

# Voorschrift Informatiebeveiliging Rijksdienst 1994.

*Vaststelling van de Aanwijzingen voor informatiebeveiliging*

Besluit van 22 juli 1994

De Minister-President,

Overwegende,

- dat het functioneren van de rijksdienst, zowel intern als in relatie met de maatschappij, in belangrijke mate bepaald wordt door de integriteit, beschikbaarheid en exclusiviteit van de ondersteunende informatiesystemen en de daarin opgenomen informatie,
- dat behoefte bestaat aan een uniform beleidskader met betrekking tot informatiebeveiliging, dat op hoofdlijnen vastlegt hoe het informatiebeveiligingsbeleid binnen de rijksdienst dient te worden gevormd en gevoerd,
- dat de zorgplicht die is neergelegd in algemene en specifieke wet- en regelgeving met betrekking tot het gebruik van informatie en informatiesystemen mede noodzaakt tot het treffen van informatiebeveiligingsmaatregelen en

*dat het wenselijk is de voorschriften voor de informatiebeveiliging in de rijksdienst te actualiseren.*

Gelet op

- artikel 9 van het Besluit Informatievoorziening in de Rijksdienst 1990

Handelend in overeenstemming met het gevoelen van de ministerraad;

Besluit:

## Artikel 1 Begripsbepalingen

In dit besluit wordt verstaan onder:

- afhankelijkheidsanalyse:*  
het vaststellen in hoeverre bestuurs- of bedrijfsprocessen die door informatiesystemen ondersteund worden, afhankelijk zijn van de betrouwbaarheid van deze systemen en het vaststellen welke potentiële schades kunnen optreden als gevolg van het falen van deze informatiesystemen;
- beschikbaarheid:*  
de mate waarin een informatiesysteem in bedrijf is op het moment dat de organisatie het nodig heeft;
- betrouwbaarheid:*  
de mate waarin de organisatie zich kan verlaten op een informatiesysteem voor zijn informatievoorziening;
- calamiteitenparagraaf:*  
opsomming van alle maatregelen welke tot uitvoering moeten komen indien zich een situatie voordoet waarbij de beschikbaarheid, integriteit en/of exclusiviteit van een informatiesysteem in beduidende mate niet aan de eisen voldoen;
- exclusiviteit:*  
de mate waarin de toegang tot en de kennisname van een informatiesysteem en de informatie daarin is beperkt tot een gedefinieerde groep van gerechtigden;
- informatiebeveiliging:*  
het treffen en onderhouden van een samenhangend pakket van maatregelen ter waarborging van de beschikbaarheid, integriteit en exclusiviteit van een informatiesysteem en daarmee van de informatie daarin;
- informatiebeveiligingsplan:*  
opsomming van alle beveiligingsmaatregelen en/of de vindplaatsen daarvan welke voor een informatiesysteem of een verantwoordelijkheidsgebied van kracht zijn;
- informatiesysteem:*  
een geheel van gegevensverzamelingen, personen, procedures, programmatuur en opslag-, verwerkings- en communicatie-apparatuur;
- integriteit:*  
de mate waarin een informatiesysteem zonder fouten is;

- j. *kwiteit*:  
de mate waarin het geheel van eigenschappen van een informatiesysteem voldoet aan de uit het gebruiksdoel voortvloeiende eisen;
- k. *kwetsbaarheidsanalyse*:  
het vaststellen van de invloed van het manifest worden van bedreigingen op het functioneren van een informatiesysteem of een verantwoordelijkheidsgebied;
- l. *systeemexploitatie*:  
de zorg voor het functioneren van een deel van een informatiesysteem;
- m. *systeemverwerving*:  
de zorg voor het ontwikkelen, kopen, huren e.d. en het uitvoeren van aanpassingen aan (delen van) een informatiesysteem zoals procedures, programmatuur en/of apparatuur;
- n. *verantwoordelijkheidsgebied*:  
een geheel van voorzieningen dat ter beschikking staat aan een of meerdere informatiesystemen en waarvoor de verantwoordelijkheid eenduidig is toe te wijzen aan één organisatorische eenheid;

## Artikel 2 Plaatsbepaling en reikwijdte

- a. Dit voorschrift geldt voor de Rijksdienst waartoe gerekend worden de ministeries met de daaronder ressorterende diensten, bedrijven en instellingen.
- b. Dit voorschrift geldt voor het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.
- c. Informatiebeveiliging is een lijnverantwoordelijkheid en vormt een onderdeel van de kwaliteitszorg voor bedrijfs- en bestuursprocessen en de ondersteunende informatiesystemen.
- d. Informatische relaties tussen een departement en een andere instantie gaan vergezeld van schriftelijke afspraken over het vereiste betrouwbaarheidsniveau en de wijze waarop zekerheid wordt verkregen over de realisatie daarvan.

## Artikel 3 Beveiligingsdocument

De secretaris-generaal van een departement stelt het informatiebeveiligingsbeleid vast in een beleidsdocument en draagt dit beleid uit. Het document omvat tenminste:

- a. De strategische uitgangspunten en randvoorwaarden die het departement hanteert ten aanzien van informatiebeveiliging, met name de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid.
- b. De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden.
- c. De eenduidige en volledige indeling van informatievoorzieningsfaciliteiten in informatiesystemen en verantwoordelijkheidsgebieden en toewijzing van de verantwoordelijkheden daarvoor aan lijnmanagers.
- d. De wijze waarop het beleid vertaald wordt naar concrete maatregelen en de wijze waarop deze gefinancierd worden.
- e. De gemeenschappelijke betrouwbaarheidseisen en maatregelen die voor het departement van toepassing zijn.
- f. De wijze waarop geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging door medewerkers gemeld worden en de wijze waarop deze worden afgehandeld.
- g. De wijze waarop en de frequentie waarmee volgens een vastgesteld schema
  - i. het informatiebeveiligingsbeleid geëvalueerd wordt en
  - ii. de toereikendheid van het informatiebeveiligingsbeleid alsmede de implementatie en de uitvoering daarvan wordt beoordeeld door een onafhankelijke deskundige.
- h. De wijze waarop het beveiligingsbewustzijn wordt bevorderd.

## **Artikel 4 Zorgplicht lijnmanagement**

Het lijnmanagement draagt er zorg voor dat voor elk informatiesysteem en voor elk verantwoordelijkheidsgebied op systematische wijze bepaald wordt welk stelsel van maatregelen uit hoofde van informatiebeveiliging getroffen dient te worden. Deze zorgplicht omvat tenminste:

- a) Voor elk informatiesysteem wordt een afhankelijkheidsanalyse uitgevoerd, uitmondend in aan het informatiesysteem te stellen betrouwbaarheidseisen.
- b) Voor elk verantwoordelijkheidsgebied wordt een analyse uitgevoerd, uitmondend in aan het verantwoordelijkheidsgebied te stellen betrouwbaarheidseisen.
- c) Voor elk informatiesysteem en voor elk verantwoordelijkheidsgebied worden de bedreigingen geïdentificeerd en geanalyseerd.
- d) Voor elk informatiesysteem en voor elk verantwoordelijkheidsgebied worden dusdanig maatregelen gekozen dat door middel van een kwetsbaarheidsanalyse aangetoond kan worden dat aan de gestelde betrouwbaarheidseisen wordt voldaan.
- e) Voor elk informatiesysteem en voor elk verantwoordelijkheidsgebied wordt een informatiebeveiligingsplan opgesteld. Hierin is een calamiteitenparagraaf opgenomen waarvan de effectiviteit periodiek wordt getoetst.
- f) Elk informatiebeveiligingsplan wordt periodiek geëvalueerd en eventueel aangepast aan veranderde omstandigheden.

## **Artikel 5 Zorgplicht lijnmanagement, vervolg**

Het lijnmanagement draagt er zorg voor dat voor elk bestuurs- of bedrijfsproces de maatregelen die uit hoofde van de informatiebeveiliging van toepassing zijn op de ondersteunende informatiesystemen worden vastgelegd, geïmplementeerd en/of uitgedragen en dat de werking ervan volgens een vastgesteld schema wordt gecontroleerd. Deze zorgplicht betreft tenminste:

- a) Voor elk informatiesysteem worden de uit het informatiebeveiligingsplan voortvloeiende maatregelen voor de gebruikers vastgelegd en uitgedragen door het lijnmanagement.
- b) Voor elk informatiesysteem worden de uit het informatiebeveiligingsplan voortvloeiende maatregelen voor systeemexploitatie schriftelijk vastgelegd.
- c) Indien de systeemexploitatie geheel of gedeeltelijk is uitbesteed, dient volgens een vastgesteld schema een onafhankelijk oordeel over de kwaliteit van de bij de opdrachtnemer getroffen informatiebeveiligingsmaatregelen en over het handhaven en naleven daarvan te worden verlangd.
- d) Voor elk informatiesysteem worden de uit het informatiebeveiligingsplan voortvloeiende maatregelen voor systeemverwerving door het lijnmanagement schriftelijk vastgelegd.
- e) De uit het informatiebeveiligingsplan voortvloeiende maatregelen voor systeemverwerving worden getoetst op hun implementatie en werking.

## **Artikel 6 Slotbepaling**

a. Ingetrokken worden:

1. de Aanwijzingen inzake de beveiliging van persoonsgegevens, verwerkt en opgeslagen in geautomatiseerde gegevensverwerkende systemen bij de Rijksoverheid, vastgesteld bij besluit van de minister-president van 16 juli 1982;
2. Het Voorschrift inzake de beveiliging van gerubriceerde gegevens, verwerkt en opgeslagen in geautomatiseerde systemen bij de Rijksoverheid, vastgesteld bij besluit van de minister-president van 25 maart 1980.

b. Dit besluit treedt in werking met ingang van 1 januari 1995.

c. Dit besluit kan worden aangehaald als het Besluit voorschrift informatiebeveiliging rijksdienst 1994.

Dit besluit zal worden gepubliceerd in de Staatscourant. Van de ter inzage legging van de toelichting op het besluit zal mededeling worden gedaan in de Staatscourant.

's-Gravenhage, 22 juli 1994.

De Minister-President, Minister van Algemene Zaken,  
R. F. M. Lubbers.