Gereedschap rubriceren

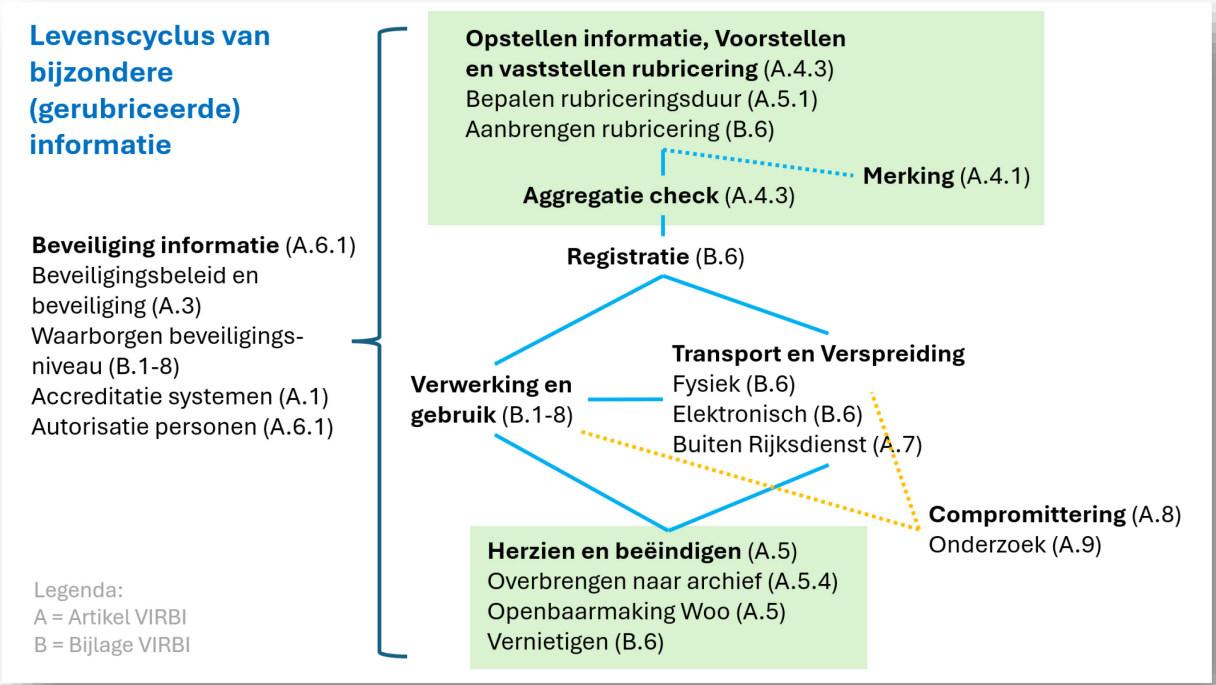
0.97 – 4 juni 2026

Contents

1. Inleiding

Deze handleiding is een beknopte uitleg behorend bij het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI) 2025 en is opgesteld voor alle medewerkers van de Rijksdienst om te verduidelijken wanneer en hoe bijzondere informatie te rubriceren.

Deze handleiding gaat allereerst, en in het meeste detail, in op de groen gemarkeerde delen van de levenscyclus van bijzondere (gerubriceerde) informatie. De overige punten worden korter toegelicht, in het tweede deel van deze handleiding.



Deze handleiding gaat in op de meest relevante en voor de hand liggende aandachtspunten van het VIRBI. Voor een volledig overzicht blijft de VIRBI zelf leidend.

Het VIRBI is geen geïsoleerd voorschrift maar raakt aan verschillende andere voorschriften en wetten. Sommige hiervan worden expliciet in het VIRBI genoemd, bijvoorbeeld:

- • **Wet bescherming staatsgeheimen:** Deze wet vormt de grondslag voor de definitie van staatsgeheimen waarvan de geheimhouding nodig is voor het belang van de Staat (of zijn bondgenoten).
- **Wetboek van Strafrecht:** In deze wet is de strafbaarheid geregeld van ongeautoriseerde toegang of onzorgvuldige behandeling van staatsgeheimen.

- **Kernenergiewet:** In deze wet wordt specifieke informatie bij wet aangewezen als staatsgeheim en valt daarmee buiten het standaardregime van herbeoordeling.
- **Wet veiligheidsonderzoeken (Wvo):** Verwijst naar de leidraden voor het aanwijzen van vertrouwensfuncties die toegang mogen hebben tot gerubriceerde informatie.
- **Wet open overheid (Woo):** Bij een Woo-verzoek moet de rubricering opnieuw worden beoordeeld en eventueel beëindigd.
- **Archiefwet 1995:** Deze wet beschrijft de procedure voor het overbrengen van gerubriceerde informatie naar een rijksarchiefbewaarplaats.
- **Algemene Verordening Gegevensbescherming (AVG):** Voor 'verwerking' van informatie sluit het VIRBI aan bij de AVG. Ook wordt de AVG genoemd bij het melden van incidenten aan toezichthouders.
- **Kaderwet ZBO's:** Het VIRBI 2025 is ook van toepassing is op ZBO's op grond van artikel 41 van deze wet.

Daarnaast raken de volgende wetten ook direct of indirect aan (gevoelige of gerubriceerde) informatie die extra beveiliging verdient:

- **Wet politiegegevens (Wpg):** Bevat expliciete eisen aan (passende) technische en organisatorische beveiligingsmaatregelen, geheimhouding en controlemechanismen.
- **Besluit politiegegevens (Bpg):** Werkt de Wpg verder uit, met bijvoorbeeld bepalingen over beveiliging en (periodieke) audits.
- **Wet justitiële en strafvorderlijke gegevens (Wjsg):** Bevat (net als Wpg) een beveiligingsplicht (“passend beveiligingsniveau…”) en governance-eisen rond verwerking/verstrekkingen.
- **Besluit justitiële en strafvorderlijke gegevens (Bjsg):** Nadere uitwerking van de Wjsg over verwerking en voorwaarden in dit domein.
- **Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017):** Bevat het kader waarbinnen AIVD/MIVD werken en (dus) ook de omgang met gevoelige/gerubriceerde informatie in dat domein.
- **Wetboek van Strafrecht:** Strafbaarstelling van (spionage-) activiteiten die schade geven aan nationale veiligheid, de veiligheid van personen, vitale infrastructuur en hoogwaardige technologieën.

2. Opstellen informatie

Het is belangrijk om het begrip “informatie” goed te interpreteren.

In het VIRBI is informatie een breed begrip. Informatie is onafhankelijk van het gebruikte medium en onafhankelijk van het feit of de informatie formeel is vastgesteld.

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.

De organisatie rondom rubricering en de taken en verantwoordelijkheden worden in een ander document uitgewerkt en toegelicht, zie:

- Gereedschap voor Governance VIRBI implementatie

3. Voorstellen en vaststellen rubricering

Rubriceren is het proces waarbij de opsteller van de bijzondere informatie een voorstel tot rubricering doet en de rubricering aanbrengt op de informatie. Vervolgens stelt de vaststeller van de inhoud van de informatie ook de rubricering vast. In het VIRBI zijn deze stappen formeel beschreven en is de vaststeller van de rubricering de minister, staatssecretaris, secretaris-generaal of een door de secretaris-generaal gemandateerd rubriceringsambtenaar.

In de praktijk wordt het voorstellen en vaststellen van rubricering onderdeel gemaakt van de standaard processen van een organisatie. Hierbij kunnen opsteller en vaststeller ook dezelfde persoon zijn. Of kan de opsteller de medewerker en de vaststeller de leidinggevende zijn (lijnmanagement).

Belangrijk is ook te melden dat rubriceren een kwaliteitsaspect is van informatie-management en als zodanig opgenomen moet worden binnen informatiemanagement processen.

Voorbeeld van een geïntegreerd rubriceringsproces:

- Bij het aanmaken van een nieuw document vraagt het documentbeheersysteem om de vereiste rubricering te kiezen. Dit wordt dan automatisch aangebracht in de kop- en voettekst van het document.
- Bij het accorderen van een document in het documentbeheersysteem door een teamhoofd wordt de rubricering automatisch mee-geaccordeerd en vastgesteld.

Als een geïntegreerd rubriceringsproces wordt ingericht voor structurele verwerking van (nationale) gerubriceerde informatie (inclusief taken, procedures en informatiesystemen) dan moet dit proces vooraf worden geaccrediteerd door de Secretaris Generaal.

In het VIRBI wordt niet voorgeschreven dat de vaststeller van een hoger rubriceringsniveau ook een hogere positie moet hebben in het lijnmanagement. De vaststeller kan dus de direct leidinggevende zijn van de opsteller.

Op enkele punten van het VIRBI wordt een verband gelegd tussen rubriceringsniveau en positie in de organisatie. Dit gaat echter niet over de relatie tussen opsteller en vaststeller en de positie in het lijnmanagement:

- Als van de VIRBI-voorschriften in de bijlage wordt afgeweken, dan wordt dit voor Dep.V goedgekeurd door een Directeur en voor Stg.C/Stg.G/Stg.ZG door ten minste een Directeur Generaal.

Het rubriceringsniveau en de rubriceringsduur van de bijzondere informatie wordt bepaald 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.

Er kan verwarring zijn rond de termen *rubricering* en *classificatie*. De verwarring wordt vergroot doordat “classified information” de Engelse term is voor “gerubriceerde informatie”. Het verschil hiertussen is:

- *Classificatie* wordt meestal gebruikt voor het systematisch groeperen van informatie, data, processen of systemen om deze groepen vervolgens verschillend te behandelen. Classificatie kan soms leiden tot *merking* (zie verderop).
- *Rubricering* is het groeperen van informatie in vier rubriceringsniveaus gebaseerd op de nadelige gevolgen als de informatie bekend wordt bij niet-geautoriseerden.

Rubricering is daarmee een subset van classificatie. Het meenemen van rubricering in een classificatieschema is dus mogelijk.

Er kan ook verwarring zijn rond het begrip *labelen van informatie (labeling)*. In ISO 27001 is *labelen* van informatie een beheersmaatregel die informatie classificeert en van een label voorziet volgens het informatieclassificatieschema van de organisatie. Vaak gaat zo’n schema uit van vertrouwelijkheid, integriteit en beschikbaarheid van de informatie. Labels maken de gevoeligheid en waarde van informatie zichtbaar, zodat passende beveiligingsmaatregelen kunnen worden getroffen.

Rubricering is hierbij ook een subset van classificatie en labeling. Het aanbrengen van rubricering via labeling is dus mogelijk.

4. Rubriceringsniveaus volgens VIRBI

Er zijn vier rubriceringniveaus:

- **Departementaal VERTROUWELIJK** (afgekort Dep. V.);
- **Staatsgeheim CONFIDENTIEE**L (afgekort Stg. C.);

- **Staatsgeheim GEHEIM** (afgekort Stg. G.);
- **Staatsgeheim ZEER GEHEIM** (afgekort Stg. ZG.).

Informatie moet niet onnodig hoog worden gerubriceerd, en moet ook niet onnodig lang gerubriceerd blijven. Dit maakt toepassing van VIRBI effectiever en efficiënter, maakt procedures eenvoudiger en bespaart kosten. Ook voorkomt het onterechte incidenten als informatie bekend wordt die niet of niet meer gerubriceerd had moeten zijn.

Het rubriceringsniveau van de bijzondere informatie wordt bepaald op basis van de **te verwachten nadelige gevolgen** als (een deel van) deze informatie bekend wordt bij niet-geautoriseerden. Dit wordt op basis van **twee criteria** bepaald: **schade en belang**. Dit weer wordt bepaald in een risicoanalyse waarbij wordt gekeken naar waarschijnlijkheid en impact.

Het VIRBI benoemt drie **schadeniveaus**:

- Schade: beperkte nadelige invloed;
- Ernstige schade: nadelige invloed, korte termijn geen alternatieven;
- Zeer ernstige schade: onmisbaar, geen alternatieven mogelijk.

Het VIRBI benoemt de volgende **vitale belangen** die nadelige gevolgen kunnen ondervinden:[1]

- Territoriale veiligheid
- Fysieke veiligheid
- Economische veiligheid
- Ecologische veiligheid
- Sociale en politieke stabiliteit
- Internationale rechtsorde en stabiliteit

Het bovenstaande bevat alle handreikingen die het VIRBI geeft voor rubricering van bijzondere informatie. Dit is relatief kort en bestrijkt niet alle mogelijke situaties. Daarom wordt dit in de volgende paragrafen verder uitgewerkt en toegelicht. Deze uitwerking is echter gemaakt op basis van “best effort” en heeft geen formele status.

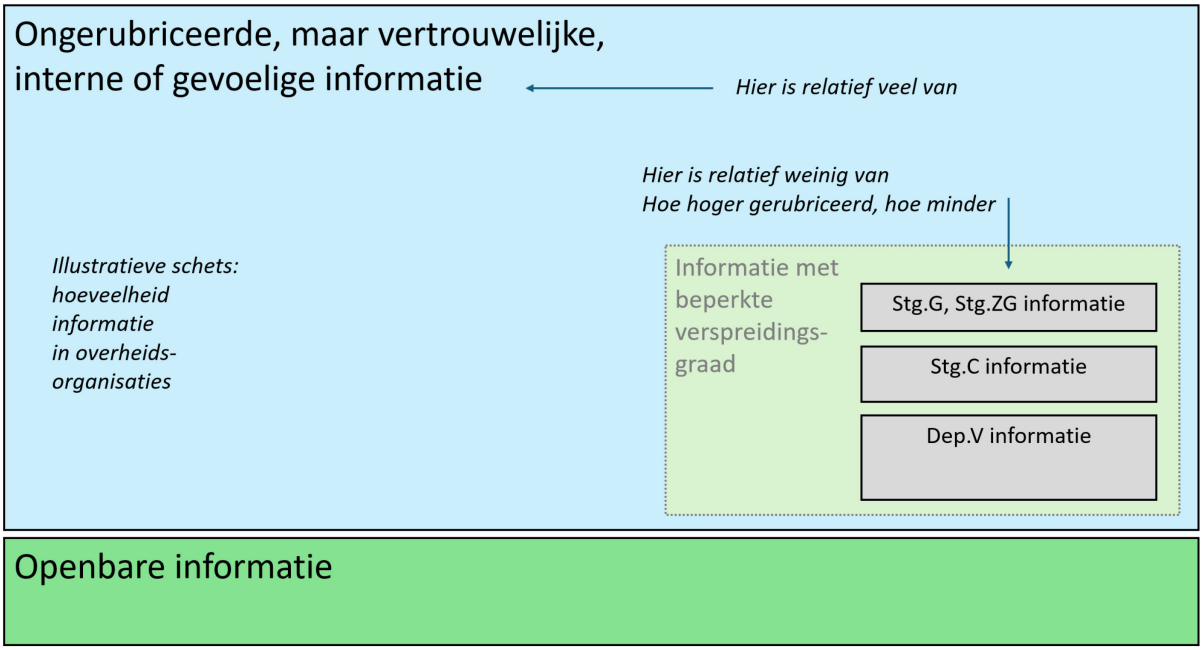
[1] Deze belangen zijn geïntroduceerd in: De Veiligheidsstrategie voor het Koninkrijk der Nederlanden. Deze is gepresenteerd in de Kamerbrief 30 821, nr. 178 over Nationale Veiligheid d.d. 3 april 2023, kst-30821-178. Zij zijn ook gebruikt in de: Rijksbrede Risicoanalyse Nationale Veiligheid, Analistennetwerk Nationale Veiligheid, 2022.

5. Rubriceringsniveaus in context

Naast de vier bovenstaande, formeel vastgestelde rubriceringsniveaus kunnen in de praktijk de volgende niveaus van gevoeligheid en schade worden onderscheiden.[2]

Informatie	Rubricerings-niveau	Schadeniveau	Frequentie van voorkomen
Ongerubriceerd Niet gevoelig Publiceerbaar Openbaar	Ongerubriceerd	Geen impact op individuen, organisaties of nationaal belang	Alle overheids-organisaties bezitten, maken of verwerken deze informatie
Ongerubriceerd Maar gevoelig of intern	Ongerubriceerd Mogelijk een merking of TLP markering	Eenvoudig te herstellen schade voor openbare orde, werking van de overheid, privacy van burgers, organisaties, veiligheid of welzijn van burgers	Alle overheids-organisaties bezitten, maken of verwerken deze informatie

Schematisch kan deze verzameling van informatie als volgt worden weergegeven. Daarbij zijn ook de hoeveelheden van de informatie indicatief geschetst. Bij specifieke organisaties kunnen de hoeveelheden gerubriceerde informatie groter zijn.



[2] Deze tabel en de figuur zijn geïnspireerd op: New Zealand Government Information Security Classification System, Table 1: Classification Levels mapped to Business Impact Levels. Hij is bedoeld als illustratie en heeft geen formele status.

6. Categorieën en voorbeelden van mogelijk rubriceerbare informatie

6.1. In nationale documenten

Binnen de Rijksdienst zijn verschillende handreikingen voor rubricering in omloop. De status van sommige hiervan is duidelijker dan die van andere. [3] [4] [5] [6] [7] De handreikingen komen overeen op hoofdlijnen maar verschillen op details. Soms zijn ze zelfs tegenstrijdig op details. In het algemeen worden de volgende schadevormen en (veiligheids-) belangen genoemd op basis waarvan informatie voor rubricering in aanmerking komt:

Schade	Toelichting
Schade aan de veiligheid van de Staat	Dit omvat de territoriale integriteit, de soevereiniteit en de veiligheid van bondgenoten of internationale organisaties waarbij Nederland is aangesloten.
Schade aan de democratische rechtsorde	Informatie die het functioneren van de rechtspraak, het openbaar bestuur of de grondrechten van burgers kan ondermijnen.
Schade aan de sociale en politieke stabiliteit	Gegevens die kunnen leiden tot maatschappelijke ontwrichting, ernstige openbare ordeproblemen of het wegvallen van het publiek vertrouwen in de overheid.
Economische en financiële schade	Informatie die de vitale economische belangen, de stabiliteit van de financiële sector of de overheidsfinanciën raakt.
Verstoring van de internationale rechtsorde	Informatie die diplomatieke betrekkingen schaadt of de effectiviteit van internationale instituties belemmert.
Gevaar voor de fysieke veiligheid	Informatie waarvan kennisname kan leiden tot dodelijke slachtoffers, gewonden of een gebrek aan primaire levensbehoeften.
Verstoring van vitale infrastructuur	Gegevens over processen die essentieel zijn voor het overleven of het ongestoord functioneren van de samenleving.

[3] Rijksbrede Risicoanalyse Nationale Veiligheid, Analistennetwerk Nationale Veiligheid, Juli 2022, Tabel 1 Nationale veiligheidsbelangen – Dit is een formeel beleidsdocument
[4] De Veiligheidsstrategie voor het Koninkrijk der Nederlanden (2023-2029), Nawerk, Veiligheidsbelangen en impactcriteria – Dit is een formeel beleidsdocument
[5] NCTV Stappenplan Rubricering, ongedateerd - De status van dit document is niet exact bekend, maar de informatie is nuttig.
[6] Handleiding Rubricering, IBR, Versie 1.7, juni 2015 – Dit is een handreiking zonder formele status, maar hij is destijds met zorg opgesteld. De genoemde schadebedragen kunnen intussen verouderd zijn.
[7] Rijksbreed rubriceringsbesluit, Bijlage 1: Voorbeelden standaard informatie, ongedateerd fragment – De status van dit document is niet meer te achterhalen, maar de informatie is nuttig.

Schade	Toelichting
Schending van de persoonlijke levenssfeer	Privacygevoelige informatie van burgers, bewindslieden of leden van het Koninklijk Huis.
Verlies van technologische voorsprong	Informatie over hoogwaardige of sensitieve technologieën die van strategisch belang zijn voor Nederland.

Onder deze categorieën vallen diverse soorten informatie, gegevens en documenten zoals:

Categorie	Toelichting
Defensie en Krijgsmacht	Plannen over de slagkracht van de strijdkrachten, technische gegevens over wapensystemen en militaire plannen.
Regeringszaken	Notulen van de (Rijks)ministerraad, onderraden en ministeriële commissies, evenals besluitenlijsten en persoonlijke zaken van bewindslieden.
Inlichtingen- en Veiligheidsdiensten	Informatie over de effectiviteit van diensten zoals de AIVD of MIVD, operationele methodieken en gegevens over informanten.
Diplomatie	Informatie die diplomatieke relaties kan schaden of internationale spanningen kan vergroten. Strategieën voor internationale onderhandelingen, diplomatieke berichten.
Koninklijk Huis	Gegevens over de eenheid van de Kroon en kwetsbare informatie over (de reizen van) leden van het Koninklijk Huis.
Vitale Infrastructuur	Beveiligingsplannen van vitale objecten en technische blauwdrukken van energie- of waternetwerken.
Opsporing en Recht	Methodieken voor het onderzoek naar zware misdaad en informatie over ernstige inbreuken op de rechtsorde.
Economie en Financiën	Gegevens die wezenlijke materiële schade kunnen toebrengen aan de nationale economie, overheidsfinanciën of handelsbelangen.
Economie en Bedrijfsleven	Concurrentiegevoelige bedrijfsgegevens die onder geheimhouding zijn verstrekt aan de overheid.
Wetenschap en Technologie	Unieke knowhow van kennisinstituten en informatie over 'dual-use' technologieën (die zowel civiel als militair gebruikt kunnen worden).
Persoonsgegevens	Gevoelige informatie over burgers of publieke figuren, zoals opgenomen in datasets van de overheid.

Informatie mag daarbij **nooit** gerubriceerd worden om wettelijke overtredingen, bestuurlijke fouten of inefficiëntie te verbergen.

Daarbij worden de schadevormen en categorieën globaal als volgt verdeeld over de vier rubriceringsniveaus. Dit is echter alleen indicatief, er is geen formeel vastgestelde meetlat:

Rubriceringsniveau	Indicatieve (niet formeel vastgestelde) voorbeelden
Departementaal VERTROUWELIJK (Dep. V) **Aard van de schade:** Nadeel aan de belangen van één of meer ministeries. De maatschappelijke gevolgen zijn beperkt in tijd en omvang.	• Schade aan departementen groter dan €100.000. [Belangrijk, zie voetnoot[8]] • Politieke schade aan een bewindspersoon of verlies van publiek respect. • Informatie over de krijgsmacht met nadelige gevolgen voor slagkracht, informatie over onderhandelingen, en de beveiliging van vitale objecten. • Persoonsgegevens van risicoklasse 2 of hoger.
Staatsgeheim CONFIDENTIEEL (Stg. C) **Aard van de schade:** Schade aan de vitale belangen van de Staat of bondgenoten.	• Schade groter dan €1 miljoen of €500 miljoen (afhankelijk van het gehanteerde schadekader). • Individueel dodelijk slachtoffer. • Reizen van leden van het Koninklijk Huis, besluitenlijsten van de Ministerraad, informatie over zware misdaadonderzoeken, en proliferatierisico's (niet-nucleair).
Staatsgeheim GEHEIM (Stg. G) **Aard van de schade:** Ernstige schade aan vitale belangen.	• Schade aan de economie of Staat groter dan €100 miljoen of €5 miljard. • Aftreden van het kabinet, externe bemiddeling noodzakelijk bij diplomatieke schade. • Groepen dodelijke slachtoffers. • Kwetsbare informatie over het Koninklijk Huis, ernstige aantasting van de slagkracht van de krijgsmacht, proliferatierisico's m.b.t. kernenergie of NBC-wapens, en opsporingsmethodieken voor ernstige inbreuken op de rechtsorde.

[8] De opmerkingen over bedragen, aantallen slachtoffers, risicoklassen etc. hebben geen formele status. Het is dus niet de bedoeling om dit zonder verdere uitwerking als meetlat te gebruiken. Het advies is om dit als inspiratie te gebruiken voor een eigen, bijvoorbeeld departementaal, schadekader. Hierbij kunnen de kwantitatieve indicaties ook door kwalitatieve indicaties vervangen worden (beperkt, ernstig, zeer ernstig, met op de eigen situatie toegeschreven voorbeelden).

Rubriceringsniveau	Indicatieve (niet formeel vastgestelde) voorbeelden
Staatsgeheim ZEER GEHEIM (Stg. ZG) **Aard van de schade:** Zeer ernstige schade aan vitale belangen.	• Schade groter dan €1 miljard of €50 miljard. • Parlementaire crisis, lange termijn schade aan relaties met bondgenoten of het ontstaan van oorlog. • Veel doden. • Aantasting van de eenheid van de Kroon, directe aantasting van de interne stabiliteit, zeer ernstige schade aan de belangen van informanten, en de volledige notulen van de (Rijks)ministerraad.

Het NCSC heeft een methodiek[9] gepubliceerd voor het in kaart brengen van de te beschermen belangen van een organisatie. Dit is zeker nuttig:

- Stap 1: Schep de randvoorwaarden
- Stap 2. Verkrijg mandaat en draagvlak
- Stap 3: Breng de TBB's in kaart
- Stap 4: Onderneem vervolgstappen

Als hulpmiddel heeft het NCSC ook een *Inspiratielijst te beschermen belangen*[10] gepubliceerd. Ook deze is nuttig.

In de *Wet Open Overheid* worden ook categorieën van informatie genoemd die:

- Niet zomaar openbaar gemaakt mogen worden
- Altijd openbaar gemaakt moeten worden

Deze zijn opgesomd in het hoofdstuk over de Woo, later in dit document. Dit is ook nuttige inspiratie.

In de BIO worden ook categorieën van informatie genoemd die extra beveiliging verdienen. Deze zijn opgesomd in het hoofdstuk over de BIO, later in dit document. Dit is ook nuttige inspiratie.

In de *Handleiding Kwetsbaarheidsonderzoek spionage* (KWAS) van de AIVD staat een overzicht van mogelijke te beschermen belangen en ook een bijbehorende methodiek en vragenlijst. [11]

In de Wet politiegegevens, Besluit politiegegevens, Wet justitiële en strafvorderlijke gegevens en Besluit justitiële en strafvorderlijke gegevens worden onder meer de volgende categorieën van informatie genoemd die extra beveiliging verdienen:

[9] https://www.ncsc.nl/risicomanagement/hoe-breng-ik-mijn-te-beschermen-belangen-kaart

[10] https://www.ncsc.nl/api/media/sites/default/files/Inspiratielijst%20te%20beschermen%20belangen.pdf

[11] https://www.aivd.nl/documenten/2011/02/17/handleiding-kwetsbaarheidsonderzoek-spionage

Politiegegevens:

- Gegevens over informanten
- Infiltranten en getuigenbescherming
- Verdachten en veroordeelden.
- Slachtoffers van strafbare feiten of personen van wie wordt vermoed dat zij slachtoffer kunnen worden.
- Derden, zoals getuigen of personen die banden onderhouden met verdachten of slachtoffers.
- Embargo-onderzoeken: Onderzoeken met levensbedreigende risico's, politieke gevoeligheid of publiciteitsgevoeligheid.
- Themaverwerking en inlichtingen: Gegevens van ernstige misdrijven, zoals terrorisme.
- Genetische gegevens en biometrische gegevens (zoals dactyloscopische gegevens of gezichtsafbeeldingen) met het oog op unieke identificatie.

Justitiële en strafvorderlijke gegevens:

- Justitiële gegevens: Persoonsgegevens inzake toepassing van het strafrecht of de strafvordering.
- Strafvorderlijke gegevens: Gegevens van van een strafvorderlijk onderzoek.
- Tenuitvoerleggings-gegevens: Gegevens over strafrechtelijke beslissingen.
- Gerechtelijke strafgegevens: Gegevens van strafzaken.
- Persoonsdossiers: Gedrag of de levensomstandigheden van personen.

De Politie gebruikt de volgende rubriceringsniveaus, die als volgt af te beelden zijn op de VIRBI:

Politie INTERN[12]	Departementaal VERTROUWELIJK
Politie CONFIDENTIEEL	Staatsgeheim CONFIDENTIEEL
Politie GEHEIM	Staatsgeheim GEHEIM
Politie ZEER GEHEIM	Staatsgeheim ZEER GEHEIM

In de Wet op de inlichtingen- en veiligheidsdiensten worden onder meer de volgende categorieën van informatie genoemd die extra beveiliging verdienen:

Categorieën van informatie die ook in andere rubricerings richtlijnen wordt genoemd:

- Gegevens die de eenheid van de Kroon in gevaar kunnen brengen of de nationale veiligheid kunnen schaden.
- Informatie die de relaties van Nederland met andere landen of internationale organisaties ernstig kan schaden.

Specifieke categorieën van informatie:

- Geheime bronnen
- Informanten en agenten
- Middelen en methoden

[12] Informatiebeveiligingsafspraken IWPI (gegevensuitwisseling via de spelverdeler t.b.v. implementatie wet en protocol identiteitsvaststelling), IBA-SRK Versie 1.04 , d.d. 29 augustus 2012

- Actueel kennisniveau
- Kennis over de wijze van versleuteling van gegevens
- Identiteit van medewerkers
- Persoonsgegevens in onderzoeken

De nieuwe teksten over spionage in het Wetboek van Strafrecht impliceren dat de volgende categorieën van informatie extra zorg verdienen:[13]

- Informatie betreffende de nationale veiligheid, de veiligheid van personen, vitale infrastructuur en hoogwaardige technologieën.
- Gevoelige bedrijfsinformatie die een ander land kan misbruiken.
- Persoonsgegevens, in het bijzonder over diaspora.
- Gevoelige informatie over een bepaalde economische sector.
- Gevoelige informatie rondom politieke besluitvorming.
- Informatie die gebruikt kan worden om politieke processen te beïnvloeden, de Nederlandse economie te verzwakken of bondgenoten tegen elkaar uit te spelen.

De NIS2-richtlijn (Richtlijn (EU) 2022/2555) beschouwt informatie als beveiligingswaardig wanneer hun verlies of aantasting de werking van de interne markt, de economie of de samenleving kan ontregelen. Categorieen zijn ondermeer:

- Gerubriceerde en gevoelige overheidsinformatie.
- Incident- en dreigingsinformatie.
- Bedrijfs- en handelsgeheimen.
- Persoonsgegevens, waaronder ook IP-adressen, domeinnamen, E-mailadressen en telefoonnummers.
- Gegevens in netwerk- en informatiesystemen.
- Registratie- en infrastructuurgegevens waaronder ook domeinnaam registratiegegevens.

In het voorstel voor de Wet weerbaarheid kritieke entiteiten (Wwke), die voortvloeit uit de Europese CER-richtlijn, worden verschillende informatiecategorieën als vertrouwelijk en beveiligingswaardig aangemerkt:

- Veiligheids- en commerciële belangen
- Nationale veiligheid en defensie
- Gevoelige informatie over de infrastructuur
- Risicobeoordelingen
- Incidentgegevens
- Personeels- en screeninggegevens
- Persoonsgegevens

[13] Vanaf 15 mei: meer vormen van spionage strafbaar | Nieuwsbericht | Rijksoverheid.nl

In enkele niet geformaliseerde documenten[14] [15] worden belangen genoemd waarbij rubricering niet zou moeten plaatsvinden. Deze hebben geen formele status maar zijn nuttig als inspiratie.

- Rubricering en de daaruit voortkomende beveiligingsmaatregelen worden toegepast waar risico's bestaan die met goed management niet anderszins weg te nemen zijn.
- Informatie wordt daarom nimmer gerubriceerd teneinde:
    - wettelijke overtredingen, inefficiëntie of bestuurlijke fouten te verbergen;
    - open concurrentie onnodig te beperken; of
    - om de vrijgave te voorkomen of uit te stellen van informatie de geen bescherming nodig heeft in het kader van de belangen van de Staat of zijn bondgenoten.
- Informatie uit openbaar wetenschappelijk onderzoek die niet evident samenhangt met nationale veiligheid wordt niet gerubriceerd.

6.2. In buitenlandse documenten

Naast Nederland hebben alle andere westerse landen ook gerubriceerde informatie en rubriceringsrichtlijnen. In sommige gevallen zijn deze richtlijnen ook wettelijk vastgelegd. [16] [17] [18] [19] [20] [21] [22] [23] Hoewel terminologie en niveaus per land verschillen, zijn de onderliggende gedachten consistent. Hoewel dit geen formele status heeft in de Nederlandse context, is dit is nuttige inspiratie.

Ook hier wordt informatie gerubriceerd op basis van de mogelijke schade die kan ontstaan als zij ongeautoriseerd wordt ingezien, gewijzigd of openbaar gemaakt. De

[14] Referentiekader Rubricering, auteur niet bekend, ongedateerd
[15] Leidraad Rubriceren, auteur niet bekend, ongedateerd
[16] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, ZÁKON 412/2005 Sb., ze dne 21. září 2005 [Tsjechische Republiek]
[17] The President Executive Order 13526, Classified National Security Information, December 29, 2009 [Verenigde Staten]
[18] Issuer: Riigikogu, In force from: 01.09.2025, State Secrets and Classified Information of Foreign States Act [Estland]
[19] Code of Federal Regulations, Part 2001 Classified National Security Information and Markings [Verenigde Staten]
[20] Dz. U. 2010 Nr 182 poz. 1228, USTAWA z dnia 5 sierpnia 2010 r., o ochronie informacji niejawnych [Polen]
[21] BESLUIT (EU, Euratom) 2015/444 VAN DE COMMISSIE van 13 maart 2015 betreffende de veiligheidsvoorschriften voor de bescherming van gerubriceerde EU-informatie [EU]
[22] Cabinet Office, Government Security Classifications Policy, 5 August 2024 [Verenigd Koninkrijk]
[23] CCN-STIC-822, Procedimientos de Seguridad en el ENS. Anexo II., PROCEDIMIENTO DE CLASIFICACIÓN Y TRATAMIENTO DE LA INFORMACIÓN CLASIFICADA, PR20 [Spanje]

kernvraag is steeds: wat is de impact van verlies van vertrouwelijkheid, integriteit of beschikbaarheid? Rubricering is daarbij:

- **Contextafhankelijk** (dezelfde informatie kan in een andere context anders worden beoordeeld)
- **Tijdgebonden** (gevoeligheid kan afnemen of verdwijnen)
- **Proportioneel** (zwaardere bescherming alleen waar nodig)
- Rubricering is **impact-gedreven**, niet document- of systeem-gedreven
- De **hoogste niveaus** zijn gereserveerd voor **uitzonderlijke schade** aan de staat
- Het **merendeel** van overheidsinformatie valt in de **laagste categorieën**, mits correct beheerd
- **Over-rubricering** wordt expliciet gezien als een **risico** voor transparantie en effectiviteit

Daarbij worden de volgende categorieën onderscheiden:

Categorieën	Voorbeelden
Nationale Veiligheid en Defensie Informatie waarvan de onthulling de veiligheid, soevereiniteit of territoriale integriteit van de staat kan schaden.	• **Militaire plannen**, operaties en paraatheid. • Informatie over **wapensystemen**, munitie en militaire geografische data. • **(Militaire) Inlichtingencapaciteiten**, bronnen, methoden en lopende operaties. • Plannen voor nationale verdediging en **mobilisatie**.
Internationale Betrekkingen en Diplomatieke Informatie Informatie die essentieel is voor de diplomatieke relaties of die in vertrouwen is ontvangen van andere staten of internationale organisaties.	• **Diplomatieke correspondentie** en verslagen van internationale bijeenkomsten. • Informatie die door **bondgenoten of internationale organisaties** (zoals de NAVO of EU) onder geheimhouding is verstrekt. • **Onderhandelingsposities** in internationale verdragen of geschillen.
Openbare Orde en Wetshandhaving Het voorkomen van criminaliteit, het handhaven van de wet en de bescherming van de rechtsgang.	• Tactieken en methoden voor **surveillance** en de identiteit van undercoveragenten. • Informatie over **getuigenbeschermings-programma's** en de identiteit van kroongetuigen. • Lopende **strafrechtelijke onderzoeken** en informatie over de vervolging van georganiseerde misdaad of terrorisme.

Categorieën	Voorbeelden
Individuele Privacy en Veiligheid Gegevens waarvan de openbaarmaking de privacy van burgers kan schenden of de fysieke veiligheid van individuen in gevaar kan brengen.	• **Persoonsgegevens** zoals adressen, geboortedata en unieke identificatienummers (bijv. BSN). • **Medische informatie** en dossiers over de geestelijke of lichamelijke gezondheid. • Informatie die kan leiden tot de **identificatie van menselijke bronnen** of agenten, wat hun leven kan bedreigen.
Economische, Financiële en Commerciële Belangen Informatie die schade kan toebrengen aan de economie van de staat, de stabiliteit van financiële markten of de commerciële belangen van de overheid en partners.	• **Marktgevoelige informatie** die invloed kan hebben op aandelenkoersen of valutamarkten (bijv. rentebesluiten van de centrale bank). • **Commerciële geheimen** en intellectueel eigendom (patenten) verkregen tijdens aanbestedingen of onderzoek. • Informatie over de import en export van **strategische goederen**.
Interne Overheidsprocessen en Juridische Privileges Bescherming van de onafhankelijke besluitvorming binnen de overheid en informatie die juridisch beschermd is.	• **Legal Professional Privilege (LPP)**: Vertrouwelijke communicatie tussen een overheidsorgaan en zijn juridisch adviseurs. • **Beleidsconcepten en interne beraadslagingen** waarvan de publicatie het besluitvormingsproces zou ondermijnen. • **HR- en managementinformatie** over het personeelsbestand waar individuen identificeerbaar zijn.
Infrastructuur en Informatiebeveiliging Gegevens over de beveiliging van vitale objecten en de technische systemen die worden gebruikt om gerubriceerde informatie te beschermen.	• Plannen en technische specificaties van **beveiligingssystemen voor overheidsgebouwen** en vitale infrastructuur. • **Cryptografische materialen**, sleutels en algoritmen. • Kwetsbaarheidsanalyses van **communicatie- en informatiesystemen** (CIS).

Daarbij worden de schadevormen en categorieën globaal als volgt verdeeld over de vier rubriceringsniveaus. Daarbij kan de naamgeving en indeling van de rubriceringsniveaus op detail verschillen van de Nederlandse indeling. Dit heeft daarom geen formele status in de Nederlandse context maar kan nuttige inspiratie zijn:

Rubriceringsniveaus (vergelijkbaar met Nederlandse context)	Voorbeelden
Departementaal Vertrouwelijk (Dep.V) Onthulling is **nadelig** voor de belangen van de staat of organisatie. Het gaat vaak om kortstondige of beperkte negatieve effecten.[24]	• **Interne Overheidsprocessen:** Interne werkdocumenten, concepten en verslagen die nog niet voor publicatie geschikt zijn. • **Openbare Orde:** Informatie over routinematige veiligheidskwesties die zonder escalatie beheerd kunnen worden. • **Individuele Privacy:** Basis-persoonsgegevens die bij lekken ongemak veroorzaken maar geen directe fysieke dreiging vormen. • **Infrastructuur:** Gebruikte radiofrequenties voor routine-communicatie of technische details van niet-kritieke IT-systemen.
Staatsgeheim Confidentieel (Stg.C) Onthulling kan de belangen van de staat **schaden**. Dit niveau wordt gebruikt voor informatie die een aanzienlijke verstoring van de nationale veiligheid zou betekenen.	• **Internationale Betrekkingen:** Diplomatieke correspondentie die de relatie met een partnerland materieel kan schaden. • **Economische Belangen:** Informatie over commerciële onderhandelingen of strategische industriële belangen. • **Individuele Veiligheid:** Medische gegevens of identiteitsgegevens die bij onthulling de persoonlijke veiligheid in gevaar brengen. • **Defensie:** Tactische gegevens van wapensystemen (bijv. kustverdediging) en metingen van magnetische velden van militaire vaartuigen.
Staatsgeheim Geheim (Stg.G) Onthulling kan de belangen van de staat **ernstige schade** toebrengen.	• **Nationale Veiligheid en Defensie:** Operationele plannen van de strijdkrachten en specifieke inzetmethoden van special forces. • **Inlichtingen:** Waardevolle inlichtingenoperaties, bronnen en methoden (zoals cryptografische sleutels voor hoge niveaus). • **Internationale Betrekkingen:** Informatie die een ernstige toename van internationale spanningen of formele protesten kan veroorzaken. • **Openbare Orde:** Ernstige belemmering van het onderzoek naar georganiseerde misdaad of terrorisme.

[24] Let op: Hier zijn de omschrijvingen van de rubriceringsniveaus gebaseerd op de samenvatting van de buitenlandse documenten. Deze heeft geen formele geldigheid in de Nederlandse nationale context.

Rubriceringsniveaus (vergelijkbaar met Nederlandse context)	Voorbeelden
Staatsgeheim Zeer Geheim (Stg.ZG) Onthulling kan de wezenlijke belangen van de staat **uitzonderlijk ernstig schaden**. Vaak betreft dit onherstelbare of langdurige schade.	• **Nationale Veiligheid:** Bedreigingen voor de soevereiniteit, territoriale integriteit of het voortbestaan van de democratische orde. • **Defensie:** Het nationale defensieplan (alarmplan) of plannen voor mobilisatie bij oorlog. • **Inlichtingen:** Identificatie van undercoveragenten in vijandige omgevingen of zeer gevoelige onderscheppingsmethoden (SIGINT). • **Economie en Volksgezondheid:** Informatie die wijdverspreid verlies van levens of catastrofale schade aan de gehele nationale economie veroorzaakt.

7. Omgaan met bestaande rubricering

Bijzondere informatie van internationale herkomst behoudt zijn oorspronkelijke rubricering. Dit houdt in dat de oorspronkelijke rubricering niet verlaagd mag worden door een Nederlandse rubricering.

7.1. Multilateraal

Met betrekking tot NAVO en EU informatie wordt de volgende vergelijkingstabel gehanteerd om tot het vergelijkbaar nationaal niveau te komen. Voor informatie die bilateraal uit andere landen wordt ontvangen, wordt dit conform de bilaterale overeenkomst behandeld. Als er geen bilaterale overeenkomst is, kan middels de tabel een vergelijkbaar nationaal niveau bepaald worden voor de rubricering, in afstemming met de verstrekker of eigenaar van de informatie.

Nederland [25]	NAVO[26]	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

7.2. Bilateraal

Door middel van reen bilateraal beveiligingsverdrag regelen het Koninkrijk der Nederlanden en een bevriend land dat nationale gerubriceerde gegevens die onderling worden uitgewisseld een vergelijkbaar niveau van beveiliging ontvangen. Naast maatregelen voor de beveiliging van nationale gerubriceerde gegevens valt daaronder tevens de strafbaarstelling in het geval van compromittering van nationale gerubriceerde gegevens. Een bilateraal beveiligingsverdrag maakt de uitwisseling van nationale gerubriceerde gegevens mogelijk, maar verplicht beide landen daar niet toe.

Er zijn vele beveiligingsverdragen afgesloten, recent bijvoorbeeld met: Finland, Spanje, Republiek Polen, Slowaakse Republiek, België, Republiek Letland, Portugese Republiek, etc.

In een bilateraal beveiligingsverdrag wordt in het algemeen een vergelijkingstabel opgenomen tussen de nationale rubriceringsniveaus van beide landen, bijvoorbeeld:[27]

For the Kingdom of Spain	For the Kingdom of the Netherlands
SECRETO	Stg ZEER GEHEIM
RESERVADO	Stg GEHEIM
CONFIDENCIAL	Stg CONFIDENTIEEL
DIFUSIÓN LIMITADA	DEPARTEMENTAAL VERTROUWELIJK

[25] Zie: VIRBI, Tabel 1. Vergelijking tussen nationale rubriceringsniveaus en NAVO- en EU-rubriceringsniveaus.
[26] Verdrag tussen de Partijen bij het Noord-Atlantisch Verdrag inzake de beveiliging van gegevens, Brussel, 6 maart 1997
[27] Verdrag tussen het Koninkrijk der Nederlanden en het Koninkrijk Spanje inzake de uitwisseling en wederzijdse beveiliging van gerubriceerde gegevens, Madrid, 23 september 2021

De Rijksoverheid kan informatie alleen rubriceren volgens het nationale model (Dep.V, Stg.C, Stg.G, Stg.ZG). De Rijksoverheid kan zelf dus geen informatie maken met een internationale, multilaterale of bilaterale rubricering.
Als NL gerubriceerde informatie naar internationale partners gaat, dan wordt deze voorzien van de nationale rubricering eventueel aangevuld met een merking als "Releasable to <land, organisatie>".
De ontvangende partner kan daarmee vervolgens nagaan hoe de Nederlandse rubricering in zijn rubricerings- en beveiligingscontext past.

8. Bepalen rubriceringsduur

Rubriceringen worden verbonden aan een maximum tijdsverloop of aan een bepaalde gebeurtenis. Hoewel de duur per geval kan verschillen, noemen de bronnen een termijn van **10 jaar als het uitgangspunt** voor de rubriceringsduur. In principe moet daarom uiterlijk **tien jaar na vaststelling** onderzocht worden of de rubricering herzien of beëindigd kan worden.

In het VIRBI wordt het aangeven van de rubriceringsduur verplicht gesteld.
In de huidige praktijk is het gangbaar om de rubricering en merking aan te geven, maar het is nog niet gangbaar om hierbij ook een rubriceringsduur aan te geven.

In buitenlandse documenten worden de volgende voorbeelden gegeven van rubricering die aan tijd of omstandigheden is gebonden. Dit kan ook bruikbaar zijn in de Nederlandse context:

- Declassify On: 20201014. (specifieke datum). (VS)
- Declassify On: Completion of Operation. (specifieke gebeurtenis). (VS)
- Die VS-Einstufung endet mit Ablauf des Jahres XXXX. (Duitsland)
- Een rubricering kan geldig zijn tot de afkondiging van de mobilisatie. (Estland)
- Zonder de bijlage is de rubricering XXXX (fysieke handeling). (EU)

9. Merking

In de systematiek van de Rijksdienst is er een essentieel verschil tussen **rubricering** en **merking**, hoewel ze vaak in combinatie worden gebruikt om informatie te beschermen. Rubricering bepaalt het niveau van geheimhouding op basis van de verwachte schade, terwijl een merking extra instructies geeft over de specifieke behandeling of de doelgroep van de informatie.

Merkingen staan echter los van de rubricering van de informatie en daarom is dit onderwerp niet uitgebreid beschreven in het VIRBI. Maar het is wel relevant om toe te

lichten. Een belangrijk detail is dat informatie een merking kan hebben zonder officieel gerubriceerd te zijn.

Het doel van merking is het geven van **nadere aanwijzingen voor de behandeling** van de informatie of het beperken van de kring van geautoriseerden tot een specifieke groep. De kernvraag is: Wie precies mag dit zien en hoe moeten zij ermee omgaan?

Merkingen worden vaak toegevoegd als **aanvulling op de rubricering** door de opsteller. Het proces is niet gebonden aan een formele schadeberekening en vloeit vaak direct voort uit de aard van de gegevens (bijv. alle medische gegevens krijgen de merking "Medisch geheim").

9.1. TLP

Een veelgebruikte merking bij ongerubriceerde informatie is het “Traffic Light Protocol” (TLP). [28] Dit geeft nadere aanwijzingen voor het delen en verspreiden van de informatie. Voorbeelden van enkele merkingen hiervan zijn:

Merking	Toelichting
TLP:RED	Bij een rood licht, ofwel TLP:RED mag de ontvanger of de ontvangers de informatie alleen delen met de informatieverstrekker en met de mede ontvangers.
TLP:AMBER TLP:AMBER+STRICT	TLP:AMBER: geeft aan dat de informatie alleen gedeeld mag worden binnen de ontvangende organisatie of met diens klanten. Hierbij geldt het “need to know’-principe. TLP:AMBER+STRICT mag bovendien niet gedeeld worden met klanten of leveranciers.

9.2. ABDO

Voorbeelden van enkele merkingen uit de ABDO 2019 [29] zijn onder meer de volgende. Deze kunnen gecombineerd worden met een rubricering.

Merking	Toelichting
ONGERUBRICEERD	Ongerubriceerde Informatie, maar niet zonder meer bedoeld voor brede kennisname (“Need-to-Know”).
PERSONEELS-VERTROUWELIJK	Aangebracht op Informatie met persoonsgegevens. Kennisname door niet-gerechtigden kan de belangen van een persoon schaden.
COMMERCIEEL VERTROUWELIJK	Aangebracht op Informatie met bedrijfs- en fabricagegegevens. Kennisname door niet-gerechtigden kunnen de belangen van het bedrijf of de Staat schaden.

[28] NCSC - Traffic Light Protocol (TLP): informatie op een veilige manier delen
[29] ABDO, Algemene Beveiligingseisen voor Defensieopdrachten 2019

Merking	Toelichting
MEDISCH GEHEIM	Aangebracht op Informatie over de lichamelijke of geestelijke gesteldheid van een persoon. Kennisname door niet-gerechtigden kan de belangen van een persoon schaden.
CRYPTOGRAFISCH MATERIAAL (vaak bij gerubriceerde informatie)	Aangebracht op gerubriceerde Informatie die betrekking heeft op gerubriceerd cryptografisch sleutelmateriaal. Deze Informatie mag alleen worden behandeld door personen die als crypto-custodian zijn geregistreerd. Kennisname door niet gerechtigden kan bijdragen aan het ontcijferen van vercijferde informatie door niet-gerechtigden.

9.3. Internationale merking in Nederlandse context

Op internationale gerubriceerde en ongerubriceerde informatie kan ook merking zijn aangebracht. Het doel hiervan is hetzelfde als bij nationale informatie namelijk:

- **Descriptoren:** Termen die worden gebruikt om bepaalde categorieën informatie met speciale gevoeligheden te identificeren (bijv. *PERSONAL DATA* of *COMMERCIAL*). Eventueel om aan te geven dat informatie ongerubriceerd is maar desondanks niet onbeperkt publiceerbaar is (bijv. LIMITÉ, NATO UNCLASSIFIED).
- **Hanteringsinstructies:** Specifieke aanwijzingen over wie de informatie mag inzien of hoe deze moet worden verspreid (bijv. *RECIPIENTS ONLY, RELEASABLE TO NORWAY*).
- **Nationale kanttekeningen (Caveats):** Gebruikt om de verspreiding te beperken tot onderdanen van specifieke landen (bijv. *UK EYES ONLY*).

Voor de Nederlandse context geldt hierbij:

- Wanneer een oorspronkelijke rubricering wordt gevolgd door een ‘Vrij te geven aan’- of ‘Releasable to (REL)’-merking, dan wordt deze merking gehandhaafd.

10. Aanbrengen rubricering

Gerubriceerde informatie moet worden voorzien van een passend niveau van rubricering. De opsteller brengt de rubricering (en eventueel rubriceringsduur en merking) aan op de informatie.,

10.1. Aanwijzingen ABDO en ABRO

Omdat het begrip informatie in het VIRBI vele verschijningsvormen kent, zijn er ook verschillende manieren van het aanbrengen van de rubricering. ABDO en ABRO [30] [31] geven hier de volgende aanwijzingen:

De rubricering wordt op de volgende manier fysiek of digitaal op papier, documenten, gegevensdragers en systemen geplaatst:

- **Documenten:** De rubricering moet aan de **boven- en onderkant van elke bladzijde** worden aangebracht, evenals op de omslag en eventuele bijlagen. Als een document verschillende rubriceringsniveaus bevat, wordt de **hoogste rubricering** op elke bladzijde vermeld. Daarnaast wordt aan het begin van **iedere alinea** de bijbehorende afkorting (bijv. Stg. G) geplaatst.
- **Verwijderbare gegevensdragers:** Deze worden voorzien van een sticker, gravure of tekst met watervaste stift die het hoogste niveau van de opgeslagen informatie aangeeft.
- **Werkstations en laptops:** Rubriceringsstickers worden aangebracht op de **systeemkast** en de **bovenzijde van het beeldscherm** (of de klep van een laptop).
- **Digitale informatie** (zoals e-mail of gegevensverzamelingen): De rubricering wordt als **metadata** meegegeven of samen met de informatie verzonden, zodat het ontvangende systeem of de gebruiker direct op de hoogte is van het rubriceringsniveau.

Het VIRBI is een interne regeling die uitsluitend geldt voor de Rijksdienst zelf (ministeries, uitvoeringsorganisaties en ZBO's). De ABDO en ABRO zijn eisen die contractueel worden opgelegd aan private partijen en leveranciers buiten de overheid. Doel en scope zijn dus verschillend en ABDO en ABRO geven geen verplichtingen aan de Rijksdienst zelf. Maar de ABDO en ABRO lopen op veel punten gelijk met interne regelgeving zoals BIO en VIRBI en zijn dus bruikbaar als inspiratie en nadere invulling van eisen.

11. Aggregatie

De toelichting bij Lid 1 en Lid 3 van het VIRBI zegt het volgende, maar werkt dit niet verder uit:

- Door aggregatie van bijzondere informatie ontstaat er een (digitale) en vaak gedecentraliseerde database, waarin bundeling, aggregatie of combinatie van

[30] ABDO, Algemene Beveiligingseisen voor Defensieopdrachten 2019
[31] STAATSCOURANT, Nr. 42214, 9 december 2025, ABRO 2026, Algemene Beveiligingseisen voor Rijksoverheidsopdrachten 2026, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

informatie kan leiden tot een **vergroting van mogelijke schade** en daarmee ook het **rubriceringsniveau** en de bijhorende **maatregelen**.
- De eisen aan een verwerking kunnen ook voortkomen uit de risico's gepaard gaande met aggregatie of verrijking van gegevens in de verwerking.

De rubricering en beveiliging van een aggregatie van bijzondere informatie blijft een lastig punt. In de praktijk kan dit tot uitgebreide discussie leiden. Er zijn verschillende keuzes mogelijk, die allemaal consistent zijn met de huidige tekst van het VIRBI. Zie de nationale en internationale voorbeelden hieronder. Waarschijnlijk is dit een keuze die op "case by case" basis genomen moet worden. Een gedachte die uit ABRO kan worden overgenomen is dat dit "binnen redelijke grenzen" moet gebeuren.

11.1. Aanwijzingen ABDO en ABRO

In ABDO en ABRO wordt hierover het volgende gezegd. Dit is echter geen formeel voorschrift in de context van de VIRBI. Dit is in alle gevallen situationeel maatwerk en geen a-priori vereiste:

- Wanneer … alle personeelsgegevens van een departement op straat komen, kan de bedrijfsvoering van het hele departement schade oplopen. Daarom zal een verzameling personeelsgegevens in soms hoger gerubriceerd en zwaarder beveiligd moeten worden. Dit is in alle gevallen maatwerk.
- Op het moment dat meerdere gerubriceerde processen op dezelfde infrastructuur worden verwerkt, kan er sprake zijn een grote concentratie van te beschermen belangen. In geval van compromittatie is de schade aanzienlijk groter. Dit kan ertoe leiden dat de infrastructuur hoger gerubriceerd en zwaarder beveiligd moet worden. Dit is in alle gevallen maatwerk.
- In geval van … kennisaggregatie, kunnen **binnen redelijke grenzen** additionele organisatorische, personele, fysieke of cyber- beveiligingsmaatregelen worden voorgeschreven.
- Systemen waarop zich een grote concentratie van TBB bevindt op rubriceringsniveau RN, zijn geplaatst in een ruimte die op TBB niveau RN+1 is beveiligd.
- Grote concentraties Staatsgeheimen op één locatie kunnen aanleiding zijn om die locatie bij Koninklijk Besluit te benoemen tot een Verboden Plaats. Een Verboden Plaats wordt op TBB 1-niveau beveiligd.

11.2. In internationale documenten

Internationale bronnen stellen ook dat de aggregatie van informatie (het verzamelen of bundelen van verschillende gegevens) de gevoeligheid van het geheel kan verhogen, wat kan leiden tot een hogere rubricering of de noodzaak voor striktere beveiligingsmaatregelen. Hierbij wordt vaak de keuze gelaten tussen:

- Het rubriceringsniveau gelijk houden voor de geaggregeerde verzameling (RN) maar de beveiligingsmaatregelen verhogen naar een hoger niveau. Dit zijn dan maatregelen passend bij het volgende, hogere rubriceringsniveau (RN+1).
- Het rubriceringsniveau en de beveiligingsmaatregelen beide verhogen (RN+1).

Een Canadese richtlijn stelt dat naarmate het aantal 'assets' toeneemt, de schade bij een compromis ook kan groeien. Een voorbeeld is een lijst met adressen: één adres kan 'Protected A' zijn, terwijl een lijst van 10.000 adressen 'Protected B' kan worden.[32] Hoewel dit geen formele status heeft in de Nederlandse context, is dit is nuttige inspiratie.

12. Beëindigen en herzien van rubricering

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.

Uitsluitend de functionaris die de rubricering heeft vastgesteld, zijn ambtsopvolger of een daartoe door de secretaris-generaal aangewezen functionaris is bevoegd de rubricering te herzien of te beëindigen. Derubriceren kan ook plaatsvinden na de periodieke toetsing en evaluatie. De lijnmanager is verantwoordelijk voor de periodieke toetsing en evaluatie. Op informatie die langdurig bewaard wordt is de archiefwet van toepassing.

Bijzondere informatie die krachtens een verdrag is verkregen, heeft per definitie een niet- Nederlandse rubricering. Indien de informatie niet meer nodig is, kan deze worden teruggestuurd of worden vernietigd, overeenkomstig het verdrag.

12.1. Overbrengen naar archief

Het algemene uitgangspunt is dat de rubricering van bijzondere informatie vervalt op het moment dat deze wordt overgebracht naar een rijksarchiefbewaarplaats. Dit hangt samen met de Archiefwet 1995 [33], die bepaalt dat archiefbescheiden in een bewaarplaats in principe openbaar zijn.

Archiefdiensten stellen de meeste informatie openbaar beschikbaar, zowel online als in hun studiezalen. Soms blijft bepaalde informatie tijdelijk geheim, bijvoorbeeld uit privacyoverwegingen of om de staatsveiligheid te beschermen. In die gevallen kunnen

[32] Do you work with sensitive information? - Canada.ca
[33] Archiefwet 1995, Wet van 28 april 1995, houdende vervanging van de Archiefwet 1962 (Stb. 313) en in verband daarmede wijziging van enige andere wetten.

mensen de documenten niet direct inzien of alleen op aanvraag en onder bepaalde voorwaarden.

Hoewel de rubricering dus normaliter vervalt, kan de zorgdrager (de minister) besluiten dat de rubricering gehandhaafd of herzien moet blijven. Dit gebeurt op basis van de volgende stappen:

- De zorgdrager moet advies inwinnen bij de **algemene rijksarchivaris** en de **rubriceringsambtenaar**.
- Beperkingen aan de openbaarheid kunnen alleen worden gesteld voor een bepaalde termijn en met het oog op de **veiligheid van de Staat of zijn bondgenoten**, de eerbiediging van de persoonlijke levenssfeer, of het voorkomen van onredelijke benadeling van andere belangen.
- Het besluit om de openbaarheid te beperken moet worden gevoegd bij de verklaring van overbrenging.

In de huidige Archiefwet worden de volgende termijnen genoemd:

- **Standaardtermijn overbrenging 20 jaar:** De zorgdrager is verplicht archiefbescheiden die voor blijvende bewaring in aanmerking komen over te brengen wanneer ze ouder zijn dan twintig jaar.
- **Uiterste termijn overbrenging 30 jaar:** Deze overbrenging moet uiterlijk plaatsvinden binnen tien jaar nadat de bescheiden de leeftijd van twintig jaar hebben bereikt (dus wanneer ze 30 jaar oud zijn).
- **Openbaarheid na 75 jaar:** Beperkingen aan de openbaarheid die zijn gesteld bij overbrenging, vervallen in principe wanneer de archiefbescheiden ouder zijn dan 75 jaar, tenzij de minister anders beslist.

In de nieuwe archiefwet wordt deze termijn verkort de overbrengingstermijn tot 10 jaar.[34]

12.2. Wet Open Overheid

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 gederubriceerd, moeten deze onleesbaar worden gemaakt.

[34] Nieuwe archiefwet aangenomen door Tweede Kamer | Open Overheid

12.2.1. Informatie die niet zomaar openbaar gemaakt mag worden

Voor de volgende categorieën informatie worden in de Woo[35] uitzonderingen gemaakt op basis van mogelijke schade. Dit is dus ook nuttige inspiratie bij afwegingen over rubricering.

Het openbaar maken van informatie ingevolge de Woo blijft achterwege voor zover dit:

- de eenheid van de Kroon in gevaar zou kunnen brengen;
- de veiligheid van de Staat zou kunnen schaden;
- bedrijfs- en fabricagegegevens betreft die door natuurlijke personen of rechtspersonen vertrouwelijk aan de overheid zijn meegedeeld;
- persoonsgegevens betreft als bedoeld in … de Uitvoeringswet Algemene verordening gegevensbescherming … ;
- nummers betreft die dienen ter identificatie van personen die bij wet of algemene maatregel van bestuur zijn voorgeschreven … in de Uitvoeringswet Algemene verordening gegevensbescherming … .

Het openbaar maken van informatie blijft eveneens achterwege voor zover het belang daarvan niet opweegt tegen de volgende belangen:

- de betrekkingen van Nederland met andere landen en staten en met internationale organisaties;
- de economische of financiële belangen van de Staat, andere publiekrechtelijke lichamen of bestuursorganen, in geval van milieu-informatie slechts voor zover de informatie betrekking heeft op handelingen met een vertrouwelijk karakter;
- de opsporing en vervolging van strafbare feiten;
- de inspectie, controle en toezicht door bestuursorganen;
- de eerbiediging van de persoonlijke levenssfeer;
- de bescherming van … concurrentiegevoelige bedrijfs- en fabricagegegevens;
- de bescherming van het milieu waarop deze informatie betrekking heeft;
- de beveiliging van personen en bedrijven en het voorkomen van sabotage;
- het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen.

[35] Wet open overheid, Wet van 25 oktober 2021, houdende regels over de toegankelijkheid van informatie van publiek belang (Wet open overheid).

12.2.2. Informatie die openbaar moet zijn

Dit zijn de soorten informatie die de overheid uit zichzelf openbaar moet maken en die dus niet in aanmerking komen voor rubricering:[36]

- Wetten en andere regels;
- Andere besluiten die voor iedereen gelden (besluiten van algemene strekking);
- Ontwerpen van wetten, voorschriften en besluiten waarover advies is gevraagd;
- Inzicht in de organisatie en werkwijze, zoals de taken en bevoegdheden van overheidsorganisaties;
- Hoe mensen de overheid kunnen bereiken en hoe zij informatie kunnen opvragen;
- Documenten bedoeld voor behandeling in de Kamer, de Provinciale Staten, de gemeenteraad of het algemeen bestuur van een waterschap;
- Vergaderstukken en verslagen van de Eerste en Tweede Kamer en hun commissies, en van de verenigde vergadering van de Staten-Generaal;
- Vergaderstukken en verslagen van Provinciale Staten, gemeenteraden en algemene besturen van waterschappen; Toetsing Regeldruk
- Agenda's en besluitenlijsten van de vergaderingen van de ministerraad, gedeputeerde staten, colleges van burgemeester en wethouders en dagelijkse besturen van waterschappen;
- Adviezen over ontwerpen van wetten en regels, en van adviescolleges (zoals het) of adviescommissies (bijvoorbeeld van gemeenten);
- Afspraken van de overheid met andere organisaties, bijvoorbeeld met andere overheden, bedrijven of maatschappelijke organisaties (convenanten);
- Jaarplannen en jaarverslagen;
- Overeenkomsten voor het verstrekken van subsidies , bijvoorbeeld voor ontwikkelingshulp;
- Woo-verzoeken, met daarbij het besluit en de verstrekte informatie;
- Onderzoeksrapporten van ambtenaren of andere organisaties;
- Besluiten die de overheid neemt, zoals een vergunning voor een bedrijf of burger (beschikkingen);
- Schriftelijke oordelen in klachtprocedures.

12.3. Vernietiging

Bij het vernietigen of wissen van informatie wordt de informatie onherstelbaar verwijderd of onbeschikbaar gemaakt. Hierbij wordt gecontroleerd of alle informatie onherstelbaar verwijderd is. Hiervan wordt verslag gemaakt.[37]

---

[36] Hoofdlijnen Wet open overheid | Wet open overheid (Woo) | Rijksoverheid.nl
[37] BASELINE INFORMATIEBEVEILIGING OVERHEID 2, BIO 2, 24 september 2025, versie 1.2 definitief

Vernietiging voor hogere rubriceringen vraagt een speciale aanpak:

- Af te stoten gegevensdragers worden fysiek vernietigd. (Stg.ZG)
- Van vernietiging van bijzondere informatie wordt een proces-verbaal opgemaakt. (Stg.G en Stg.ZG)
- Voor zeer gevoelige informatie (Stg.G en Stg.ZG) moeten organisaties een plan hebben voor vernietiging in buitengewone omstandigheden waarbij de staatsveiligheid in gevaar is.

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. Er wordt bij voorkeur gebruik gemaakt van producten waarvoor de Unit Weerbaarheid van het Nationaal Bureau voor Verbindingsbeveiliging (NBV) een positief inzetadvies afgegeven heeft.

Bijzondere informatie die krachtens een verdrag is verkregen, moet worden vernietigd, overeenkomstig de in het verdrag gemaakte afspraken.

12.4. Aanwijzingen ABDO en ABRO

Medium	Dep.V	Stg. C	Stg. G	Stg. ZG
Papier	Versnipperen L < 30mm B < 5mm	Versnipperen L < 25mm B < 3mm	Versnipperen L < 25 mm B < 3mm	Versnipperen L < 25 mm B < 3mm en verbranden
Papier i.h.k.v. internationale opdracht	Versnipperen max. 25mm^2	Versnipperen max. 25mm^2	Versnipperen max. 25mm^2	Versnipperen max. 25mm^2
Film	Versnippe-ren	Versnipperen (vernietigingsklasse P4[1], max. 160mm^2)	Versnipperen (vernietigings-klasse P5[1], max. 30mm^2)	Versnipperen (vernietigings-klasse P5[1], max. 30mm^2) en verbranden
Optische gegevens-dragers (CD/DVD)	Breken	Versnipperen (vernietigings-klasse O4[1], max. 30mm^2)	Versnipperen (vernietigings-klasse O5[1], max. 10mm^2)	Versnipperen (vernietigings-klasse O5[1], max. 10mm^2) en verbranden
Tapes	Versnippe-ren	Versnipperen (vernietigings-klasse T4[1], max. 160mm^2)	Versnipperen (vernietigings-klasse T5[1], max. 30mm^2)	Versnipperen (vernietigings-klasse T5[1], max. 30mm^2) en verbanden

Medium	Dep.V	Stg. C	Stg. G	Stg. ZG
Harde schijf	Doorboren	Versnipperen (vernietigings-klasse H4[1], max. 2000mm^2)	Versnipperen (vernietigings-klasse H5[1], max. 320mm^2)	Versnipperen (vernietigings-klasse H5[1], max. 320mm^2) en verbanden
USB stick	Doorboren	Versnipperen (vernietigings-klasse E4[1], max. 30mm^2)	Versnipperen (vernietigings-klasse E5[1], max. 10mm^2)	Versnipperen (vernietigings-klasse E5[1], max. 10mm^2) en verbranden
Overig	Breken	Versnipperen	Versnipperen	Versnipperen en verbranden

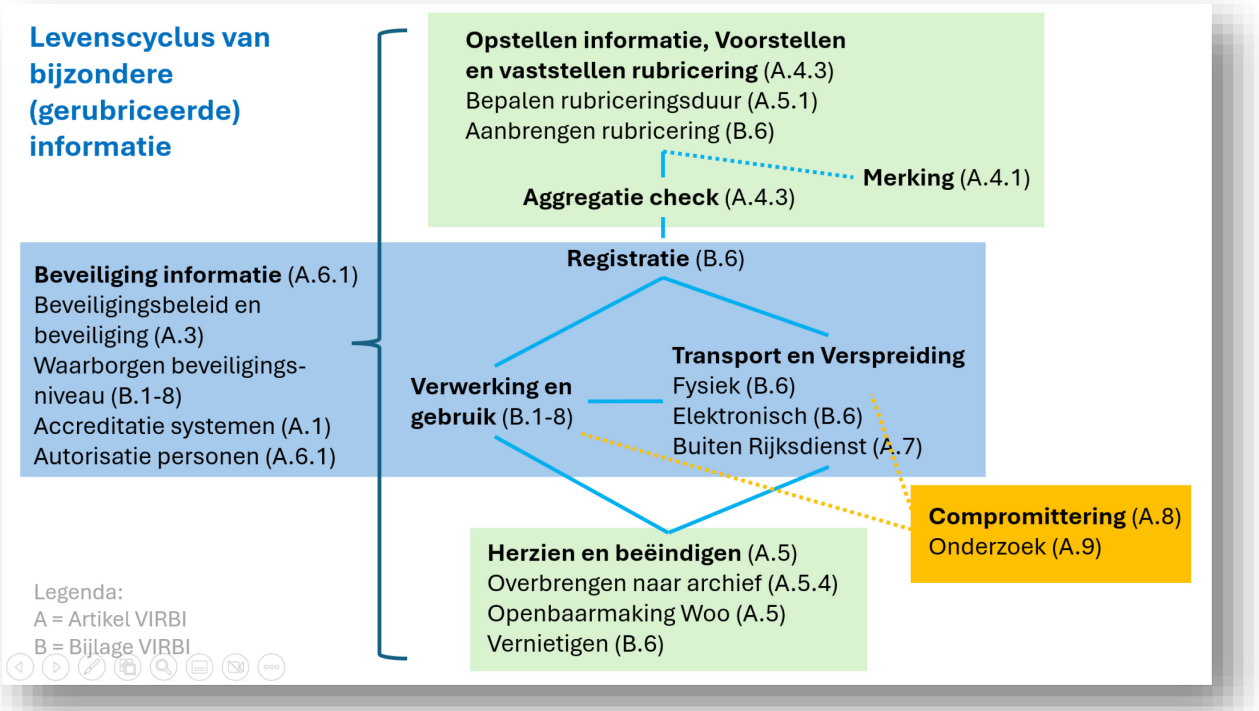
[1] = Conform DIN 66399

13. Overige aandachtspunten VIRBI

De meest unieke aandachtspunten van het VIRBI zijn in de voorgaande paragrafen nader toegelicht. Dit zijn de groen gemarkeerde delen van de levenscyclus van bijzondere (gerubriceerde) informatie.

Het oranje gemarkeerde deel van de levenscyclus, “Compromittering”, is ook specifiek voor het VIRBI en wordt hieronder nader toegelicht.

De blauw gemarkeerde delen van de levenscyclus komen sterk overeen met de klassieke manier van beheren en beveiligen en zijn ook voor een groot deel zelfverklarend. Waar zij dat niet zijn, kan voor inspiratie worden teruggevallen op vergelijkbare normen als BIO, ABDO en ABRO. Ook dit wordt hieronder toegelicht.



14. Compromittering

Het oranje gemarkeerde deel van de levenscyclus, “Compromittering”, is specifiek voor het VIRBI. Gedurende de hele levenscyclus van gerubriceerde informatie worden processen en systemen gemonitord op inbreuken. Bij een vermoeden van compromittering wordt direct een onderzoeksproces gestart om schade te beperken. Hierbij houdt de BVA toezicht. Dit omvat:

- Passende maatregelen om compromittering tijdig te detecteren.
- Een ingericht onderzoeksproces voor analyse van incidenten.
- Rapportage van verlies, mogelijke compromittering of ongeoorloofde bekendmaking aan de media.
- Uitvoeren van veiligheidsonderzoeken en schadeanalyses na een incident.

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.

In specifieke situaties kan een dergelijk onderzoek diepgaand en uitgebreid zijn, tot aan kamervragen, audits en commissies van toezicht. Bijvoorbeeld:

- In 2016 vond een onderzoek plaats naar het gebruik van een privé e-mailaccount van een minister voor werkgerelateerd e-mailverkeer. Om de omvang van het incident vast te stellen, gaf de minister de Auditdienst Rijk (ADR) de opdracht om de documenten in zijn Gmail-account te onderzoeken.

Dat onderzoek toonde aan dat de minister inderdaad gerubriceerde, zelfs staatsgeheime, documenten in zijn Gmail-account had opgeslagen.[38]

- In 2023 zijn twee personen aangehouden op verdenking van het bezitten en naar buiten brengen van staatsgeheime informatie. Betrokkenen hadden beschikking (gehad) over deze staatsgeheimen in het kader van hun werkzaamheden voor de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) heeft naar aanleiding hiervan nader onderzoek gestart.[39]

Een casus als de volgende zou ook een diepgaand en uitgebreid onderzoek verdienen, maar hierover is geen openbare informatie beschikbaar. Deze casus betrof ook internationaal gerubriceerde informatie, dus hier zou de melding en onderzoek extra uitgebreid zijn geweest:

- In 2013 is een ambtenaar van het Ministerie van Buitenlandse zaken veroordeeld tot een gevangenisstraf van twaalf jaar. De rechtbank achtte bewezen dat hij jarenlang structureel en in opdracht van de Russische buitenlandse inlichtingendienst (SVR) vertrouwelijke documenten heeft doorgespeeld aan de Russische Federatie. Hij speelde honderden documenten door over politieke en militaire aangelegenheden rond de NAVO en de EU.[40]

Het VIRBI zelf en ook het *Gereedschap voor Governance VIRBI implementatie* beschrijven de procedure en de rollen rond toezicht, incidenten en compromittering in detail. Op hoofdlijnen:

- Altijd zijn betrokken en geinformeerd:
  - de ambtenaar die de compromittering constateert, de leidinggevende en/of gegevenseigenaar en de BVA/BA.
- Bij ernstige incidenten worden daarboven nog betrokken en geinformeerd:
  - de BVA/BA van andere betrokken organisaties, de SG, de NSA/NSA Militair, de commissie van onderzoek en het hoofd AIVD/MIVD.

15. Buiten de Rijksdienst brengen

De VIRBI heeft geen directe werking buiten de Rijksdienst, maar eist wél dat bij “buiten de Rijksdienst brengen” voldoende zekerheid bestaat dat de informatie conform VIRBI wordt beveiligd.

[38] Kamp had staatsgeheim document in eigen Gmail-account - Security.NL
[39] Toezichtrapport over het handelen van de AIVD in relatie tot de verdenking van het lekken van staatsgeheimen door NCTV-medewerkers, CTIVD nr. 81, 14 oktober 2025
[40] 12 jaar celstraf voor spionerende ambtenaar — BijzonderStrafrecht.nl

16. Nationale normen als uitwerking van VIRBI

Als illustratie geeft de onderstaande tabel een globaal beeld van enkele punten waarop de verschillende normen kunnen helpen bij de uitwerking en implementatie van het VIRBI.

De stelling van dit hoofdstuk is dat er voldoende vastgestelde nationale normen aanwezig zijn om alle praktische uitwerkingsvragen van het VIRBI te beantwoorden.

VIRBI-onderdeel	Voorbeelden uit BIO 2	Voorbeelden uit ABDO / ABRO
Governance & Risico	Inrichting van het Information Security Management Systeem (ISMS) op basis van ISO 27001/27002.	Specifieke rollen voor de externe context: Beveiligingsfunctionaris (BF) en Cyber-BF.
Personeel	Basishygiëne voor screening en bewustzijn.	Gedetailleerd proces voor VGB/VOG aanvragen en ontheffing uit vertrouwensfuncties voor externen.
Fysieke Beveiliging	Fysieke beveiliging van locaties en gebouwen op basis van BIO-maatregelen.	Diepgaande OBER-methodiek, bewakingsrendement-berekeningen en NEN-normen voor fysieke barrières.
ICT & Cyber	Generieke maatregelen voor endpoint- en netwerkbeveiliging.	Specifieke eisen voor encryptie, hardened software, TEMPEST en verwerking op eigen systemen.
Ketens & Leveranciers	Inkoopeisen en management van leveranciersrelaties.	Strenge autorisatieprocedure voor Onderaannemers en 'Government-to-Government' transportregels.
Cloud	N.v.t. (Algemene BIO-regels gelden)	Specifiek toetsingskader voor clouddiensten (CSP's) voor niveau TBB 4.

16.1. BIO

Als illustratie geeft de onderstaande tabel een globaal beeld van enkele punten waarop de BIO kan helpen bij de uitwerking en implementatie van het VIRBI.

De aanname is dat elk onderdeel van de Rijksdienst aan BIO moet voldoen. Dus waar de eisen van BIO overeenkomen met eisen van het VIRBI voor de aanwezige gerubriceerde informatie hoeven misschien geen aanvullende maatregelen genomen te worden. Het is dus goed om VIRBI en BIO samen te gebruiken.

De aanname is dat veel maatregelen voor basis hygiëne ook bijdragen aan de naleving van het VIRBI.

VIRBI Uitgangspunten en minimum niveau beveiliging	**Voorbeelden van mogelijke uitwerking in de BIO**
1. Veilig personeel	DEEL 2 BIO–OVERHEIDSMAATREGELEN 6.01.01 Screeningsbeleid - Basishygiëne, overheidsrisico
2. Beheer van bedrijfsmiddelen	5.09.01 Inventaris van bedrijfsmiddelen - Basishygiëne, ketenhygiëne
3. Fysieke beveiliging en beveiliging van de omgeving	8.03.01 Fysiek en/of logisch isoleren van informatie - Basishygiëne
4. Toegangsbeveiliging	5.18.02 Alle toegangsrechten worden beoordeeld. – Basishygiëne 8.18.01 Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen. - Overheidsrisico
5. Beveiligingseisen voor ICT-voorzieningen	5.08.01 Er moet een expliciete risicoafweging worden uitgevoerd voor het vaststellen van de beveiligingseisen. - Ketenhygiëne
6. Communicatie-beveiliging	7.10.03 Transport van geclassificeerde informatie voldoet aan vooraf opgestelde Betrouwbaarheidseisen. – Overheidsrisico 8.21.04 Bij transport van gegevens over netwerken worden de gegevens versleuteld. - Basishygiëne
7. Beheer van bijzondere informatie	6.03.01 Iedereen kent de speciale eisen voor gerubriceerde omgevingen. - Basishygiëne
8. Incidenten en compromittering	5.24.01 Er is een meldloket voor informatiebeveiligingsincidenten. - Basishygiëne, ketenhygiëne

De BIO geeft aan dat de volgende categorieen van informatie aanvullende beveiliging verdienen. Dit helpt bij het bepalen van te rubriceren informatie:

- (Bijzondere) persoonsgegevens
- Gevoelige of interne informatie
- Gerubriceerde informatie

Daarbij moeten ook de volgende impactsgebieden worden afgewogen:

- Politieke schade aan een bestuurder
- Diplomatieke schade
- Financiële gevolgen
- Directe imagoschade
- Verlies van publiek respect of vertrouwen
- Organisatiebrede negatieve publiciteit
- Significant verlies van motivatie van medewerkers
- Belangrijk verlies van management control

16.2. ADBO

Als illustratie geeft de onderstaande tabel een globaal beeld van enkele punten waarop de ABDO kan helpen bij de uitwerking en implementatie van het VIRBI.

VIRBI Uitgangspunten en minimum niveau beveiliging	**Voorbeelden van mogelijke uitwerking in de ABDO**
	1. Bestuur en Organisatie
1. Veilig personeel	2. Personeel
2. Beheer van bedrijfsmiddelen	4. Cyber
3. Fysieke beveiliging en beveiliging van de omgeving	3. Fysiek Bijlage 19 - Bouwkundige maatregelen Bijlage 19.1 - Overzicht normen braakwering Bijlage 19.2 - Normentabel inbraakwerende maatregelen Bijlage 20 - Elektronische maatregelen Bijlage 21 - Reactieve maatregelen Bijlage 21.1 - Proces alarmopvolging
4. Toegangsbeveiliging	3. Fysiek Bijlage 31 - Gebruikers, IT-beheerders en accounts
5. Beveiligingseisen voor ICT-voorzieningen	4. Cyber
6. Communicatie-beveiliging	4. Cyber Bijlage 22 - Transport en verzenden van een fysieke TBB Bijlage 22.2 - Verzenden van een BI in het binnenland Bijlage 22.3 - Verzenden van een BI naar het buitenland
7. Beheer van bijzondere informatie	Bijlage 7 – Rubricerings-aanduidings-lijst

8. Incidenten en compromittering	1.9 Beveiligingsincidenten Bijlage 9 - Incident Handling procedure

In het ABDO geven de volgende bijlagen een nuttige invulling van fysieke beveiligingsmaatregelen:

- Bijlage 19 - Bouwkundige maatregelen
- Bijlage 19.1 - Overzicht normen braakwering
- Bijlage 19.2 - Normentabel inbraakwerende maatregelen
- Bijlage 20 - Elektronische maatregelen
- Bijlage 21 - Reactieve maatregelen
- Bijlage 21.1 - Proces alarmopvolging

16.3. ABRO

Als illustratie geeft de onderstaande tabel een globaal beeld van enkele punten waarop de ABRO kan helpen bij de uitwerking en implementatie van het VIRBI.

VIRBI Uitgangspunten en minimum niveau beveiliging	**Voorbeelden van mogelijke uitwerking in de ABRO**
	1. Bestuur en Organisatie Bijlage 1: Inrichten beveiligingsorganisatie Bijlage 2: Beveiligingsfunctionaris Bijlage 3: Cryptobeheerder
1. Veilig personeel	2. Personeel
2. Beheer van bedrijfsmiddelen	1.1 Inrichten van de beveiligingsorganisatie 3.1 Organisatorische maatregelen
3. Fysieke beveiliging en beveiliging van de omgeving	3. Fysiek Bijlage 5: Fysieke beveiliging Bijlage 6: Bouwkundige maatregelen
4. Toegangsbeveiliging	Bijlage 5: Fysieke beveiliging
5. Beveiligingseisen voor ICT-voorzieningen	4. Cyber
6. Communicatie-beveiliging	4. Cyber Bijlage 7: Transport en verzenden Bijlage 8: Labeling en vernietiging van Gegevensdragers Bijlage 9: Goedgekeurde middelen Bijlage 10: Scrubber
7. Beheer van bijzondere informatie	Bijlage 4: Overzicht van Te Beschermen Belangen
8. Incidenten en compromittering	1.7 Beveiligingsincidenten
	5. Cloud Bijlage 11: Cloud

Een van de belangrijkste uitwerkingen in het ABRO is het "positief beveiligings-rendement". Dit wordt ook in het VIRBI genoemd, maar daar niet verder uitgewerkt.

Het beveiligingsrendement is afhankelijk van het vertragende effect van getroffen beveiligingsmaatregelen in het fysieke domein (**Uitsteltijd**) in relatie tot de **Interventietijd**.
Er is sprake van een **positief Beveiligingsrendement** wanneer de Uitsteltijd langer is dan de Interventie tijd. In dit geval zal Interventie voorkomen dat er **Compromittatie** plaatsvindt.
Er is sprake van een **negatief Beveiligingsrendement** wanneer de Uitsteltijd korter is dan de Interventie tijd. In dit geval kan Interventie pas plaatsvinden na Compromittatie en zorgt Interventie ervoor dat het tijdvak waarbinnen de Compromittatie plaatsvindt zo kort mogelijk is.

Voor het realiseren van een positief Beveiligingsrendement moet dus gekeken worden welke maatregelen nodig zijn om een dader zodanig te vertragen na alarmering dat Interventie altijd eerder plaatsvindt dan Compromittatie.

Hoewel het idee van beveiligingsrendement afkomstig is uit het **Fysieke domein**, is het goed te vertalen naar het **Cyberdomein** (SOC/SIEM moet een aanval snel ontdekken zodat de aanvallers zich niet in het netwerk kunnen settelen) en het **Personele domein** (insider threat moet snel genoeg ontdekt worden voordat de insider veel vertrouwelijke informatie kan laten lekken).

16.4. Rijkscloudbeleid

In het Rijkscloudbeleid[41] wordt het volgende gezegd over gerubriceerde informatie in de cloud:

- **Dep.V:** Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) sluit de inzet van Publieke clouddiensten voor informatiesystemen op Departementaal Vertrouwelijk niveau niet meer bij voorbaat uit.
- **Hogere rubriceringen:** Het gebruik van publieke clouddiensten is niet toegestaan voor staatsgeheim gerubriceerde informatie (Stg.C, Stg,G, Stg.ZG).

Op dit moment wordt gewerkt aan een nieuwe versie van het rijkscloudbeleid. De verwachting is dat deze eisen gelijk blijven.

[41] Rijksbreed cloudbeleid 2022, Tweede Kamer, vergaderjaar 2021–2022, 26 643, nr. 904

16.5. NkBR

Het Normenkader Beveiliging Rijkskantoren (NkBR) is de praktische vertaling en uitwerking van het 'Zoneringmodel rijkskantoren, Model voor de inrichting en beveiliging van de Te Beschermen Belangen'. Het NkBR is gerubriceerd als Departementaal Vertrouwelijk en daardoor alleen beschikbaar voor medewerkers van de Rijksoverheid.

- **DepV-informatie** wordt structureel verwerkt, behandeld en besproken in minimaal Zone 2 (beveiligd gebied conform het NkBR of een en als gelijkwaardig beschouwde ruimte) en incidenteel in Zone 1 (conform het NkBR of een en als gelijkwaardig beschouwde ruimte).
- In het geval van thuiswerk bepaalt het departementaal beleid hoe om te gaan met het bespreken, verwerken en behandelen van DepV-informatie.
- **Stg.C, Stg.G en Stg.ZG-informatie** wordt structureel verwerkt, behandeld en besproken in tenminste een extra beveiligd werkgebied (conform het NkBR of een als gelijkwaardig beschouwde ruimte).

Het NkBR is onderdeel van de adviesdiensten van het Rijksvastgoedbedrijf voor het verantwoord en integraal beveiligen van Rijkskantoren met fysieke maatregelen en voorzieningen. Het uitgangspunt daarbij zijn de Te Beschermen Belangen en een risicoanalyse.

Interessant onderdeel van dit dienstenpakket is ook het *Handboek ICT-huisvesting en Bekabeling* (HIB)[42], als kader voor de inrichting van ICT-ruimtes en –bekabeling in Rijkskantoren en andere gebouwen.

16.6. VBV 32000

Apparatuur kan energie uitstralen waaruit de door dit apparaat verwerkte informatie kan worden gereconstrueerd. Hierbij bestaat het gevaar dat bij apparaten die gerubriceerde informatie verwerken deze informatie op afstand kan worden meegelezen. Dit verschijnsel heet TEMPEST.

Om bijzondere informatie - waaronder staatsgeheimen - zo goed mogelijk te beschermen tegen TEMPEST is er nationaal beleid gemaakt en vastgelegd in document VBV 32000 (B), 6 november 2006.[43]

- Voor **Stg.C, Stg.G en Stg.ZG-informatie** worden TEMPEST-maatregelen getroffen conform het Beleidsadvies Compromitterende straling (Verbinding Beveiliging Voorschrift (VBV) 32000).

[42] Handboek ICT huisvesting en bekabeling, Versie 3.0, d.d. 01-09-2025, Rijksvastgoedbedrijf (RVB)
[43] Dit document is op te vragen bij de Nationale TEMPEST Autoriteit (NTA). Nationale TEMPEST Autoriteit (NTA) | Informatiebeveiliging | AIVD

Voor TEMPEST-maatregelen voor gerubriceerde NAVO- of EU-gerubriceerde informatie geldt NAVO- of EU beleid.

16.7. VBV 41000

De bescherming van cryptografische middelen geschiedt **voor alle rubriceringen** conform VBV 41000.

De Unit Weerbaarheid van de AIVD schrijft Verbindingsbeveiligingsvoorschriften (VBV's) voor, waarin beveiligingsmaatregelen ten aanzien van specifieke deelaspecten worden beschreven. VBV's zijn zelf gerubriceerd en zijn op te vragen bij de Unit Weerbaarheid[44] van de AIVD.

17. ZBO wet- en regelgeving

De essentiële eis voor ZBO's staat in de *Kaderwet zelfstandige bestuursorganen*[45] die eist dat een zelfstandig bestuursorgaan zorg draagt voor de technische en organisatorische voorzieningen ter beveiliging van zijn gegevens tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van die gegevens.

Het VIRBI 2025 geldt ook voor ZBO's, conform artikel 41 van de kaderwet ZBO's van 1 juli 2022. Dit artikel zegt:

- Een zelfstandig bestuursorgaan draagt op de voet van de ter zake voor de Rijksdienst geldende voorschriften zorg voor de nodige technische en organisatorische voorzieningen ter beveiliging van zijn gegevens tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van die gegevens.

Het exacte samenspel tussen de Kaderwet, sectorwetgeving en VIRBI moet in de praktijk verder worden uitgewerkt. Relevant hierbij is de prioriteit van een wet versus een besluit en voorschrift.

De eis van de Kaderwet wordt vervolgens op verschillende manieren uitgewerkt in specifieke sectorwetgeving met specifieke regels over geheimhouding, gegevensverwerking, gegevensdeling, beveiliging en soms "exclusiviteit" (wie de gegevens mag gebruiken en waarvoor). Die regels bestaan naast de VIRBI, BIO en generieke kaders zoals AVG/UAVG, Archiefwet, Wet open overheid, etc. Voorbeelden hiervan zijn:

[44] Bescherming van (digitale) overheidsdiensten | Informatiebeveiliging | AIVD
[45] https://wetten.overheid.nl/BWBR0020495/2022-07-01/0, Artikel 41

- *Kadasterwet*[46] – Eist technische en organisatorische maatregelen om gegevens te beveiligen tegen verlies, aantasting en onbevoegde wijziging, kennisneming of verstrekking. Ook kunnen beperkingen worden vastgesteld voor verstrekking van inlichtingen en kunnen persoonsgegevens worden afgeschermd.
- *Wegenverkeerswet 1994*[47] - Er zijn regels voor de inrichting en het beheer van het kentekenregister, inclusief de gegevens, persoonsgegevens en persoonsgegevens van strafrechtelijke aard.
- *Handelsregisterwet 2007*[48] - De Kamer van Koophandel draagt zorg voor beschikbaarheid, werking en beveiliging van het handelsregister.
- *Wet op het financieel toezicht*[49] - De Algemene Rekenkamer is verplicht tot geheimhouding van ontvangen vertrouwelijke gegevens of inlichtingen. Het is verboden om vertrouwelijke gegevens of inlichtingen bekendheid te geven anders dan voor de uitvoering van de wet.
- *Instellingswet Autoriteit Consument en Markt*[50] - Verstrekking van gegevens vindt uitsluitend plaats als de geheimhouding van de gegevens of inlichtingen in voldoende mate is gewaarborgd, en voldoende is gewaarborgd dat de gegevens of inlichtingen niet zullen worden gebruikt voor een ander doel dan waarvoor deze worden verstrekt.
- *Wet studiefinanciering 2000*[51] - Er worden regels gesteld ter waarborging van de persoonlijke levenssfeer. Daarbij worden in ieder geval regels gesteld over: hoe gegevensverwerking plaatsvindt; welke technische en organisatorische maatregelen worden genomen tegen verlies of onrechtmatige verwerking; hoe wordt gewaarborgd dat de verwerkte persoonsgegevens alleen worden verwerkt voor het doel waarvoor zij zijn verzameld, en hoe daarop wordt toegezien. Ook zijn er regels voor gegevensuitwisseling met andere staten.

Geen van deze normen eist expliciete maatregelen voor rubricering of merking van gegevens.

ZBO's verwerken vooral bijzondere/gevoelige persoonsgegevens en ketengegevens, maar zelden echte staatsgeheimen. De "exclusiviteit" geldt vooral voor: doelbinding (alleen voor uitvoering/handhaving), geheimhoudingsplichten, gesloten verstrekkingsartikelen (alleen aan limitatief opgesomde partijen) en sanctionering (bestuurlijk/disciplinair/strafrechtelijk).

[46] https://wetten.overheid.nl/BWBR0004541/2026-01-01, Artikel 3d, Artikel 107b
[47] https://wetten.overheid.nl/BWBR0006622/2026-01-01, Artikel 42,
[48] https://wetten.overheid.nl/BWBR0021777/2025-07-16, Artikel 4, Artikel 41a
[49] https://wetten.overheid.nl/BWBR0020368/2025-11-19/0, Artikel 1
[50] https://wetten.overheid.nl/BWBR0033043/2025-09-01/0, Artikel 4
[51] https://wetten.overheid.nl/BWBR0011453/2026-01-01/0, Artikel 9.1, Artikel 9.6

Maar tegelijkertijd passen de maatregelen in deze wetten goed bij de maatregelen in het VIRBI en zijn hier zeker niet strijdig mee.

18. Overige wetgeving

Heel veel wetten bevatten een geheimhoudingsverplichting en stellen daarmee, expliciet of impliciet, eisen aan bescherming van gegevens. Maar ook hier geldt dat dit vooral doelbinding, geheimhoudingsplichten, verstrekkingsartikelen en sanctionering betreft en geen expliciete staatsgeheimen. Voorbeelden hiervan zijn:

- Algemene wet bestuursrecht
- Jeugdwet
- Wet bescherming klokkenluiders
- Wet bevordering integriteitsbeoordelingen door het openbaar bestuur
- Wet kwaliteit, klachten en geschillen zorg
- Wet maatschappelijke ondersteuning 2015
- Wet verplichte geestelijke gezondheidszorg
- Rijkswet Onderzoeksraad voor veiligheid
- Rijkswet Raad voor de rechtshandhaving
- Wet ter voorkoming van witwassen en financieren van terrorisme
- Etc.

Een gestructureerde analyse van de bestaande wetgeving is te vinden in het Onderzoek Wetgevingskader Informatieveiligheid[52] in Bijlage A: De onderzochte informatieveiligheidsregels.

19. Interessante buitenlandse normen

Er zijn publieke buitenlandse normen beschikbaar voor rubricering en het omgaan met gerubriceerde documenten. Deze laten zien tot welk detail men richtlijnen voor rubricering kan uitwerken.

Binnen de Nederlandse nationale context moet dit eerder als een afschrikwekkend voorbeeld gezien worden. Niet als een voorbeeld om na te volgen. Binnen de Nederlandse context lijkt het beter om deze situaties op case-by-case basis te behandelen als zij zich eventueel voordoen en dit niet allemaal vooraf uit te werken.

[52] Onderzoek Wetgevingskader Informatieveiligheid, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, VKA, Berenschot, d.d. 15-3-2020

20. Voorbeeld detailproces rubricering en derubricering

Rubricering van informatie[53]

- Voorlopige rubricering
- Afgeleide rubricering
- Procedures voor afgeleide rubricering
- Duur van de rubricering
- Rubricering van aankoopinformatie
- Rubricering van informatie die aan het publiek is vrijgegeven
- Gerubriceerde informatie vrijgegeven zonder de juiste bevoegdheid
- Herrubricering van informatie die is gederubriceerd en aan het publiek is vrijgegeven met de juiste bevoegdheid
- Informatie die is gederubriceerd en aan het publiek is vrijgegeven zonder de juiste bevoegdheid
- Rubricering of herrubricering na ontvangst van een verzoek om informatie
- Rubricering van niet-overheidsonderzoek en -ontwikkelinginformatie
- Verzoeken om bepaling van de rubricering

Derubricering en wijzigingen in rubricering

- Derubriceringbeleid
- Processen voor derubricering
- Bevoegdheid tot derubricering
- Richtlijnen voor derubricering
- Intrekken of wijzigen van rubriceringmarkeringen
- Speciale procedures voor cryptologische informatie
- Permanent waardevolle documenten
- Documenten waarvan is vastgesteld dat ze geen permanente historische waarde hebben
- Verlenging van de rubricering tot na 25 jaar voor niet-geplande documenten
- Automatische derubricering
- Openbare vrijgave van automatisch gedeclassificeerde documenten
- Grondslag voor uitsluiting of vrijstelling van automatische derubricering
- Vertragingen bij automatische derubricering
- Technieken voor derubriceringbeoordeling
- Uitzonderingen van automatische derubricering

[53] Department of Defense, MANUAL NUMBER 5200.01, Volume 1, February 24, 2012 , SUBJECT: DoD Information Security Program: Overview, Classification, and Declassification

21. Detaillijst te rubriceren gegevensdragers en aanbrengen van rubricering

In buitenlandse documenten zijn uitgebreide lijsten te vinden van mogelijk te rubriceren informatiedragers en uitgewerkte voorbeelden van hoe de rubricering op deze informatiedragers aangebracht dient te worden.

Binnen de Nederlandse nationale context moet dit eerder als een afschrikwekkend voorbeeld gezien worden. Niet als een voorbeeld om na te volgen. Binnen de Nederlandse context lijkt het beter om deze situaties op case-by-case basis te behandelen als zij zich eventueel voordoen en dit niet allemaal vooraf uit te werken. Hierbij kunnen de buitenlandse normen dan inspiratie geven.

Rubricering in de digitale omgeving[54]

- E-mailberichten
- Webpagina's
- URL's
- Dynamische documenten
- Bordberichten en blogs
- Wiki's
- Instant messaging, chat en chatrooms
- Attachments, Bijgevoegde bestanden
- IT-systemen en media

Speciale informatiemedia

- Blauwdrukken, technische tekeningen, grafieken en kaarten
- Fotografische media
- Digitale videodiscs (dvd's), videobanden, speelfilms en webvideo's
- Geluidsopnamen
- Microfilm, microfiche en soortgelijke microformmedia
- Verwijderbare elektronische opslagmedia
- Memorandum
- Personeelsoverzicht
- Werkdocumenten
- Presentatieslides, bronnen op presentatieslides
- Referenties

[54] Department of Defense, MANUAL NUMBER 5200.01, Volume 2, February 24, 2012, SUBJECT: DoD Information Security Program: Marking of Information

22. Algemene aandachtspunten rubricering en beveiliging

In buitenlandse documenten over rubricering en beveiliging van gerubriceerde informatie komen, bijna altijd, de volgende onderwerpen aan de orde. Het kan soms nuttig zijn om te kijken hoe andere landen hier mee omgaan.[55] [56] [57] [58] [59]

Algemene Grondslagen en Organisatie

- **Verantwoordelijkheden:** De rollen van autoriteiten op interministerieel en organisatieniveau, de verantwoordelijkheden van houders van informatie en de aanstelling van beveiligingsfunctionarissen.
- **Juridisch kader:** Verwijzingen naar wetgeving, strafrechtelijke sancties bij schending van het geheim en de duur van de geldigheid van de voorschriften.

Rubricering en aanbrengen rubricering

- **Rubriceringsproces:** De autoriteit om te classificeren, de graden van rubricering (zoals Secret en Top Secret), en de procedures voor declassificatie of herziening van de status.
- **Aanbrengen rubricering:** Voorschriften voor het aanbrengen van rubriceringen en merkingen op fysieke documenten, in de elektronische omgeving en op opslagmedia.
- **Aggregatie:** Richtlijnen over hoe verzamelingen van gegevens (compilatie) tot een hogere rubricering kunnen leiden.

Personele Veiligheid en Toegangsbeheer

- **Autorisatie en Screening:** Procedures voor het verkrijgen van een veiligheidsmachtiging (clearance/habilitation), inclusief noodprocedures en regels voor buitenlandse onderdanen.
- **Need-to-know:** Het bepalen van de noodzaak tot toegang en de verantwoordelijkheid van de persoon die de informatie deelt.

---

[55] Department of Defense, MANUAL NUMBER 5200.01, Volume 3, February 24, 2012, SUBJECT: DoD Information Security Program: Protection of Classified Information

[56] Title 32 —National Defense, Subtitle B —Other Regulations Relating to National Defense, Chapter XX — Information Security Oversight Office, National Archives and Records Administration, Part 2001 Classified National Security Information

[57] Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), Vom 13. März 2023, GMBl 2023 S. 542-620 vom 12.04.2023

[58] Secrétariat général de la défense et de la sécurité nationale, Direction de la protection et de la sécurité de l'État, INSTRUCTION GÉNÉRALE INTERMINISTÉRIELLE SUR LA PROTECTION DU SECRET DE LA DÉFENSE NATIONALE

[59] PROCEDIMIENTO DE CLASIFICACIÓN Y TRATAMIENTO DE LA INFORMACIÓN CLASIFICADA, PR20, Centro riptológico Nacional, CCN-STIC-822, Procedimientos de Seguridad en el ENS. Anexo II.

- **Scholing en Training:** Veiligheidsbewustzijn, initiële oriëntatie en periodieke bijscholing voor personeel en functionarissen.

Fysieke Beveiliging en Opslag

- **Beveiligde zones:** Inrichting van zones, open opslaggebieden en de beveiliging van locaties en gebouwen.
- **Bergmiddelen:** Normen voor kluizen, beveiligingscontainers, sloten en het beheer van combinaties en sleutels.
- **Controles:** Dagelijkse veiligheidschecks, inspecties van faciliteiten en toelatingsmiddelen.

Informatiebeveiliging (IT en Cybersecurity)

- **Accreditatie:** Het proces voor het goedkeuren van IT-systemen en netwerken voor het verwerken van gerubriceerde informatie.
- **Technische maatregelen:** Cryptografie (cryptomiddelen), afscherming tegen parasitaire signalen (Tempest/abstrahlschutz) en beveiliging van mobiele apparatuur.
- **Netwerkbeveiliging:** Connecties tussen systemen, beveiliging van transmissielijnen en het gebruik van sociale netwerken.

Beheer gerubriceerde informatie gedurende de levenscyclus

- **Administratie en Registratie:** Het bijhouden van registers, inventarissen en de tracering van documenten binnen een organisatie.
- **Reproductie en Vertaling:** Regels voor het kopiëren en vertalen van geclassificeerde documenten.
- **Transport en Transmissie:** Veilig verzenden via koeriers, elektronische middelen (fax, telefoon) en het handmatig meevoeren van materiaal (briefcases).
- **Vernietiging:** Procedures voor de definitieve vernietiging van documenten en IT-media, inclusief noodvernietigingsplannen.

Incidenten en Risicobeheer

- **Behandeling van inbreuken:** Rapportage van verlies, mogelijke compromittering of ongeoorloofde bekendmaking aan de media.
- **Onderzoek van inbreuken:** Uitvoeren van veiligheidsonderzoeken en schadeanalyses na een incident.
- **Risicomanagement:** Algemene principes voor risicoanalyse en het beheer van veiligheidsrisico's.

Externe Betrekkingen en Industriële Veiligheid

- **Internationale uitwisseling:** Regels voor het delen van informatie met andere staten (zoals de VS, het VK of Australië) en internationale organisaties (NAVO, EU).
- **Industriële veiligheid:** Beveiliging binnen geclassificeerde contracten en de screening van bedrijven (vestigingsmachtiging) en hun personeel.

23. Specifieke aandachtspunten voor opsporing

Binnen het domein opsporing gelden extra eisen bij het rubriceren van informatie. Opsporing van strafbare feiten wordt uitgevoerd onder gezag van het Openbaar Ministerie door de Nationale Politie en de Bijzondere Opsporingsdiensten. Informatie wordt verkregen onder de Wet Strafvordering (WvSv) en verwerkt onder de Wet politiegegevens (Wpg). Voor de samenwerking is het nodig dat genoemde diensten dezelfde lijn hanteren waar het gaat om het rubriceren van informatie. WvSv en Wpg bepalen niet een rubriceringsniveau. Daarom wordt de volgende lijn gebruikt:

Departementaal Vertrouwelijk	• Wpg 9, opsporing criminaliteit
Staatsgeheim CONFIDENTIEEL (Stg. C)	• Zware georganiseerde zware criminaliteit. Zoals terrorisme en sancties (statelijke actoren); • Embargo onderzoeken conform besluit politiegegevens, art. 2.13 lid 1f; • Wpg 9, zware georganiseerde criminaliteit; • Bedrijfsvoeringsinformatie, bepaalde gevoelige informatie t.a.v. de bedrijfsvoering.
Staatsgeheim GEHEIM (Stg. G)	• Inlichtingen, uit heimelijk domein zoals criminele inlichtingen; • Wpg art. 10 verwerkingen; • Wpg art. 12 bruto verwerkingen.
Staatsgeheim ZEER GEHEIM (Stg. ZG)	• Inlichtingen, identificerende gegevens informanten. • Wpg art. 12.

24. Colofon:

Wil je reageren? Dat kan naar het volgende e-mailadres: CISORijk@minbzk.nl.

Dit gereedschap is tot stand gekomen met een brede werkgroep en maakt deel uit van de gereedschapskist ter ondersteuning van implementatie van het VIRBI 2025.

De BVA Rijk en de CISO Rijk zijn sponsoren van deze gereedschapskist.

Dit document is een toegankelijke en korte versie. Er is een uitgebreider document beschikbaar over rubriceren. Wil je dat ontvangen neem dan contact op via CISORijk@minbzk.nl.

25-5-2026

= = = = =