STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 30222
8 september 2025

# Besluit van de Minister-President, Minister van Algemene Zaken van 21 augustus 2025, nr. 9070201, houdende voorschrift informatiebeveiliging Rijksdienst bijzondere informatie 2025

De Minister-President, Minister van Algemene Zaken,

Handelende in overeenstemming met het gevoelen van de ministerraad,

Besluit:

**Artikel 1. Begripsbepalingen**

In dit besluit wordt verstaan onder:
*accreditatie:* het verlenen van toestemming voor ontvangst, beheer, vernietiging en verwerking van gerubriceerde informatie;
*bijzondere informatie:* informatie waar kennisname door niet-geautoriseerden nadelige gevolgen kan hebben voor de (vitale) belangen van de Nederlandse staat, voor zijn bondgenoten of voor één of meer ministeries;
*compromittering:* kennisname dan wel mogelijkheid tot kennisname van bijzondere informatie door niet geautoriseerden;
*informatiesysteem:* een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie;
*Rijksdienst:* alle organisatieonderdelen waarvoor de ministeriële verantwoordelijkheid onverkort geldt;
*rubriceren:* bepalen van het rubriceringsniveau en -duur van de bijzondere informatie op basis van de te verwachten nadelige gevolgen voor de vitale belangen van Nederland en de Nederlandse staat, voor zijn bondgenoten of voor één of meer ministeries als (een deel van) deze informatie bekend wordt bij niet-geautoriseerden;
*rubriceringsambtenaar:* ambtenaar bevoegd tot het vaststellen van rubriceringen, hiertoe gemandateerd door de secretaris-generaal;
*rubriceringsniveau:* aanduiding van de verwachte nadelige gevolgen voor de vitale belangen van Nederland en de Nederlandse staat, voor zijn bondgenoten of voor één of meer ministeries als de informatie of een deel daarvan bekend wordt bij niet- geautoriseerden;
*vaststeller van de rubricering:* minister, staatssecretaris, secretaris-generaal of een door de secretaris-generaal gemandateerd rubriceringsambtenaar;
*verwerking:* een bewerking of een geheel van bewerkingen met betrekking tot bijzondere informatie, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van bijzondere informatie;
*zorgdrager:* degene die bij of krachtens de wet belast is met de zorg voor de archiefbescheiden.

**Artikel 2. Plaatsbepaling en reikwijdte**

1. Dit besluit geldt voor de Rijksdienst.

2. Dit besluit is van toepassing op de beveiliging van bijzondere informatie van de Rijksdienst onverminderd het bepaalde in het Besluit voorschrift informatie beveiliging rijksdienst 2007 (VIR 2007), het Besluit BVA-stelsel Rijksdienst 2021 en het Besluit CIO-stelsel Rijksdienst 2021.

3. Bijzondere informatie die krachtens een verdrag of internationale overeenkomst is verkregen, behoudt de toegekende rubricering en wordt beveiligd volgens het overeenkomstige nationale beveiligingsniveau. Voor zover voor de beveiliging van dergelijke informatie als gevolg van het verdrag of de internationale overeenkomst afwijkende bepalingen bestaan worden deze bepalingen toegepast.

**Artikel 3. Beveiligingsbeleid**

1. Het ministeriële beveiligingsbeleid dat door de secretaris-generaal van het betreffende ministerie wordt vastgesteld omvat ten minste de uitgangspunten voor de beveiliging van, de toegang tot,

het omgaan met en verwerken van bijzondere informatie zoals bedoeld in dit voorschrift en de wijze waarop:
a. het ministerie informatie rubriceert;
b. de secretaris-generaal van het betreffende ministerie vooraf accreditatie verleent voor het verwerken van bijzondere informatie;
c. het ministerie toezicht uitoefent op de beveiliging van bijzondere informatie.

2. De beveiligingsautoriteit dan wel beveiligingsautoriteit Rijk heeft de volgende taken:
a. het bewaken van het integrale karakter en de consistentie van rijksbrede kaders voor integrale beveiliging, het bevorderen van een departementale dan wel interdepartementale aanpak van beveiligingsvraagstukken, alsmede het toezicht op de werking van de integrale beveiliging van de Rijksdienst;
b. de coördinatie van de integrale aanpak van de beveiliging van gerubriceerde informatie;
c. wanneer er sprake is van een inbreuk op de beveiliging, worden onmiddellijk maatregelen dan wel noodmaatregelingen getroffen om verdere inbreuk te voorkomen;
d. het onderzoeken of en wanneer compromittering van bijzondere informatie heeft plaatsgevonden. Indien dit het geval is, doen zij hiervan mededeling aan de secretaris-generaal en adviseren zij over de noodzaak om een commissie van onderzoek in te stellen. Tevens doen zij, indien van toepassing, melding conform de geldende wet- en regelgeving.

3. De beveiligingsautoriteit dan wel beveiligingsautoriteit Rijk betrekt bij zijn taken, genoemd in het tweede lid, het advies van de chief information officer dan wel chief information officer Rijk wanneer beveiligingsvraagstukken een digitale component hebben.

**Artikel 4. Rubriceringen**

1. Informatie waarvan de geheimhouding vanwege de vitale belangen van Nederland en de Nederlandse staat, van zijn bondgenoten of één of meer ministeries is geboden, moet worden voorzien van een passend niveau van rubricering.

2. Bijzondere informatie wordt als volgt gerubriceerd:
a. Staatsgeheim ZEER GEHEIM, afgekort 'Stg.ZG' of 'Stg. ZEER GEHEIM', indien kennisname door niet-geautoriseerden zeer ernstige schade kan toebrengen aan een van de vitale belangen van Nederland en de Nederlandse staat, of zijn bondgenoten;
b. Staatsgeheim GEHEIM, afgekort 'Stg.G' of 'Stg. GEHEIM', indien kennisname door niet-geautoriseerden ernstige schade kan toebrengen aan een van de vitale belangen van Nederland en de Nederlandse staat, of zijn bondgenoten;
c. Staatsgeheim CONFIDENTIEEL, afgekort 'Stg.C' of 'Stg. CONFIDENTIEEL', indien kennisname door niet-geautoriseerden schade kan toebrengen aan een van de vitale belangen van Nederland en de Nederlandse staat, of zijn bondgenoten;
d. Departementaal VERTROUWELIJK, afgekort 'Dep.V' of 'Dep. VERTROUWELIJK', indien kennisname door niet-geautoriseerden schade kan toebrengen aan de belangen van één of meerdere ministeries of bondgenoten van de Nederlandse staat.

3. De opsteller van de informatie doet een voorstel tot rubricering en brengt deze aan op de informatie. De vaststeller van de inhoud van de informatie stelt tevens de rubricering vast.

**Artikel 5. Herzien en beëindigen van de rubricering**

1. Rubriceringen worden verbonden aan een maximum tijdsverloop of aan een bepaalde gebeurtenis. Na die periode of na die gebeurtenis weegt de vaststeller van bijzondere informatie af of herziening, dan wel beëindiging van de rubricering, aan de orde is.

2. Van het eerste lid kan worden afgeweken in die gevallen waarin de rubricering betrekking heeft op:
a. Bijzondere informatie die krachtens een verdrag of internationale overeenkomst is verkregen;
b. Staatsgeheimen die door de wet als zodanig zijn aangewezen.

3. Uitsluitend de vaststeller van de rubricering is bevoegd de rubricering te herzien of te beëindigen.

4. Bij overbrenging van bijzondere informatie naar een rijksarchiefbewaarplaats als bedoeld in de Archiefwet 1995 vervalt de rubricering, tenzij de zorgdrager, na advies van de algemene rijksarchivaris en de rubriceringsambtenaar, bepaalt dat deze gehandhaafd dan wel herzien moet worden.

**Artikel 6. Eisen aan de beveiliging**

1. Bijzondere informatie en de verwerking ervan worden zodanig beveiligd dat:

a. alleen personen die daartoe zijn geautoriseerd, de informatie verwerken voor zover dit noodzakelijk is voor een goede uitoefening van hun taak;
b. passende maatregelen zijn getroffen om compromittering tijdig te detecteren, en een onderzoeksproces is ingericht voor de grondige analyse van dergelijke incidenten.

2. De beveiliging is ingericht op basis van risicomanagement. De bijlage bij dit besluit bevat de uitgangspunten en het minimale beveiligingsniveau voor de bescherming van de vertrouwelijkheid van bijzondere informatie en de verwerking ervan in informatiesystemen.

3. Bijzondere informatie die krachtens een verdrag of een internationale overeenkomst is verkregen wordt uitsluitend verwerkt nadat de autoriteit, die krachtens het betreffende verdrag verantwoordelijk is voor de beveiligingsregels ter bescherming van bijzondere informatie, haar goedkeuring aan de beveiliging heeft gegeven.

**Artikel 7. Buiten de Rijksdienst brengen van bijzondere informatie**

1. Bij het buiten de Rijksdienst brengen van bijzondere informatie, anders dan op grond van een wettelijke verplichting tot openbaarmaking, blijven de eisen aan de beveiliging in dit besluit en het toezicht daarop onverkort van kracht.

2. Bijzondere informatie die krachtens een verdrag of een internationale overeenkomst is verkregen wordt uitsluitend na voorafgaande toestemming van het land of de internationale organisatie van herkomst doorgegeven aan externe partijen.

**Artikel 8. Compromittering van bijzondere informatie**

1. Elke ambtenaar is verplicht aan de beveiligingsautoriteit van het betreffende ministerie onmiddellijk mededeling te doen van een inbreuk of mogelijke inbreuk op de beveiliging die leidt tot compromittering van bijzondere informatie.

2. Indien de compromittering betrekking heeft op bijzondere informatie die is verkregen van een ander ministerie of krachtens een verdrag of internationale overeenkomst, doet de beveiligingsautoriteit bovendien mededeling aan het betreffende ministerie of de krachtens het verdrag of de internationale overeenkomst voor de beveiliging van die bijzondere informatie verantwoordelijke instantie.

**Artikel 9. Commissie van onderzoek**

1. De secretaris-generaal stelt een commissie van onderzoek in indien sprake is van ernstige compromittering van bijzondere informatie, waarbij onafhankelijke evaluatie noodzakelijk wordt geacht om de toedracht, gevolgen en eventuele verantwoordelijkheden vast te stellen.

2. Indien de secretaris-generaal een commissie van onderzoek instelt, stelt de commissie een onderzoek in naar:
a. de wijze waarop de compromittering heeft plaatsgevonden;
b. de aard en de omvang van de schade aan de belangen van het ministerie, de vitale belangen van Nederland en de Nederlandse staat, of aan zijn bondgenoten;
c. de te nemen maatregelen om de schade te beperken en herhaling te voorkomen.

3. De commissie voert, indien de gecompromitteerde bijzondere informatie (mede) afkomstig is van een ander ministerie, haar onderzoek uit in overleg met de BVA van dat ministerie. In het geval dat de gecompromitteerde bijzondere informatie krachtens een verdrag of internationale overeenkomst is verkregen voert de commissie haar onderzoek uit in samenwerking met de instantie die krachtens het verdrag of de internationale overeenkomst verantwoordelijk is voor de beveiliging ervan.

4. De secretaris-generaal treft, op basis van de bevindingen van de commissie van onderzoek, maatregelen om de schade die de compromittering heeft toegebracht aan de veiligheid of andere gewichtige belangen van het ministerie, aan de vitale belangen van Nederland en de Nederlandse staat, of aan zijn bondgenoten, te beperken en herhaling van de compromittering te voorkomen.

5. Indien het de compromittering van een staatsgeheim betreft, stelt de secretaris-generaal het hoofd van de Algemene Inlichtingen- en Veiligheidsdienst in kennis van de uitkomsten van het onderzoek. In afwijking van de eerste volzin stelt de secretaris-generaal van het Ministerie van Defensie de Militaire Inlichtingen- en Veiligheidsdienst op de hoogte van de uitkomsten van het onderzoek.

**Artikel 10. Evaluatie**

Dit besluit wordt drie jaar na inwerkingtreding geëvalueerd en vervolgens elke drie jaar.

**Artikel 11. Overgangsrecht**

Rubriceringen die zijn vastgesteld vóór inwerkingtreding van dit besluit worden uiterlijk tien jaar na vaststelling door de vaststeller onderzocht op de mogelijkheid om de rubricering te herzien of te beëindigen, en voor bestaande, reeds gerubriceerde informatie, waarbij volledig wordt voldaan aan de maatregelen, genoemd in het Besluit voorschrift informatiebeveiliging rijksdienst bijzondere informatie 2013 (VIRBI 2013), zijn organisaties gedurende een overgangsperiode van zes maanden niet gehouden te voldoen aan de hierop aanvullende maatregelen zoals deze in de bijlage bij dit besluit zijn opgenomen.

**Artikel 12. Intrekking VIRBI 2013**

Het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013) wordt ingetrokken.

**Artikel 13. Inwerkingtreding**

Dit besluit treedt in werking met ingang van de dag na de datum van uitgifte van de Staatscourant waarin het wordt geplaatst.

**Artikel 14. Citeertitel**

Dit besluit wordt aangehaald als: Besluit voorschrift informatiebeveiliging rijksdienst bijzondere informatie 2025.

Dit besluit zal met de toelichting in de Staatscourant worden geplaatst.

*De Minister-President, Minister van Algemene Zaken,*
*H.W.M. Schoof*

## BIJLAGE. UITGANGSPUNTEN EN MINIMUM NIVEAU BEVEILIGING

Deze bijlage beschrijft de uitgangspunten en het beveiligingsniveau voor de bescherming van de vertrouwelijkheid van bijzondere informatie en de verwerking daarvan in informatiesystemen.

De voor de bescherming van vertrouwelijkheid van bijzondere informatie te nemen maatregelen worden bepaald aan de hand van een risicoanalyse, maar beslaan ten minste de in onderstaande tabellen weergegeven te hanteren uitgangspunten en te nemen maatregelen. Indien wordt afgeweken van het onderstaande wordt dat in de risicoanalyse vastgelegd met redenen omkleed inclusief eventueel aanvullende mitigerende maatregelen. Voor Dep.V wordt dit ten minste goedgekeurd door een directeur en voor STG ten minste door een DG.

**Tabel 1: Uitgangspunten en minimumniveau van beveiliging.**

| | | Dep.V | Stg.C | Stg.G | Stg.ZG |
|---|---|---|---|---|---|
| A | De Baseline Informatiebeveiliging Overheid (BIO) vormt de basis, met normen, maatregelen en risicomanagement als uitgangspunt. Daarbovenop worden, de in dit document aangegeven aanvullende maatregelen vereist voor gerubriceerde informatie, waarbij de maatregelen toenemen in strengheid bij toenemend risiconiveau. De risicoacceptatie neemt af bij toenemende hoogte van rubricering. | V | V | V | V |
| B | Iedere organisatie hanteert een 'Three Lines of Defense'-model voor doorlopend risicobeheer, naleving en controle. | V | V | V | V |
| C | Minimaal een keer per jaar controleert de BVA de implementatie en vastlegging daarvan.<br>(Maakt deel uit van de 'Three Lines of Defense'-aanpak. Controles worden uitgevoerd om te waarborgen dat beveiligingsmaatregelen zijn geïmplementeerd en nageleefd.) | V | V | V | V |
| D | Openbare en private bronnen worden actief gemonitord als onderdeel van risicomanagement. Dit omvat organisaties zoals de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), de politie, het Nationaal Cyber Security Centrum (NCSC), het Europees Agentschap voor Netwerk- en Informatiebeveiliging (ENISA), en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD).' | V | V | V | V |
| E | De Unit Weerbaarheid van de AIVD schrijft Verbindingsbeveiligingsvoorschriften (VBV's) voor, waarin beveiligingsmaatregelen ten aanzien van specifieke deelaspecten worden beschreven. Waar mogelijk wordt in deze bijlage verwezen naar bestaande VBV's. VBV's zijn op te vragen bij de Unit Weerbaarheid van de AIVD. | V | V | V | V |
| F | Beveiliging in lagen: De beveiliging is opgebouwd uit meerdere lagen om te voorkomen dat de beveiliging afhankelijk is van één enkele maatregel. Deze lagen omvatten maatregelen voor zowel preventie en detectie van aanvallen als voor de voorbereiding op incident response en impactminimalisatie. Het doel is een geïntegreerde security architectuur te hanteren, oftewel een systeem van maatregelen die gezamenlijk de inventarisatie, preventie, detectie, respons en herstel omvatten inclusief besturing (governance). | V | V | V | V |
| G | Least privilege: Alleen de autorisaties die iemand nodig heeft om zijn of haar taak te kunnen vervullen, worden toegekend. | V | V | V | V |
| H | Need-to-know: Personen hebben alleen toegang tot bijzondere informatie als het noodzakelijk is dat zij deze kennen voor de uitoefening van hun functie. | V | V | V | V |
| I | Zero trust-systemen: Elk systeem beschouwt andere systemen als onbetrouwbaar totdat het tegendeel is bewezen en er adequate maatregelen zijn getroffen om veilig informatie uit te wisselen met vertrouwde systemen. | V | V | V | V |
| J | Analyse van de Te Beschermen Belangen (TBB): Identificeer deze TBB's en prioriteer de bescherming daarvan. | V | V | V | V |
| K | Maandelijks controleert de lijnmanager (of laat controleren) op naleving en vastlegging van deze controle.<br>(Maakt deel uit van de 'Three Lines of Defense'-aanpak. Controles worden uitgevoerd om te waarborgen dat beveiligingsmaatregelen zijn geïmplementeerd en nageleefd.) | | | V | V |

Een V in de bovenstaande tabel houdt in: bij dit niveau van rubricering maatregel verplicht toepassen.

In de volgende acht hoofdstukken komen de diverse onderdelen aan de orde.
1. Veilig personeel
2. Beheer van bedrijfsmiddelen

3. Fysieke beveiliging en beveiliging van de omgeving
4. Toegangsbeveiliging
5. Beveiligingseisen voor ICT-voorzieningen
6. Communicatiebeveiliging
7. Beheer van bijzondere informatie
8. Incidenten en compromittering

## 1. Veilig personeel

### Doelstelling

Organisaties moeten zeker stellen dat personen hun verantwoordelijkheden en verplichtingen kennen en geschikt zijn voor de rol of functie die zij vervullen. Daarnaast dienen organisaties de risico's van menselijk handelen te beperken.

### Eisen

Ieder persoon die structureel gaat werken met bijzondere informatie, dient voorafgaand aan indiensttreding een aan zijn functievervulling gerelateerd veiligheidsonderzoek te ondergaan. Voor het bepalen of een functie als vertrouwensfunctie moet worden aangewezen, dient de betreffende leidraad aanwijzen vertrouwensfuncties van de AIVD (civiele sector) en MIVD (militaire sector) te worden gevolgd.

Bij aanvang, beëindiging of wijziging van het dienstverband waarin gewerkt is met bijzondere informatie, wordt zeker gesteld dat de geheimhoudingsplicht geborgd is.

**Tabel 3. Minimale maatregelen voor veilig personeel voor, tijdens en na het dienstverband.**

| | | Dep.V | Stg.C | Stg.G | Stg.ZG |
|---|---|---|---|---|---|
| A | Personen die in aanraking komen met bijzondere informatie beschikken over een Verklaring Omtrent het Gedrag (VOG). | * | | | |
| B | Personen die structureel in aanraking komen met bijzondere informatie beschikken over een geldige Verklaring van geen bezwaar (VGB) voor de betreffende vertrouwensfunctie | | V | V | V |
| C | De BVA/BA houdt toezicht op de afhandeling van beveiligingsincidenten rond bijzondere informatie. | V | V | V | V |
| D | In de functieomschrijvingen van personeel dat inzage heeft in bijzondere informatie is de eigen verantwoordelijkheid voor beveiliging vastgelegd. | V | V | V | V |
| E | Personen die in aanraking komen met bijzondere informatie, dienen aanvullend op de eed/belofte, een geheimhoudingsverklaring te ondertekenen. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding. | V | V | V | V |
| F | Bij beëindiging van een functie waarbij iemand in aanraking komt met bijzondere informatie wordt zeker gesteld dat de betreffende persoon geen toegang meer heeft tot die informatie, noch deze in zijn/haar bezit heeft. | V | V | V | V |
| G | Er is een security awareness programma specifiek voor bijzondere informatie, passend bij het rubriceringsniveau. | V | V | V | V |
| H | Personen die in aanraking komen met bijzondere informatie zijn verplicht om het security awareness programma te volgen. | V | V | V | V |
| I | Er wordt voldoende informatie vastgelegd om een onderzoek van compromittering mogelijk te maken. | V | V | V | V |
| J | Informatie zoals bedoeld in I wordt minimaal 3 maanden bewaard om achteraf onderzoek mogelijk te maken. | V | V | V | V |
| K | Informatie over compromittering wordt gedurende minimaal een bepaalde termijn bewaard. | 3 jaar | 5 jaar | 5 jaar | 5 jaar |

Een V houdt in: bij dit niveau van rubricering maatregel verplicht toepassen.
Een * in de tabel verwijst op een aantal plekken voor DepV naar de BIO.

## 2. Beheer van bedrijfsmiddelen

### Doelstelling

Het handhaven van een adequaat, ordelijk en controleerbaar beheer van alle bedrijfsmiddelen waarop, waarmee of waardoor bijzondere informatie wordt verwerkt.

### Eisen

Bedrijfsmiddelen waarop, waarmee of waardoor bijzondere informatie wordt verwerkt, dienen te zijn geregistreerd en aan een eigenaar te zijn toegewezen.

**Tabel 4: Minimale maatregelen voor het management van bedrijfsmiddelen.**

| | | Dep.V | Stg.C | Stg.G | Stg.ZG |
|---|---|---|---|---|---|
| A | Registreer alle middelen en de personen aan wie deze zijn uitgereikt of aan wie toegang tot bedrijfsmiddelen wordt verleend. | * | V | V | V |
| B | Registreer de locatie/ standplaats van alle middelen en de toewijzing aan een eigenaar. | * | V | V | V |
| C | Er is een centraal register met een actueel overzicht van de locatie/ standplaats van alle middelen en de bijbehorende eigenaren. | * | V | V | V[1] |
| D | Minimaal eens per jaar wordt de actualiteit van het centrale register vastgesteld. | V | V | V | V |
| E | Stel een procedure vast voor het inleveren, opnieuw inzetten of vernietiging van geregistreerde middelen. | V | V | V | V |

[1] Vanwege need-to-know scheiding wordt het overzicht van Stg.ZG-middelen separaat geregistreerd.

Een V houdt in: bij dit niveau van rubricering maatregel verplicht toepassen.
Een * in de tabel verwijst op een aantal plekken voor DepV naar de BIO.

## 3. Fysieke beveiliging en beveiliging van de omgeving

### Doelstelling

Het waarborgen van toereikende weerstand tegen (pogingen tot) ongeautoriseerde fysieke toegang van locaties, gebouwen en ruimtes (waaronder kluizen) waar zich bijzondere informatie bevindt of wordt verwerkt.

### Eisen

Voor elke locatie, gebouw en ruimte waar zich bijzondere informatie bevindt of wordt verwerkt, dienen systematisch de beveiligingsmaatregelen in beeld te zijn gebracht voor fysieke toegangsbeheersing. Hierbij is ten minste voorzien in:

- Het aanbrengen van zonering c.q. compartimentering en per zone de rubricering en/of het TBB-niveau te bepalen,
- Het regelen van een ordelijk toegangsbeleid en sleutelbeheer,
- Het toewijzen van ruimtes waar bijzondere informatie zich bevindt of wordt verwerkt.

Om toegang te krijgen tot ruimtes waarin bijzondere informatie wordt verwerkt, worden afhankelijk van het rubriceringsniveau, steeds zwaardere beveiligingsmaatregelen getroffen.

**Tabel 5: Uitgangspunten zonering en verwerking van gerubriceerde gegevens.**

| | | Dep.V | Stg.C | Stg.G | Stg.ZG |
|---|---|---|---|---|---|
| A | DepV-informatie wordt *structureel* verwerkt, behandeld en besproken[1] in minimaal *Zone 2* (beveiligd gebied conform het NkBR[2] of een en als gelijkwaardig beschouwde ruimte) *en incidenteel in Zone 1* (conform het NkBR of een en als gelijkwaardig beschouwde ruimte).<br>Dit betekent dat het structureel verwerken van dep. V informatie in een zone 1 een afwijking is waarvoor een exceptie nodig is.<br>Een organisatiegeboden aanscherping is daarbij toegestaan. In het geval van thuiswerk bepaalt het departementaal beleid hoe om te gaan met het bespreken, verwerken en behandelen van DepV-informatie. | V | | | |
| B | Bijzondere informatie wordt structureel verwerkt, behandeld en besproken in tenminste een extra beveiligd werkgebied (conform het NkBR of een als gelijkwaardig beschouwde ruimte). | | V | V | V |

[1] Met 'besproken' wordt bedoeld: elk overleg waarin bijzondere informatie besproken wordt.
[2] Normenkader Beveiliging Rijkskantoren (is niet voor alle gebouwen van de Rijksoverheid van toepassing)

**Tabel 5.1 – Minimale eisen fysieke beveiliging locaties en gebouwen**

| | | | | | |
|---|---|---|---|---|---|
| C | De beveiliging is zodanig ingericht dat ongeautoriseerde toegang tot locaties en gebouwen en pogingen daartoe worden gedetecteerd. | * | | | |
| D | De beveiliging is zodanig ingericht dat ongeautoriseerde toegang tot locaties en gebouwen en pogingen daartoe worden gedetecteerd en dat tijdig interventie plaatsvindt, ook na kantooruren. De vertragingstijd is dusdanig dat detectie van ongeautoriseerde toegang en pogingen daartoe plaatsvindt op een tijdstip dat interventie mogelijk maakt. | | V | V | V |
| E | Bezoekers worden geregistreerd. | V | V | V | V |
| F | Bijzondere informatie wordt zoveel mogelijk geconcentreerd. | V | V | V | V |
| G | Tegengaan van afluisteren, ook van gesproken informatie, zicht op en reflectie van informatie (bijvoorbeeld via beeldschermen of spiegelende oppervlakken). | V | V | V | V |
| H | De medewerker verantwoordelijk voor de verwerking van bijzondere informatie, dient te voorkomen dat niet-geautoriseerde personen kennis kunnen nemen van bijzondere informatie. | V | V | V | V |
| I | Er zijn TEMPEST-maatregelen getroffen conform het Beleidsadvies Compromitterende straling (Verbindingsbeveiligingsvoorschrift (VBV 32000)[1]. | | V | V | V |
| J | Voorafgaand aan de ingebruikname van een werkruimte of andere beveiligde zone dient er, volgens het Nationaal TSCM/EVO Beleidsadvies, een Technical Surveillance Counter-Measures (TSCM)/ Elektronisch Veiligheidsonderzoek en indien nodig een geluidsdempingsmeting uitgevoerd te zijn. | | V | V | V |
| K | Periodiek en bij elke bouwkundige aanpassing of het toevoegen van nieuwe middelen (zoals: ICT-apparatuur, meubilair, schilderijen en relatiegeschenken) in een beveiligde zone dient er, volgens het Nationaal TSCM/EVO Beleidsadvies, een Technical Surveillance Counter-Measures (TSCM)/Elektronisch Veiligheidsonderzoek en indien nodig een geluidsdempingsmeting uitgevoerd te worden. | | V | V | V |
| L | Bezoekers worden geregistreerd indien zij toegang (kunnen) hebben tot bijzondere informatie in ruimten die zij betreden. | | V | V | V |
| M | Niet-geautoriseerde personen worden begeleid wanneer zij ruimtes waarin bijzondere informatie aanwezig is, betreden. | | V | V | V |
| N | Er wordt voorkomen dat bezoekers kennisnemen van bijzondere informatie waar zij niet toe geautoriseerd zijn. | | V | V | V |
| O | Personen die een ruimte gaan betreden waar bijzondere informatie wordt verwerkt, bewaren alle persoonlijke elektronica (computers, tablets, telefoons, bio-wearables et cetera) buiten deze ruimte. | | V | V | V |
| | *Opbergen van informatie* | | | | |
| P | Bij het verlaten van de werkplek wordt bijzondere informatie in een goedgekeurd bergmiddel opgeborgen. | V | V | V | V |
| *Sleutelbeheer* | | | | | |
| Q | De uitgifte van sleutels wordt geregistreerd. | V | V | V | V |
| R | Niet in gebruik zijnde sleutels worden veilig opgeborgen. | V | V | V | V |
| S | Er worden gecertificeerde sleutels gebruikt. | | V | V | V |
| *Fysieke netwerkbescherming* | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| T | Netwerkapparatuur en bekabeling worden fysiek beschermd conform het rubriceringsniveau van de onvercijferde informatie die er mee wordt verwerkt. | V | V | V | V |
| *Controles op onderhoud, plaatsing en vervanging van apparatuur:* | | | | | |
| U | Externe reparatie is gebonden aan door de BVA vastgestelde procedures. | V | V | V | V |
| V | Reparatie vindt op locatie plaats, tenzij bijzondere informatie verwijderd is met goedgekeurde middelen. | V | V | V | V |
| W | Onderhoud vindt plaats door personen die in bezit zijn van een passende VGB. | | V | V | V |
| X | Onderhoud door extern personeel vindt alleen plaats onder begeleiding van eigen personeel. | | | | V |

[1] Hiervoor kan advies worden aangevraagd bij de Nationale TEMPEST Autoriteit (NTA).

Een V houdt in: bij dit niveau van rubricering maatregel verplicht toepassen.
Een * in de tabel verwijst op een aantal plekken voor DepV naar de BIO.

## 4. Toegangsbeveiliging

### Doelstelling

Het waarborgen van een beheerste en gecontroleerde toegang tot voorzieningen waarin zich bijzondere informatie bevindt of wordt verwerkt.

### Eisen

Voorzie in procedures en regels voor toegangsrechten tot, logging en monitoring van netwerkdiensten, besturingssystemen en applicaties waar zich gerubriceerde informatie bevindt.

Voorzie in een stelsel van logische toegangsbeveiligingsmaatregelen dat is gerelateerd aan de relevante dreiging en het rubriceringsniveau.

**Tabel 6. Minimale maatregelen voor toegangsbeveiliging.**

| | | Dep.V | Stg.C | Stg.G | Stg.ZG |
|---|---|---|---|---|---|
| | *Identificatie en authenticatie:* | | | | |
| A | Het moet de gebruiker duidelijk zijn wat de maximale rubricering is van de informatie die verwerkt mag worden op een systeem. | V | V | V | V |
| B | Gebruikersnamen garanderen dat activiteiten worden herleid naar individuen. | V | V | V | V |
| C | Gebruikers worden vooraf geïdentificeerd en geautoriseerd. | V | V | V | V |
| D | Pas multifactor authenticatie toe. | * | V | V | V |
| E | Toegang tot bijzondere informatie wordt op individueel niveau bepaald. | V | V | V | V |
| F | Toegang tot systemen kan op groepsniveau worden bepaald mits het lidmaatschap van de groep herleidbaar is op het individu. | V | V | Niet toegestaan. | Niet toegestaan. |
| G | Wachtwoorden worden vercijferd opgeslagen. | V | V | V | V |
| H | Stel minimum eisen aan wachtwoordlengte, -complexiteit en -versleuteling en wijzigingsfrequentie. | V | V | V | V |
| I | Wachtwoorden worden zodanig behandeld dat ze beschermd zijn tegen ongeautoriseerde kennisname. | V | V | V | V |
| J | Toegang tot een account wordt na een aantal direct achtereenvolgende foutieve inlogpogingen geblokkeerd. | * | 5 | 4 | 3 |
| | *Logische toegangscontrole:* | | | | |
| K | Toegang tot ICT-voorzieningen wordt enkel verschaft op basis van need-to-know. | V | V | V | V |
| L | Er worden procedures vastgesteld voor het verkrijgen van toegang tot bijzondere informatie. | V | V | V | V |
| | *De toegang tot het werkstation wordt beveiligd:* | | | | |
| M | De toegangsbeveiliging wordt automatisch geactiveerd. | 10m | 10m | 5m | 5m |

| | | Dep.V | Stg.C | Stg.G | Stg.ZG |
|---|---|---|---|---|---|
| N | Informatie wordt vercijferd opgeslagen en het vercijfermechanisme en het sleutelbeheer is goedgekeurd door de Minister van Binnenlandse Zaken en Koninkrijksrelaties voor inzet binnen de Rijksdienst of de BA Defensie voor gebruik binnen Defensie voor de betreffende rubricering. | V | V | V | V |
| O | Toegang tot beheerfuncties is voorbehouden aan die personen die van deze functies gebruik moeten maken. | V | V | V | V |
| P | De toegangsrechten van de gebruikers worden periodiek geëvalueerd. | * | V | V | V |
| | *Netwerk toegangscontroles:* | | | | |
| Q | De autorisaties van alle gebruikers zijn vastgelegd. | V | V | V | V |
| R | Het is toegestaan om beheer op afstand uit te laten voeren. | V | Niet toegestaan | Niet toegestaan | Niet toegestaan |
| | *De aansluiting met netwerken beveiligen:* | | | | |
| S | Koppeling met externe netwerken is alleen toegestaan middels goedgekeurde koppelvlakken. | V | V | V | V |

Een V houdt in: bij dit niveau van rubricering maatregel verplicht toepassen.
Een * in de tabel verwijst op een aantal plekken voor DepV naar de BIO.

## 5. Beveiligingseisen voor ICT-voorzieningen

### Doelstelling

Het waarborgen van een passend niveau van beveiliging gedurende de gehele levenscyclus van ICT-voorzieningen waarin bijzondere informatie wordt verwerkt.

### Eisen

Voorafgaand aan verwerving, ontwikkeling, onderhoud en afstoot van informatiesystemen waarin bijzondere informatie wordt verwerkt, dienen de dreigingen en risico's in beeld te zijn gebracht. Voor het gebruik en beheer van informatiesystemen is het beveiligingsniveau in overeenstemming met de dreigingen en risico's.

**Tabel 7: Minimale maatregelen voor de levenscyclus van ICT-voorzieningen.**

| | | Dep.V | Stg.C | Stg.G | Stg.ZG |
|---|---|---|---|---|---|
| A | De configuratie van de hard- en software moet zijn vastgelegd. | * | V | V | V |
| B | Alle wijzigingen in apparatuur, software of procedures moeten controleerbaar zijn. | * | V | V | V |
| C | Er moet een autorisatiematrix zijn voor wijzigingen en de procedure voor wijzigingen moet zijn vastgelegd. | * | V | V | V |
| D | Gedurende de gehele levenscyclus van een systeem worden minimaal jaarlijks audits, inspecties, reviews en tests uitgevoerd om te controleren of de beveiligingsmaatregelen effectief zijn.<br>Deze controles worden uitgevoerd door deskundige specialisten die beschikken over de juiste onderzoeksmiddelen en beproefde onderzoeksmethoden. | Self assessment | Onafhankelijk deskundige | Onafhankelijk deskundige | Onafhankelijk deskundige |
| E | De verantwoordelijkheden en procedures voor het adequaat beheer en juist gebruik van de ICT-voorzieningen waarin bijzondere informatie wordt verwerkt, zijn vastgesteld. | * | V | V | V |
| F | Bij uitbesteding van (delen van) de dienstverlening dient een zelfde beveiligingsniveau te worden gerealiseerd als geldt bij de interne dienstverlening. De uitbestedende partij/eigenaar blijft verantwoordelijk voor de beveiliging. | * | V | V | V |
| G | Bij informatieverwerking in ketens blijft de eigenaar van de bijzondere informatie verantwoordelijk voor het hanteren van het juiste beveiligingsniveau in de gehele keten. | V | V | V | V |
| H | Voorafgaand aan de inkoop van ICT-middelen en fysieke voorzieningen, extern personeel evenals voorafgaand en tijdens een opdrachttoets omtrent het verwerken van bijzondere informatie, dient contact te worden opgenomen met de BVA om de juiste normen, kaders, wet- en regelgeving te kunnen hanteren en het accreditatieproces te starten. | * Zie ook tabel 1, maatregel A | V | V | V |
| I | Accreditatie van ICT-voorzieningen worden periodiek of na een concrete aanleiding uitgevoerd, | * Zie ook tabel 1, maatregel A | V | V | V |

Een V houdt in: bij dit niveau van rubricering maatregel verplicht toepassen.
Een * in de tabel verwijst op een aantal plekken voor DepV naar de BIO.

## 6. Communicatiebeveiliging

### Doelstelling

Het waarborgen van een wederzijds vergelijkbaar beveiligingsniveau voor de vertrouwelijkheid bij communicatie van bijzondere informatie.

### Eisen

De vertrouwelijkheid van informatie moet gehandhaafd blijven tijdens (elektronisch) transport buiten gecontroleerd gebied. Voorzie in een passende set van maatregelen indien bijzondere informatie de organisatie of beveiligde omgeving verlaat.

**Tabel 8: Minimale maatregelen voor verzending van gerubriceerde informatie.**

| | | Dep.V | Stg.C | Stg.G | Stg.ZG |
|---|---|---|---|---|---|
| | *Controles op documenten en gegevensdragers:* | | | | |
| A | Af te stoten gegevensdragers worden eerst gewist met een door de BVA voor de desbetreffende rubricering goedgekeurde methode. | V | V | V | |
| B | Af te stoten gegevensdragers worden fysiek vernietigd. | | | | V |
| C | De hoogste rubricering van informatie wordt op gegevensdragers aangegeven. | V | V | V | V |
| D | Elk document is tenminste voorzien van:<br>• Rubriceringsniveau;<br>• Rubriceringsduur;<br>• Vaststeller (functie) van de rubricering;<br>• Datum vaststelling;<br>• Bladzijdenummering en totaal aantal bladzijden waaruit het document bestaat. | V | V | V | V |
| E | Een gegevensverzameling (ongeacht welke vorm) is tenminste voorzien van (meta) gegevens van:<br>• Rubriceringsniveau;<br>• Rubriceringsduur;<br>• Vaststeller (functie) van de rubricering;<br>• Datum vaststelling;<br>• Omvang. | V | V | V | V |
| F | Gegevensdragers die onversleutelde bijzondere informatie bevatten en afgedrukte informatie in documentvorm worden beveiligd bewaard. | V | V | V | V |
| G | Er worden niet meer kopieën van bijzondere informatie gemaakt dan strikt noodzakelijk. | V | V | V | V |
| H | Informatie wordt alleen gedeeld op basis van de verspreidingscriteria van de opsteller. | V | V | V | V |
| I | Bij het overnemen van tekstpassages, blijft het rubriceringsniveau van het origineel onverkort van kracht. | V | V | V | V |
| J | Informatie (inclusief gegevensdragers) wordt vernietigd door middel van een door de BVA voor de desbetreffende rubricering goedgekeurde wijze waarvan vooraf, door onafhankelijke deskundigen, is aangetoond dat reconstructie van de informatie wordt voorkomen. | V | V | V | V |
| K | Van alle exemplaren van documenten met bijzondere informatie worden de volgende gegevens vastgelegd:<br>• Uniek exemplaarnummer;<br>• Opsteller;<br>• Ontvanger;<br>• De in het oorspronkelijke document gebruikte merkingen (zoals 'Vrij te geven aan', 'Releaseable to' of 'REL'). | | V | V | V |
| L | Het bijmaken van kopieën en/ of reproducties (zowel fysiek als digitaal) van bijzondere informatie wordt geregistreerd. | | | V | V |
| M | Het kopiëren en/of reproduceren van bijzondere informatie is voorbehouden aan daartoe aangewezen personen. | | | V | V |
| N | Van vernietiging van bijzondere informatie wordt een proces-verbaal opgemaakt. | | | V | V |
| | *Registratie – de verblijfplaats van de informatie is traceerbaar:* | | | | |
| O | Geregistreerd wordt welke persoon de informatie onder zijn berusting heeft. | | | V | V |

| | | Dep.V | Stg.C | Stg.G | Stg.ZG |
|---|---|---|---|---|---|
| P | Geregistreerd wordt welke persoon de informatie heeft ingezien. | | | V | V |
| | *Fysiek transport:*<br>*De beveiliging van informatie moet tijdens fysiek transport buiten gecontroleerd gebied gehandhaafd blijven:* | | | | |
| Q | Fysieke verzending van bijzondere informatie dient te geschieden met ministerieel goedgekeurde middelen zoals sealbags of andere verzegelingen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is. | V | V | V | V |
| R | Verzending wordt gereed gemaakt door daartoe aangewezen personen c.q. afdeling. | V | V | V | V |
| S | Verzending vindt nationaal plaats per aangetekende en traceerbare verzending of door een BVA goedgekeurde commerciële koerier. | | V | | |
| T | Verzending vindt internationaal plaats per aangetekende en traceerbare verzending of als onbegeleide diplomatieke zending. | | V | | |
| U | Verzending vindt zowel binnen als buiten Nederland plaats per door het ministerie aangewezen koerier. | | | V | |
| V | De ontvanger verstuurt een ontvangstbevestiging naar de verzender. | | | V | V |
| W | Transport vindt binnen Nederland plaats per door het ministerie aangewezen koerier. | | | | V |
| X | Transport vindt buiten Nederland plaats per koerier[1] als diplomatieke zending. | | | | V |
| | *Materiaal dat niet met de voorafgaande methoden kan worden verzonden:* | | | | |
| Y | Wordt verzonden per door de BVA goedgekeurde koerier. | V | V | | |
| Z | Wordt verzonden per Nederlands of bondgenootschappelijk militair transport of per door de SG goedgekeurde koerier. | | | V | V |
| | *Meenemen van bijzondere informatie buiten gecontroleerd gebied (plaats van tewerkstelling):* | | | | |
| A1 | Bijzondere informatie wordt uitsluitend meegenomen buiten de daarvoor aangewezen zones indien dit voor de voortgang van de werkzaamheden noodzakelijk is en hiervoor door de lijnmanager toestemming is verleend. | | V | V | |
| B1 | Token voor de toegang tot de informatie wordt gescheiden van de informatie meegenomen. | | | V | V |
| C1 | De BVA stelt voorschriften op voor het registreren van het meenemen. | | | V | V |
| D1 | Bijzondere informatie wordt niet buiten de daarvoor aangewezen zones of locaties meegenomen. Transport vindt plaats op de hiervoor beschreven wijze. | | | | V |
| | *Elektronisch transport:*<br>*De beveiliging van informatie moet tijdens elektronisch transport buiten gecontroleerd gebied gehandhaafd blijven:* | | | | |
| E1 | De rubricering wordt samen met de informatie verzonden. | V | V | V | V |
| F1 | Het versturen van berichten wordt geregistreerd. | | V | V | V |
| G1 | De ontvangst van het bericht wordt geregistreerd. | | V | V | V |
| H1 | De ontvangst van het bericht wordt bevestigd. | | | V | V |
| | *Vertrouwelijkheid van informatie over netwerken:* | | | | |
| I1 | Bijzondere informatie die wordt verspreid via netwerken wordt vercijferd[2]. | V | V | V | V |
| J1 | Het vercijfermiddel is door de Minister van Binnenlandse Zaken en Koninkrijksrelaties goedgekeurd voor de betreffende rubricering. Voor Defensie geldt goedkeuring door de eigen BA. | V | V | V | |
| K1 | De goedkeuring van een (cryptografisch) beveiligingsmiddel gebeurt door het hoofd van de AIVD namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties, op basis van advies van de Werkgroep Bijzondere Informatiebeveiliging (WBI) of diens rechtsopvolger, na evaluatie door de Unit Weerbaarheid van de AIVD[3]. Voor Defensie gebeurt de goedkeuring door de BA Defensie. | V | V | V | V |
| L1 | De bescherming van cryptografische middelen geschiedt conform VBV 41000. | V | V | V | V |
| M1 | Digitale verwerking van informatie die krachtens een verdrag of een internationale overeenkomst is verkregen, dient met door de verstrekkende instantie goedgekeurde cryptografische middelen te geschieden. | V[4] | V[4] | V | V |

| | | Dep.V | Stg.C | Stg.G | Stg.ZG |
|---|---|---|---|---|---|
| N1 | Digitale verwerking van bijzondere informatie dient met goedgekeurde (cryptografische) beveiligingsmiddelen te geschieden, in overeenstemming met de bijbehorende inzetadviezen en verbindingsbeveiligingsvoorschriften. De Secretaris-generaal van het ministerie verleent toestemming voor de inzet van (cryptografische) beveiligingsmiddelen voor digitale verwerking van bijzondere informatie, met inachtneming van maatregelen K1 en O1. | V[5] | V | V | V |
| O1 | Voor het gebruik en de inzet van (cryptografische) beveiligingsmiddelen voor ICT-voorzieningen wordt advies ingewonnen van de Unit Weerbaarheid van de AIVD. | | V | V | V |

1 Het verzenden per koerier als diplomatieke zending vindt plaats door tussenkomst van het Ministerie van Buitenlandse Zaken, een diplomatieke of beroeps consulaire vertegenwoordiger van Nederland, de Gouverneur van Aruba, Gouverneur van Bonaire of de Gouverneur van Curaçao.
2 Dep. VERTROUWELIJK gerubriceerde informatie hoeft niet vercijferd te worden indien verzending plaatsvindt via een intern netwerk dat zich binnen één locatie bevindt.
3 Zie ook Instellingsregeling WBI, Staatscourant 2005, 139 pagina 8.
4 Voor equivalenten van Dep. VERTROUWELIJK en Stg. CONFIDENTIEEL geldt dat binnen Nederland ook nationaal goedgekeurde (cryptografische) beveiligingsmiddelen mogen worden ingezet.
5 Voor DepV kan de toestemmingsverlening gedelegeerd worden aan de BVA.

Een V houdt in: bij dit niveau van rubricering maatregel verplicht toepassen.

## 7. Beheer van bijzondere informatie

### Doelstelling

Risico's voor bijzondere informatie worden procesmatig beheerst.

### Eisen

Voorzie in maatregelen die duidelijke en veilige beheersing van, omgang met, kopiëring en vernietiging van bijzondere informatie mogelijk maken.

**Tabel 9: Minimale maatregelen voor beheer van bijzondere informatie.**

| | | Dep.V | Stg.C | Stg.G | Stg.ZG |
|---|---|---|---|---|---|
| A | Er is een register van bijzondere informatie, inclusief datum van afgifte, persoon van afname, datum van teruggave en status van vernietiging. | | V | V | V |

Een V houdt in: bij dit niveau van rubricering maatregel verplicht toepassen.

## 8. Incidenten en compromittering

### Doelstelling

Het waarborgen van een gedegen detectie, afhandeling, melding, en opvolging van incidenten en compromitteringen met betrekking tot bijzondere informatie.

### Eisen

Voorzie in maatregelen die in het geval van incidenten en compromittering voorzien in detectie en de impact minimaliseren en isoleren.

Voorzie in maatregelen die in het geval van incidenten en compromittering degelijk forensisch onderzoek hiernaar mogelijk maken.

**Tabel 10: Minimale maatregelen voor beheersing van incidenten en compromittering.**

| | | Dep.V | Stg.C | Stg.G | Stg.ZG |
|---|---|---|---|---|---|
| A | Incidenten en compromittering van bijzondere informatie worden direct gemeld aan de BVA, die dit meldt bij de aangewezen toezichthouders. Zie Artikel 8, lid 2. | V | V | V | V |
| B | Incidenten en compromittering van bijzondere informatie worden tijdig door de BVA/BA gemeld aan de eigenaar van de bijzondere informatie. | V | V | V | V |

| | | Dep.V | Stg.C | Stg.G | Stg.ZG |
|---|---|---|---|---|---|
| C | Incidenten en compromittering van bijzondere informatie die verkregen is krachtens een verdrag worden direct gemeld bij de NSA. Voor Defensie betreft dat de NSA Militair. | V | V | V | V |
| D | Specifieke normen en maatregelen die genomen dienen te worden ter voorbereiding op en mitigatie van incidenten en compromittering van bijzondere informatie, worden beschreven in een Verbindings Beveiligings Voorschrift (VBV). Dit voorschrift wordt nog vastgesteld door de Unit Weerbaarheid (UWB) van de AIVD. | V | V | V | V |
| E | Er is een register bij de BVA/BA van alle meldingen en signalen van (mogelijke) incidenten of compromittering verband houdend met bijzondere informatie. | | V | V | V |

Een V houdt in: bij dit niveau van rubricering maatregel verplicht toepassen.

## TOELICHTING

### Algemeen

Het VIRBI is geactualiseerd en aangescherpt. In de kamerbrief van juli 2023 over de geactualiseerde routekaarten zijn diverse resultaten gecommuniceerd, o.a. over de routekaart digitale weerbaarheid (thema 2) waaronder; Besluit over kaders en richtlijnen rondom HGI: herziening VIRBI.
Referentie kamerbief geactualiseerde routekaarten: https://www.Rijksoverheid.nl/documenten/kamerstukken/2023/07/13/kamerbrief-i-strategie-rijk-actualisatie-routekaarten-evaluatie-i-agenda

Het voorgaande VIRBI dateert uit 2013 en reden voor de aanscherping van maatregelen voor de beveiliging van gerubriceerde informatie is dat de AIVD structureel een onverminderd hoog niveau van digitale dreiging tegen Nederlandse belangen signaleert. Recente incidenten bewijzen dit, gezien de aanhoudende dreiging vanuit meerdere statelijke actoren. Met de huidige geopolitieke situatie en het huidige informatiebeveiligingsstelsel is de Rijksoverheid onvoldoende in staat om adequaat weerstand te bieden tegen de dreiging. Daarom is het van belang om de digitale weerbaarheid van de Rijksoverheid te versterken, met name in de beveiliging van nationaal en internationaal gerubriceerde informatie.

De algehele actualisatie is uitgevoerd op basis van de huidige inzichten. De aanscherping betreft een aantal concrete, minimaal te nemen maatregelen die zijn opgenomen in bijlage.
Er zijn handreikingen in ontwikkeling over verschillende onderwerpen die de implementatie van het VIRBI ondersteunen.
Daarnaast ligt de nadruk op adequaat risicomanagement. Risicomanagement vormt de basis voor risicobeheersing en de te nemen maatregelen.

Ten aanzien van de grondslag van het VIRBI:
De grondslag van het besluit is gelegen in de onderlinge afspraken tussen departementen, die worden aan de MR voorgelegd en vervolgens door de MP ondertekend. Het VIRBI is dus een collegiaal besluit van de ministerraad (MR). Het VIRBI geldt als aanvulling op het VIR, enkel op terrein van bijzondere vertrouwelijkheid.
In de toelichting van het VIR2007 is het volgende opgenomen: Het Beveiligingsvoorschrift Rijksdienst 2005 (BVR) kan gezien worden als een ‘kapstok’ waaraan vele elementen van beveiliging opgehangen kunnen worden. Centraal in het BVR staat de Beveiligingsambtenaar (BVA) die namens de secretaris-generaal belast is met de beveiliging van het Ministerie. Dit omvat ook de zorgplicht voor het VIR en VIRBI. Het VIRBI benadrukt de zorgplicht van ieder Ministerie en van diens lijnmanagement voor de beveiliging van bijzondere informatie bij de rijksdienst.

In dit voorschrift wordt met ’secretaris-generaal (SG)’ de SG van het betreffende ministerie bedoeld.

Financiële impact: Eventuele financiële impact van de implementatie van het VIRBI komt voor eigen rekening van de departementen.

### Artikelsgewijs

#### *Artikel 1 Begripsbepalingen*

Accreditatie: Onder accreditatie wordt verstaan het verlenen van toestemming voor ontvangst, beheer, vernietiging, verwerking en verdere verspreiding van gerubriceerde informatie. Accreditatie betekent met andere woorden het formeel machtigen en goedkeuren van de verwerking van gerubriceerde informatie, met inachtneming van de operationele omgeving. Het is een vorm van (preventief) toezicht, met als doel het waarborgen van een juist beveiligingsniveau voor de aangewezen Te Beschermen Belangen.

Compromittering: Compromittering betekent dus ongeautoriseerde kennisname van bijzondere informatie maar ook de mogelijkheid tot ongeautoriseerde kennisname van bijzondere informatie. In de toelichting op de artikelen 8 en 9 wordt nader ingegaan op compromittering.

Informatiesysteem: Het betreft hier het geheel van mensen, processen en technologie. Rijsdienst: Het VIRBI 2025 geldt ook voor ZBO’s conform artikel 41 van de kaderwet ZBO’s van 1 juli 2022. In dit voorschrift wordt met ‘informatie’ bedoeld: dat het onafhankelijk is van het gebruikte medium en onafhankelijk of de informatie is vastgesteld. De term informatie kan ook slaan op data, metadata, gegevens et cetera. Het voorschrift betreft dus informatie in ruste (bijvoorbeeld opgenomen in documenten of databases), in bewerking (bijvoorbeeld in het geheugen van een computer) of in

communicatie (telefoongesprekken, digitale of fysieke vergaderingen of gesprekken, datacommunicatie, andere elektromagnetische signalen et cetera). Een systeem of proces dat bijzondere informatie verwerkt moet hier ook als informatie worden gelezen.

Kennisname van bijzondere informatie dient beperkt te blijven tot geautoriseerde personen. Autorisatie vraagt om een expliciete en aantoonbare toestemming, waarbij de eisen aan de autorisatieprocedure met het rubriceringsniveau toenemen. Het is bij het verlenen van autorisatie niet voldoende dat een beoogde ontvanger over een Verklaring omtrent gedrag (VOG) of Verklaring van geen bezwaar (VGB) van het juiste niveau beschikt. Er dient een afzonderlijke afweging gemaakt te worden over de functionele noodzaak tot kennisname door de betrokkene.

Rubriceren: Voordat aan informatie een rubricering en rubriceringsduur kan worden toegekend, worden eerst afwegingen gemaakt over de te voorziene nadelige gevolgen die met een redelijke kans op kunnen treden; dit is nader uitgewerkt in de toelichting op artikel 4. De betekenis van de rubriceringsduur is nader uitgewerkt in de toelichting bij artikel 5, lid 1.

Rubriceringsambtenaar: In principe zijn dit de beveiligingsautoriteit (BVA), zijn plaatsvervanger of andere inhoudelijk deskundigen. In de praktijk wijst de SG een rubriceringsambtenaar aan.

Rubriceringsniveaus: Er bestaan vier rubriceringsniveaus. De rubriceringen verschillen in de ernst van de nadelige gevolgen die zijn voorzien bij ongeautoriseerde kennisname. De toelichting op artikel 4 gaat hier nader op in.

Vaststeller: In de praktijk wijst de SG een rubriceringsambtenaar aan.

Verwerking: voor dit begrip is aangesloten bij de definitie van het begrip ‘verwerking’ in de Algemene Verordening Gegevensbescherming (AVG), met dien verstande dat bijzondere, oftewel gerubriceerde, informatie meer omvat dan alleen persoonsgegevens. Het begrip is dan ook breder dan het begrip in de AVG.

Zorgdrager: Op grond van artikel 23, eerste lid van de Archiefwet 1995 dragen de ministers zorg voor de archiefbescheiden die niet zijn overgebracht naar een rijksarchiefbewaarplaats. Als zorgdrager heeft de minister de bevoegdheid bij overbrenging beperkingen aan de openbaarheid te stellen.
Het begrip zorgdrager volgt uit de huidige archiefwet. Als dit begrip in een nieuwe archiefwet niet meer genoemd is, zal het VIRBI daarop worden aangepast.

### *Artikel 2 Plaatsbepaling en reikwijdte*

Lid 1:
De artikelen bevatten op hoofdlijnen de werkwijze voor de behandeling van bijzondere informatie en de wijze van rubriceren. De uitwerking heeft dezelfde zeggingskracht en geeft nadere aanwijzingen over de inrichting van de rubricering en de verwerking van bijzondere informatie.
Tot de Rijksdienst behoren alle organisatieonderdelen waarvoor de ministeriële verantwoordelijkheid onverkort geldt. Het VIRBI 2025 geldt ook voor Zelfstandige Bestuursorganen (ZBO’s).[1] Het VIRBI 2025 heeft geen directe werking buiten de Rijksdienst. Het kan echter noodzakelijk zijn om bijzondere informatie buiten de Rijksdienst te brengen. Het voorschrift staat dit alleen toe als voldoende zekerheid bestaat dat de informatie in overeenstemming met dit voorschrift wordt beveiligd. Centraal staat hierbij het waarborgen van de vertrouwelijkheid middels proportionele maatregelen. In het ministeriële beveiligingsbeleid (artikel 3) dient dit verder te worden uitgewerkt. Regels voor het buiten de Rijksdienst brengen van bijzondere informatie worden gegeven in artikel 7.

Lid 2:
Het VIRBI 2025 is het raamwerk in aanvulling op het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (VIR 2007) en de Baseline Informatiebeveiliging Overheid. Het geeft de regels voor de Rijksdienst voor de integrale beveiliging van bijzondere informatie.
Het VIR 2007 geeft de regels voor de informatiebeveiliging voor de Rijksdienst. Het is een raamwerkregeling in de zin dat de werkwijze om tot een verantwoorde beveiliging te komen bepaald is, zonder een minimaal beveiligingsniveau voor de Rijksdienst op te leggen.
Waar het VIR 2007 betrekking heeft op de gehele betrouwbaarheid van informatiesystemen, is alleen de vertrouwelijkheid van informatie het onderwerp van het VIRBI 2025. Dit houdt in dat voor de bescherming van de integriteit en beschikbaarheid van de informatie in informatiesystemen en informatie-verwerkende processen afwegingen in overeenstemming met het VIR gemaakt moeten worden. In de bijlage zijn eisen opgenomen die ook werking kunnen hebben op beschikbaarheid en

[1] Zie Artikel 41 van de kaderwet ZBO’s.

integriteit. Dit geldt ook voor de bescherming van de vertrouwelijkheid van informatie die niet is gerubriceerd.

Lid 3:
Bijzondere informatie van internationale herkomst behoudt zijn oorspronkelijke rubricering. Dit houdt in dat de oorspronkelijke rubricering niet verlaagd mag worden door een Nederlandse rubricering. Op dergelijke bijzondere informatie is primair niet het VIRBI, maar zijn internationale verdragen (EU, NAVO, General Security Agreement, Memorandum of Understanding, Letter of Intent, bilaterale afspraken et cetera) van toepassing. In deze verdragen is opgenomen dat, behoudens enkele uitzonderingen, de nationale regelgeving wordt gevolgd:
1. Het VIRBI 2025: Het ministerie draagt zelf zorg voor een afdoende beveiliging en verantwoording;
2. Het verdrag kan een aantal uitzonderingen geven voor de beveiligingsmaatregelen waaraan moet worden voldaan. Deze komen neer op een uiterst beperkte ruimte voor eigenstandig risicomanagement en mogelijk gescheiden verwerking van bijzondere informatie van nationale en internationale herkomst.

Toestemming voor verwerking van internationaal gerubriceerde informatie dient verkregen te worden van de Security Accreditation Authority (SAA). De secretaris-generaal van het ministerie is de SAA voor civiele omgevingen en de beveiligingsautoriteit van het Ministerie van Defensie voor defensie-omgevingen. Deze zijn verantwoordelijk om voorafgaand aan een toestemmingverlening (accreditatie), te (laten) onderzoeken of de beveiliging van de informatie voor wat betreft de bescherming van de nationale en internationale belangen aan de vereisten voldoet. Voorafgaand aan de accreditatie van verwerkingen van internationaal gerubriceerde informatie is goedkeuring nodig vereist van de National Security Authority (NSA) respectievelijk civiel en militair.

De AIVD vervult de rol van NSA voor NAVO, EU en ESA voor het civiele domein; de verantwoordelijkheid voor de NSA militair is belegd bij het Hoofd van de afdeling beveiligingsautoriteit bij de Directie Bedrijfsvoering en Evaluatie van het Ministerie van Defensie. NAVO en EU vereisen dat respectievelijk NAVO- en EU-goedgekeurde cryptomiddelen gebruikt worden, waarbij ook nationale producten ingezet mogen worden voor RESTRICTED en CONFIDENTIAL, mits geaccrediteerd met toestemming van NSA. De NSA voert tevens de controle op de beveiliging uit en verzorgt de verdere afhandeling naar de internationale organisaties. Het ministerie blijft zelf verantwoordelijk voor een afdoende beveiliging van de nationale belangen (voor zowel beschikbaarheid, integriteit als de vertrouwelijkheid).

De overige Information Assurance functies die door de EU en NAVO worden onderscheiden, zijn belegd bij de AIVD middels het Organisatiebesluit AIVD 2023 (National Communication and Information Systems Security Authority (NCSA), National Distribution Authority (NDA) en National TEMPEST Authority (NTA) voor NAVO; Information Assurance Authority-autoriteit (IAA), Tempest- autoriteit, Crypto Approval Authority (CAA), Crypto Distribution Authority (CDA) en TEMPEST Authority (TA) voor EU.

De verantwoordelijkheid voor de NSA militair is belegd bij het Hoofd van de afdeling beveiligingsautoriteit bij de Directie Bedrijfsvoering en Evaluatie van het Ministerie van Defensie.

Personen die in aanraking (kunnen) komen met gerubriceerde NAVO-, EU- of ESA-informatie en/ of toegang moeten krijgen tot deze organisaties, moeten beschikken over een Personnel Security Clearance (PSC) van de NSA. Een PSC is iets anders dan een verklaring van geen bezwaar (VGB). Voor zowel een PSC als een VGB wordt een veiligheidsonderzoek uitgevoerd, waarvan de omvang en diepgang in lijn is met de functie of de werkzaamheden. Over het algemeen geeft de NSA alleen PSCs af aan personen met de Nederlandse nationaliteit.

Met betrekking tot NAVO en EU informatie wordt de volgende vergelijkingstabel gehanteerd om tot het vergelijkbaar nationaal niveau te komen.

**Tabel 1. Vergelijking tussen nationale rubriceringsniveaus en NAVO- en EU-rubriceringsniveaus.**

| Nederland | NAVO | EU |
|---|---|---|
| Departementaal VERTROUWELIJK | NATO RESTRICTED | RESTREINT UE/EU RESTRICTED |
| Staatsgeheim CONFIDENTIEEL | NATO CONFIDENTIAL | CONFIDENTIAL UE/EU CONFIDENTIAL |
| Staatsgeheim GEHEIM | NATO SECRET | SECRET UE/EU SECRET |
| Staatsgeheim ZEER GEHEIM | COSMIC TOP SECRET | TRÈS SECRET UE/EU TOP SECRET |

Met betrekking tot informatie die bilateraal uit andere landen wordt ontvangen, wordt dit conform de bilaterale overeenkomst behandeld. Indien er geen bilaterale overeenkomst is, kan middels de bovenstaande tabel een vergelijkbaar nationaal niveau bepaald worden voor de rubricering, in

afstemming met de verstrekker of eigenaar van de informatie.
Het kan noodzakelijk zijn om aan informatie gelijktijdig zowel nationale als internationale rubriceringen toe te kennen. Indien bijvoorbeeld documenten zijn samengesteld met informatie uit verschillende bronnen met verschillende rubriceringen dan behoudt de informatie iedere oorspronkelijke rubricering van de broninformatie.
Wanneer een oorspronkelijke rubricering wordt gevolgd door een 'Vrij te geven aan'- of 'Releasable to (REL)'-merking, dan wordt deze merking gehandhaafd.

***Artikel 3 Beveiligingsbeleid***

Dit artikel geeft met betrekking tot bijzondere informatie aanvullende bepalingen ten opzichte van de eisen die het VIR 2007 in artikel 3 aan het beveiligingsbeleid stelt. Het ministeriële beleid geeft de aanwijzingen voor de wijze waarop de medewerkers met bijzondere informatie omgaan; het VIRBI 2025 geeft de kaders voor dit ministerieel beleid.

Lid 1:
Het VIRBI 2025 bevat, ten opzichte van het VIR 2007, drie aanvullende onderwerpen voor het beleid. De onderwerpen hebben betrekking op de wijze waarop het ministerie informatie rubriceert, de wijze waarop de secretaris-generaal vooraf toestemming verleent voor het verwerken van bijzondere informatie en de wijze waarop het ministerie toezicht uitoefent op de beveiliging van bijzondere informatie. De onderwerpen kunnen onderdeel uitmaken van een integraal beleidsdocument of afzonderlijk worden vastgelegd.
Onder a:
Dit omvat zowel de wijze waarop binnen het ministerie tot rubricering wordt besloten als de te hanteren criteria om tot de juiste rubricering te komen. Belangrijk is hierbij af te wegen dat naarmate het rubriceringsniveau van informatie hoger ligt, de beveiligingseisen toenemen.
Onder b:
Het belang dat met bijzondere informatie gemoeid is, maakt een expliciete afweging op centraal niveau noodzakelijk om reeds op voorhand te waarborgen dat de informatieverwerking zorgvuldig geschiedt. Daarom wordt in het beleid vastgelegd hoe vooraf toestemming wordt gegeven voor het verwerken van bijzondere informatie. Mandatering van toestemmingverlening is mogelijk en kan voor verschillende rubriceringsniveaus verschillend worden ingevuld.
Voor bijzondere informatie en informatiesystemen wordt, onder andere ten behoeve van die centrale afweging, in het ministeriële integrale beveiligingsbeleid beschreven op welke wijze bepaald wordt met welke dreigingen (onderkend of voorspelbaar) en welke risico's (voorstelbaar) rekening gehouden moet worden en hoe dit overzicht van dreigingen en risico's actueel gehouden wordt.
Nationale accreditatie: De secretaris-generaal van het betreffende ministerie moet vooraf toestemming (accreditatie) verlenen voor de verwerking van bijzondere informatie. De Unit Weerbaarheid (AIVD) biedt organisaties een reeks van goedgekeurde producten voor de beveiliging van hun digitale informatie. Goedkeuring wordt pas afgegeven na evaluatie van het product, waarin onderzocht wordt of het product voldoende bescherming biedt voor de verwerking van bijzondere informatie.
Voor vragen over de inzet van informatiebeveiligingsproducten die door de Unit Weerbaarheid geëvalueerd zijn, kunt u terecht bij de Unit Weerbaarheid.
Onder c:
Behalve de initiële toestemming voor de verwerking van bijzondere informatie stelt het VIRBI 2025 in de bijlage ook eisen aan het toezicht tijdens de verwerking. Hierbij wordt een minimale frequentie van toezicht gegeven die hoger is naarmate het rubriceringsniveau ook hoger ligt. Ook worden voor Stg. Confidentieel en hoger gerubriceerde informatie eisen gesteld aan de administratie met betrekking tot kennisname.
Besluit BVA-stelsel Rijksdienst 2021: Het lijnmanagement is verantwoordelijk voor de integrale beveiliging van hun dienstonderdeel. De BVA heeft namens de secretaris-generaal de departementale toezichthoudende rol.

***Nadere invulling van de toewijzing van verantwoordelijkheden voor ketens van informatiesystemen***

Het VIR 2007 bepaalt dat de verantwoordelijkheid voor ketens van informatiesystemen aan lijnmanagers wordt toegewezen. Het VIRBI 2025 stelt eisen aan de beveiliging van bijzondere informatie, ook informatie die in ketens wordt verwerkt.
De functionaris onder wiens verantwoordelijkheid de bijzondere informatie wordt verwerkt zorgt er voor en ziet erop toe dat de beveiliging van de bijzondere informatie in overeenstemming met de eisen wordt ingericht, ook door de lijnmanagers die verantwoordelijk zijn voor de ketens van informatiesystemen voordat de bijzondere informatie daarin wordt opgenomen. Ook waar delen van ketens zich buiten de rijksdienst bevinden dient zekerheid te bestaan dat aan de beveiligingseisen is voldaan.

Lid 2:

Onder a:
De beveiligingsautoriteit is verantwoordelijk voor het toezicht op en de consistentie van de beveiligingsmaatregelen binnen het betreffende ministerie dan wel rijksbreed. Er wordt gezorgd voor een gezamenlijke, gecoördineerde aanpak van de beveiliging van vertrouwelijke gegevens, zodat gevoelige informatie op het juiste niveau wordt beschermd. Dit omvat ook het bevorderen van samenwerking binnen en tussen ministeries om beveiligingsproblemen integraal aan te pakken.
Onder b:
Er wordt gezorgd voor een gezamenlijke, gecoördineerde aanpak van de beveiliging van vertrouwelijke gegevens, zodat gevoelige informatie op het juiste niveau wordt beschermd. Dit omvat ook het bevorderen van samenwerking binnen en tussen ministeries om beveiligingsproblemen integraal aan te pakken.
Onder c:
Bij beveiligingsinbreuken worden direct (nood)maatregelen genomen om verdere schade te voorkomen, bijvoorbeeld door het blokkeren van toegang of het aanpassen van systemen. Ook hier is het van belang het advies van de CISO mee te wegen wanneer beveiligingsissues een digitale component hebben. Daar waar van toepassing zijn andere C-rollen betrokken.
Onder d:
Als er aanwijzingen zijn voor compromittering van vertrouwelijke informatie, wordt dit onderzocht en gemeld aan de secretaris-generaal. Er kan ook een commissie worden ingesteld voor nader onderzoek en er wordt voldaan aan de meldingsverplichtingen volgens de wet- en regelgeving.

Lid 3:
De BVA(Rijk) weegt het advies van de CISO(Rijk) mee in zijn/haar afwegingen wanneer beveiligingsissues een digitale component hebben. Samenwerken is bevorderlijk voor het adequaat adresseren van beveiligingsissues. Daar waar van toepassing geldt dat ook voor andere C-rollen, bijvoorbeeld bij privacy issues is de CPO(Rijk) betrokken.

### *Artikel 4 Rubriceringen*

In de Wet bescherming staatsgeheimen is in de titel aangegeven dat Staatsgeheimen gegevens betreffen waarvan de geheimhouding door het belang van de Staat wordt geboden. In artikel IIA van de Wet bescherming staatsgeheimen is opgenomen dat onder de veiligheid van de Staat ook wordt verstaan de veiligheid van diens bondgenoten. Informatie waarvan de geheimhouding is geboden door het belang van één of meerdere ministeries of één of meer bondgenoten van de Staat en niet als Staatsgeheim is gerubriceerd, wordt als Departementaal Vertrouwelijk gerubriceerd.
De inschaling van de rubricering wordt op basis van twee criteria bepaald: schade en belang.
In het VIRBI hebben we gekozen om de ‘de Nederlands staat’ te noemen, maar de Wet bescherming staatsgeheimen uit 2013 heeft het over ‘de Staat’. We bedoelen daar telkens hetzelfde mee, met andere woorden als we het over ‘de Staat’ hebben bedoelen we ‘de Nederlandse Staat.’

**Schade**

De mate van schade aan een belang is mede bepalend voor de hoogte van de rubricering. Uitgegaan is van de volgende criteria in oplopende volgorde:
a. Schade: beperkte nadelige invloed;
b. Ernstige schade: nadelige invloed, korte termijn geen alternatieven;
c. Zeer ernstige schade: onmisbaar, geen alternatieven mogelijk.

**Belang**

De mate van vitaliteit van de (nationale) belangen van de Staat of haar bondgenoten of een belang van een of meerdere ministeries is mede bepalend voor de hoogte van de rubricering. Voor de bepaling van de (vitale) belangen van de Staat of haar bondgenoten is aangesloten op de vitale belangen in Veiligheidsstrategie voor het Koninkrijk der Nederlanden[2]. Deze vitale belangen zijn als volgt gedefinieerd:
a. Territoriale veiligheid: het ongestoord functioneren van het Koninkrijk der Nederlanden en zijn EU en NAVO bondgenoten als onafhankelijke staten in brede zin, dan wel de territoriale veiligheid in enge zin;
b. Fysieke veiligheid: het ongestoord functioneren van de mens in het Koninkrijk der Nederlanden en zijn omgeving;
c. Economische veiligheid: het ongestoord functioneren van het Koninkrijk der Nederlanden als een effectieve en efficiënte economie;

[2] Tweede Kamer, vergaderjaar 2022–2023, stuk 30 821, nr. 178.

d. Ecologische veiligheid: het ongestoord blijven voortbestaan van de natuurlijke leefomgeving in en nabij het Koninkrijk der Nederlanden;
e. Sociale en politieke stabiliteit: het ongestoorde voortbestaan van een maatschappelijk klimaat waarin groepen mensen goed met elkaar kunnen samenleven binnen de kaders van de democratische rechtstaat van het Koninkrijk der Nederlanden en daarin gedeelde kernwaarden;
f. Internationale rechtsorde en stabiliteit: het goed functioneren van het internationale stelsel van normen en afspraken, gericht op het bevorderen van de internationale vrede en veiligheid, inclusief mensenrechten, en effectieve multilaterale instituties en regimes, alsmede het goed functioneren van staten grenzend aan het Koninkrijk der Nederlanden en in de directe omgeving van de Europese Unie.

Belangen van een of meerdere ministeries betreffen het ongestoord functioneren van het ministerie in de uitvoering van zijn taken of ter realisatie van zijn doelen. Conform de tabel in de toelichting bij artikel 2, lid 3, wordt bijzondere informatie gerubriceerd door NAVO en EU beveiligd volgens het overeenkomstige nationale beveiligingsniveau.

Een rubricering kan aangevuld worden door een of meerdere merkingen. Hiermee kan een specifieke beperking van de kring van gerechtigden worden aangegeven. Merkingen staan echter los van de rubricering van de informatie en dit onderwerp is daarom niet opgenomen in deze regeling.

Lid 2, onder a, b en c:
Benadrukt wordt de aansluiting met artikel 98 en verder van het Wetboek van Strafrecht, dat de strafbaarheid regelt van misdrijven met betrekking tot staatsgeheimen, zoals het ongeautoriseerd toegang proberen te verkrijgen tot of het onzorgvuldig behandelen van staatsgeheimen. Artikel 98 en verder van het Wetboek van Strafrecht hanteert de term ‘een inlichting’; de in het VIRBI 2025 gebruikte term ‘informatie’ sluit de term ‘een inlichting’ in.

Lid 2, onder d:
Departementaal Vertrouwelijk gerubriceerde informatie betreft primair het belang van één of meerdere ministeries of één of meer bondgenoten van de Staat. De maatschappelijke consequenties als gevolg van ongeautoriseerde kennisname blijven voor dit rubriceringniveau beperkt in tijd en omvang.

Lid 3:
Het vaststellen van rubricering gebeurt expliciet met het vaststellen van de inhoud of de informatie. Bij het accumuleren van bijzondere informatie behoort rekening te worden gehouden met het aggregatie-effect, waardoor een grote hoeveelheid niet-gevoelige informatie gevoelig kan worden. Door aggregatie van bijzondere informatie ontstaat er een (digitale) en vaak gedecentraliseerde database, waarin bundeling, aggregatie of combinatie van informatie kan leiden tot een vergroting van mogelijke schade en daarmee ook het rubriceringsniveau en de bijhorende maatregelen. In de conceptfase wordt de informatie behandeld conform het niveau van beveiliging gekoppeld aan het voorstel tot rubricering van de steller, totdat het definitieve niveau van rubricering is bepaald door degene die de inhoud vaststelt, waarna de beveiliging conform het vastgestelde rubriceringsniveau wordt behandeld.

### *Artikel 5 Herzien en beëindigen van de rubricering*

De geheimhouding van bijzondere informatie is noodzakelijk voor een specifieke periode of verbonden aan een bepaalde gebeurtenis, maar zal niet automatisch vervallen. De rubricering moet daarom worden voorzien van een maximum tijdsverloop of bepaalde gebeurtenis, na dit tijdsverloop of deze bepaalde gebeurtenis dient de noodzaak tot en de hoogte van de rubricering opnieuw te worden vastgesteld. Hiermee wordt enerzijds voorkomen dat informatie onnodig lang beveiligd wordt en anderzijds wordt de geheimhouding van informatie geborgd zolang dit noodzakelijk is. Er kan eventueel een verzoek worden ingediend, door personen die geautoriseerd zijn om kennis te nemen van die informatie, bij de vaststeller van de rubricering van de informatie, om te voorkomen dat informatie onnodig gerubriceerd blijft. Een termijn van 10 jaar is hierbij het uitgangspunt.
Bij een verzoek in het kader van de Wet Open Overheid (Woo) wordt op grond van artikel 5.1 de rubricering opnieuw beoordeeld. De rubricering van de informatie of delen daarvan moet (en) worden beëindigd als geen van de uitzonderingsgronden van de Woo aan de orde is en als het belang van openbaarheid zwaarder weegt dan het belang gediend met de uitzonderingsgrond.
Informatie die wordt vrijgegeven op basis van een dergelijk verzoek kan immers niet langer gerubriceerd zijn. Indien delen niet kunnen worden ge-de-rubriceerd, moeten deze onleesbaar worden gemaakt.

Bijzondere informatie die krachtens een verdrag of internationale overeenkomst is verkregen en Staatsgeheimen die door de wet als zodanig zijn aangewezen, vallen buiten dit regime. Bijzondere informatie die krachtens een verdrag is verkregen, heeft per definitie een niet- Nederlandse rubrice-

ring. De informatie dient overeenkomstig de in het verdrag overeengekomen beveiligingsregime te worden beveiligd. Indien de informatie niet meer nodig is, kan deze worden teruggestuurd of worden vernietigd, overeenkomstig het verdrag. Informatie die door de wet als zodanig is aangewezen, valt eveneens buiten het gestelde in het eerste lid van dit artikel. De Kernenergiewet en het Geheimhoudingsbesluit Kernenergiewet zijn hiervan voorbeelden.
Uitsluitend de vaststeller van de rubricering, zoals bedoeld in Artikel 1, sub f, is bevoegd de rubricering te herzien of te beëindigen. De vaststelling is functie- en niet persoonsgebonden. De vaststeller van de informatie blijft ook na reorganisaties (onderbrengen bij een ander deel van of buiten de Rijksdienst) of overdracht van functies naar een ander deel van of buiten de Rijksdienst, de zorgplicht houden voor de bijzondere informatie, tenzij expliciet vóór een dergelijke reorganisatie of functieoverdracht is bepaald dat de zorgplicht niet over gaat. Indien de zorgplicht niet over gaat, zal de zorgdrager bij een voornemen of plicht tot herziening of beëindiging van de rubricering overleg voeren met de nieuwe rubriceringsambtenaar van de organisatie waar de bijzondere informatie is ondergebracht.
Omdat uitsluitend de vaststeller mag her-rubriceren, behoudt afgeleid werk de oorspronkelijke rubricering van het gebruikte bronmateriaal, tenzij in overeenstemming met de oorspronkelijke vaststeller een andere rubricering kan worden vastgesteld. Het is dus niet zonder meer toegestaan om uittreksels of overzichten lager te rubriceren dan het bronmateriaal dat hiervoor gebruikt is.
Uitsluitend de secretaris-generaal van het ministerie dat de oorspronkelijke rubricering heeft vastgesteld kan functionarissen mandateren om de rubricering te herzien.

Lid 4 is vooral bedoeld als herinnering. In de Archiefwet 1995, artikel 14 is bepaald dat archiefbescheiden die in een archiefbewaarplaats berusten, behoudens het bepaalde in de artikelen 15, 16 en 17, openbaar zijn. De rubricering vervalt dus bij overbrenging naar een rijksarchiefbewaarplaats, tenzij de zorgdrager, i.c. de Minister, in overleg met de vaststeller van de rubricering besluit dat de rubricering ook in de archiefbewaarplaats geldt, gelet op de belangen die in artikel 15, eerste lid van de Archiefwet 1995 staan opgesomd. Bij overbrenging is het op grond van de Archiefwet 1995 de zorgdrager, i.c. de Minister, die de beperkingen aan de openbaarheid vaststelt, na advies van de algemene rijksarchivaris. Relevant is in dergelijke gevallen de eisen aan de beveiliging die de zorgdrager (eigenaar van de informatie) stelt ook expliciet kenbaar te maken. De beheerder van de archiefbewaarplaats is eveneens gehouden aan het VIR 2007 en, voor zover het bijzondere informatie betreft, het VIRBI 2025.

### *Artikel 6 Eisen aan de beveiliging*

Lid 1:
Van belang is dat de eisen volgend uit het VIRBI 2025 niet alleen zien op de informatie maar ook op het geheel van de verwerking. Het proces of het informatiesysteem dat gebruikt wordt voor verwerking van bijzondere informatie moet meegewogen worden. De eisen aan een verwerking kunnen ook voortkomen uit de risico's gepaard gaande met aggregatie of verrijking van gegevens in de verwerking. De eisen in artikel 6, lid 1, sub a en b, gelden voor het geheel van een verwerkend systeem. Dat betekent dat fysieke omgevingen, personen en processen, inclusief binnen of buiten de Rijksdienst uitbestede delen, moeten worden meegenomen in de beveiliging. Van belang is het denken in ketens.

Lid 2:
Bij gebruik van de afwijkingsruimte gegeven in het tweede lid dienen in de verantwoording van de afwijking de beveiligingsdoelstellingen te worden meegewogen, conform het principe 'pas toe of leg uit'.
Onder risicomanagement wordt verstaan het inzichtelijk en systematisch inventariseren, beoordelen en – door het treffen van maatregelen – beheersbaar maken van risico's op basis van een kans en impact analyse, die het bereiken van de doelstellingen van de organisatie bedreigen dan wel bevorderen, op een zodanige wijze dat verantwoording kan worden afgelegd over de gemaakte keuzes. Hierbij wordt ook inzichtelijk gemaakt welke restrisico's worden geaccepteerd en wie daartoe bevoegd is. Met betrekking tot de dreiging van specifieke tegenstanders, hun capaciteiten en modus operandi kan de BVA informatie aanreiken. Een deel van de informatie betrekt de BVA van de AIVD, de MIVD, de NCTV en andere niet voor eenieder toegankelijke bronnen van organisaties die op dit terrein een taak hebben. Het geheel wordt zo opgezet dat verantwoording afgelegd kan worden over de gemaakte keuzes en het bereikte beveiligingsniveau. In de bijlage worden de eisen die aan de vertrouwelijkheid worden gesteld nader benoemd. Specifiek voor de beveiliging van bijzondere informatie geldt dat voor de toepassing en naleving van de eis van vertrouwelijkheid (exclusiviteit) een dusdanige set van maatregelen is toegepast dat de risico's die de verwerking en de aard van de te beschermen bijzondere informatie met zich meebrengen, adequaat zijn afgedekt. Dit wordt aangeduid als een positief beveiligingsrendement. Er wordt aangesloten bij de rijkskaders voor risicomanagement en accreditatie.

Lid 3:
Dit lid geeft aan dat er op basis van internationale verdragen of internationale overeenkomsten beperkingen bestaan waardoor voor de beveiliging van betreffende bijzondere informatie verantwoor-

ding aan een andere autoriteit verschuldigd is. Afhankelijk van wat er in het verdrag of overeenkomst is vastgelegd, voor EU, NAVO en ESA is het de NSA. Zie ook de toelichting bij artikel 2, lid 3 sub 3.

### *Artikel 7 Buiten de rijksdienst brengen van bijzondere informatie*

Het kan noodzakelijk zijn om bijzondere informatie buiten de rijksdienst te brengen. Hiervan is sprake zodra de informatie ter beschikking wordt gesteld aan mensen of instanties waarop het VIRBI 2025 niet van toepassing is, dus zodra zij buiten de reikwijdte gesteld in artikel 2, lid 1 van dit voorschrift vallen. De lijnmanager die verantwoordelijk is voor de informatie, zoals bedoeld in artikel 4 van het VIR 2007, dient zorg te dragen voor een toereikende beveiliging en te voorzien in de mogelijkheid en bevoegdheid om toezicht en controle hierop uit te oefenen, alvorens de betreffende bijzondere informatie buiten de rijksdienst wordt gebracht. Bijzondere informatie wordt uitsluitend buiten de rijksdienst gebracht indien de secretaris-generaal, of de door hem aangewezen ambtenaar, vooraf toestemming heeft verleend. Bij structurele informatieoverdracht naar externe partijen kan door het ministerie een generieke regeling worden getroffen, waarmee de voorwaarden centraal worden vastgelegd. Daar waar noodzakelijkerwijs informatie door omstandigheden direct buiten de Rijksdienst moet worden gebracht, wordt achteraf verantwoording afgelegd over de noodzaak en de getroffen maatregelen.

### *Artikel 8 Compromittering van bijzondere informatie*

1. Elke ambtenaar is verplicht de beveiligingsautoriteit (BVA) van het betreffende ministerie onmiddellijk mededeling te doen van een (mogelijke) inbreuk op de beveiliging die leidt tot compromittering van bijzondere informatie.
2. Indien de compromittering betrekking heeft op bijzondere informatie die is verkregen van een ander ministerie of krachtens verdrag of internationale overeenkomst, doet de in lid 2 genoemde functionarissen bovendien mededeling aan dat betreffende ministerie of de krachtens het verdrag of de internationale overeenkomst voor de beveiliging van die bijzondere informatie verantwoordelijke instantie.

Algemeen:
De AIVD is eerste en centraal aanspreekpunt voor de gehele rijksdienst met uitzondering van het Ministerie van Defensie. Centrale melding van vermoedelijke en feitelijke ongeautoriseerde kennisname maakt het mogelijk om trends en verbanden te ontdekken binnen deze meldingen.
Waar andere partijen schade kunnen krijgen als gevolg van de (vermoedelijke) ongeautoriseerde kennisname van bijzondere informatie worden deze partijen geïnformeerd en betrokken bij het onderzoek. Voor internationale informatie geldt dat waar overeengekomen de NSA medezeggenschap heeft over het onderzoek.
In het begrip compromittering zit ook de mogelijkheid tot kennisname. Zie ook artikel 1, Begripsbepalingen.

### *Artikel 9 Commissie van onderzoek*

Deze commissie bestaat uit één of meer ambtenaren die met het uitvoeren van onderzoeken ervaring hebben, die niet betrokken zijn bij de compromittering en die niet onmiddellijk ondergeschikt zijn aan bij de compromittering betrokken ambtenaren. De commissie is gerechtigd kennis te nemen van de informatie, inclusief de betrokken informatiesystemen, die op de compromittering betrekking heeft, is ook gerechtigd betrokken locaties te onderzoeken en te betreden en de bij de compromittering betrokken ambtenaren, alsmede de ambtenaar die de rubricering heeft vastgesteld, te horen. Het rapport van bevindingen dient te worden beoordeeld op de noodzaak tot rubricering.
Voordat een interne commissie van onderzoek van start gaat wordt expliciet de afweging gemaakt of sprake is van een strafbaar feit in welk kader aangifte vereist is. Er wordt dan geen zelfstandig intern onderzoek opgestart, wel wordt direct bepaald in overleg met de opsporingsinstantie of en zo ja, welke gegevens veilig gesteld moeten worden en op welke wijze dit gebeurt.
Het is van belang om ten behoeve van het uitvoeren van dergelijke onderzoeken gebruik te kunnen maken van expertise op Rijksniveau. De BVA's kunnen dan een beroep doen op hun collega's of andere experts om hen bij te staan en te ondersteunen in een dergelijk onderzoek.
De Algemene Inlichtingen- en Veiligheidsdienst of de Militaire Inlichtingen- en Veiligheidsdienst kunnen de commissie bij haar onderzoek terzijde staan.

### *Artikel 10 Evaluatie*

Het betreft een maximale evaluatiecyclus van drie jaren en zo nodig sneller als daar aanleiding toe is.

### *Artikel 11 Overgangsrecht*

Het VIRBI 2025 vervangt de eerdere versie uit 2013.

### *Artikel 12 Intrekking VIRBI 2013*

Reeds bestaande gerubriceerde informatie hoeft niet als gevolg van de inwerkingtreding van het VIRBI 2025 opnieuw te worden beoordeeld en gerubriceerd. Dit wordt uiterlijk 10 jaar na vaststelling door de vaststeller of diens rechtsopvolger onderzocht;
Voor bestaande, reeds gerubriceerde informatie, waarbij volledig wordt voldaan aan de maatregelen zoals benoemd in het besluit van 1 juni 2013, zijn organisaties gedurende een overgangsperiode van 6 maanden niet gehouden te voldoen aan de hierop aanvullende maatregelen zoals deze in de bijlage zijn opgenomen.

### *Artikel 13 Inwerkingtreding*

Dit besluit treedt in werking nadat het VIRBI 2025 is vastgesteld in de ministerraad en gepubliceerd in de Staatscourant.

### *Artikel 14 Citeertitel*

We gebruiken de naam: Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2025. In het dagelijks gebruik spreken we afgekort over: VIRBI 2025.

*De Minister-President, Minister van Algemene Zaken,*
*H.W.M. Schoof*