgerzaken.

Een kopie wordt bewaard bij de externe back-up.

2. Termen en definities

Voor dit hoofdstuk wordt verwezen naar het “Informatiebeveiligingsbeleid” en het “Algemeen Handboek Informatiebeveiliging”.

3. Structuur van deze norm

Voor de invulling van dit handboek is uitgegaan van de beveiligingseisen van algemene aard die in het beveiligingsbeleid zijn gedefinieerd.

In het handboek zijn de afspraken, maatregelen en procedures vastgelegd die het verloren gaan van informatie moet voorkomen. Ook het tegengaan van ongeoorloofd gebruik van informatie krijgt de aandacht.

3.1 Hoofdstukken

In dit handboek is dezelfde hoofdstukindeling aangehouden als in het "Informatiebeveiligingsbeleid".
Door het volgen van deze indeling, zijn enkele hoofdstuk en paragrafen niet nader beschreven of slechts heel summier.
Deze "lege" hoofdstukken en paragrafen zijn niet verwijderd, omdat er dan geen relatie kan worden gelegd met het "Informatiebeveiligingsbeleid".
Voor deze "lege" hoofdstukken en paragrafen wordt, voor gemeentebrede voorwaarden en regels, verwezen naar het "Algemeen Handboek Informatiebeveiliging".
In enkele gevallen is een onderwerp in geen van de handboeken beschreven. Voor die onderwerpen is er dan nog geen beleid ontwikkeld.

In dit handboek zijn enkele hoofdstukken verder uitgebreid omdat de voorschriften van de BRP, Reisdocumenten en Rijbewijzen dermate gedetailleerd zijn, dat deze niet onder één van de hoofdstukken/paragrafen van de Code voor Informatiebeveiliging kunnen worden geplaatst. Ook de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) is in dit opzicht niet toereikend.

3.2 Hoofdbeveiligingscategorieën

4. Risicobeoordeling en risicobehandeling

Voor dit hoofdstuk wordt verwezen naar het “Informatiebeveiligingsbeleid” en het “Algemeen Handboek Informatiebeveiliging”.

4.1 Beoordelen van de beveiligingsrisico’s

4.2 Behandelen van beveiligingsrisico’s

5. Beveiligingsbeleid

Voor dit hoofdstuk wordt verwezen naar het “Informatiebeveiligingsbeleid” en het “Algemeen Handboek Informatiebeveiliging”.

5.1 Informatiebeveiligingsbeleid

5.1.1 Beleidsdocument voor informatiebeveiliging

5.1.1.1 Verstrekkingen aan binnengemeentelijke afnemers

5.1.1.1.1 Gemeentelijke verordening

De Verordening Basisregistratie personen van de gemeente regelt welke verbanden er binnengemeentelijk zijn met de BRP, welke binnengemeentelijke afnemers en welke vrije derden er zijn. Verder regelt de verordening voor welk doel de gegevens worden verstrekt en onder welke voorwaarden.

5.1.1.2 Handmatige verstrekkingen

5.1.1.2.1 Procedure voor gegevensverstrekking

Handmatige gegevensverstrekking kan aan iedere afnemer of derde plaatsvinden.

Verstrekking vindt pas plaats nadat de identiteit van de verzoeker deugdelijk is vastgesteld.

5.1.1.2.2 Verstrekkingen aan burgers

Verstrekkingen aan de burger zelf (of aan een ander persoon alleen met een machtiging van die burger) geschieden over het algemeen via uittreksels.

5.1.2 Beoordeling van informatiebeveiligingsbeleid

6. Organisatie van informatiebeveiliging

Voor dit hoofdstuk wordt verwezen naar het “Informatiebeveiligingsbeleid” en het “Algemeen Handboek Informatiebeveiliging”.

6.1 Interne organisatie

6.1.1 Betrokkenheid van de directie bij informatiebeveiliging

6.1.2 Coördinatie van informatiebeveiliging

6.1.3 Toewijzing van verantwoordelijkheden voor informatiebeveiliging

6.1.4 Goedkeuringsproces voor IT-voorzieningen

6.1.5 Geheimhoudingsovereenkomst

6.1.6 Contact met overheidsinstanties

6.1.7 Contact met speciale belangengroepen

6.1.8 Onafhankelijke beoordeling van informatiebeveiliging

6.2 Externe partijen

6.2.1 Identificatie van risico’s die betrekking hebben op externe partijen

6.2.2 Beveiliging behandelen in de omgang met klanten

6.2.3 Beveiliging in overeenkomsten met een derde partij

7. Beheer van bedrijfsmiddelen

Voor dit hoofdstuk wordt verwezen naar het “Informatiebeveiligingsbeleid” en het “Algemeen Handboek Informatiebeveiliging”.

7.1 Verantwoordelijkheid voor bedrijfsmiddelen

7.1.1 Inventarisatie van bedrijfsmiddelen

7.1.2 Eigendom van bedrijfsmiddelen

7.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen

7.1.3.1 Beheerregeling

Voor het beheer van de BRP is een Beheerregeling opgesteld.

7.1.3.2 Beheer reisdocumenten

De reisdocumenten kennen een zeer strikt regime voor het omgaan met aanvragen tot aan het uiteindelijke uitreiken van de reisdocumenten. Verschillende functionarissen hebben hierbij een rol.

7.1.3.3 Beheer rijbewijzen

Evenals de reisdocumenten kennen de rijbewijzen een vast voorgeschreven regime. Verschillende functionarissen vervullen een specifieke taak.

7.2 Classificatie van informatie

7.2.1 Richtlijnen voor classificatie

7.2.2 Labeling en verwerking van informatie

8. Beveiliging van personeel

Er kunnen maatregelen genomen worden tegen risico's waar het personeel op de afdeling Burgerzaken en soms het personeel binnen het gehele gemeentehuis mee geconfronteerd kunnen worden. Om op voorhand problemen te voorkomen zijn hier maatregelen voor getroffen.

8.1 Voorafgaand aan het dienstverband

8.1.1 Rollen en verantwoordelijkheden

8.1.1.1 Tijdelijk personeel

Alle eisen, regels, procedures enz. zoals deze in dit handboek zijn opgenomen, gelden voor iedere medewerker. Zij kunnen tijdelijk in dienst zijn, op contractbasis werken of welke overeenkomst dan ook aan de aanwezigheid van een medewerker ten grondslag ligt.

8.1.2 Screening

De nieuw aan te stellen personeelsleden van de afdeling Burgerzaken (vast en tijdelijk - dienstverband) worden vooraf 'gescreend'. Dit wordt onderzocht door de afdeling P&O.

8.1.2.1 Opleidingsniveau

Alle medewerkers hebben een kennis en opleidingsniveau dat past bij de werkzaamheden die in het kader van de BRP, reisdocumenten of rijbewijzen worden verricht.

Het maken van onopzettelijke fouten wordt met deze kennis en opleiding teruggedrongen.

Bij wijziging van wetgeving op het gebied van de BRP, reisdocumenten of rijbewijzen (en andere vakgebieden) is het een goed gebruik dat de medewerkers van de afdeling Burgerzaken de voor hun taak relevante opleiding(en) volgen.

8.1.3 Arbeidsvoorwaarden

8.2 Tijdens het dienstverband

8.2.1 Directieverantwoordelijkheid

8.2.1.1 Aangewezen ambtenaren

8.2.1.1.1 Verklaringen onder ede of belofte

Indien bij een (eerste) inschrijving geen documenten overgelegd kunnen worden, is dit nog geen reden om geen gegevens op te nemen. Niet iedere ambtenaar kan dit doen. Door het college van B&W worden conform artikel 2.8 lid 2 sub e van de wet BRP hiervoor ambtenaren aangewezen.

8.2.1.1.2 Aangewezen ambtenaren reisdocumenten

8.2.1.1.2.1 De burgemeester

De burgemeester is bij wet bevoegd aanvragen voor een reisdocument van een ingezetene in ontvangst te nemen en het centraal geproduceerde reisdocument uit te reiken.

8.2.1.1.2.2 De Beveiligingsfunctionaris

De beveiligingsfunctionaris verricht geen uitvoerende werkzaamheden rond de reisdocumenten en beschikt over voldoende mogelijkheden om zijn taken adequaat te vervullen.

De aanwijzing van de beveiligingsfunctionaris en zijn plaatsvervanger en eventuele latere wijzingen worden aan het agentschap BPR gemeld via het standaardformulier “Registratie Beveiligingsfunctionaris” (B5).

8.2.1.1.2.3 De autorisatiebevoegden reisdocumenten

De burgemeester wijst per aanvraaglocatie tenminste twee ambtenaren aan die zullen functioneren als autorisatiebevoegde aanvraagstation overeenkomstig de gebruikershandleiding bij het aanvraagstation.

8.2.1.1.2.4 Verwerkingsbevoegden RAAS

De burgemeester benoemt de medewerkers die verwerkingsbevoegd zijn in het RAAS (conform art. 78 PUN 2001).

De ABR bepaalt welke medewerkers welke handelingen op het RAAS mogen verrichten.

8.2.1.1.2.5 Ontvangstbevoegden reisdocumenten

Overeenkomstig art. 81 van de PUN 2001 wijst de burgemeester per uitgiftelocatie ten minste drie ambtenaren aan om zendingen van reisdocumenten, identificatiekaarten en foto- en handtekeningformulieren in ontvangst te nemen.

Een kopie van de gewaarmerkte postmachtiging wordt bewaard in het personeelsdossier.

8.2.1.1.2.6 Aanvraag- en uitreikbevoegden

De burgemeester benoemt de medewerkers die bevoegd zijn tot het in behandeling nemen van de aanvragen en het uitreiken van reisdocumenten..

8.2.1.1.2.7 Lokaal beheerder

Uitsluitend medewerkers die door de ABR als lokaal beheerder zijn geautoriseerd mogen de beheerstaken op het RAAS.

8.2.1.1.3 Aangewezen ambtenaren rijbewijzen

8.2.1.1.3.1 De burgemeester

Evenals voor de reisdocumenten is de burgemeester bij wet bevoegd de aanvraag voor een rijbewijs van een ingezetene in ontvangst te nemen en het centraal geproduceerde rijbewijs uit te reiken.

8.2.1.1.3.2 De Beveiligingsfunctionaris

Ook voor de rijbewijzen is er een beveiligingsfunctionaris en die wordt ook benoemd door de burgemeester (art. 128 lid 6 Reglement rijbewijzen). De taken bestaan uit het beheer en het toezicht houden op de naleving van de beveiligingsprocedures.

De beveiligingsfunctionaris rijbewijzen is één en dezelfde persoon als de beveiligingsfunctionaris reisdocumenten.

8.2.1.1.3.3 De autorisatiebevoegden rijbewijzen

Overeenkomstig art. 128 lid Reglement rijbewijzen wijst de burgemeester per uitgiftelocatie tenminste twee ambtenaren van zijn gemeente aan die binnen het NRD backofficestation zullen functioneren als de autorisatiebevoegde rijbewijzen (ABR).

8.2.1.1.3.4 Ontvangstbevoegden rijbewijzen

Overeenkomstig art. 1 van de Regeling bestelling, transport en beveiliging rijbewijzen wijst de burgemeester per uitgiftelocatie ten minste twee ambtenaren aan om zendingen van rijbewijzen en aanvraagformulieren in ontvangst te nemen.

De levering van de reisdocumenten en de rijbewijzen geschiedt gelijktijdig. Daarom zijn de ontvangstbevoegden reisdocumenten en de ontvangstbevoegden rijbewijzen dezelfde personen.

8.2.1.1.3.5 Aanvraag- en uitreikbevoegden

De burgemeester wijst overeenkomstig art. 1 van de Regeling bestelling, transport en beveiliging rijbewijzen ten minste twee medewerkers aan die bevoegd zijn tot het bestellen (het in behandeling nemen van de aanvragen) en uitreiken van rijbewijzen. Deze RYA's kunnen, na autorisatie door de ABR, alle werkzaamheden op het NRD Backofficestation verrichten.

8.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

8.2.2.1 Voorlichting

Alle medewerkers zijn voorgelicht rond beveiligingszaken. Ze hebben stukken gelezen en voorlichtingsbijeenkomsten bijgewoond.

Een actueel exemplaar van het Handboek Burgerzaken is aanwezig op de afdeling Burgerzaken, inclusief alle bijlagen.

8.2.2.2 Instructies m.b.t. handelen bij een overval

Er is een instructie "Hoe te handelen bij een overval". Alle medewerkers van de afdeling Burgerzaken hebben kennis genomen van deze instructie.

8.2.3 Disciplinaire maatregelen

8.2.3.1 Maatregelen wanneer geheimhouding geschonden wordt

Het ten onrechte verstrekken van persoonsgegevens is op allerlei manieren omgeven door waarborgen. Desondanks is het niet uit te sluiten dat gegevens bewust of onbewust terechtkomen bij personen en instanties die daar geen recht op hebben. Al deze maatregelen zijn er op gericht om te voorkomen dat er nog meer bekend wordt.

8.2.3.1.1 Interne schending geheimhouding

Indien uit één van de voorgaande controles of anderszins blijkt dat de geheimhouding van BRP gegevens geschonden wordt, wordt dit gemeld bij de secretaris.

8.2.3.1.2 Externe schending geheimhouding

Indien op welke manier dan ook blijkt dat informatie ongeautoriseerd extern is terechtgekomen, wordt direct de toegang tot de BRP geblokkeerd.

Het college bepaalt of hierover informatie naar buiten wordt gebracht. Met name wordt hierbij gedacht aan het informeren van de gedupeerde burger.

8.3 Beëindiging of wijziging van het dienstverband

8.3.1 Beëindiging van verantwoordelijkheden

8.3.2 Retournering van bedrijfsmiddelen

8.3.3 Blokkering van toegangsrechten

9. Fysieke beveiliging en beveiliging van de omgeving

9.1 Beveiliging van ruimten

9.1.1 Fysieke beveiliging van de omgeving

9.1.2 Fysieke toegangsbeveiliging

9.1.2.1 Archiefruimte

De gemeente bewaart veel (bron)documenten, dossiers en andere zaken in een aparte archiefruimte. Ook de afdeling Burgerzaken heeft een apart gedeelte binnen deze ruimte.

9.1.2.1.1 Centrale archiefruimte

Brondocumenten ouder dan 1 jaar worden overgebracht naar het centrale archief van de gemeente.

9.1.2.1.2 Beveiliging van de archiefruimte

De deur van het archief is beveiligd tegen inbraak en brandvertragend.

9.1.2.2 Afdeling Burgerzaken

De afdeling Burgerzaken van de gemeente is de plaats waar de meest recente brondocumenten bewaard worden. Op de afdeling Burgerzaken staan ook werkstations met de BRP applicatie.

9.1.2.2.1 Kluis op de afdeling Burgerzaken

Op de afdeling Burgerzaken is een inpandige kluis aanwezig voor een veilige opslag van belangrijke en/of waardevolle objecten.

Daarnaast bevindt zich in deze inpandige kluisruimte nog een separate kluis voor opslag van rijbewijzen en reisdocumenten.

9.1.2.2.2 Beveiliging van de kluis

De deur van de kluis op de afdeling Burgerzaken is beveiligd tegen inbraak en brandvertragend.

9.1.3 Beveiliging van kantoren, ruimten en faciliteiten

9.1.4 Bescherming tegen bedreigingen van buitenaf

9.1.5 Werken in beveiligde ruimten

9.1.6 Openbare toegang en gebieden voor laden en lossen

9.1.6.1 Ontvangst van zendingen reisdocumenten

Dagelijks tussen 8.00 en 8.30 uur worden de geproduceerde reisdocumenten bezorgd.
De ontvangen documenten worden gecontroleerd met de melding van verzending in het RAAS en vervolgens ingeklaard in het RAAS.

9.1.6.2 Ontvangst van zendingen rijbewijzen

Gelijktijdig met de reisdocumenten worden de geproduceerde rijbewijzen bezorgd en ingeklaard.

9.2 Beveiliging van apparatuur

9.2.1 Plaatsing en bescherming van apparatuur

9.2.1.1 RAAS

De RAASserver staat in de serverruimte bij de afdeling systeembeheer.
De apparatuur wordt onderhouden door Morpho.

9.2.1.2 NRD Backofficestation

Het NRD Backofficestation staat bij de afdeling Burgerzaken en is niet zichtbaar voor het publiek.
De apparatuur wordt onderhouden door de RDW.

9.2.2 Nutsvoorzieningen

9.2.3 Beveiliging van kabels

9.2.4 Onderhoud van apparatuur

9.2.5 Beveiliging van apparatuur buiten het terrein

9.2.6 Veilig verwijderen of hergebruik van apparatuur

9.2.7 Verwijdering van bedrijfseigendommen

10. Beheer van communicatie- en bedieningsprocessen

10.1 Bedieningsprocedures en verantwoordelijkheden

10.1.1 Gedocumenteerde bedieningsprocedures

10.1.2 Wijzigingsbeheer

10.1.2.1 Versiebeheer BRP

De kern van de BRP-applicatie wordt gevormd door goedgekeurde (geschouwd en getoetste) programmatuur.

Indien noodzakelijk wordt na installatie van de programmatuur dit gemeld aan het agentschap BPR.

10.1.3 Functiescheiding

10.1.3.1.1 Functiescheiding reisdocumenten

De PUN 2001 schrijft voor dat er functiescheiding moet zijn tussen de medewerkers die verstrekken, beheren en uitreiken. Onder verstrekken moet in dit kader verstaan worden “het accepteren van de aanvraag”, omdat op dat moment al wordt bepaald dat het document geproduceerd en uitgereikt zal gaan worden. In de hiervoor vermelde stappen loopt dit traject tot en met het samenstellen van het aanvraagbestand.

10.1.3.1.2 Geïmplementeerde functiescheiding reisdocumenten

In de PUN 2001 is voorschreven dat moet zijn voorzien in een adequate functiescheiding. Door de omvang van de gemeente en dan met name tijdens vakanties is het soms niet altijd mogelijk aan deze verplichting te voldoen. Op de momenten dat functiescheiding onvoldoende wordt gerealiseerd, zijn compenserende maatregelen van kracht.

10.1.3.1.3 Functiescheiding rijbewijzen

Ook het rijbewijzentraject kent een voorgeschreven functiescheiding tussen het aanvragen en uitreiken van het rijbewijs.

De andere taken kunnen zowel door de ABR als de RYA worden verricht.

10.1.3.1.4 Geïmplementeerde functiescheiding rijbewijzen

Het probleem van de functiescheiding geldt niet alleen voor de reisdocumenten, maar ook voor de rijbewijzen. Zeker omdat er functiescheiding moet zijn voor de balietaken.

10.1.4 Scheiding van faciliteiten voor ontwikkeling, testen en productie

10.2 Beheer van dienstverlening door een derde partij

10.2.1 Dienstverlening

10.2.2 Controle en beoordeling van dienstverlening door de derde partij

10.2.3 Beheer van wijzigingen in dienstverlening door een derde partij

10.3 Systeemplanning en acceptatie

10.3.1 Capaciteitsbeheer

10.3.2 Systeemacceptatie

10.4 Bescherming tegen virussen en 'mobile code'

10.4.1 Maatregelen tegen virussen

10.4.2 Maatregelen tegen 'mobile code'

10.5 Back-up

10.5.1 Reservekopieën maken (back-ups)

De systeembeheerder maakt van alle data en programmatuur elke nacht een (full) back-up.

10.5.1.1 Dagelijkse back-up reisdocumenten

Elke nacht wordt automatisch een back-up gemaakt van het RAAS. Na het maken van de back-up wordt gecontroleerd of deze is geslaagd. Elke dag heeft een eigen tape. De dag staat aangetekend op de rug van de tape. De dagelijkse back-up van de reisdocumenten valt onder de verantwoordelijkheid van de autorisatiebevoegde reisdocumenten.

10.5.1.2 Back-up rijbewijzen

Het NRD Backofficestation bevat zelf geen gegevens. Het maken van een back-up is dan ook niet van toepassing.

10.5.1.3 Beveiliging berichten via netwerk

De berichten welke via het netwerk worden ontvangen en verzonden, worden automatisch beveiligd via de dagelijkse back-up.

Daarnaast worden de berichten 2 werkdagen in de mailbox binnen het GBA/BRP-netwerk bewaard.

10.5.1.4 Beveiliging berichten reisdocumenten

De berichten van de reisdocumenten worden automatisch beveiligd via de dagelijkse back-up.

10.5.1.5 Beveiliging berichten rijbewijzen

Omdat in het NRD Backofficestation geen informatie wordt opgeslagen, is de beveiliging van berichten niet aan de orde.

10.6 Beheer van netwerkbeveiliging

10.6.1 Maatregelen voor netwerken

10.6.2 Beveiliging van netwerkdiensten

10.7 Behandeling van media

10.7.1 Beheer van verwijderbare media

10.7.2 Verwijdering van media

10.7.3 Procedures voor de behandeling van informatie

10.7.3.1 Identificatie algemeen

Binnen de afdeling Burgerzaken geldt een vrij stringent beleid met betrekking tot het vaststellen van de identiteit van een persoon die zich meldt voor het doen van een bepaalde aangifte dan wel een bezoek aan de afdeling Burgerzaken brengt om één of ander product van de afdeling Burgerzaken te verkrijgen.

10.7.3.1.1 Vaststellen identiteit zonder document als bedoeld in art. 1 Wet op de Identificatieplicht

Het gebeurt nog wel eens dat iemand zijn identiteitsbewijs verloren is, of niet bij zich heeft. In eerste instantie zal betrokkene worden gevraagd een ander document te overleggen aan de hand waarvan de identiteit afgeleid kan worden.

10.7.3.1.2 Identificatie bij postverwerking

Ook bij het verwerken van post dient identificatie plaats te vinden.

10.7.3.1.3 Identificatie bij digitale verzoeken en aangiften

De gemeenten hebben de opdracht om steeds meer verzoeken en aangiften digitaal af te handelen. De identificatie geschiedt dan via DigiD.

10.7.3.2 Gegevensverwerking

Gegevensverwerking vormt de basis van een actuele, juiste en volledige BRP. Tevens moet hier ook onder worden verstaan, het toetsen, verzamelen en archiveren van brondocumenten en het doen van kennisgevingen.

10.7.3.2.1 Inschrijving geprivilegieerden

10.7.3.2.2 Adreskoppeling BAG-BRP

Na de invoering van de BAG als basisadministratie adres en gebouwen, worden de adresgegevens in de BRP nadrukkelijk gekoppeld aan de specifieke gebouwgegevens in de BAG via de verwijzende sleutel (identificatiecode verblijfplaats) naar de adresseerbare objecten in de BAG (verblijfsobject, standplaats of een ligplaats).

10.7.3.2.3 Inschrijving op een briefadres

10.7.3.2.4 Terugmeldingen

De aanwijzing van de BRP als Basisregistratie houdt in dat een deel van de BRP-gegevens is aangewezen als authentiek. Afnemers van de BRP zijn verplicht, om deze gegevens uit de BRP over te nemen.

10.7.3.2.5 Adresonderzoek

10.7.3.2.6 Handleiding best

10.7.3.2.7 Bestuurlijke boete

10.7.3.2.8 Mutatieverslagen op papier

De gegevensbeheerder laat dagelijks de mutatieverslagen en controlelijsten printen.

10.7.3.2.9 Gebruikte brondocumenten

De gegevensbeheerder ziet er op toe dat verwerkte brondocumenten tenminste 5 werkdagen worden bewaard in de kluis van de afdeling Burgerzaken. Daarna vindt archivering plaats in het centraal archief.

10.7.3.2.10 Opschonen BRP-bestanden

De BRP bestanden met hierin de BRP berichten worden eenmaal per maand opgeschoond. Afgeronde berichtencycli ouder dan 1 maand worden dan verwijderd.

10.7.3.3 Verstrekkingen uit de BRP

10.7.3.3.1 Wie gegevens verstrekt kan krijgen

Om duidelijk aan te kunnen geven welke gegevens van een burger aan wie kunnen worden verstrekt, is het noodzakelijk een definitie te geven van de gebruikte termen in de wet- en regelgeving. In de wet- en regelgeving worden twee groepen instanties onderscheiden die informatie kunnen ontvangen.

De gemeente heeft de bevoegdheid om naast de afnemers en (verplichte en bijzondere) derden nog andere zogenaamde “vrije derden” te benoemen. Deze vrije derden moeten wel vallen binnen het wettelijke kader van de wet BRP (artikel 3.9).

10.7.3.3.2 Vormen van gegevensverstrekking

Persoonsgegevens uit de BRP kunnen in verschillende vormen verstrekt worden. Een van de uitgangspunten bij de opzet van de BRP is, dat afnemers en geautoriseerde derden automatisch de gegevens verstrekt krijgen waar men recht op heeft.

10.7.3.3.3 Verstrekkingen via het berichtenverkeer

Na de ingebruikname van GBA-V Full Service vinden er geen verstrekkingen meer plaats via het berichtenverkeer. Een uitzondering hierop is de verstrekking aan de GBA-V.

Gemeenten krijgen geen berichten meer van en sturen geen berichten meer naar afnemers. Uitzondering hierop zijn vrije berichten. Deze kunnen gemeenten nog wel sturen en ontvangen.

10.7.3.3.4 Protocolplicht

In de wet BRP is de protocollering geregeld van verstrekkingen van persoonsgegevens vanwege de bescherming van de persoonlijke levenssfeer. In artikel 3.22 van de wet is de verplichting van het college vastgelegd.

10.7.3.3.4.1 Instructies protocollering

Protocolleren wil zeggen dat wordt vastgelegd: over wie, wanneer, door wie, welke gegevens en aan wie informatie is verstrekt.

10.7.3.3.4.2 Protocolgegevens

Ten einde te kunnen constateren dat de richtlijnen correct worden uitgevoerd, zal periodieke controle op de uitvoering hiervan plaatsvinden.

10.7.3.4 Verwerking van reisdocumenten

Zoals eerder vermeld kent het traject van de reisdocumenten een aantal voorgeschreven stappen.

Voor het verwerken van de aanvraag en het uitreiken van het reisdocument geldt een verplichte functiescheiding.

10.7.3.4.1 Beheerstaken

Naast de hiervoor genoemde activiteiten zijn er binnen het RAAS een aantal beheerstaken die voor het grootste gedeelte uitgevoerd worden door de lokaal beheerder. In de handleiding van het RAAS zijn deze taken uitgebreid beschreven.

10.7.3.5 Aanvraagprocedure reisdocumenten

Het aanvragen van een reisdocument is een fraudegevoelig moment, vooral bij een eerste aanvraag. Een onrechtmatige verstrekking heeft grote gevolgen en kan moeilijk worden opgespoord. Voordat een aanvraag in behandeling kan worden genomen moet een uitgebreide identificatie plaatsvinden.

10.7.3.5.1 Vaststellen identiteit

Indien de aanvrager in het bezit is van een ander of oud reisdocument, wordt de identiteit aan de hand van dat document vastgesteld.

10.7.3.5.1.1 Oud reisdocument

Indien de aanvrager in het bezit is van een oud reisdocument dat ingehouden moet worden, dan wordt de identiteit van de aanvrager vastgesteld m.b.v. dit document. De identiteitsvaststelling geschiedt o.a. door vergelijking van de foto met de persoon.

Worden onregelmatigheden bij het oude document geconstateerd, dan dient dit eerst te worden opgehelderd alvorens een nieuwe aanvraag in behandeling kan worden genomen.

10.7.3.5.1.2 Ander reisdocument

Is de aanvrager in het bezit van een reisdocument dat niet ingehouden moet worden, dan wordt de identiteit op dezelfde wijze vastgesteld.

10.7.3.5.1.3 Nog geen reisdocument

Het is begrijpelijk dat bij een eerste aanvraag van een reisdocument niet altijd een ander identificerend document kan worden overgelegd en zeker geen ander reisdocument. Toch is het van het grootste belang dat de identiteit van de aanvrager deugdelijk wordt vastgesteld.

10.7.3.5.2 De pasfoto

Bij de aanvraag van een nieuw reisdocument moet een pasfoto worden aangeboden.

10.7.3.5.3 Vingerafdrukken

Van kinderen jonger dan twaalf worden geen vingerafdrukken afgenomen.

10.7.3.5.4 Verlopen reisdocument

Een reisdocument dat op het moment van de aanvraag verlopen is, wordt direct ingehouden. Is het oude reisdocument op het moment van de aanvraag nog niet verlopen dan kan dit worden ingeleverd.

Op verzoek kan het oude reisdocument “onbruikbaar gemaakt” worden teruggeven.

10.7.3.5.5 Meervoudige vermissing

Bij een meervoudige vermissing (driemaal een vermissing in een periode van 5 jaar) wordt een verzoek aan het ministerie van Binnenlandse Zaken gericht om de betrokkene op de signaleringslijst te plaatsen (zie hiervoor de circulaire van 30 maart 2011 kenmerk 2011-2000106454).

10.7.3.5.6 Toestemmingsverklaring

Voordat een aanvraag van een minderjarige of een onder curatele gestelde in behandeling kan worden genomen moet een toestemmingsverklaring voorzien van handtekening van alle gezaghouder(s) (voor een kind veelal van vader én moeder) worden overgelegd. Een kind vanaf 12 jaar en een onder curatele gestelde kan zonder toestemming een NIK aanvragen.

10.7.3.6 Opslag media reisdocumenten

De media van de reisdocumenten worden op dezelfde wijze behandeld als van de BRP. De reisdocumenten kennen echter nog een aantal specifieke media die hierna worden vermeld.

10.7.3.6.1 Opslag periferie

Alle documenten, opslagmedia, programmatuur, documentatie en overige materialen, evenals de ontvangen en ingeklaarde reisdocumenten bevinden zich tijdens werktijden in de kluisruimte bij burgerzaken, zodat deze voor onbevoegden onbereikbaar zijn.

10.7.3.6.2 Nog niet opgehaalde reisdocumenten

Indien een reisdocument twee maanden na productie nog niet is opgehaald wordt hierover een brief verzonden aan de aanvrager.

10.7.3.6.3 Vernietiging oude en niet opgehaalde reisdocumenten

Ingehouden reisdocumenten worden dagelijks vernietigd door deze te versnipperen.

10.7.3.6.4 Onjuist geproduceerde reisdocumenten

Een onjuist geproduceerd reisdocument (misdruk) of een reisdocument met een verkeerde tenaamstelling wordt per aangetekende post, vergezeld met formulier C10, naar Morpho gezonden.

10.7.3.7 Verstrekking reisdocumenten

De reisdocumenten kennen zelf geen verstrekkingsregime.

10.7.3.8 Verwerking van rijbewijzen

Evenals de reisdocumenten kent het traject van de rijbewijzen een aantal voorgeschreven stappen.

10.7.3.9 Aanvraagprocedure rijbewijzen

Indien de aanvrager woonachtig is in Nederland, moet de aanvraag om afgifte van een rijbewijs worden ingediend bij de gemeente, waar betrokkene als ingezetene is ingeschreven in de BRP.

10.7.3.9.1 Het aanvraagformulier

Het aanvraagformulier wordt door de BRP-applicatie geproduceerd en bevat in ieder geval de gegevens die van de RDW zijn ontvangen.

10.7.3.9.2 De pasfoto

De eisen die aan de pasfoto worden gesteld zijn gelijk aan de eisen die gelden voor de reisdocumenten.

10.7.3.9.3 Vermissing oud rijbewijs

Bij een verzoek om afgifte van een nieuw rijbewijs wegens vermissing of diefstal, moet een door de Nederlandse politie opgemaakt proces-verbaal worden overgelegd.

10.7.3.10 Opslag media rijbewijzen

De media van de rijbewijzen worden op dezelfde manier behandeld als de reisdocumenten.

10.7.3.10.1 Nog niet opgehaalde rijbewijzen

Aan de hand van de in het rijbewijzenregister opgeslagen gegevens wordt maandelijks gecontroleerd op rijbewijzen die langer dan één maand in de voorraad staan en dus nog niet zijn afgehaald door de desbetreffende houder.

10.7.3.10.2 Vernietiging oude rijbewijzen

Ingeleverde en ingenomen rijbewijzen worden meteen vernietigd.

10.7.3.10.3 Onjuiste en niet opgehaalde rijbewijzen

Van onjuist geproduceerde rijbewijzen en rijbewijzen die niet binnen drie maanden zijn opgehaald, wordt een proces-verbaal opgemaakt. Het proces-verbaal en de rijbewijzen worden naar de RDW gezonden.

10.7.3.11 Verstrekking rijbewijzen

De rijbewijzen kennen zelf geen verstrekkingsregime.

10.7.3.12 Rechten van de burger

Dit hoofdstuk bevat daarom niet alleen de maatregelen bij schending van de geheimhouding, maar ook controles om de schending te ontdekken en de rechten van de burger te waarborgen.

10.7.3.12.1 Algemeen

Naast een aantal verplichtingen heeft een burger ook een aantal rechten. In verband met de privacy zijn deze rechten van groot belang. In de rechten van de burger is bepaald of de

gemeente spontaan informatie moet verstrekken of dat de burger een verzoek in moet dienen om gebruik te kunnen maken van zijn recht.

De burger heeft de volgende rechten:

- Recht op verkrijging van een afschrift;
- Inzagerecht;
- Recht van naamgebruik
- Correctierecht;
- Recht op geheimhouding van gegevens;
- Recht op kennisname van gegevensverstrekking;
- Recht op verwijdering van gegevens.

10.7.4 Beveiliging van systeemdocumentatie

10.8 Uitwisselen van informatie

10.8.1 Beleid en procedures voor informatie-uitwisseling

10.8.2 Uitwisselingsovereenkomsten

10.8.2.1 Uitreikprocedure reisdocumenten

Bij een geaccepteerde aanvraag wordt een afhaalbewijs verstrekt aan de burger. Een week na de aanvraag kan de burger zijn nieuwe reisdocument afhalen. Bij het afhalen moet het afhaalbewijs worden overgelegd en eventueel het nog in te leveren (oude) reisdocument.

10.8.2.1.1 Vermissing of ingenomen reisdocument bij uitreiking

Indien het oude reisdocument nog ingeleverd moet worden en dit kan niet worden overgelegd, dan is hiervan een proces-verbaal of een verklaring van inname vereist.

10.8.2.1.2 Aanvrager is verhuisd

Indien de aanvrager op moment van uitreiking naar een andere gemeente is verhuisd, moet het document in die andere gemeente worden uitgereikt.

10.8.2.2 Uitreikprocedure rijbewijzen

De aanvrager kan het rijbewijs na 5 werkdagen bij het gemeentehuis afhalen.

Er wordt geen melding in het systeem gemaakt, dat het oude rijbewijs is ingenomen. Dit in tegenstelling tot de reisdocumenten.

10.8.2.2.1 Vermissing oude rijbewijs

Indien de aanvrager in het bezit is van een oud rijbewijs, dan moet dit ingeleverd worden. Kan het rijbewijs niet worden ingenomen omdat het tussen aanvraag en uitreiking is zoekgeraakt, dan moet een door de politie opgemaakt proces-verbaal worden ingeleverd.

10.8.2.2.2 De aanvrager is verhuisd

Indien de aanvrager op het moment van de uitreiking naar een andere gemeente is verhuisd, dan moet hij toch het nieuwe rijbewijs afhalen in de gemeente waar de aanvraag is gedaan.

10.8.2.3 Tussentijdse melding van vermissing reisdocumenten

Indien een reisdocument als vermist wordt aangegeven, dan is hiervan een proces-verbaal vereist.

10.8.3 Fysieke media die worden getransporteerd

10.8.4 Elektronische berichtenuitwisseling

Het verstrekken of uitwisselen van BRP-gegevens via externe datacommunicatie, anders dan het BRP-netwerk, is niet toegestaan.

10.8.5 Systemen voor bedrijfsinformatie

10.9 Diensten voor e-commerce

10.9.1 E-commerce

10.9.2 Onlinetransacties

10.9.3 Openbare beschikbare informatie

10.10 Controle

10.10.1 Aanmaken audit-logbestanden

10.10.2 Controle op systeemgebruik

10.10.2.1 Controle op gebruik functies

10.10.3 Bescherming van informatie in logbestanden

10.10.3.1 Logging BRP

Alle mutaties die ingebracht worden, worden gelogd. Het is mogelijk om verwerkte mutaties nogmaals te verwerken ingeval van calamiteiten.

10.10.4 Logbestanden van administrators en operators

10.10.5 Registratie van storingen

10.10.6 Synchronisatie van systeemklokken

11. Toegangsbeveiliging

11.1 Bedrijfseisen ten aanzien van toegangsbeheersing

11.1.1 Toegangsbeleid

11.2 Beheer van toegangsrechten van gebruikers

11.2.1 Registratie van gebruikers

11.2.2 Beheer van speciale bevoegdheden

11.2.2.1 IAR-kaart

Het systeem van sleutels, persoonsgebonden identificatiekaarten en pincodes is het instrument waarmee het autorisatiepatroon (IAR-kaart) vorm krijgt. De ABR's en de verwerkingsbevoegde medewerkers ontvangen een persoonlijke IAR-kaart met daarop de persoonlijke autorisatie voor het RAAS.

11.2.2.2 Opstartkaart

Door Morpho wordt per aanvraagstationlocatie twee opstartkaarten verstrekt. De ABR is verantwoordelijk voor het gebruik en het beheer van deze kaarten.

11.2.2.3 Smartcard

Het systeem van sleutels, persoonsgebonden smartcards en pincodes is het instrument waarmee het autorisatiepatroon vorm krijgt. De ABR's en de RYA's ontvangen een persoonlijke smartcard met daarop de persoonlijke gegevens en de autorisatie. Zij tekenen voor de ontvangst van de smartcard.

11.2.3 Beheer van gebruikerswachtwoorden

11.2.4 Beoordeling van toegangsrechten van gebruikers

11.2.4.1 Autorisatie BRP-gegevens

De autorisatie voor het raadplegen van persoonsgegevens uit de BRP applicatie gebeurt door de applicatiebeheerder van de afdeling Burgerzaken na schriftelijk verzoek van het betreffende afdelingshoofd van de betrokken medewerker én na parafering van dit verzoek door het hoofd afdeling Burgerzaken.

11.2.4.2 Toegang tot de reisdocumentengegevens

De toegang tot de reisdocumentengegevens is op een gelijkwaardige manier gerealiseerd als voor de BRP-gegevens.

.

11.2.4.3 Toegang tot de rijbewijsgegevens

In de BRP en het NRD Backofficestation worden geen rijbewijsgegevens opgeslagen. De rijbewijsgegevens worden elke keer opgehaald uit het centrale rijbewijzenregister bij de RDW.

De toegang tot deze gegevens wordt verkregen via de BRP of het NRD Backofficestation.

11.3 Verantwoordelijkheden van gebruikers

11.3.1 Gebruik van wachtwoorden

Alle medewerkers die gebruikmaken van het BRP-systeem hebben login codes en passwords.

Het is onder geen enkele voorwaarde toegestaan de login code en het password aan iemand bekend te maken.

11.3.2 Onbeheerde gebruikersapparatuur

11.3.3 'Clear desk'- en 'clear screen'-beleid

11.4 Toegangsbeheersing voor netwerken

11.4.1 Beleid ten aanzien van het gebruik van netwerkdiensten

11.4.2 Authenticatie van gebruikers bij externe verbindingen

11.4.3 Identificatie van netwerkapparatuur

11.4.4 Bescherming op afstand van poorten voor diagnose en configuratie

11.4.5 Scheiding van netwerken

11.4.6 Beheersmaatregelen voor netwerkverbindingen

11.4.7 Beheersmaatregelen voor netwerkrouting

11.5 Toegangsbeveiliging voor besturingssystemen

11.5.1 Beveiligde inlogprocedures

11.5.2 Gebruikersidentificatie en –authenticatie

11.5.3 Systemen voor wachtwoordbeheer

11.5.4 Gebruik van systeemhulpmiddelen

11.5.5 Time-out van sessies

11.5.6 Beperking van verbindingstijd

11.6 Toegangsbeheersing voor toepassingen en informatie

11.6.1 Beperken van toegang tot informatie

11.6.2 Isoleren van gevoelige systemen

11.7 Draagbare computers en telewerken

11.7.1 Draagbare computers en communicatievoorzieningen

11.7.2 Telewerken

12. Verwerving, ontwikkeling en onderhoud van informatiesystemen

Voor dit hoofdstuk wordt verwezen naar het “Informatiebeveiligingsbeleid” en het “Algemeen Handboek Informatiebeveiliging”.

12.1 Beveiligingseisen voor informatiesystemen

12.1.1 Analyse en specificatie van beveiligingseisen

12.2 Correcte verwerking in toepassingen

12.2.1 Validatie van invoergegevens

12.2.1.1.1 Kwaliteitscontroles

Periodiek vinden kwaliteitscontroles plaats.

De resultaten worden met de medewerkers besproken tijdens het afdelingsoverleg.

12.2.2 Beheersing van interne gegevensverwerking

12.2.3 Integriteit van berichten

12.2.4 Validatie van uitvoergegevens

12.3 Cryptografische beheersmaatregelen

12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen

12.3.2 Sleutelbeheer

12.4 Beveiliging van systeembestanden

12.4.1 Beheersing van operationele programmatuur

12.4.2 Bescherming van testdata

12.4.3 Toegangsbeheersing voor broncode en programmatuur

12.5 Beveiliging bij ontwikkelings- en ondersteuningprocessen

12.5.1 Procedures voor wijzigingsbeheer

12.5.2 Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem

12.5.3 Restricties op wijzigingen in programmatuurpakketten

12.5.4 Uitlekken van informatie

12.5.5 Uitbestede ontwikkeling van programmatuur

12.6 Beheer van technische kwetsbaarheden

12.6.1 Beheersing van technische kwetsbaarheden

13. Beheer van informatiebeveiligingsincidenten

Voor dit hoofdstuk wordt verwezen naar het “Informatiebeveiligingsbeleid” en het “Algemeen Handboek Informatiebeveiliging”.

13.1 Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken

13.1.1 Rapportage van informatiebeveiligingsgebeurtenissen

13.1.2 Rapportage van zwakke plekken in de beveiliging

13.2 Beheer van informatiebeveiligingsincidenten en –verbeteringen

13.2.1 Verantwoordelijkheden en procedures

13.2.2 Leren van informatiebeveiligingsincidenten

13.2.3 Verzamelen van bewijsmateriaal

14. Bedrijfscontinuïteitsbeheer

Voor dit hoofdstuk wordt verwezen naar het “Informatiebeveiligingsbeleid” en het “Algemeen Handboek Informatiebeveiliging”.

14.1 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

14.1.1 Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer

14.1.2 Bedrijfscontinuïteit en risicobeoordeling

14.1.3 Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging

14.1.4 Kader voor de bedrijfscontinuïteitsplanning

14.1.5 Testen, onderhoud en herbeoordelen van bedrijfscontinuïteitsplannen

15. Naleving

15.1 Naleving van wettelijke voorschriften

15.1.1 Identificatie van toepasselijke wetgeving

15.1.2 Intellectuele eigendomsrechten (Intellectual Property Rights, IPR)

15.1.3 Bescherming van bedrijfsdocumenten

15.1.4 Bescherming van gegevens en geheimhouding van persoonsgegevens

15.1.5 Voorkomen van misbruik van IT-voorzieningen

15.1.6 Voorschriften voor het gebruik van cryptografische beheersmaatregelen

15.2 Naleving van beveiligingsbeleid en –normen en technische naleving

15.2.1 Naleving van beveiligingsbeleid en –normen

15.2.1.1 BRP

Communicatie naar de medewerkers vindt plaats via het reguliere afdelingsoverleg.

15.2.1.1.1 Controle op het naleven van voorschriften en afspraken

Eenmaal per kwartaal wordt er door het hoofd afdeling Burgerzaken een controle uitgevoerd op het nakomen van beveiligingsafspraken en voorschriften op de afdeling Burgerzaken.

15.2.1.1.2 Controle op versie- en documentatiebeheer

Eenmaal per kwartaal wordt er door het hoofd afdeling Burgerzaken een controle uitgevoerd of de afspraken rond versiebeheer en de actualisatie van documentatie goed uitgevoerd worden.

15.2.1.1.3 Controle op toegekende en geïmplementeerde autorisaties

Voor de uitvoering van wettelijke taken is het noodzakelijk dat medewerkers toegang hebben tot de BRP.

15.2.1.1.4 Controle op naleving instructies

Door het hoofd afdeling Burgerzaken wordt tijdens het functioneringsgesprek de naleving van de instructies, om de integriteit van de BRP te waarborgen, aan de orde gesteld.

15.2.1.2 Reisdocumenten

15.2.1.2.1 Dagelijkse controle reisdocumenten

Dagelijks worden controles uitgevoerd om fraude, onjuiste verstrekkingen en inconsistenties zoveel mogelijk te voorkomen.

15.2.1.2.2 Controle aanwezige reisdocumenten

Eenmaal per maand wordt door de ABR een controle uitgevoerd of de feitelijk aanwezige reisdocumeten overeenkomt met de administratieve voorraad in het RAAS.

15.2.1.2.3 Controle afhandeling systeemsignalen reisdocumenten

Periodiek (éénmaal per maand) wordt door de ABR een controle uitgevoerd op de afhandeling van systeemsignalen. Indien blijkt dat signalen niet of niet correct zijn afgehandeld, wordt dit besproken met de geautoriseerde medewerkers.

15.2.1.3 Rijbewijzen

15.2.1.3.1 Dagelijkse controle rijbewijzen

Dagelijks wordt gelijktijdig de controle op de reisdocumenten en de controle op de rijbewijzen uitgevoerd.

15.2.1.3.2 Maandelijkse controle

Maandelijks wordt de voorraad rijbewijzen gecontroleerd aan de hand van de in het rijbewijzenregister opgeslagen gegevens.

15.2.2 Controle op technische naleving

15.3 Overwegingen bij audits van informatiesystemen

15.3.1 Beheersmaatregelen voor audits van informatiesystemen

15.3.2 Bescherming van hulpmiddelen voor audits van informatiesystemen