4 Administratieve organisatie

Onder administratieve organisatie wordt de minimale set van organisatorische maatregelen verstaan, die noodzakelijk is voor een verantwoord gebruik en beheer van de vreemdelingenadministratie. Hiermee dient de kwaliteit van de gegevens en de correcte uitvoering van de vreemdelingenadministratie te worden gewaarborgd. Onderstaande organisatorische maatregelen zijn verplicht voor elke geautomatiseerde vreemdelingenregistratie.

4.1 Beveiliging tegen ondeskundig en onbevoegd gebruik

Om de geautomatiseerde vreemdelingenadministratie te beveiligen tegen ondeskundig en onbevoegd gebruik dient voor de verstrekking van gegevens gebruik te worden gemaakt van autorisaties.
Autorisatie geeft hierbij tevens de mogelijkheid tot functiescheiding.

Bij het toekennen van autorisaties zijn de volgende toewijzingen aan gebruikers van toepassing.

Gebruikers:
- Korpschefs (Kc);
- IND;
- CRV;
- speciaal gemachtigden (overig), nog niet aangewezen.

Functionaliteiten:
- opvoeren van gegevens;
- wijzigen van gegevens;
- raadplegen van gegevens;
- verwijderen van gegevens.

4.1.1 Autorisatie-matrix CRV

CRV	Kc	IND	GBA[1]	overig
opvoeren	+			
wijzigen	+			
raadplegen	+			
verwijderen [2]	-			

1) GBA = Gemeentelijke Basisadministratie; adresmutaties, geboorten, overlijden, wijzigingen nationaliteit etc. zullen via de Gemeentelijke Basisadministratie naar de betreffende geautomatiseerde vreemdelingenadministratie gezonden worden.
2) De verwijdering van gegevens uit het CRV is een geautomatiseerde activiteit (zie 3.1).

4.1.2 Autorisatie-matrix geautomatiseerde vreemdelingenadministratie

vreemd. adm.	Kc	IND	GBA	overig
opvoeren	+			
wijzigen	+			
raadplegen	+			
verwijderen	+[1)]			

1) Verwijderen van gegevens is alleen mogelijk zolang de vreemdeling nog niet in het CRV bekend is.

4.1.3 Autorisaties op lokaal niveau

Binnen iedere gebruikersorganisatie dient men een verdere onderverdeling van autorisaties te maken. De verantwoordelijkheid van de verdere onderverdeling ligt bij het hoofd van de gebruikersorganisatie en dient te worden onderhouden door het applicatiebeheer. Autorisaties dienen altijd schriftelijk te worden verleend. Het beheer van autorisaties dient te allen tijde door daartoe bevoegde controlerende instanties opvraagbaar te zijn.

4.2 Continuïteit in verwerking en beschikbaarheid van gegevens

Continuïteit is de redelijke zekerheid dat de gegevensverwerking ongestoord voortgang **zal** kunnen vinden. Dat wil zeggen dat ook na ernstige storingen de gegevensverwerking binnen redelijke termijnen kan worden hervat.

4.2.1 Actualiteit van gegevens

De geautomatiseerde vreemdelingenadministratie dient altijd actueel te zijn. Mutaties in de geautomatiseerde vreemdelingenadministratie dienen binnen 24 uur aan het CRV te worden doorgegeven.

Registratie van gegevens in een geautomatiseerde vreemdelingenadministratie bestemd voor de IND dienen binnen 24 uur bij de IND bekend te zijn.

4.2.2 Beschikbaarheid van gegevens

Het CRV is in principe continu beschikbaar voor raadpleging.
In geval van calamiteiten kan het CRV voor vreemdelingendiensten maximaal 12 uur buiten dienst zijn.

In geval van calamiteiten kan het CRV voor de overige gebruikers maximaal 24 uur buiten dienst zijn.

4.3 Controle op juistheid van de gegevens

4.3.1 Maatregelen om de controleerbaarheid te vergroten

Controle op de juistheid van de gegevens is belangrijk voor een goed werkende vreemdelingenadministratie.
Een grote controleerbaarheid van de gegevens is daarom noodzakelijk.

Controleerbaarheid is het gemak waarmee de juistheid en de volledigheid (in het verloop van de tijd) gecontroleerd kunnen worden.
Om de controleerbaarheid te bevorderen zijn de volgende maatregelen van belang.

- Van alle kritische transacties dient geregistreerd te worden wie deze het laatst gemuteerd heeft. Van alle belangrijke gegevens, waaronder de verblijfsstatus, wordt de volledige mutatie-historie bewaard.

- Van alle gegevens die naar de IND verzonden worden, dient de historie te worden bewaard.

- Er wordt door de centrale verwerkingsorganisatie een registratie bijgehouden van alle toegangspogingen tot het CRV.

4.3.2 Algemene controle

Bij elke gelegenheid waarbij een vreemdeling in contact komt met de korpschef, dient de korpschef zoveel mogelijk na te gaan of de geregistreerde gegevens nog met de feitelijke situatie overeenkomen.

4.3.3 Controle op dubbele registratie

De korpschef voert controles uit om te voorkomen dat vreemdelingen binnen de vreemdelingenadministratie meerdere malen geregistreerd staan. Bij identificatie van een vreemdeling raadpleegt hij daartoe zowel zijn eigen vreemdelingenadministratie als het CRV.

Wanneer ondanks deze controle alsnog (mogelijke) dubbele registraties in het CRV worden aangetroffen, rapporteert de korpschef dit aan de korpschef die de laatste mutatie heeft uitgevoerd. De desbetreffende korpschef dient de mogelijke dubbele registratie te controleren en actie te ondernemen.

4.3.4 Controle bij kritische transacties

Als kritische transacties in de geautomatiseerde vreemdelingenadministratie kunnen worden beschouwd:
- identificatie van een vreemdeling;
- registratie van een verblijfsstatus;
- registratie van afgegeven documenten;
- registratie van de meldingsplicht;
- de functies met financiële componenten.

Vanwege het feit dat met name de verblijfstitel van een vreemdeling een kwalitatief belangrijk gegeven binnen de administratie is, dienen aan de verwerking van deze kritische transacties bijzondere eisen te worden gesteld. Beschreven moet worden hoe in de organisatie de bewaking van deze kritische transacties geregeld is. (Bijvoorbeeld door controle achteraf, controle voorafgaand aan uitreiking document, steekproefsgewijze controle of systeemcontroles.)

Deze beschrijvingen dienen ten allen tijde door daartoe bevoegde controlerende instanties opvraagbaar te zijn.

4.4 Beveiliging

Onder beveiliging wordt verstaan de functionele beveiliging en fysieke beveiliging.

4.4.1 Functionele beveiliging

Functionele beveiliging is de bescherming van de gegevens in het informatiesysteem tegen menselijke fouten, tegen ongeoorloofde toegang en tegen verminking of verlies tijdens verwerking.
Dit omvat tevens de bescherming van de persoonlijke levenssfeer.

De gegevens die in de geautomatiseerde vreemdelingenadministratie worden verwerkt, dienen onder een privacyreglement te vallen. Dit privacyreglement wordt door de korpschef vastgesteld. Het privacyreglement moet gelijke tred houden met toekomstige ontwikkelingen van het systeem. Een door de Registratiekamer goedgekeurd model-privacyreglement is aan te vragen bij de het IND-hoofdkantoor, Stafafdeling Uitvoeringsbeleid & Documentatie.

De gegevens, informatiefuncties en werkstations dienen afgeschermd te zijn tegen personen die niet bevoegd zijn.

4.4.2 Fysieke beveiliging

Fysieke beveiliging is de beveiliging van de gegevensverwerking tegen technische fouten, storingen, fysieke daden door onbevoegden en calamiteiten. De volgende plannen dienen daarom opgesteld te worden:
- calamiteitenplan;
- beveiligingsplan;
- uitwijkplan;
- rampenplan.

Deze plannen zullen ten allen tijde door daartoe bevoegde controlerende instanties opvraagbaar moeten zijn.