Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie

24 februari 2004/Nr. 04M464166

De Minister-President, Minister van Algemene Zaken,
Handelende in overeenstemming met het gevoelen van de ministerraad,

Besluit:

A. Algemeen

Artikel 1. Verklaring van de gebruikte begrippen
In dit besluit wordt verstaan onder:
a. bijzondere informatie: staatsgeheimen en overige bijzondere informatie waarvan kennisname door niet gerechtigden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries;
b. staatsgeheim: bijzondere informatie waarvan de geheimhouding door het belang van de Staat of zijn bondgenoten wordt geboden;
c. rubriceren: vaststellen en aangeven dat een gegeven bijzondere informatie is en het bepalen en aangeven van de mate van beveiliging die aan deze informatie moet worden gegeven;
d. merking: aanduiding die een bepaalde wijze van behandelen van bijzondere informatie aangeeft;
e. beveiligen: beschermen van bijzondere informatie tegen kennisname door niet gerechtigden;
f. minister: elke minister voor wat het onder zijn leiding staande ministerie en de daaronder ressorterende diensten, bedrijven en instellingen betreft;
g. compromittering: de kennisname dan wel de mogelijkheid tot kennisnemen door een niet gerechtigde van bijzondere informatie;
h. Vir: Besluit voorschrift informatiebeveiliging rijksdienst 1994;
i. Wvo: Wet veiligheidsonderzoeken;
j. Wob: Wet openbaarheid van bestuur;
k. BVA: de beveiligingsambtenaar als bedoeld in het Beveiligingsvoorschrift I, 1949;
l. BIB-beraad: Bijzondere Informatie Beveiligingsberaad, zoals ingesteld door de Ministers van Binnenlandse Zaken, van Buitenlandse Zaken en van Defensie op 1 juni 1998 (Stct. 110), laatstelijk gewijzigd op 17 maart 2000 (Stct. 96).

Toelichting
Het Vir bevat algemene regels voor de beveiliging van informatie binnen de rijksoverheid.
Binnen deze informatie bestaat informatie waarvan de kennisname door niet gerechtigden schade of nadeel op kan leveren voor de Staat, zijn bondgenoten of een of meer ministeries. Om deze reden moeten er bij deze informatie hogere eisen worden gesteld aan de waarborging van de exclusiviteit, dat wil zeggen de mate waarin de toegang tot de informatie is beperkt tot een gedefinieerde groep van gerechtigden. Deze informatie wordt bijzondere informatie genoemd.
Bijzondere informatie bestaat uit staatsgeheimen en uit overige kwetsbare informatie (niet-staatsgeheime bijzondere informatie), die weliswaar geen staatsgeheim is, maar toch meer beveiliging behoeft dan het algemene beveiligingsniveau biedt. Niet-staatsgeheime bijzondere informatie is dikwijls al op basis van een departementale regeling gemerkt, bijvoorbeeld 'BZ-vertrouwelijk' voor informatie, waarvan kennisname door niet bevoegden kan leiden tot nadelige gevolgen voor het Ministerie van Buitenlandse Zaken. Voorbeelden van categorieën niet-staatsgeheime bijzondere informatie zijn opgenomen in bijlage 2 van dit voorschrift. Deze voorbeelden hebben geen limitatief karakter; ze dienen als hulpmiddel bij het vastleggen in het beleidsdocument van de soorten bijzondere informatie die zich op een ministerie bevinden (zie artikel 13, tweede lid, onder a).
Er moeten pas hogere eisen aan de waarborging van de exclusiviteit worden gesteld indien er risico's zijn die dat rechtvaardigen. Daarom stelt de definitie van 'bijzondere informatie' in artikel 1 onder a als eis dat er sprake moet zijn van nadelige gevolgen voor de belangen van de Staat, zijn bondgenoten of van één of meer van zijn ministeries indien niet-gerechtigden hiervan kunnen kennisnemen. Het nadeel kan soms zo ernstig zijn, dat er sprake is van schade. In bijlage 2 van dit voorschrift zijn voorbeelden opgenomen van categorieën van informatie waarbij sprake kan zijn van de hier bedoelde nadelige gevolgen.
Gerechtigd om kennis te nemen van staatsgeheimen zijn personen met een verklaring van geen bezwaar op grond van de Wet veiligheidsonderzoeken (Wvo); in alle gevallen van kennisname van bijzondere informatie is een 'need to know' vereist, dat wil zeggen dat voor de betrokkene toegang tot de bijzondere informatie noodzakelijk is om een uit zijn functie voortvloeiende taak te kunnen vervullen.
De omschrijving van het begrip staatsgeheim is ontleend aan de omschrijving die het Wetboek van Strafrecht geeft in artikel 98.
Wat de verhouding van dit voorschrift tot de Wet openbaarheid van bestuur (Wob) betreft, wordt op het volgende gewezen. Het aanwijzen van informatie als 'bijzonder' betekent dat het beveiligingsregime van dit voorschrift op deze informatie moet worden toepast. Dit betekent uiteraard niet dat als dergelijke informatie op grond van de Wob wordt opgevraagd, dit verzoek zonder meer kan worden geweigerd. In dat geval wordt bezien of tot openbaarmaking kan worden overgegaan. Van openbaarmaking kan slechts worden afgeweken indien daarvoor een grond aanwezig is als bedoeld in artikel 10 of 11 van de Wob.

Artikel 2. Reikwijdte en verhouding tot het VIR
1. Dit voorschrift geldt voor de rijksdienst, waartoe gerekend worden de ministeries met de daaronder ressorterende diensten, bedrijven en instellingen.
2. Op de beveiliging van bijzondere informatie zijn de bepalingen van dit voorschrift in aanvulling op het Vir van toepassing.

Toelichting
Dit voorschrift is een aanvulling op het Vir, dat betrekking heeft op de beveiliging van informatie in het algemeen. Bijzondere informatie maakt immers deel uit van de totale bij de overheid aanwezige informatie. Dit betekent dat bij de beveiliging van bijzondere informatie zowel de regels van het VIR als de regels van dit voorschrift gevolgd moeten worden.
Evenals het Vir geldt het Vir-bi voor de rijksdienst. Tot de rijksdienst behoren de ministeries met hun directoraten-generaal, centrale en stafdirecties, buitendiensten en intern verzelfstandigde dienstonderdelen. Anders gezegd: alle organisaties op rijksniveau waarvoor de ministeriële verantwoordelijkheid onverkort geldt.
Op zelfstandige bestuursorganen is het voorschrift niet automatisch van toepassing. Het blijft de verantwoordelijkheid van de individuele ministers om er zorg voor te dragen dat dit voorschrift op individuele zelfstandige bestuursorganen van overeenkomstige toepassing wordt verklaard indien er bij een individueel

zelfstandig bestuursorgaan sprake is van bijzondere informatie. Dit kan geschieden in de instellingswetgeving voor nieuw te creëren zelfstandige bestuursorganen of in een afzonderlijk informatiestatuut waarin afspraken worden vastgelegd tussen een zelfstandig bestuursorgaan en de minister.

Artikel 3. Buiten de rijksdienst brengen van bijzondere informatie
1. Indien het noodzakelijk is bijzondere informatie buiten de rijksdienst te brengen, anders dan op grond van een wettelijke openbaarmakingsverplichting, wordt dit niet gedaan dan nadat is vast gesteld dat voldoende waarborgen aanwezig zijn dat deze bijzondere informatie wordt beveiligd overeenkomstig de in dit voorschrift neergelegde regels door de persoon of instantie buiten de rijksdienst die de bijzondere informatie zal ontvangen.
2. Verstrekking van bijzondere informatie als bedoeld in het eerste lid, vindt niet eerder plaats dan nadat de secretaris-generaal dan wel een door hem daartoe aangewezen ambtenaar heeft vastgesteld dat de persoon of instantie aan wie onderscheidenlijk waaraan de bijzondere informatie wordt verstrekt deze informatie beveiligt overeenkomstig de exclusiviteitseisen die ingevolge dit besluit aan de beveiliging van de desbetreffende categorie bijzondere informatie worden gesteld.
3. Bijzondere informatie die krachtens een internationaal verdrag of een internationale overeenkomst is verkregen wordt uitsluitend na voorafgaande toestemming van het land of de internationale organisatie van herkomst doorgegeven aan een derde land of een andere organisatie.

Toelichting
De werking van dit voorschrift strekt zich niet verder uit dan tot de rijksdienst. Het kan echter noodzakelijk zijn bijzondere informatie ook buiten de rijksdienst te brengen. Dit kan bijvoorbeeld het geval zijn als opdrachten bij het bedrijfsleven worden geplaatst waarbij gerubriceerde informatie ter beschikking moet worden gesteld. Het voorschrift staat dit alleen toe als er voldoende zekerheid bestaat dat de informatie in overeenstemming met dit voorschrift wordt beveiligd. In de praktijk betekent dit dat er met organisaties die niet tot de rijksdienst behoren afspraken moeten worden gemaakt, waarbij de naleving van de in dit voorschrift vastgelegde beveiligingsregels wordt overeengekomen.
Het derde lid van deze bepaling bevat het 'derde-landen principe'. Dit principe houdt in dat bijzondere informatie van internationale herkomst niet wordt verstrekt zonder voorafgaande toestemming van het land of de internationale organisatie die de informatie hebben verstrekt. Het 'derde-landen principe' vormt een essentiële voorwaarde bij internationale samenwerking. De in het derde lid bedoelde toestemming voor het doorgegeven van bijzondere informatie kan voor bepaalde gevallen vooraf generiek worden verleend.

Artikel 4. Beveiliging van bijzondere informatie van internationale herkomst
Bijzondere informatie die krachtens een internationaal verdrag of overeenkomst is verkregen wordt beveiligd volgens dit voorschrift. Voor zover het verdrag of de overeenkomst afwijkende of verdergaande beveiligingsbepalingen bevat worden die afwijkende of verdergaande bepalingen toegepast.

B. Rubriceringen

Artikel 5. Rubriceringen en merkingen
1. Staatsgeheimen worden als volgt gerubriceerd:
a. Stg. ZEER GEHEIM
indien kennisnemen door niet gerechtigden zeer ernstige schade kan toebrengen aan het belang van de Staat of zijn bondgenoten;
b. Stg. GEHEIM
indien kennisnemen door niet gerechtigden ernstige schade kan toebrengen aan het belang van de Staat of zijn bondgenoten;
c. Stg. CONFIDENTIEEL
indien kennisnemen door niet gerechtigden schade kan toebrengen aan het belang van de Staat of zijn bondgenoten.
2. Bijzondere informatie die geen staatsgeheim is, wordt als volgt gerubriceerd:
Dep. VERTROUWELIJK
indien kennisnemen door niet gerechtigden nadeel kan toebrengen aan het belang van één of meer ministeries.
3. De rubricering kan worden aangevuld met een merking, die een bepaalde wijze van behandelen aangeeft.
4. Indien praktisch uitvoerbaar, worden rubriceringen, merkingen en de duur van de rubricering altijd duidelijk aangebracht.

Toelichting
Onder rubriceren wordt verstaan: het vaststellen en aangeven dat een gegeven bijzondere informatie is en het bepalen en aangeven van de mate van beveiliging die aan deze informatie moet worden gegeven.
Het rubriceren kan worden opgesplitst in een aantal stappen. In de eerste plaats moet worden vastgesteld of informatie als staatsgeheim of als niet-staatsgeheime bijzondere informatie moet worden beschouwd. Er is sprake van een staatsgeheim als het belang van de Staat of zijn bondgenoten in het geding is en indien kennisname door niet gerechtigden kan leiden tot schade aan deze belangen.
Er is sprake van niet-staatsgeheime bijzondere informatie indien kennisname door niet gerechtigden kan leiden tot nadeel aan het belang van één of meer ministeries. Indien bij de schending van de geheimhouding het nadeel aan het belang van één of meer ministeries zo ernstig is, dat sprake is van schade, zal er doorgaans sprake zijn van schade aan de belangen van de Staat of van zijn bondgenoten en dus van een staatsgeheim.
In de tweede plaats moet de rubricering worden vastgesteld. De rubricering zelf, dat wil zeggen de mate van beveiliging die aan informatie wordt gegeven, wordt bepaald door de mate van nadeel of schade die kan worden geleden indien een niet gerechtigde kennis neemt van de informatie.
Het schema, dat in bijlage 2 van dit voorschrift is opgenomen, verduidelijkt het voorgaande.
Gedeelten van of bijlagen bij informatie kunnen onderling verschillend worden gerubriceerd. Bij die gedeelten of op die bijlagen dient de desbetreffende rubricering afzonderlijk te worden vermeld. De informatie als geheel dient tenminste zo hoog te zijn gerubriceerd als het hoogst gerubriceerde gedeelte of de hoogst gerubriceerde bijlage.
Uitgangspunt bij het rubriceren zijn de in het beleidsdocument (zie artikel 13, tweede lid) opgenomen criteria voor het rubriceren.
De wijze waarop de rubricering op de informatie moet worden aangebracht staat vermeld in de Matrix exclusiviteitseisen, bijlage 3 van dit voorschrift.
Indien het niet praktisch uitvoerbaar is om de rubricering op de informatie aan te brengen, wordt de gebruiker van de informatie op de hoogte gesteld van de rubricering.
Middels een merking kan een specifieke beperking van de kring van gerechtigden worden aangegeven. Zo wordt bijvoorbeeld op het Ministerie van Defensie de merking 'NL/GE eyes only' gebruikt voor informatie die alleen met Duitsland mag worden uitgewisseld.

Artikel 6. Duur rubricering
1. Rubriceringen worden aan een tijdsverloop van maximaal tien jaar of aan een bepaalde gebeurtenis gebonden.
2. Van het eerste lid van deze bepaling kan worden afgeweken in die gevallen waarin de rubricering betrekking heeft op:
a. bijzondere informatie die krachtens een internationaal verdrag of overeenkomst is verkregen;
b. staatsgeheimen die door de wet als zodanig zijn aangewezen;
c. bijzondere informatie die een onderdeel vormt van een plan, systeem, project, enz. waarvoor een langdurige geheimhouding noodzakelijk is;
d. bijzondere informatie waarbij bronbescherming, modus operandi of, in het geval van inlichtingen- en veiligheidsdiensten, het actuele kennisniveau in het geding is.

3. Rubriceringen die op grond van het in het tweede lid gestelde zijn uitgezonderd, worden uiterlijk twintig jaar na vaststelling door de ambtenaar als bedoeld in artikel 8 onderzocht op de mogelijkheid om de rubricering te herzien of te beëindigen.

Toelichting
Beveiligingsmaatregelen brengen als regel extra werkzaamheden en daardoor extra kosten met zich mee. Onnodig beveiligen moet daarom worden vermeden. Om deze reden gaat het voorschrift er vanuit dat rubriceringen in beginsel tijdelijk zijn. De rubricering is gebonden aan een termijn van maximaal tien jaar of aan een bepaalde gebeurtenis; bij dit laatste moet bijvoorbeeld gedacht worden aan de afloop van onderhandelingen. Indien de rubricering is gebonden aan een bepaalde gebeurtenis moet dit op de informatiedrager zijn aangeven door degene die de inhoud van de informatie vaststelt.
Na een periode van maximaal tien jaar of nadat de bepaalde gebeurtenis heeft plaatsgevonden vervalt de rubricering automatisch.
Slechts in vier gevallen, genoemd in artikel 6, tweede lid, is het mogelijk van deze regel af te wijken:
1. De rubricering heeft betrekking op informatie die krachtens een internationaal verdrag of een internationale overeenkomst is verkregen. In dit geval blijft de rubriceringsduur van kracht die wordt gehanteerd door het land of door de organisatie waarvan de informatie oorspronkelijk afkomstig is.
2. Het betreft staatsgeheimen die door de wet als zodanig zijn aangewezen (bijvoorbeeld de Kernenergiewet en het Geheimhoudingsbesluit Kernenergiewet, KB 17 juni 1971).
3. De bijzondere informatie maakt onderdeel uit van een plan, systeem, project, enz. waarvoor de termijn van tien jaar in verband met de levensduur hiervan te kort is.
4. Een langere rubriceringsduur is noodzakelijk vanuit het oogpunt van bronbescherming of bescherming van modus operandi. Bij inlichtingen- en veiligheidsdiensten kan een langere rubriceringsduur noodzakelijk zijn om te voorkomen dat zicht wordt gegeven op het actuele kennisniveau.
Om te voorkomen dat ook in deze gevallen langer wordt beveiligd dan noodzakelijk is, bepaalt het derde lid van dit artikel dat deze informatie moet worden geherrubriceerd of gederubriceerd wanneer de overwegingen waarop de rubricering werd aangebracht, niet meer in dezelfde mate of in het geheel niet meer gelden. Uiterlijk twintig jaar nadat de rubricering is vastgesteld, dient de informatie hierop onderzocht te worden.
De rubricering en de duur van de rubricering moeten altijd duidelijk zijn aangebracht, zie artikel 5, vierde lid van dit voorschrift.

Artikel 7. Rubriceringsfunctie
1. De opsteller van de informatie doet een voorstel tot rubricering en brengt deze aan op de informatie.
2. De rubricering wordt vastgesteld door degene die de inhoud van de informatie vaststelt.

Toelichting
De rubricering van informatie wordt in eerste instantie gegeven door de opsteller ervan. De verantwoordelijkheid voor de vaststelling van de rubricering berust bij degene die de inhoud van de informatie vaststelt. In geval van twijfel kan deze zich wenden tot de BVA. De BVA oefent toezicht uit op het rubriceren. Dit vloeit voort uit zijn toezichthoudende taak die omschreven is in artikel 14 van dit voorschrift.

Artikel 8. Herzien en beëindigen van rubriceringen
Uitsluitend degene die de rubricering heeft vastgesteld, degene die hem in zijn functie is opgevolgd, dan wel een daartoe door of namens de secretaris-generaal aangewezen ambtenaar is bevoegd de rubricering te herzien of te beëindigen.

Toelichting
Herrubricering of derubricering kan, behoudens de uitzondering van artikel 10, derde lid, alleen geschieden door de volgende personen:
– degene die de inhoud van de informatie heeft vastgesteld;
– zijn ambtsopvolger;
– een door of namens de secretaris-generaal daartoe aangewezen ambtenaar.
Dit laatste geval kan zich bijvoorbeeld voordoen als de functie van degene die de inhoud van de informatie heeft vastgesteld is komen te vervallen.
Indien de rubricering wordt herzien of beëindigd moet de rubricering verwijderd worden. In het geval dat de rubricering wordt herzien, wordt de nieuwe rubricering in de onmiddellijke nabijheid of op de plaats van de oude rubricering aangebracht.
De daartoe bevoegde ambtenaar draagt er, voorzover mogelijk, tevens zorg voor dat aan de ontvangers van de informatie wordt meegedeeld dat de informatie geherrubriceerd c.q. gederubriceerd is indien wordt afgeweken van de standaardtermijn of de bepaalde gebeurtenis als bedoeld in artikel 6, eerste lid, dan wel de termijn die ingevolge artikel 6, tweede lid is vastgesteld.

Artikel 9. Rubriceringen vastgesteld vóór het inwerkingtreden van dit voorschrift
Rubriceringen die zijn vastgesteld vóór het inwerkingtreden van dit voorschrift worden uiterlijk twintig jaar na vaststelling door de ambtenaar als bedoeld in artikel 8 onderzocht op de mogelijkheid om de rubricering te herzien of te beëindigen.

Toelichting
Deze bepaling moet voorkomen dat informatie langer wordt beveiligd dan noodzakelijk is.

Artikel 10. Rubriceringen in het geval van overbrenging naar een archiefbewaarplaats
1. Bij overbrenging van bijzondere informatie naar een archiefbewaarplaats als bedoeld in de Archiefwet 1995 vervallen de daarop aangebrachte rubriceringen.
2. Indien daartoe aanleiding bestaat, wordt door het overbrengende ministerie de rubricering opnieuw vastgesteld nadat advies is ingewonnen van de beheerder van de archiefbewaarplaats. Hierbij wordt op de informatie aangegeven: 'Deze rubricering is aangebracht bij de overbrenging naar een archiefbewaarplaats'.
Het bepalen van nieuwe rubriceringen vindt mede plaats aan de hand van inventarislijsten, die ingevolge artikel 9, derde lid, van het Archiefbesluit 1995 worden vastgesteld. De inventarislijsten bevatten daartoe informatie over de oorspronkelijk aangebrachte rubriceringen.
3. Indien de oorspronkelijke rubricering werd vastgesteld door een ander ministerie dan het overbrengende ministerie, dan wel door een internationale organisatie of een buitenlandse mogendheid, wordt daaraan advies gevraagd.
4. De bij de overbrenging aangebrachte rubriceringen worden aan een bepaald tijdsverloop gebonden.

Toelichting
Ingevolge de Archiefwet 1995 moeten archiefbescheiden die niet voor vernietiging in aanmerking komen en die ouder zijn dan twintig jaar naar een archiefbewaarplaats worden overgebracht. Bij de over te brengen bescheiden kan zich informatie bevinden die gerubriceerd is. Veel van die rubriceringen zijn na verloop van twintig jaar niet meer juist. Om praktische redenen is daarom bepaald dat bij de overbrenging naar een archiefbewaarplaats in beginsel alle eerder aangebrachte rubriceringen vervallen. Indien daartoe aanleiding bestaat, wordt door het overbrengende ministerie de rubricering opnieuw vastgesteld; uit artikel 15 Archiefwet 1995 volgt dat bij bijzondere informatie slechts beperkingen mogen worden gesteld aan de openbaarheid met het oog op de eerbiediging van de persoonlijke levenssfeer, het belang van de Staat of zijn bondgenoten of het anders-

zins voorkomen van onevenredige bevoordeling of benadeling van betrokken natuurlijke personen of rechtspersonen dan wel van derden. Bovendien mag deze beperking slechts gelden voor een bepaalde termijn. Het bepalen van nieuwe rubriceringen vindt mede plaats aan de hand van inventarislijsten die ingevolge artikel 9, derde lid, van het Archiefbesluit 1995 worden vastgesteld.
Indien informatie door het overbrengende ministerie werd ontvangen van een ander ministerie, van een internationale organisatie of van een buitenlandse mogendheid, vindt daarmee overleg plaats over de vraag of er nog steeds sprake is van bijzondere informatie. Bij materiaal dat afkomstig is van een ander ministerie beslist hierover uiteindelijk het overbrengende ministerie indien hierover binnen een overeen te komen termijn geen advies is ontvangen. Bij materiaal van niet-Nederlandse herkomst is het advies van de internationale organisatie of de buitenlandse mogendheid beslissend. Indien niet expliciet toestemming wordt verkregen voor beëindiging of herziening blijft de oorspronkelijke rubricering van kracht. De bij de overbrenging vastgestelde rubriceringen zijn altijd tijdelijk. Dit geldt dus ook voor rubriceringen op informatie van niet-Nederlandse herkomst. Om verwarring met de vervallen rubriceringen te voorkomen, worden de bij de overbrenging vastgestelde rubriceringen duidelijk als zodanig herkenbaar aangebracht.

Artikel 11. Rubricering van bijzondere informatie van internationale herkomst
Bijzondere informatie die krachtens een internationaal verdrag of overeenkomst is verkregen, behoudt de aan die informatie toegekende rubricering en wordt beveiligd volgens het overeenkomstige nationale beveiligingsniveau.

Toelichting
Bijzondere informatie van internationale herkomst houdt de oorspronkelijk toegekende rubricering. Indien er geen overeenkomstige Nederlandse rubricering is, moet gezocht worden naar een Nederlandse rubricering die qua beveiligingsniveau zo veel mogelijk overeenkomt met de rubricering van het land c.q. de organisatie van herkomst.
In bijlage 1 van dit voorschrift is een transponeringstabel opgenomen die het Nederlandse equivalent geeft van de internationale rubriceringen.

C. Exclusiviteitseisen

Artikel 12. Eisen met betrekking tot de bescherming van de exclusiviteit
1. Bijzondere informatie wordt zodanig beveiligd dat alleen personen die daartoe zijn gerechtigd bijzondere informatie kunnen behandelen of inzien voorzover dit noodzakelijk is voor een goede uitoefening van hun taak en dat inbreuken op de beveiliging worden gedetecteerd en gedegen onderzoek naar (mogelijke) inbreuken mogelijk is.
2. De uitwerking van de in het eerste lid vermelde exclusiviteitseisen staat vermeld in bijlage 3 behorend bij dit voorschrift. De Minister van Binnenlandse Zaken en Koninkrijksrelaties kan na advies van het BIB-beraad of zijn rechtsopvolger, deze bijlage aanpassen.
3. Van de in het tweede lid bedoelde uitwerking van de exclusiviteitseisen mag uitsluitend worden afgeweken indien:
a. dit in een bepaald geval noodzakelijk is; en
b. de secretaris-generaal schriftelijk toestemming heeft verleend en de afwijking en de noodzaak daartoe schriftelijk worden vastgelegd.
Indien het de beveiliging van een staatsgeheim betreft is tevens voorafgaand overleg vereist met het hoofd van de Algemene Inlichtingen- en Veiligheidsdienst, dan wel de Beveiligingsautoriteit indien het de beveiliging betreft van een bij het Ministerie van Defensie berustend staatsgeheim.

Toelichting
Alleen personen die daartoe zijn gerechtigd, mogen bijzondere informatie behandelen of inzien, voorzover dat noodzakelijk is voor een goede uitoefening van hun taak. Gerechtigd om kennis te nemen zijn personen met een ‘need to know’, dat wil zeggen dat voor de betrokkene toegang tot de bijzondere informatie noodzakelijk is om een uit zijn functie voortvloeiende taak te kunnen vervullen. Bovendien is bij kennisname van staatsgeheimen een verklaring van geen bezwaar op grond van de Wvo vereist.
Het Vir stelt geen concrete eisen aan de beveiliging van informatie maar biedt een methodiek om langs de weg van de afhankelijkheidsanalyse tot betrouwbaarheidseisen te komen. In het Vir wordt onder betrouwbaarheid verstaan de mate waarin de organisatie zich kan verlaten op een informatiesysteem voor zijn informatievoorziening. De hieraan te stellen eisen – betrouwbaarheidseisen – kunnen worden onderverdeeld in eisen ten aanzien van de exclusiviteit, de integriteit en beschikbaarheid. Artikel 12 van het Vir-bi geeft eisen met betrekking tot de bescherming van de exclusiviteit van de informatie. Bijzondere informatie heeft immers als kenmerk dat de gevolgen voor de Staat, zijn bondgenoten of de diverse ministeries bij onbevoegde kennisname veel ernstiger kunnen zijn dan bij onbevoegde kennisname van informatie, waarop uitsluitend het VIR van toepassing is, het geval is. Voor zover dat noodzakelijk is om de exclusiviteit te waarborgen zijn eisen met betrekking tot integriteit meegenomen. Omdat overigens geen bijzondere eisen hoeven te gelden voor de integriteit en beschikbaarheid van bijzondere informatie, kan met de afhankelijkheids- en kwetsbaarheidsanalyse conform het Vir worden volstaan.
In verband met de steeds voortschrijdende techniek is er voor gekozen om in het nieuwe voorschrift geen techniek-afhankelijke beveiligingsmaatregelen voor te schrijven, maar beveiligingseisen. Techniek-afhankelijke beveiligingsmaatregelen zijn immers tijdgebonden.
De uitwerking van de in het eerste lid van artikel 12 genoemde eisen is opgenomen in bijlage 3 van dit voorschrift. De Minister van Binnenlandse Zaken en Koninkrijksrelaties kan op basis van een daartoe door het BIB-beraad of zijn rechtsopvolger verstrekt advies, deze bijlage wijzigen. Op deze wijze kan in de toekomst snel worden ingespeeld op nieuwe ontwikkelingen zonder dat het voorschrift zelf behoeft te worden gewijzigd.
Volgens de opzet van bijlage 3 hoort bij ieder rubriceringsniveau een aparte set exclusiviteitseisen. In beginsel is het niet toegestaan van de in de bijlage voorgeschreven exclusiviteitseisen af te wijken. Volgens het derde lid van artikel 12 is afwijking alleen mogelijk indien dat in een specifieke situatie noodzakelijk is. Zo kan het bijvoorbeeld voorkomen dat bepaalde exclusiviteitseisen in een bepaalde situatie c.q. omgeving niet adequaat blijken te zijn in verband met een specifieke dreiging. Ook kan er sprake zijn van een tijdelijk afwijkende situatie in het geval van een verbouwing. In deze gevallen moet de secretaris-generaal schriftelijk toestemming verlenen en moet schriftelijk worden vastgelegd aan welke voorgeschreven exclusiviteitseis niet wordt voldaan en waarom de afwijking in dit geval noodzakelijk is. Bij staatsgeheimen is bovendien voorafgaand overleg met het hoofd van de Algemene Inlichtingen- en Veiligheidsdienst vereist. Indien het de beveiliging betreft van staatsgeheimen die bij het Ministerie van Defensie berusten is voorafgaand overleg met de Beveiligingsautoriteit vereist. Uiteraard blijft ook in deze gevallen de eindverantwoordelijkheid voor de beveiliging van een ministerie bij de secretaris-generaal berusten (zie artikel 1 van het Beveiligingsvoorschrift I 1949).
Uiteraard zal in overmachtssituaties de schriftelijke toestemming achteraf door de secretaris-generaal kunnen worden verleend; bij staatsgeheimen kan in dergelijke gevallen het overleg met het hoofd van de Algemene Inlichtingen- en Veiligheidsdienst c.q. de Beveiligingsautoriteit in een later stadium plaatsvinden.

D. Organisatie

Artikel 13. Secretaris-generaal

1. De secretaris-generaal is belast met de algemene zorg voor de beveiliging van bijzondere informatie en oefent toezicht uit op de implementatie van het beleid ter zake.
2. Bij het vaststellen van het informatiebeveiligingsbeleid als bedoeld in artikel 3 Vir draagt de secretaris-generaal er zorg voor dat het beleidsdocument tevens omvat:
a. de uitwerking van de uitgangspunten voor het rubriceren binnen het ministerie;
b. de wijze waarop de secretaris-generaal vooraf toestemming verleent voor het verwerken van staatsgeheimen in informatiesystemen;
c. de wijze waarop het informatiebeveiligingsbeleid voor wat betreft bijzondere informatie iedere twee jaar wordt geëvalueerd door een onafhankelijke deskundige;
d. de wijze waarop personeelsleden, die werkzaamheden verrichten waarbij kennis wordt genomen van bijzondere informatie, op de hoogte worden gebracht van de voor hen geldende beveiligingsrichtlijnen;
e. de wijze waarop de lijnmanager rapporteert over de beveiliging van bijzondere informatie die valt onder zijn verantwoordelijkheid;
f. de uitgangspunten voor de noodvernietiging van bijzondere informatie.
3. De onderdelen van het beveiligingsbeleid die betrekking hebben op de beveiliging van staatsgeheimen worden door de secretaris-generaal vastgesteld in overleg met het hoofd van de Algemene Inlichtingen- en Veiligheidsdienst. Bij het Ministerie van Defensie vindt het overleg plaats met de Beveiligingsautoriteit.

Toelichting

De aanhef van artikel 3 van het Vir luidt: 'De secretaris-generaal van een departement stelt het informatiebeveiligingsbeleid vast in een beleidsdocument en draagt dit beleid uit'.
Artikel 13 van dit voorschrift sluit hierop aan door te bepalen dat de algemene zorg voor de beveiliging van bijzondere informatie binnen een ministerie bij de secretaris-generaal berust. De beveiliging van zowel algemene als bijzondere informatie moet worden gezien als een deel van de taak van de secretaris-generaal voor het goed doen functioneren van het ministerie en de daaronder ressorterende diensten.
Artikel 3 van het Vir omschrijft de minimale inhoud van het beleidsdocument. Artikel 13 stelt aanvullende eisen aan dit beleidsdocument waar het de beveiliging van bijzondere informatie betreft. Hiermee wordt bereikt dat de uitgangspunten voor de beveiliging van algemene en bijzondere informatie worden vastgelegd in één geïntegreerd beleidsdocument.
Voor de beveiliging van bijzondere informatie moet in het beleidsdocument worden vastgelegd welke soorten bijzondere informatie er zijn op een ministerie, wat de daarbij behorende rubricering is en wie de rubricering definitief vaststelt. Het schema dat is opgenomen in bijlage 2 van dit voorschrift, bevat voorbeelden van de soorten van informatie en het daarbij behorende rubriceringsniveau en kan als richtsnoer dienen bij het opstellen van de uitgangspunten voor het rubriceren.
Voorts moet ook de interne procedure worden vastgelegd volgens welke de secretaris-generaal toestemming verleent voor het verwerken van staatsgeheimen in een informatiesysteem.
De onafhankelijke deskundige, als bedoeld in artikel 13 tweede lid onder c, beoordeelt in hoeverre de beveiliging van bijzondere informatie in overeenstemming is met de eisen van dit voorschrift en beoordeelt de motivering in het geval de lijnmanager het noodzakelijk vindt om van een voorgeschreven maatregel af te wijken (zie artikel 12, derde lid van dit voorschrift). De functie van onafhankelijk deskundige kan bijvoorbeeld worden vervuld door een EDP-auditor of de Algemene Inlichtingen- en Veiligheidsdienst.
Het vereiste van artikel 13, tweede lid onder d kan bijvoorbeeld ingevuld worden door te bepalen dat de BVA in het kader van het aanstellingsgesprek de betrokkene op de hoogte stelt van zijn verplichtingen met betrekking tot de omgang met bijzondere informatie.
Tevens moet vastgelegd worden dat de beveiligingsinstructie na een bepaalde tijd wordt herhaald en dat daarbij aandacht wordt geschonken aan de persoonlijke omstandigheden van de betrokkene die voor de beveiliging van bijzondere informatie van belang kunnen zijn.
Verder moet in het beleidsdocument worden opgenomen dat iedere lijnmanager aan de secretaris-generaal rapporteert over de beveiliging van de bijzondere informatie die in zijn bezit is. Deze rapportage kan plaatsvinden door tussenkomst van de BVA. Deze rapportage zal in ieder geval moeten plaatsvinden bij ingebruikname van een informatiesysteem dat bijzondere informatie bevat en bij wijziging van dat systeem.
Tenslotte moet het beleidsdocument de uitgangspunten voor de noodvernietiging van bijzondere informatie bevatten. Deze uitgangspunten worden bepaald door de plaatselijke omstandigheden. Zij vormen de basis voor voorzieningen die in de calamiteitenparagraaf van het informatiebeveiligingsplan als bedoeld in artikel 4 onder e van het Vir moeten worden opgenomen.
In artikel 13 derde lid wordt bepaald dat onderdelen van het beveiligingsbeleid, die betrekking hebben op de beveiliging van staatsgeheimen, door de secretaris-generaal worden vastgesteld in overleg met het hoofd van de Algemene Inlichtingen- en Veiligheidsdienst. Overleg met de Algemene Inlichtingen- en Veiligheidsdienst is in dit geval al vereist in het kader van de Wet veiligheidsonderzoeken, waar het betreft de aanwijzing en vervulling van vertrouwensfuncties.
Bij het Ministerie van Defensie worden onderdelen van het beveiligingsbeleid, die betrekking hebben op de beveiliging van staatsgeheimen, vastgesteld in overleg met de Beveiligingsautoriteit.

Artikel 14. Beveiligingsambtenaar

1. De BVA ondersteunt de secretaris-generaal bij zijn taken als genoemd in artikel 13.
2. De BVA adviseert de lijnmanager bij zijn taak als genoemd in artikel 15.
3. De BVA oefent toezicht uit op de deugdelijkheid van de beveiliging van de bijzondere informatie. Hij voert regelmatig een inspectie uit en rapporteert zijn bevindingen aan de secretaris-generaal.
4. Voordat in een informatiesysteem bijzondere informatie wordt verwerkt stelt de BVA vast of het stelsel van beveiligingsmaatregelen toereikend is en rapporteert hierover aan de secretaris-generaal.

Toelichting

Het beveiligingsvoorschrift I, 1949, beschrijft de rol en de verantwoordelijkheden van de secretaris-generaal en de BVA ten aanzien van de beveiliging in het algemeen en beperkt zich niet tot de beveiliging van staatsgeheimen en overige bijzondere informatie. Hierdoor was herziening van het Beveiligingsvoorschrift I, 1949 in het kader van een voorschrift dat uitsluitend handelt over de beveiliging van bijzondere informatie niet mogelijk. Op veel ministeries is inmiddels een 'centrale beveiligingsfunctie' ingesteld, die belast is met de ontwikkeling en het onderhoud van het departementale beveiligingsbeleid. Het is duidelijk dat hierdoor de BVA-functie beter tot zijn recht komt.
In de opzet van dit voorschrift ondersteunt de BVA de secretaris-generaal bij zijn taken op het gebied van de beveiliging van bijzondere informatie als genoemd in artikel 13. Dit betekent dat de BVA belast kan worden met aspecten van de beveiliging van bijzondere informatie die centraal binnen een ministerie moeten worden geregeld, zoals bijvoorbeeld personele beveiliging, fysieke beveiliging en incidentafhandeling.
De rol van de BVA is zowel adviserend als toezichthoudend.
De BVA adviseert de secretaris-generaal en de lijnmanager met betrekking tot de implementatie van het voorschrift. De lijnmanager is volgens artikel 15 belast

met de dagelijkse zorg voor de beveiliging van informatiesystemen, die bijzondere informatie bevatten.
Daarnaast oefent de BVA namens de secretaris-generaal toezicht uit op een juiste implementatie van het voorschrift. Voor de ingebruikname van een informatiesysteem controleert hij of de beveiligingsmaatregelen in overeenstemming met dit voorschrift zijn geïmplementeerd. De BVA kan zich hierbij uiteraard laten adviseren door specifieke deskundigen, bijvoorbeeld op het gebied van ICT en fysieke beveiliging. Ook dan draagt de BVA de verantwoordelijkheid voor het toezicht.
Wanneer een lijnmanager in overeenstemming met artikel 12, derde lid, van oordeel is dat van een voorgeschreven maatregel moet worden afgeweken is het aan de BVA de hieraan ten grondslag liggende motivering te beoordelen; de BVA moet er op toezien dat in dat geval toch aan de exclusiviteitseisen van het voorschrift wordt voldaan.
Tenslotte moet de BVA op grond van artikel 17 het onderzoek naar aanleiding van meldingen van mogelijke compromittering van bijzondere informatie initiëren.

Artikel 15. Lijnmanager
De lijnmanager draagt er zorg voor dat de implementatie van de beveiligingsmaatregelen voor een onder zijn verantwoordelijkheid vallend informatiesysteem of verantwoordelijkheidsgebied minimaal in overeenstemming is met de exclusiviteitseisen van artikel 12 en de daaruit voortvloeiende maatregelen.

Toelichting
Volgens artikel 4 Vir is voor elk informatiesysteem de verantwoordelijkheid voor de informatiebeveiliging toegewezen aan een lijnmanager. Dit vloeit voort uit het principe van integraal management dat inhoudt dat de lijnmanager verantwoordelijk is voor personeel, financiën en informatie op zijn werkterrein. De lijnmanager beschikt over de situationele gegevens om de juiste afweging te kunnen maken over de toereikendheid van de door hem te treffen maatregelen.
Het voorschrift sluit hierbij aan door de lijnmanager verantwoordelijk te laten zijn voor de beveiliging van de bijzondere informatie binnen zijn taakveld.

Artikel 16. Minister van Binnenlandse Zaken en Koninkrijksrelaties
1. De Minister van Binnenlandse Zaken en Koninkrijksrelaties rapporteert eens in de twee jaar aan de ministerraad over de beveiliging van bijzondere informatie binnen de rijksdienst.
2. De Minister van Binnenlandse Zaken en Koninkrijksrelaties kan met instemming van de betrokken minister bij een ministerie onderzoek verrichten naar de beveiliging van staatsgeheimen. Bij het Ministerie van Defensie kan dit onderzoek worden verricht door de Militaire Inlichtingen- en Veiligheidsdienst.
3. De minister verstrekt desgevraagd informatie en verleent medewerking aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties ten behoeve van diens taken zoals genoemd in dit artikel.

Toelichting
Deze bepaling is opgenomen om rijksbreed een goed en consistent niveau te bevorderen van beveiliging van bijzondere informatie in het algemeen en van staatsgeheimen in het bijzonder. De taken van de Minister van Binnenlandse Zaken en Koninkrijksrelaties vloeien wat staatsgeheimen betreft voort uit zijn verantwoordelijkheid voor de taak van de onder hem ressorterende Algemene Inlichtingen- en Veiligheidsdienst om de beveiliging van staatsgeheimen te bevorderen (artikel 6, derde lid onder c Wiv); voor de overige bijzondere informatie wordt hierbij om praktische redenen aangesloten. Voor de Militaire Inlichtingen- en Veiligheidsdienst vloeit deze taak voort uit artikel 7, tweede lid onder d Wiv.
De in het eerste lid bedoelde rapportage van de Minister van Binnenlandse Zaken en Koninkrijksrelaties aan de ministerraad heeft ook betrekking op het Ministerie van Defensie en zal naar verwachting in ieder geval de aspecten omvatten:
– incidenten die zich hebben voorgedaan bij de beveiliging van bijzondere informatie en eventuele trends die daarbij zijn waar te nemen;
– ervaringen met de implementatie van het voorschrift en suggesties voor de oplossing van eventuele meer algemene problemen. Bij dit laatste kan onder meer worden gedacht aan de hoeveelheid bijzondere informatie die binnen een ministerie omgaat en eventuele trends die daarbij zijn waar te nemen.
Voor deze rapportage kan onder meer gebruik worden gemaakt van de gegevens afkomstig uit de evaluatie als bedoeld in artikel 13, tweede lid onder c.

E. Compromittering

Artikel 17. Compromittering van bijzondere informatie
1. Elke ambtenaar is verplicht de BVA onverwijld mededeling te doen van een inbreuk op de beveiliging die redelijkerwijs kan leiden, dan wel vermoedelijk of vaststaand heeft geleid, tot compromittering van bijzondere informatie.
2. De BVA treft, nadat hij op de hoogte is gebracht van een inbreuk op de beveiliging, onverwijld maatregelen om de beveiliging te herstellen en herhaling te voorkomen.
De BVA stelt vast of compromittering van bijzondere informatie heeft plaatsgevonden; indien dit het geval is doet hij hiervan mededeling aan de secretaris-generaal.
3. Gevallen waarbij uitsluitend 'Dep. Vertrouwelijk' gerubriceerde informatie is betrokken, behoeven slechts door de BVA aan de secretaris-generaal te worden gemeld indien sprake is van verdachte omstandigheden.
Indien de compromittering betrekking heeft op krachtens internationaal verdrag of overeenkomst verkregen bijzondere informatie, doet de BVA bovendien mededeling aan de krachtens het verdrag of de overeenkomst voor de beveiliging van die bijzondere informatie verantwoordelijke instantie.

Artikel 18. Commissie van onderzoek
1. De secretaris-generaal stelt nadat hij op de hoogte is gebracht van de compromittering van een staatsgeheim onverwijld een commissie van onderzoek in. Deze commissie bestaat uit 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 die op de compromittering betrekking heeft en de bij de compromittering betrokken ambtenaren, alsmede de ambtenaar die de rubricering heeft vastgesteld, te horen.
2. De commissie stelt een onderzoek in naar:
– de wijze waarop de compromittering heeft plaatsgevonden;
– de aard en de omvang van de schade aan de belangen van de Staat of zijn bondgenoten;
– de te nemen maatregelen om de schade te beperken en herhaling te voorkomen.
3. De commissie voert, indien het gecompromitteerde staatsgeheim afkomstig is van een ander ministerie of van een interdepartementale commissie, haar onderzoek uit in overleg met de BVA van dat ministerie of de voorzitter van die commissie. In het geval dat het gecompromitteerde staatsgeheim krachtens een internationaal verdrag of overeenkomst is verkregen voert de commissie haar onderzoek uit in samenwerking met de instantie die krachtens het verdrag of de overeenkomst verantwoordelijk is voor de beveiliging van het staatsgeheim. Indien geen redelijke verklaring voor de compromittering wordt gevonden of indien spionage wordt vermoed, kan de Algemene Inlichtingen- en Veiligheidsdienst de commissie bij haar onderzoek terzijde staan.
4. De secretaris-generaal of een door hem aangewezen ambtenaar treft, nadat de commissie van onderzoek haar werkzaamheden heeft voltooid, maatregelen om de schade die de compromittering heeft toegebracht aan de veiligheid of andere gewichtige belangen van de Staat of 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. Bij het Ministerie van Defensie wordt de Militaire Inlichtingen- en Veiligheidsdienst op de hoogte gesteld van de uitkomsten van het onderzoek.

F. Slotbepaling

Artikel 19. Slotbepaling
1. Ingetrokken worden: de Aanwijzingen voor de beveiliging van staatsgeheimen en vitale onderdelen bij de Rijksdienst van 20 januari 1989.
2. Dit besluit en de daarbij behorende bijlagen treden in werking met ingang van 1 maart 2004, met uitzondering van bijlage 3, onderdeel VII, Goedkeuring van systeemcomponenten, dat in werking treedt op 1 maart 2008.
3. Dit besluit wordt aangehaald als: Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie.

Toelichting
Het Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie treedt op 1 maart 2004 in werking. Om te voorkomen dat ICT-voorzieningen op grond van dit voorschrift voortijdig moeten worden vervangen, geldt de verplichting om uitsluitend door de Minister van Binnenlandse Zaken en Koninkrijksrelaties goedgekeurde ICT-beveiligingsproducten te gebruiken pas vanaf 1 maart 2008.

Dit besluit zal met de toelichting in de Staatscourant worden geplaatst.
Van de terinzagelegging van de bij dit besluit behorende bijlagen zal mededeling worden gedaan in de Staatscourant.

De Minister-President, Minister van Algemene Zaken,
J.P. Balkenende.

Bijlage 1. Transponeringstabel internationale rubriceringen

Vergelijking van de nationale beveiligingsrubriceringen

Nederland	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
EU-rubricering	Trés Secret UE/EU TOP Secret	Secret UE	Confidentiel UE	Restreint UE
NAVO-rubricering	Cosmic Top Secret	Nato Secret	Nato Confidential	Nato Restricted
WEU-rubricering	Focal Top Secret	WEU Secret	WEU Confidential	WEU Restricted
Duitsland	Streng Geheim	Geheim	VS - Vertraulich	VS-Nur für den Dienstgebrauch
Oostenrijk	Streng Geheim	Geheim	Vertraulich	Eingschränkt
België	Très Secret	Secret	Confidentiel	Diffusion restreinte
	Zeer Geheim	Geheim	Vertrouwelijk	Beperkte Verspreiding
Denemarken	Yderst hemmeligt	Hemmeligt	Fortroligt	Til Tjenestebrug
Finland		Erittäin salainen	Salainen	Luottamuksellinen
Frankrijk	Très Secret Défense	Secret Défense	Confidentiel Défense	Diffusion restreinte
Griekenland	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένηςχρήσης
Hongarije	Szigoruan Titkos	Titkos		
Ierland	Top Secret	Secret	Confidential	Restricted
Italië	Segretissimo	Segreto	Riservatissimo	Riservato
Luxemburg	Très Secret	Secret	Confidentiel	Diffusion restreinte
Polen	Tajne Specjalnego	Tajne	Oufne	Do Vzytku Skuzbowego
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Spanje	Secreto	Reservado	Confidencial	Difusion Limitada
Tsjechische Republiek	Prisne Tavne	Tavne	Duverne	Til Tjenetebrug
Verenigd Koninkrijk	Top Secret	Secret	Confidential	Restricted
Verenigde Staten	Top Secret	Secret	Confidential	For official use only
Zweden	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig

Bijlage 2. Schema voorbeelden van rubriceringen

	Gegevens met betrekking tot het Koninklijk Huis	Gegevens met betrekking tot de krijgsmacht	Gegevens met betrekking tot de I&V-diensten	Openbare orde	Vertrouwelijke gegevens van derden onder berusting van de Rijksdienst	Non-proliferatie	Internationale betrekkingen	Economische/ Financiële schade	Gegevens m.b.t onderzoek zware criminaliteit	Gegevens met betrekking tot de beveiliging	Onderhandelingen	Gegevens m.b.t. de ministerraad
							Compromittering kan leiden tot:					
Stg. ZEER GEHEIM	Aantasting van de eenheid van de Kroon	Buitengewoon ernstige aantasting van de slagkracht of de veiligheid van de strijdkrachten	Zeer ernstige schade aan de effectiviteit van de I&V-diensten	Directe aantasting van de interne stabiliteit			Buitengewoon ernstige schade in de relatie met bevriende landen	Zeer langdurige schade aan de economie	Zeer ernstige schade aan belangen van informanten			Notulen ministerraad
Stg. GEHEIM	Kwetsbare gegevens met betrekking tot het Koninklijk Huis	Ernstige aantasting van de slagkracht of de veiligheid van de strijdkrachten	Ernstige schade aan de effectiviteit van de I&V-diensten (i.v.m. bronbescherming)	Ernstige en grootschalige aantasting van de openbare orde		Proliferatierisico met betrekking tot kernenergie/ NBC-wapens	Toename van internationale spanningen Verstoring van de relaties met bevriende landen	Wezenlijke materiele schade aan de financiële monetaire, economische en handelsbelangen	Schade toebrengen aan de opsporing van, en de opsporingsmethodieken inzake ernstige inbreuken op de rechtsorde			
Stg. CONFIDENTIEEL	Gegevens met betrekking tot reizen van het Koninklijk Huis	Schadelijke gevolgen voor de slagkracht of de veiligheid van de strijdkrachten .	Schade aan de effectiviteit van de I&V-diensten			Proliferatierisico (overig)	Schade aan diplomatieke relaties (formeel protest)	Schadelijke gevolgen voor de financiële economische en commerciële belangen van de Staat	Schadelijke gevolgen voor het onderzoek naar de zware misdaad	Schadelijke gevolgen voor de effectiviteit van beveiligingsplannen van vitale objecten	Schadelijke gevolgen voor internationale onderhandelingen	Besluitenlijst ministerraad persoonlijke zaken met betrekking tot bewindslieden
Dep. VERTROUWELIJK	–	Nadelige gevolgen voor de slagkracht of de veiligheid van de strijdkrachten			Verstrekking is in strijd met afspraak met derden om de vertrouwelijkheid te waarborgen		Nadelige gevolgen voor de diplomatieke relaties	Ongerecht vaardigde verrijking of voordeel voor natuurlijke personen of bedrijven		Nadelige gevolgen voor de effectiviteit van beveiligingsplannen van vitale objecten	Nadelige gevolgen voor onderhandelingen	

Opmerking: cryptosleutels dragen de rubricering van de informatie waarop zij betrekking hebben.

Bijlage 3. Matrix exclusiviteitseisen

Toelichting

1. Het Voorschrift informatiebeveiliging rijksdienst bijzondere informatie (Vir-bi) deelt in artikel 5 bijzondere informatie in vier categorieën in. Bij iedere categorie behoort een verdere uitwerking van de eisen met betrekking tot de bescherming van de exclusiviteit, die in artikel 12 van het Voorschrift zijn gegeven. Onder exclusiviteit wordt verstaan de mate waarin de toegang tot en kennisname van informatie is beperkt tot een gedefinieerde groep van gerechtigden.

De in de matrix opgenomen eisen zijn in de eerste plaats gericht op het voorkomen dat niet gerechtigden bijzondere informatie kunnen behandelen of inzien of voorzover dit noodzakelijk is voor een goede uitvoering van hun taak en dat inbreuken op de beveiloging worden gedetecteerd en gedegen onderzoek naar (mogelijke) inbreuken mogelijk is.

Als een dreiging manifest wordt, is het belangrijk dat er maatregelen zijn getroffen om deze te kunnen detecteren en om zonodig te kunnen interveniëren. De tijd waarbinnen deze detectie en eventuele interventie moeten plaatsvinden is afhankelijk van de kwetsbaarheid van de informatie zoals dat blijkt uit de aan de informatie toegekende rubricering. Ook hieraan worden in de matrix eisen gesteld:

a. de beveiliging van staatsgeheimen moet zodanig ingericht zijn dat inbreuken op de beveiliging en pogingen daartoe worden gedetecteerd en dat interventie kan plaatsvinden;

b. de beveiliging van 'Dep. VERTROUWELIJK' moet zodanig zijn ingericht dat inbreuken op de beveiliging zoveel mogelijk worden gedetecteerd.

De in de matrix opgenomen eisen zijn alle gericht op de bescherming van de exclusiviteit. Om dit te bereiken zullen er in het informatiesysteem ook enkele maatregelen op het terrein van de bescherming van de integriteit moeten worden getroffen.

Bij het verzenden van stukken via netwerken is het van belang dat de gegevens met betrekking tot de ontvanger juist en authentiek zijn. Onjuistheid van deze gegevens kan er toe leiden dat onbevoegden kennis nemen van de informatie.

2. Om te komen tot de exclusiviteitseisen is een tot het aspect exclusiviteit beperkte generieke afhankelijkheids- en kwetsbaarheidsanalyse (A&K-analyse) uitgevoerd.

Voor de aspecten beschikbaarheid en integriteit kan ook voor bijzondere informatie worden volstaan met de A&K-analyse op grond van het Vir.

Deze analyse bestaat uit drie elementen:

a. *Afhankelijkheidsanalyse*

De afhankelijkheidsanalyse is uitgevoerd om onder andere te komen tot een stelsel van exclusiviteitseisen voor de verschillende rubriceringsniveaus. Voor zover dit noodzakelijk is om de exclusiviteit te waarborgen zijn de eisen met betrekking tot de integriteit meegenomen (zoals het authentiseren van berichten). Omdat de exclusiviteitseisen rechtstreeks voortvloeien uit de rubricering, is het voor de lijnmanager dus niet nodig om nog een separate afhankelijksanalyse voor het aspect exclusiviteit uit te voeren.

b. *Inventarisatie van dreigingen (dreigingsanalyse)*

Als uitgangspunt is een algemene dreigingsinventarisatie zoals die wordt gehanteerd door de AIVD en MIVD genomen (zie bladzijde 29).

c. *Kwetsbaarheidsanalyse*

Op basis van de afhankelijkheids- en dreigingsanalyse is een kwetsbaarheidsanalyse uitgevoerd.

De uit de kwetsbaarheidsanalyse voortvloeiende exclusiviteitseisen zijn in de matrix weergegeven. Hierbij is een indeling gehanteerd die in grote lijnen overeenkomt met de Code voor informatiebeveiliging.[1]

3. Indien het voor de lijnmanager in een bepaald geval noodzakelijk is om van de in de matrix vermelde eisen af te wijken, moet de secretaris-generaal hiervoor schriftelijk zijn toestemming verlenen en moet de afwijking en noodzaak hiertoe schriftelijk zijn vastgelegd. Indien het de beveiliging van een staatsgeheim betreft is tevens voorafgaand overleg met het hoofd van de Algemene Inlichtingen- en Veiligheidsdienst dan wel met de Beveiligingsautoriteit, indien het de beveiliging van een bij het Ministerie van Defensie berustend staatsgeheim betreft, vereist (zie art. 12 van het voorschrift). Uiteraard zal deze toestemming in overmachtsituaties ook achteraf kunnen worden verleend.

Ter illustratie worden hier een aantal voorbeelden gegeven waarin het mogelijk is om af te wijken van de in de matrix voorgeschreven exclusiviteitseisen.

Uit andere hoofde is reeds voldaan aan de eisen conform de matrix of dat er bestaat een situatie bestaat waarin de in de matrix vermelde exclusiviteitseisen elkaar versterken.

De eisen blijken in een bepaalde situatie c.q. omgeving niet toereikend te zijn. Dit komt omdat door het algemene karakter van de inventarisatie van dreigingen geen rekening is gehouden met de specifieke dreiging in een bepaalde situatie c.q. omgeving. In een dergelijke situatie moet de lijnmanager besluiten om een op zijn specifieke situatie toegesneden kwetsbaarheidsanalyse uit te voeren en volgens de uitkomst daarvan maatregelen van een hoger beveiligingsniveau te treffen.

Er is sprake van een tijdelijk afwijkende situatie. Hiervan kan sprake zijn bij een verbouwing of na een calamiteit. In een dergelijke situatie mag de lijnmanager besluiten tijdelijk van de in de matrix voorgeschreven exclusiviteitseisen af te wijken mits wordt gekozen voor andere maatregelen die een gelijkwaardige beveiliging bieden.

Voorwaarde blijft echter wel dat zo veel mogelijk aan de eisen met betrekking tot de bescherming van de exclusiviteit, zoals genoemd in artikel 12 van het Voorschrift, wordt voldaan.

Voorwaarde blijft echter wel dat zo veel mogelijk aan de eisen met betrekking tot de bescherming van de exclusiviteit, zoals genoemd in artikel 12 van het Voorschrift, wordt voldaan.

4. In de matrix wordt verschillende keren de BVA genoemd. Dit betekent niet dat alle aan de BVA opgedragen werkzaamheden door hem persoonlijk moeten worden uitgevoerd Hij kan anderen hiermee belasten om de werkzaamheden namens hem uit te voeren. De eindverantwoordelijkheid ligt echter wel bij de BVA.

5. In de matrix zijn gebieden van exclusiviteitseisen gegeven. Ieder gebied is per categorie uitgewerkt in één of meer specifieke eisen. De eisen worden op vier manieren gesteld:

a. er is geen keuzemogelijkheid;
Met een √-teken is aangegeven dat aan de beveiligingseis moet worden voldaan en voor welke rubriceringen dit geldt (zie bijvoorbeeld 'Fysieke beveiliging van locaties en gebouwen' onder b).

b. er is een keuzemogelijkheid om aan de eis te voldoen;
Indien aan een eis op verschillende wijzen kan worden voldaan zijn alle mogelijkheden in de matrix aangegeven (zie bijvoorbeeld 'Fysieke beveiliging van locaties en gebouwen' onder f). Met een }-teken is aangegeven uit welke maatregelen, gegeven de rubricering, de lijnmanager kan kiezen.

c. de eis verschilt per categorie in zwaarte;
Indien een eis per categorie verschilt is dit in de matrix aangegeven (zie bijvoorbeeld 'Fysieke beveiliging van locaties en gebouwen' onder a). Met een √-teken is per categorie aangegeven dat aan de eis voor de desbetreffende rubricering moet worden voldaan.

d. de eis bestaat uit meerdere onderdelen;
Indien een eis voor een bepaalde rubricering uit meerdere onderdelen bestaat is dit in de matrix aangegeven (zie bijvoorbeeld 'Beveiliging tegen diefstal/ ongeautoriseerd meenemen' onder a). Met een √-teken is aangegeven dat aan de eis voor de desbetreffende rubricering moet worden voldaan.

6. Zie voor de specifieke beveiliging van verbindingen met de nadruk op het gebruik van nationale verbindingsapparatuur en het gebruik van cryptomidde-

len: VBV 41000 dan wel VBV 41300 en de bij de apparatuur behorende goedkeuringsdocumenten (VBV 94…).

7. Implementatie richtlijnen

Als handreiking bij de implementatie van de exclusiviteitseisen is/wordt voor een aantal deelaspecten een aparte leidraad opgesteld. Hierover kunt u informatie inwinnen bij de afdeling Beveiligingsbevordering van de Directie Beveiliging van de Algemene Inlichtingen- en Veiligheidsdienst dan wel bij het Ministerie van Defensie tot het Bureau Beveiligingsautoriteit of bij de veiligheidsfunctionaris van uw onderdeel.

8. Definitie van in de matrix gehanteerde begrippen:

Beveiligd gebied: een afgebakend fysiek gebied waarin een aantal beveiligingsmaatregelen is geïmplementeerd.

Interventietijd: de tijd die verloopt vanaf het moment van signalering van een aanvalspoging tot het moment van onderbreken daarvan door daartoe aangewezen personeel.

Token: fysiek hulpmiddel ter identificatie en authenticatie van de gebruiker.

VBV .....: verbindingsbeveiligingsvoorschriften uitgegeven door het Nationaal Bureau voor Verbindingsbeveiliging.

Verboden plaats: plaats als bedoeld in de Wet bescherming staatsgeheimen (Stb. 1951, 92).

Vertragingstijd: de tijd die ontstaat wanneer beveiligingsmaatregelen een aanvalspoging vertragen.

Verwisselbare gegevensdragers: verwisselbare harde schijven, diskettes, cd's, dvd's, enz.

Dreigingen/kwetsbaarheden

Algemeen

Bij het vaststellen van de betrouwbaarheidseisen zijn de in onderstaande tabel weergegeven dreigingen en kwetsbaarheden toegepast.

ZL = Zeer Laag
L = Laag
M = Gemiddeld
H = Hoog
ZH = Zeer Hoog

Omschrijving	Dreiging	Kwetsbaarheid
Technische Storingen		
Misrouteren van berichten	ZL	L
Storing op gegevens- en applicatieservers	L	M
Storing op authenticatie- en netwerkmanagement-server	L	L
Storing in gegevensopslag	L	L
Storing in printerfaciliteiten	M	M
Storing op netwerkdistributiecomponenten	L	M
Storing van netwerk management of operationhost	L	L
Storing van netwerkdiensten	ZL	L
Storing in systeem en netwerksoftware	ZL	L
Storing in applicatiesoftware	ZL	L
Menselijk falen		
Fouten van (netwerk) operators	H	L
Fouten van onderhoudsmonteurs (hardware)	M	L
Fouten van systeem- en softwareprogrammeurs (software)	L	L
Fouten van eindgebruikers	M	M
Bedreigingen van menselijke aard		
Personeelstekort	ZL	L
Zich voordoen als een andere mederwerker door eigen personeel	ZH	M
Zich voordoen als een medewerker door onderhoudspersoneel	M	H
Zich voordoen als een medewerker door buitenstaanders	ZH	M
Ongeauthoriseerd gebruik van programma's	M	M
Introductie van virussen	H	H
Trojaanse paarden	H	H
Misbruik van systeemmiddelen	L	M
Afluisteren van lokale netwerk door eigen personeel	ZL	M
Afluisteren van lokale netwerk door onderhoudspersoneel	ZL	H
Afluisteren van lokale netwerk door buitenstaanders	ZL	L
Diefstal door eigen personeel	ZH	H
Diefstal door buitenstaanders	M	M

Exclusiviteitseisen Bijzondere Informatie

I. Rubricering (Classificatie) en Beheer van Bedrijfsmiddelen (hoofdstuk 5) (1)

		Categorie			
1	Invoer-/uitvoercontroles	Stg.ZG	Stg.G	Stg.C	Dep.V
a	Bij tonen van bijzondere informatie op een beeldscherm moet de rubricering worden weergegeven (2)	v*	v*	v*	

II. Beveiligingseisen ten aanzien van Personeel (hoofdstuk 6)

		Categorie			
1	Personeel (3)	Stg.ZG	Stg.G	Stg.C	Dep.V
a	In de functieomschrijvingen van personeel dat inzage heeft in bijzondere informatie is de verantwoordelijkheid voor beveiliging vastgelegd	v*	v*	v*	v*
b	Personeel dat in aanraking komt met bijzondere informatie tekent een geheimhoudingsverklaring	v*	v*	v*	v*
c	Personeel screenen (4)				
	– Het personeel dat werkzaamheden verricht met betrekking tot staatsgeheimen bezit een verklaring van geen bezwaar voor vervullen van een A-functie (5)	v*			
	– Het personeel dat werkzaamheden verricht met betrekking tot staatsgeheimen bezit een verklaring van geen bezwaar voor vervullen van een B-functie (6)		v*		
	– Het personeel dat werkzaamheden verricht met betrekking tot staatsgeheimen bezit een verklaring van geen bezwaar voor vervullen van een C-functie (7)			v*	
2	Beveiligingsscholing en -training	Stg.ZG	Stg.G	Stg.C	Dep.V
a	De BVA zet een beveiligingsbewustzijnbevorderend programma op en zorgt voor uitvoer	v*	v*	v*	v*
3	Accounting (Vastleggen gebruikershandelingen) (8)	Stg.ZG	Stg.G	Stg.C	Dep.V
a	Er wordt voldoende informatie vastgelegd om een onderzoek van een (vermoed) incident mogelijk te maken (9)	v*	v*	v*	v*
b	Informatie wordt gedurende een bepaalde periode bewaard om achteraf onderzoek mogelijk te maken	3 mnd	3 mnd	3 mnd	3 mnd
c	Informatie over een (vermoed) incident wordt gedurende een bepaalde termijn bewaard	5 jr	5 jr	5 jr	3 jr
4	Audit (Toezicht op gebruikershandelingen)	Stg.ZG	Stg.G	Stg.C	Dep.V
a	Informatie over de beveiligingsrelevante handelingen van de gebruiker wordt regelmatig nagekeken				
	– De BVA bekijkt dagelijks alle informatie	v*			
	– De BVA bekijkt dagelijks een samenvatting van de informatie		v*		
	– De BVA bekijkt wekelijks een samenvatting van de informatie			v*	
	– De BVA bekijkt maandelijks een samenvatting van de informatie				v*
5	Netwerkbeveiligingsbeheer	Stg.ZG	Stg.G	Stg.C	Dep.V
a	De netwerkbeheerder houdt toezicht op de netwerkstatus om ongeautoriseerd gebruik te signaleren	v*	v*	v*	v*

III. Fysieke Beveiliging en Beveiliging van de Omgeving (hoofdstuk 7)

		Categorie			
1	Fysieke beveiliging van locaties en gebouwen (10)	Stg.ZG	Stg.G	Stg.C	Dep.V
a	Ongeautoriseerde toegang en pogingen daartoe detecteren en interveniëren (11)				
	– De beveiliging is zodanig ingericht dat ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd en dat tijdig interventie plaatsvindt	v*	v*	v*	

			Categorie			
		– De beveiliging is zodanig ingericht dat ongeautoriseerde toegang wordt gedetecteerd				v*
	b	Fysieke beveiliging van omgeving				
		– De ruimte waarin bijzondere informatie (in het daartoe geëigende bergmiddel) zich bevindt, moet voldoende fysieke weerstand (11) bieden	v*	v*	v*	
	c	Bijzondere informatie wordt zoveel mogelijk binnen bepaalde werkruimten geconcentreerd	v*	v*	v*	v*
	d	Het binnenkomen en verlaten controleren				
	i	Het binnentreden en verlaten is zodanig geregeld dat er sprake is van gecontroleerde toegang op individueel niveau	v*	v*	v*	
	e	Bezoekers worden begeleid binnen ruimtes waarin bijzondere informatie aanwezig is	v*	v*	v*	v*
	f	Waarnemen van buitenaf				
	i	Door of in overleg met de BVA zijn maatregelen getroffen om te voorkomen dat niet gerechtigden van buitenaf kennis kunnen nemen van bijzondere informatie	v*	v*	v*	v*
	g	Ruimten na werktijd controleren				
	i	Bewakingspersoneel oefent na kantooruren permanent controle uit	}	}	}	}
	li	Bewakingspersoneel loopt na kantooruren controlerondes				
	lii	Na kantooruren worden de ruimten met technische middelen van voldoende niveau bewaakt				
2	Sleutelbeheer		Stg.ZG	Stg.G	Stg.C	Dep.V
	a	De uitgifte van sleutels wordt geregistreerd	v*	v*	v*	v*
	b	Niet in gebruik zijnde sleutels worden veilig opgeborgen (12)	v*	v*	v*	v*
	c	Gecertificeerde sleutels worden gebruikt	v*	v*	v*	
3	Fysieke netwerkbescherming		Stg.ZG	Stg.G	Stg.C	Dep.V
	a	Netwerkapparatuur en bekabeling fysiek beschermen	v*	v*	v*	v*
	b	De vertragingstijd is dusdanig dat detectie van ongeautoriseerde toegang en pogingen daartoe plaatsvindt op een tijdstip dat interventie mogelijk maakt (13)	n.v.t.	v*		
	c	Ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd.			v*	
	d	Ongeautoriseerde toegang wordt gedetecteerd				v*
4	Opbergen van informatie		Stg.ZG	Stg.G	Stg.C	Dep.V
	a	Bij het verlaten van de werkplek wordt bijzondere informatie in een daartoe geëigend bergmiddel opgeborgen	v*	v*	v*	v*
	b	De sterkte van het opbergmiddel is gerelateerd aan de rubricering en de interventietijd (14)	v*	v*	v*	v*
5	Controles op onderhoud, plaatsing en vervanging van apparatuur		Stg.ZG	Stg.G	Stg.C	Dep.V
	a	Toegang van onderhoudspersoneel controleren				
		– Onderhoud vindt plaats door gescreende personen (zie II-1)	v*	v*	v*	
		– Onderhoudspersoneel wordt begeleid door eigen personeel	v*	v*	v*	
	b	Reparaties worden gecontroleerd				
		– Reparatie vindt, voorzover mogelijk, op de locatie plaats (15)	v*	v*	v*	v*
		– Externe reparatie is gebonden aan door de BVA vastgestelde procedures	v*	v*	v*	v*

IV. Beheer van Communicatie- en Bedieningsprocessen (hoofdstuk 8)

		Categorie			
1	Controles op documenten en gegevensdragers	Stg.ZG	Stg.G	Stg.C	Dep.V
	a De hoogste rubricering van informatie wordt op verwisselbare gegevensdragers aangegeven (16)	v*	v*	v*	v*
	b De rubricering van afgedrukte informatie staat aangegeven (17)	v*	v*	v*	v*
	c Verwisselbare gegevensdragers die onversleutelde bijzondere informatie bevatten en afgedrukte informatie in documentvorm worden beveiligd opgeborgen cf. III-4	v*	v*	v*	v*
	d Het bijmaken van informatie op welke wijze dan ook reguleren				
	– Informatie wordt alleen gereproduceerd met toestemming van degene die de rubricering heeft vastgesteld (18)	v*	v*		
	– Het bijmaken van reproducties wordt geregistreerd	v*	v*		
	– Het reproduceren is voorbehouden aan daartoe aangewezen personen. In principe alleen degenen die verantwoordelijk zijn voor het bijhouden van het register	v*	v*		
	– Er worden niet meer reproducties gemaakt dan strikt noodzakelijk is	v*	v*	v*	v*
	e Het maken, afleveren, bewaren en vernietigen van informatie wordt bewaakt				
	– Informatie wordt geregistreerd en van een kenmerk voorzien	v*	v*	v*	
	– Informatie wordt van een uniek exemplaarnummer voorzien	v*	v*		
	– Van vernietiging wordt een proces-verbaal opgemaakt	v*	v*		
	– Informatie wordt vernietigd door middel van een door de BVA voor de desbetreffende rubricering goedgekeurde wijze (19)	v*	v*	v*	v*
	f Gegevensdragers veilig afstoten (20)				
	– Gegevensdragers worden fysiek vernietigd	v*			
	– Af te stoten gegevensdragers worden eerst gewist met een door de BVA voor de desbetreffende rubricering goedgekeurde methode		v*	v*	v*
2	Registratie (21)	Stg.ZG	Stg.G	Stg.C	Dep.V
	a De verblijfplaats van de informatie is traceerbaar				
	– Geregistreerd wordt welke persoon de informatie onder zijn berusting heeft	v*	v*		
	– Geregistreerd wordt welke persoon de informatie heeft ingezien	v*	v*		
3	Beheersing randapparatuur (printers, routers, servers, etc.)	Stg.ZG	Stg.G	Stg.C	Dep.V
	a De informatie wordt alleen behandeld op daartoe geschikte randapparatuur (zie ook III-3a)	v*	v*	v*	
	b Printers worden in ruimtes geplaatst die geschikt zijn voor de hoogste rubricering die met de printer wordt verwerkt	v*	v*	v*	
	c Modems en netwerkcomponenten worden in fysiek afgeschermde ruimtes geplaatst	n.v.t	v*	v*	v*
4	Fysiek transport	Stg.ZG	Stg.G	Stg.C	Dep.V
	a De beveiliging van informatie moet tijdens fysiek transport buiten gecontroleerd gebied gehandhaafd blijven				
	– Transport vindt binnen Nederland plaats per door het ministerie aangewezen koerier met ontvangstbewijs (22)	v*			
	– Transport vindt buiten Nederland plaats per koerier (23) met ontvangstbewijs als diplomatieke zending	v*			
	– Verzending vindt zowel binnen als buiten Nederland plaats per door het ministerie aangewezen koerier, indien dit niet mogelijk is per aangetekende post met ontvangstbewijs (22)		v*		

			Categorie			
		– Verzending vindt nationaal plaats per aangetekende post of per door de BVA goedgekeurde commerciële koerier			v*	
		– Verzending vindt internationaal plaats per aangetekende post of als onbegeleide diplomatieke zending			v*	
	b	Verzending vindt plaats in dubbele enveloppe of door de BVA goedgekeurde sealbag (24)	v*	v*	v*	
	c	Met de informatie wordt een door de geadresseerde terug te sturen ontvangstbewijs (20) bijgevoegd	v*	v*		
	d	Verzending wordt gereed gemaakt door daartoe aangewezen personen c.q. afdeling	v*	v*	v*	v*
	e	Materiaal dat niet met de voorafgaande methoden kan worden verzonden				
		– Per Nederlands of bondgenootschappelijk militair transport of per door de Minister van BZK/Defensie gescreende commerciële koerier	v*			
		– Per door de Minister van BZK/Defensie gescreende commerciële koerier		v*		
		– Per door de BVA goedgekeurde commerciële koerier			v*	v*
	f	Meenemen van bijzondere informatie buiten gecontroleerd gebied (plaats van tewerkstelling)				
		– Uitsluitend meenemen buiten gecontroleerd gebied indien dit voor de voortgang van de werkzaamheden noodzakelijk is en hiervoor door de lijnmanager schriftelijk toestemming is verleend	v*	v*	v*	v*
		– Informatie wordt niet mee naar huis genomen	v*			
		– Informatie wordt niet meegenomen naar het buitenland (25)	v*			
		– Token voor de toegang wordt gescheiden van de informatie meegenomen	v*	v*		
		– De BVA stelt voorschriften op voor het registreren van het meenemen	v*	v*		
		– Informatie wordt meegenomen in een door de BVA goedgekeurd transportmiddel	v*	v*		
5		Elektronisch transport	Stg.ZG	Stg.G	Stg.C	Dep.V
	a	De beveiliging van informatie moet tijdens elektronisch transport buiten gecontroleerd gebied gehandhaafd blijven				
		– Het versturen van berichten wordt geregistreerd	n.v.t.	v*	v*	
		– De rubricering wordt samen met de informatie verzonden	n.v.t.	v*	v*	v*
		– De ontvangst van het bericht wordt bevestigd	n.v.t.	v*		
		– De ontvangst van het bericht wordt geregistreerd	n.v.t.	v*	v*	
	b	De beveiliging van informatie moet tijdens elektronisch transport binnen gecontroleerd gebied gehandhaafd blijven				
		– Koppeling met intern netwerk is niet toegestaan	v* (25)			
6		Vertrouwelijkheid van informatie over netwerken	Stg.ZG	Stg.G	Stg.C	Dep.V
	a	Informatie verspreid via netwerken vercijferen Het vercijfermechanisme incl. het sleutelbeheer, is door de Minister van Binnenlandse Zaken en Koninkrijksrelaties goedgekeurd voor de betreffende rubricering (zie VBV92002) (27)	v* (25)	v*	v*	v*

V. Toegangsbeveiliging (informatiesystemen) (hoofdstuk 9)

			Categorie			
1		Identificatie en authenticatie	Stg.ZG	Stg.G	Stg.C	Dep.V
	a	Het eerste scherm vermeldt de wettelijke strafbaarheid van ongeautoriseerde toegang	v*	v*	v*	v*
	b	Gebruikersnamen garanderen dat activiteiten worden herleid naar individuen	v*	v*	v*	v*
	c	Gebruikers worden vooraf geïdentificeerd en geautoriseerd (zie ook VIII-1)	v*	v*	v*	v*
	d	De identiteit van een gebruiker wordt mede vastgesteld middels token of biometrie	v*	v*		

			Categorie			
e		Keuze van wachtwoorden				
	i	Wachtwoorden worden gegenereerd	}	}	}	}
	ii	Wachtwoorden worden gecontroleerd				
f		Wachtwoorden worden opgeslagen met behulp van een eenzijdig vercijferalgoritme	v*	v*	v*	v*
g		Wachtwoorden worden frequent gewijzigd	30 dagen	30 dagen	30 dagen	√
h		De inlogdialoog helpt ongeautoriseerde gebruikers niet om toegang te verkrijgen (27)	v*	v*	v*	v*
i		De gebruiker krijgt buiten normale kantoortijden alleen met behulp van door de BVA gestelde regels toegang	v*	v*		
j		Wachtwoorden worden zodanig behandeld dat ze niet kunnen worden gecompromitteerd	v*	v*	v*	v*
k		Het aantal foutieve inlogpogingen is beperkt	3	3	3	5
l		Overschrijding van het aantal foutieve inlogpogingen leidt tot definitieve blokkering van de toegang (te herstellen door of namens de BVA)	v*	v*	v*	
2	Logische toegangscontrole		Stg.ZG	Stg.G	Stg.C	Dep.V
a		Er worden procedures vastgesteld voor het verkrijgen van toegang tot bijzondere informatie	v*	v*	v*	v*
b		De toegang tot het werkstation wordt beveiligd				
		– Toegangsbeveiliging lock wordt automatisch geactiveerd bij verwijderen van een token (indien aanwezig)	}	}	}	}
		– Toegangsbeveiliging lock wordt geactiveerd bij intikken van een toetscombinatie/muisklik				
		– Toegangsbeveiliging lock wordt automatisch geactiveerd	5 min	5 min	10 min	30 min
c		Informatie vercijferd opslaan				
		– Het vercijfermechanisme is incl. het sleutelbeheer door de Minister van Binnenlandse Zaken en Koninkrijksrelaties goedgekeurd voor de desbetreffende rubricering (zie VBV 92002)	v*	v*	v*	v*
d		Toegang tot beheerfuncties is voorbehouden aan die personen die van deze functies gebruik moeten maken	v*	v*	v*	v*
e		De toegangsrechten van de gebruikers worden periodiek geëvalueerd	30 dagen	90 dagen	90 dagen	180 dagen
3	Netwerk toegangscontroles		Stg.ZG	Stg.G	Stg.C	Dep.V
a		De autorisaties van alle gebruikers vastleggen	v*	v*	v*	v*
b		Remote diagnostic service (onderhoud op afstand) beschermen tegen ongeautoriseerde toegang				
		– Remote diagnostic service door leverancier is verboden	v*	v*		
		– Er zijn procedures vastgesteld voor het uitvoeren van remote diagnostic service door leverancier			v*	
		– Verstuurde informatie via remote diagnostics naar leverancier wordt meegelezen			v*	
		– Remote diagnostic service door leverancier is alleen toegankelijk als het strikt noodzakelijk is			v*	v*
c		De aansluiting met netwerken beveiligen				
		– Koppeling met netwerken is niet toegestaan	v* (25)			
		– Koppeling met externe netwerken is niet toegestaan	√	√		
		– Koppeling met netwerken die niet onder het beheer staan van de eigen organisatie tast de betrouwbaarheid van het eigen netwerk niet aan			v*	v*

VI. Ontwikkeling en Onderhoud van Systemen (hoofdstuk 10)

			Categorie			
1	Systeembeheercontroles		Stg.ZG	Stg.G	Stg.C	Dep.V
a		De configuratie van de hard- en software moet zijn vastgelegd	v*	v*	v*	v*

		Categorie			
b	Alle wijzigingen in apparatuur, software of procedures moeten controleerbaar zijn	v*	v*	v*	v*
c	Er moet een autorisatiematrix en procedure voor wijzigingen in de software zijn	v*	v*	v*	v*

VII. Goedkeuring

		Categorie			
1	Goedkeuring van systeemcomponenten	Stg.ZG	Stg.G	Stg.C	Dep.V
a	Door de Minister van Binnenlandse Zaken en Koninkrijksrelaties na evaluatie voor de desbetreffende rubricering goedgekeurde ICT-beveiligingsproducten (28) worden gebruikt (zie ook VBV 92002(A))	v*	v*	v*	v*

VIII. TEMPEST

		Categorie			
1	Voorkomen compromitterende Straling	Stg.ZG	Stg.G	Stg.C	Dep.V
a	Zie Beleidsadvies Compromitterende Straling (VBV 32000)	v*	v*	v*	v*

IX. Naleving (hoofdstuk 12)

		Categorie			
1	Controles op naleving	Stg.ZG	Stg.G	Stg.C	Dep.V
a	Controles worden uitgevoerd om te waarborgen dat beveiligingsmaatregelen zijn geïmplementeerd en nageleefd				
	– Maandelijks vindt controle door of namens de lijnmanager op de naleving en vastlegging daarvan plaats	v*	v*		
	– Minimaal eens per jaar vindt controle door de BVA op de implementatie en vastlegging daarvan plaats	v*	v*	v*	v*

Maatregelen optioneel
De navolgende maatregelen kunnen afhankelijk van de situatie aanvullend op de voorafgaande verplichte maatregelen worden getroffen.

Verboden plaats

		Categorie			
1	Aanwijzen verboden plaats	Stg.ZG	Stg.G	Stg.C	Dep.V
a	De Wet bescherming staatsgeheimen biedt de mogelijkheid om elke plaats (ruimte of gebouw) waarin staatsgeheimen aanwezig zijn aan te wijzen als verboden plaats (Wet bescherming staatsgeheimen 1951)	v*	v*	v*	

Afluisteren

		Categorie			
1	Voorkomen afluisteren	Stg.ZG	Stg.G	Stg.C	Dep.V
a	Werkruimtes dienen regelmatig te worden gecontroleerd op de aanwezigheid van afluisterapparatuur (29)	v*	v*	v*	

Eindnoten bij de matrix
(1) Verwijzing naar het betreffende hoofdstuk in de 'Code voor Informatiebeveiliging'
(2) Indien technisch mogelijk
(3) Geldt zowel voor vast, tijdelijk en ingehuurd personeel
(4) Beheers- en onderhoudsfuncties waarbij kennis kan worden genomen van de in het systeem aanwezige bijzondere informatie dan wel mogelijkheid bieden de continuïteit van de informatievoorziening ernstig te verstoren kunnen vanuit integriteitsoogpunt worden aangewezen vertrouwensfunctie.

(5) A-functies: Functies waarin werkzaamheden worden verricht met betrekking tot zeer geheim en lager gerubriceerde informatie

(6) B-functies: Functies waarin werkzaamheden worden verricht met betrekking tot geheim en lager gerubriceerde informatie

(7) C-functies: Functies waarin werkzaamheden worden verricht met betrekking tot confidentieel gerubriceerde informatie

(8) Accounting gegevens dragen de rubricering van de informatie waarop zij betrekking hebben. Deze gegevens dienen conform dit voorschrift en het Vir beveiligd te worden.

(9) Door het ICT-beveiligingsproduct moeten in ieder geval worden vastgelegd: datum, tijd, gebruiker, soort handeling, identificatie van apparaat waarop de handeling plaats vond.

Dit dient tijdens de goedkeuringsprocedure zie VII te worden geverifieerd.

(10) Voor de fysieke beveiliging van cryptomiddelen zie ook VBV 41000 en VBV 92002

(11) Zie uitvoeringsrichtlijnen Vir-bi Fysieke beveiliging en beveiliging van de omgeving

(12) Niet in gebruik zijnde sleutels dienen veilig te worden opgeborgen. Dit dient minimaal te gebeuren in een bergmiddel gelijkwaardig aan de inschaling van het bergmiddel waarin de gegevens zijn opgeborgen.

(13) Apparatuur waarop Stg ZEER GEHEIM wodt verwerkt mag niet gekoppeld zijn aan een ander netwerk zie V-3c

(14) Bergmiddelen

Installatie

In onderstaande matrix is aangegeven welke bergmiddelen dienen te worden geïnstalleerd. Bij het bergen van Stg. GEHEIM en hoger gerubriceerd materiaal, moet het bergmiddel deugdelijk worden verankerd als het bergmiddel lichter is dan 1000 Kg

Er wordt van uit gegaan dat een braakpoging, wordt gedetecteerd en dat er tijdig wordt geïntervenieerd (interventietijd).

Deze interventietijd kan op verschillende manieren worden gerealiseerd, b.v. door een elektronisch detectiesysteem met adequate opvolging, door het lopen van controlerondes, enz.

De interventietijd mag nooit meer dan 4 uur bedragen (bij Stg. ZEER GEHEIM niet meer dan 2 uur).

Rubricering Interventietijd	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL
0–15 min	SAFE 3	SAFE 2	SAFE 2
15–30 min	CEN 1	SAFE 3	SAFE 2
30–120 min	CEN 2	CEN 1	SAFE 3
120–240 min	Niet toegestaan	CEN 2	CEN 1

Figuur 1 Matrix bergmiddelen

Voor het niveau Dep. VERTROUWELIJK geldt dat het bergmiddel afsluitbaar moet zijn.

Hiervoor geldt geen maximale interventietijd.

SAFE 2 en SAFE 3 zijn inschalingen volgens de NCP/VNS-normering (zie ook Handboek beveiligingstechniek van het Nederlands Centrum voor Preventie Uitgave Ten Hage Stam ISBN 904400 011 X)

SAFE 2: Enkelwandige meubelkluizen met een buitenmantel van minimaal 2 mm plaatstaal en een deur van minimaal 6 mm.

SAFE 3: Dubbelwandige meubelkluizen met een buitenmantel van tenminste 2 mm plaatstaal en een deur van minimaal 6 mm.

Het slot moet voldoen aan VdS klasse 1 met bepantsering.

CEN 1 en CEN 2 zijn inschalingen volgens NEN-EN-1143-1

Voor de volledigheid wordt de dekkingsindicatie van inschalingen weergegeven:

SAFE 2: € 2500,–

SAFE 3: € 5000,–

CEN 1: € 9000,–

CEN 2: € 23000,–

Bergmiddelen die Stg. GEHEIM of hoger gerubriceerde informatie bevatten zijn voorzien van een sleutelslot en een cijfercombinatieslot.

(15) Indien het niet mogelijk is de informatie vooraf te wissen dan wel de harde schijf vooraf te verwijderen moet reparatie altijd op locatie plaats te vinden.

(16) Wijze van aanbrengen van rubriceringen op verwisselbare gegevensdrager

Een gegevensdrager draagt de rubricering van de informatie met de hoogste rubricering die zich op de gegevensdrager bevindt. Deze rubricering wordt aangevuld met een omschrijving van de zich op de gegevensdrager bevindende informatie en de datum waarop de rubricering is vastgesteld.

(17) Wijze van aanbrengen van rubriceringen

Documenten

Onder een document wordt verstaan al datgene waarin gegevens ter raadpleging zijn vastgelegd (zoals een brief, aantekening, rapport, memorandum, tekening, foto, diskette, cd, dvd, enz.).

Indien praktisch uitvoerbaar, wordt een gedeelte van een document waarin bijzondere informatie is vastgelegd op een in het oog lopende wijze gemarkeerd onder vermelding van de rubricering van de bijzondere informatie. In het geval dat een document meerdere stukken bijzondere informatie bevat wordt de rubricering van elk van die stukken bijzondere informatie op deze wijze aangebracht.

Op afgedrukte informatie als geheel wordt de rubricering op een in het oog lopende wijze aan de rechter boven- en onderkant van iedere bladzijde en op de eventuele omslag aangebracht.

Indien dit praktisch niet uitvoerbaar is, wordt de rubricering op zodanige wijze aangebracht dat de rubricering de gebruiker van het document niet kan ontgaan. Indien de op een document als geheel aangebrachte rubricering verband houdt met een in een bijlage vastgelegd staatsgeheim, kan aan de rubricering worden toegevoegd: ‘Zonder bijlage (nr. ...) draagt deze informatie geen rubricering/de rubricering .....’.

Op een document waarop een rubricering is aangebracht worden de aanduiding van de ambtenaar die de rubricering heeft vastgesteld en de datum waarop de vaststelling heeft plaatsgevonden vermeld.

Op een verzameling documenten als geheel wordt de rubricering op een in het oog lopende wijze op de omslag aangebracht. Indien dit praktisch niet uitvoer is, wordt de rubricering op zodanige wijze aangebracht dat de rubricering de gebruiker van de verzameling documenten niet kan ontgaan.

Materiaal

Onder materiaal wordt al datgene anders dan een document waarin gegevens zijn vastgelegd (zoals een machine, apparaat, wapen, enz.).

Op materiaal wordt de rubricering op zodanige wijze aangebracht dat de rubricering de gebruiker van het materiaal

niet kan ontgaan. Indien dit praktisch niet uitvoerbaar is, wordt de gebruiker in een begeleidend schrijven op de hoogte gesteld van de rubricering.

(18) Bij een geheim gerubriceerd document kan de ambtenaar die de rubricering heeft vastgesteld bepalen dat het document niet zonder zijn toestemming wordt bijgemaakt. Dit wordt als volgt aangegeven: 'Dit document mag zonder toestemming niet worden bijgemaakt'.

Toestemming tot het bijmaken wordt verleend door de ambtenaar die de rubricering heeft vastgesteld, de ambtenaar die hem in zijn functie heeft opgevolgd dan wel door een daartoe door de secretaris-generaal aangewezen ambtenaar.

(19) Indien gebruik wordt gemaakt van versnipperapparatuur moeten de snippers aan de volgende eisen voldoen:

Maatregelen	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK	Opmerking
Grootte Snipper	X				lengte < 20 mm, breedte < 1,5 mm
Grootte Snipper		X			Lengte < 25 mm breedte < 3 mm
Grootte Snipper			X	X	lengte < 30 mm Breedte < 5 mm
Grootte Snipper	cryptosleutels	cryptosleutels	cryptosleutels	cryptosleutels	lengte < 12 mm Breedte < 0,8mm

In het geval van verwerking van grote hoeveelheden (bulk verwerking) van Stg. GEHEIM en lager gerubriceerde documenten, mag na toestemming van de BVA hiervan worden afgeweken, met dien verstande dat de geproduceerde snipper niet langer is dan 50 mm en niet breder dan 1,5 mm.

Indien versnipperen van cryptosleutels niet mogelijk is, dient de informatie onder toezicht verbrand te worden.

(20) Gegevensdragers kunnen binnen de eigen organisatie worden hergebruikt indien deze eerst zijn gewist met een door BVA aangegeven methode voor de betreffende rubricering aangegeven methode.

Gegevensdragers waarop 'zeer geheim' gerubriceerde gegevens zijn opgeslagen mogen nooit een lagere rubricering krijgen. Ook niet nadat de gegevens zijn gewist.

Hergebruik buiten de eigen organisatie is niet toegestaan. De betreffende media dienen te worden te worden vernietigd.

(21) Voor elektronische omgeving zie IV-1f.

(22) Bij het verzenden van een geheim of hoger gerubriceerd staatsgeheim wordt in de binnenenveloppe een ontvangstbewijs bijgesloten. Dit bewijs vermeldt het kenmerk en het eventuele aan de informatie toegekende nummer.

De ontvanger zendt het ontvangstbewijs ondertekend en gedateerd terug naar de afzender. De afzender ziet er op toe dat hij het ontvangstbewijs terugontvangt en doet, indien dit niet binnen redelijke tijd plaatsvindt, navraag. Heeft dit geen resultaat dan stelt de afzender de BVA hiervan op de hoogte.

(23) 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 of de Gouverneur van de Nederlandse Antillen of Aruba.

(24) 'Sealbags' zijn alleen toegestaan bij het gebruik van interne post of koeriers.

Indien gebruik wordt gemaakt van dubbele enveloppen draagt de binnen enveloppe de rubricering welke ook het document als geheel draagt. De buiten enveloppe draagt geen rubricering. De binnenenveloppe wordt zodanig gesloten dat openen zonder verbreken van de sluiting of beschadigen van de enveloppe niet mogelijk is. Voorts worden zodanige enveloppen gebruikt dat met behulp van een technisch middel kennis nemen van de inhoud zonder openen van de enveloppen niet mogelijk is.

(25) Indien het noodzakelijk is om in het buitenland over een zeer geheim gerubriceerd staatsgeheim te beschikken, moet de informatie in overeenstemming met deze matrix naar het buitenland worden verzonden.

(26) Koppeling via een netwerk is alleen toegestaan na vooraf verkregen toestemming van de AIVD dan wel de Beveiligingsautoriteit van het Ministerie van Defensie

(27) Dep. VERTROUWELIJK gerubriceerde informatie hoeft niet vercijferd te worden indien verzending plaatsvindt via een intern netwerk dat zich binnen één locatie bevindt.

Stg. GEHEIM en Stg. CONFIDENTIEEL gerubriceerde informatie hoeft niet vercijferd te worden indien verzending plaatsvindt via een intern netwerk dat zich binnen één gebouw bevindt en alle gebruikers een verklaring van geen bezwaar hebben voor het hoogste rubriceringsniveau op het netwerk, ook al hebben zij geen gelijke 'need-to-know' ('system high') en wordt voldaan aan VBV32000.

(28) Het inlog scherm moet slechts vragen om gebruikersidentificatie en wachtwoord, dus geen informatie over het systeem weergeven.

(29) ICT-beveiligingsproducten moeten met gunstig resultaat zijn geëvalueerd op basis van de WBI bepaalde evaluatiecriteria. Op grond van dit evaluatieresultaat verleent het hoofd van de Algemene Inlichtingen- en Veiligheidsdienst namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties, door tussenkomst van de WBI, goedkeuring voor het gebruik van het betreffende ICT-beveiligingsproduct voor de beveiliging van bijzondere informatie. Voor verder vragen kunt u zich wenden tot de AIVD/NBV.

Een overzicht van de goedgekeurde producten is te vinden in het verbindingsbeveiligingsvoorschrift VBV 920002(A); Nationale goedkeuringsdocumenten. Informatie over hoe de goedgekeurde producten gebruikt moeten worden is te vinden in het verbindings-beveiligingsvoorschrift VBV 93003(A); Operationele doctrines.

(30) Bij werkruimten waar regelmatig wordt gesproken over staatsgeheimen worden door de BVA of in overleg met de BVA maatregelen getroffen om te voorkomen dat het gesprokene buiten de ruimten doordringt. De werkruimten worden zonodig gecontroleerd op de aanwezigheid van afluisterapparatuur.

[1] Code voor informatiebeveiliging: 2000. Te verkrijgen bij het Nederlands Normalisatie-Instituut, Postbus 5059, 2600 GB Delft, tel. 015-2690390, www.nen.nl.