Centrale Commissie

Informatiebeveiligingsplan

Titel Verantwoording & Vooruitblik CCMO 2022
Ingangsdatum 1 januari 2022
Versie 1.0
Status Concept

Verantwoordelijken

Opgesteld door	Functie	Handtekening

Beoordeeld door	Functie	Handtekening
5.1.2.e	5.1.2.e	

Geautoriseerd door	Functie	Handtekening
5.1.2.e	Algemeen secretaris	

Versiebeheer

Versie	Datum	Omschrijving	Naam	Status
0.1	04-02-2020	Eerste versie document	5.1.2.e	concept
0.2	13-10-2020	Tweede versie document	5.1.2.e	concept
0.3	02-12-2020	Wijzigingen management	5.1.2.e	concept
1.0	04-12-2020	Wijzigingen / goedkeuring document	5.1.2.e	Definitief

Inhoudsopgave

1. Inleiding

Het management van de Centrale Commissie Mensgebonden Onderzoek (CCMO) is verantwoordelijk voor de informatiebeveiliging en de naleving van de Algemene Verordening Gegevensbescherming (AVG). De coördinatoren informatiebeveiliging / privacybescherming en integriteit steunen het management bij het opstellen en onderhouden van het informatiebeveiligingsplan, het beleid voor informatiebeveiliging, privacy en integriteit alsmede de bijbehorende procedures, richtlijnen en werkinstructies.

In het informatiebeveiligingsplan (IB-plan) worden bedrijfsregels en afspraken opgenomen aangaande informatiebeveiliging. Het IB-plan komt tot stand op basis van verschillende risicoanalyses en wordt het hele jaar door geactualiseerd op gewijzigde omstandigheden en/of gewijzigde c.q. nieuwe wet- en regelgeving. Het IB-plan is onderdeel van het jaarplan.

Dit document stelt het management in staat om verantwoording af te leggen wat betreft de informatiebeveiliging (ICV, in control statement) en sluit aan bij de Planning & Control-cyclus van het Ministerie van VWS.

2. Informatiesystemen, AVG-registraties en TBB

Dit hoofdstuk geeft een overzicht van de informatiesystemen waar de CCMO verantwoordelijk voor is, processen en systemen waar gebruik van gemaakt wordt, de registraties van persoonsgegevens waar de CCMO verantwoordelijk voor is, de vertrouwensfuncties en de Te Beschermen Belangen.

2.1 Eigenaarschap systemen

De CCMO is verantwoordelijk voor de volgende informatiesystemen en/of websites:

Website ToetsingOnline		https://www.toetsingonline.nl
Website CCMO*	(PRO)	https://www.ccmo.nl
~~ROMERO~~	~~(DICTU)~~	~~in aanbouw https://www.romero.nl~~
LTR	(DICTU)	in aanbouw https://www.....nl

Bedrijfsvoeringapplicaties VWS* *(IDM, Marjolein, GMI, 3F, HIS, DigiInkoop, TEM, Shuttel, SSC-ICT netwerk en applicaties, Planon, AVG-register, ISMS)*,
P-Direkt* (personeel management systeem VWS)
Viadesk* (samenwerkingsruimte voor commissieleden en METC's)

* De CCMO is alleen verantwoordelijk voor de data-gegevens in de bedrijfsvoeringapplicaties van VWS, P-Direkt, Viadesk, PRO-website; niet voor het gehele systeem.

Van elk van deze systemen is een risicoanalyse aanwezig of staat in de planning om te worden uitgevoerd, om te kunnen bepalen of het systeem boven de Baseline Informatiebeveiliging Overheid valt (BIO).

De volgende systemen vallen boven de Baseline:

Geen (alle systemen zijn gerubriceerd op vertrouwelijkheidsniveau Departementaal Vertrouwelijk)

Het afgelopen jaar is het volgende gewijzigd:
Het ontwikkelingstraject ROMERO met Rijkszaak van Dictu is eind augustus 2021 stopgezet. De CCMO is gestart met een Plan B welke in eerste instantie gericht is op het zo optimaal mogelijk gebruiken van CTIS voor de Geneesmiddelen studies voor zowel de CCMO als de METC's. Er wordt een oplossing gevonden om te kunne borgen dat de CCMO en de METC's kunnen samenwerken en kunnen plannen. Voor de andere studies blijft TOL gebruikt worden. Voor LTR wordt ene oplossing gezocht. Parallel aan de tijdelijke oplossing wordt gezocht naar een vervagende applicatie voor TOL. Hiervoor zal (vermoedelijk 2022) een risicoanalyse Quickscan-IB en BIO-analyse uitgevoerd worden zodra dit mogelijk is evenals een AVG-quickscan en PIA (gegevensbeschermingseffectbeoordeling). Het nieuwe systeem zal niet boven de Baseline komen te vallen, mogelijk de tijdelijke oplossing wel.

2.2 Overzicht processen en systemen

Voor alle processen en systemen is een risicoanalyse opgesteld of staat op de planning om het gewenste beschermingsniveau vast te stellen voor de informatiesystemen.
De bijgewerkte lijst is toegevoegd als ***bijlage 1***.

Het afgelopen jaar is het volgende gewijzigd:
Er zijn wijzigingen in het beschermingsniveau van de bestaande informatiesystemen doorgevoerd met betrekking tot de open standaarden voor de beveiliging van het externe e-mail verkeer en de beveiliging van het inkomende en uitgaande verkeer van webservers welke verplicht zijn gesteld. Deze standaarden zijn onderdeel van de Wet Generieke Digitale Infrastructuur (WGDI) welke per 1 januari 2019 van kracht is.

2.3 Overzicht registraties persoonsgegevens

Een inventarisatie is uitgevoerd op het aanwezig zijn van verwerkingen van persoonsgegevens en of een verdere analyse nodig is d.m.v. het uitvoeren van een Privacy Impact Assesment (PIA). De bijgewerkte lijst is toegevoegd als ***bijlage 2***.

Het afgelopen jaar is het volgende gewijzigd:
De FG heeft in 2020 een advies uitgebracht op de DPIA van ROMERO, deze zou nog verwerkt worden in de volgende versie van deze DPIA. Dit zal komen te vervallen ivm het stopzetten van het ROMERO traject.

2.4 Vertrouwensfuncties

De CCMO heeft geen medewerkers met een vertrouwensfunctie.

2.5 Te beschermen belangen (TBB) en EU / NATO informatie

Een inventarisatie is uitgevoerd op het aanwezig zijn van Te Beschermen Belangen en EU en NATO informatie. De bijgewerkte lijsten is toegevoegd als ***bijlage 3***.

3. Verantwoording

In dit hoofdstuk komt de verantwoording over het huidige jaar op het gebied van Informatiebeveiliging. Door terug te kijken komt er een beeld tot stand over de ontwikkelingen van het afgelopen jaar.

3.1 Voortgang van de te implementeren maatregelen

N.a.v. de uitgevoerde risicoanalyses zijn de volgende risico's onderkent en geaccepteerd:

Website ToetsingOnline
Het document "Openstaande punten ToetsingOnline 2020" bevat een overzicht van openstaande aanbevelingen van o.a. de auditresultaten voor ToetsingOnline (www.toetsingonline.nl) om de risico's te verlagen. Vrijwel alle punten zijn inmiddels opgelost. Open staat nog een stukje ikv IPv6.

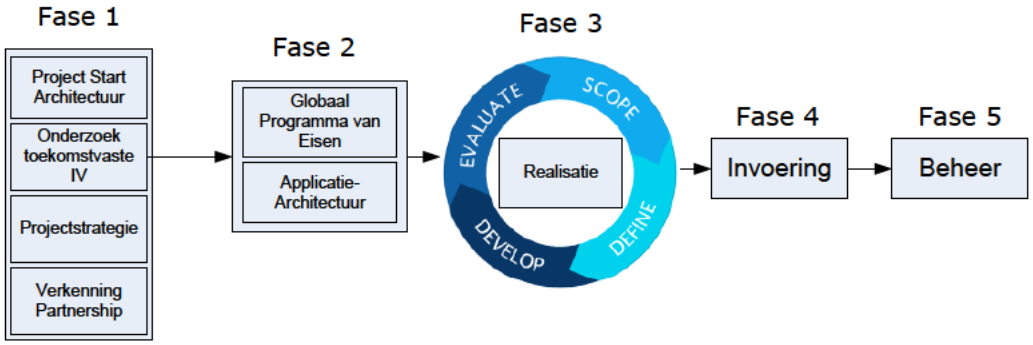
Website CCMO
De website van de CCMO (www.ccmo.nl) is ondergebracht bij Platform Rijksoverheid (PRO). Voor deze website is dit jaar geen risicoanalyse of AVG quickscan uitgevoerd.

Website Onderzoekswijs
De website Onderzoekswijs (www.onderzoekswijs.nl) is in 2020 opgeheven.

Webapplicatie Formdesk
Het online formulieren management systeem Formdesk wordt niet meer gebruikt om de verklaringen van belangen van de commissieleden te laten invullen. Er wordt naar een nieuwe applicatie gekeken om Formdesk te vervangen. In de tussentijd wordt met een Word-formulier gewerkt.

IV Vernieuwing
De CCMO maakt gebruik van verschillende ICT-systemen, zowel intern als extern, om haar wettelijke taken te kunnen uitvoeren. Er is in april 2019 gestart met de realisatie van een IV-vernieuwingsproject. De aanleiding voor dit project is meerledig; 1. het vervangen van het belangrijkste bestaande systeem ToetsingOnline (i.v.m. einde levensduur), 2. het vereenvoudigen van het applicatielandschap door integratie van diverse functionaliteiten in één systeem (i.v.m. verhoging efficiëntie werkprocessen), en 3. het realiseren van noodzakelijke koppelingen met Europese webportalen (i.v.m. nieuwe wettelijke taken CCMO). De verwachting september 2021 is dat koppelingen niet gerealiseerd kunnen worden omdat deze vanuit het webportaal te beperkt aangeboden gaan worden.
In dit IV-vernieuwingsproject wordt ook het huidige CCMO Register vervangen door een nieuw landelijk register conform de WHO normen. In het nieuwe systeem zullen ook niet-WMO onderzoeken gepubliceerd kunnen worden in het register dat het Local Trial register (LTR) genoemd wordt.
De Project Start Architectuur (PSA) van juni 2016 schetst een toekomstbeeld en een aantal kaders, uitgangspunten en adviezen opgesteld vanuit de CIO office. Bij de uitvoering van het project zal rekening gehouden worden met de vigerende rijkskaders op het gebied van architectuur, beheer en projectmanagement. Het IV vernieuwingstraject zal een geüniformeerd platform gaan bieden voor zowel de CCMO als erkende METC's. Het project bevindt zich nu in de oriëntatiefase (fase 1). Voor het LTR is een basis publicatiewebsite in Druppal in de ontwikkelingsfase. Hier wordt in het kader van de projectwijziging een bouwstop ingelast.

Minimale variant



N.a.v. de uitgevoerde risicoanalyses zijn de volgende maatregelen uitgevoerd of ingepland:

- Jaarlijkse check op geldigheid compliances (ISO / NEN certificaten) van externe leveranciers aan de hand van de BIO richtlijn 15.1.2.6 (risicofactor 16). Deze maatregel is uitgevoerd (Q2 2019).
- Het implementeren van de openstaande punten op de huidige release van ToetsingOnline, alsmede de verplichte open standaarden zoals Piwik en PKI-certificaten. Deze maatregel is uitgevoerd (Q3 2020).
- Het verhuizen van het eigenaarschap van alle domeinnamen naar Dienst Publiek en Communicatie van het Ministerie van Algemene Zaken. Deze maatregel is uitgevoerd (Q1 2019).
- Het opheffen van onderzoekswijs.nl i.v.m. nieuwe website van een andere organisatie; Deze maatregel is uitgevoerd. Het domein is in quarantaine gezet bij het Ministerie van Algemene Zaken om misbruik door kwaadwillenden te voorkomen (Q4 2019).

Acties en aanbevelingen die hieruit voortvloeien voor het komend jaar zijn:

Website ToetsingOnline

- Nieuwe risicoanalyse uitvoeren. Deze maatregel is ingepland (Q4 2021).
- Jaarlijkse check op geldigheid compliances (ISO / NEN certificaten) van de leverancier aan de hand van de BIO richtlijn 15.1.2.6 (risicofactor 16). Deze maatregel is ingepland (Q4 2021).

Website CCMO

- Het opvragen van risicoanalyses / ICV van Platform Rijksoverheid. De ICV van SSO's Deze maatregel is nog niet uitgevoerd (Q4 2021).
- Toegankelijkheidsverklarng website ccmo.nl is ingepland voor Q4 2020. Dit wordt 2021 of verder ivm aan te passen CCMO-(huisstijl)kleuren op website.

Document management systeem Marjolein

- Nieuwe risicoanalyse en AVG quickscan uitvoeren. Deze maatregel is ingepland (Q2 2021).

- Het schrijven van een procedure m.b.t. de wettelijke richtlijnen digitale archivering. Deze maatregel is ingepland (Q2 2022).
- VWS: Het faciliteren van de mogelijkheid voor sluiten van dossiers met archiefdatum aan de hand van de procedure van de CCMO m.b.t. digitale archivering. Deze maatregel kan nog niet worden ingepland.
- Hotspot Covid 19: separate omgeving creeren in Marjolein ten behoeve van de relevante stukken Hotspot Covid 19 middels Plan van Aanpak is ingepland (Q3 en Q4 2021)

Digitale samenwerkingsruimte Viadesk

- Nieuwe risicoanalyse en AVG quickscan uitvoeren om de BIR quickscan te completeren. Deze maatregel is nog niet ingepland (2021).
- Jaarlijkse controle op compliances (ISO / NEN certificaten) van de leverancier aan de hand van de BIO richtlijn 15.1.2.6 (risicofactor 16).). Deze maatregel is ingepland (Q4 2020).

Splatbox VPN verbinding Londen

- De splatbox is een virtuele PC, beheerd door SSC-ICT, welke een veilige verbinding met de website van de EMA faciliteert. Er zijn geen aanbevelingen voor dit systeem.

CTIS en EUDAMED

- De Europeesche potals CTIS (01 2022) en Eudamed (05 2022) zullen opertaioneel worden. Deze portals zullen gebruikt worden en het beheer ligt bij de EMA.

Digitale indiening

- Corona heeft als resultaat gehad dat er niet meer op gegevnsdragers studies ingediend konden worden bij de CCMO. Indiening heeft digitaal plaatsgevinden via mail, we-trasfer en vergelijkbare opties. Het streven is voor 2022 een systeem te hebben dat eenduidig is en veilig. Overwogen wordt CESP. Een risico analyse zal opgesteld dienen te worden om vast te stellen of dit een veilige optie is.

Papieren & digitale archief

- ICV van DocDirekt opvragen bij VWS kern.
- Er is nog een kwart kast met een op gegevensdragers aangeleverd archief over die reeds gedigitaiseerd verwerkt is en na 4-ogenprincipe vernietigd kan worden. Nieuwe binnenkomende stukken worden tijdelijk als fysiek archief bewaard en in Marjolein opgeslagen om vervolgens na drie maanden (na controle 4-ogen principe) te worden vernietigd. Deze maatregel is uitgevoerd (Q2 2020) en in de uitvoering lopende.
- Er is nog een deel archief bij een externe leverancier opgeslagen. Er is reeds in 2018 een project met het Ministerie van VWS gestart om dit archief z.s.m. naar DocDirekt te verplaatsen (Q4 2021).

Algemeen

- Het maken van een plan van aanpak voor het implementeren van de BIO op alle bovengenoemde systemen.
- Voor alle genoemde systemen is op basis van functies van de medewerkers een overzicht gemaakt: Het CCMO autorisatiemodel. Dit model is afgestemd met het management en dient als leidraad bij de nieuwe procedures, werkinstructies en beleid voor informatiebeveiliging binnen de organisatie. Bij binnenkomst of vertrek

van medewerkers is er een goed overzicht van welke rechten toegekend of ingetrokken moeten worden.
- Finaliseren van beleidsdocumenten, procedures en werkinstructies voor informatiebeveiliging, privacy en integriteit (2021).
- Het gebruik gaan maken van het ISMS van VWS voor opslag IB-documenten en het bewaken van de voortgang van alle IB-activiteiten.
- Informatiehuishouding op orde. Aansluiten op projectmatige aanpak Kern VWS

3.2 Incidenten

Incidenten met betrekking tot de integrale beveiliging die zich binnen de organisatie voordoen, dienen gemeld te worden bij de aangewezen coördinator informatiebeveiliging. Ernstige incidenten worden door tussenkomst van de algemeen secretaris direct aan de CISO kerndepartement van VWS gemeld.
De beveiligingsincidenten van aflopen jaar zijn geanonimiseerd in het overzicht van ***bijlage 4*** opgenomen.

Acties en aanbevelingen die hieruit voortvloeien voor het komend jaar zijn:

- Het maken van een bewustwordingsprogramma m.b.t. informatiebeveiliging, privacy en integriteit voor het jaar 2021.
- Onderdeel van het jaarplan is het volgen van twee online modules “Informatiebeveiliging” en “Privacy en AVG” op het opleidingspaspoort-platform van VWS. Medewerkers hebben van het management opdracht gekregen deze modules te volgen voor het einde van het jaar.
- Communiceren van eventuele incidenten (indien van toepassing) bij medewerkers en commissieleden van de CCMO, METC’s en gebruikers van ToetsingOnline.

3.3 Conclusie

- Het maken van een plan van aanpak voor het implementeren van de BIO op alle systemen.
- Het uitvoeren van risicoanalyses en quickscans voor alle systemen is gewenst.
- Het finaliseren van verwerkingen in het AVG register van VWS.
- Alle websites van de CCMO conformeren aan de wet GDI en de Europese standaard EN 301549, welke van kracht zijn per medio 2018. Daarnaast de nieuwe websites voorzien van een toegankelijkheidsverklaring en privacy-verklaring.Toegankelijkheid CCMO.nl (inclusief de Engelde versie) is op orde op ….
- De nieuwe websites/systemen van de CCMO voorbereiden op de wet eIDAS verordening 910/2014/EG (indien van toepassing), welke van kracht is per september 2018.
- Het verbeteren van de emailbeveiliging voor (en het monitoring hiervan op) de domeinen ccmo.nl, romero.nl en toetsingonline.nl (SPF/DKIM/DMARC).
- Het verbeteren van de toegangsbeveiliging voor (en het monitoring hiervan op) de domeinen ccmo.nl en toetsingonline.nl (DNSSEC, STARTTLS, DANE, IPv6). Voor ccmo.nl ligt een actie bij VWS om de beveiliging bij SSC-ICT te verbeteren. IPv6 is voor ToetsingOnline zou in oktober 2021 op orde moeten zijn. Oplossing middels een tussenserver bij Ilionx.

4. Vooruitblik

In dit hoofdstuk wordt aangegeven welke bijstellingen er zijn ten opzichte van het voorgaande jaar. Hierbij wordt gebruik gemaakt van de conclusies uit de verantwoording om

de bevindingen van het voorgaande jaar te adresseren.

4.1 Aanbevelingen

De CCMO zal het komende jaar zich toeleggen op het implementeren van alle technische maatregelen voor informatiebeveiliging van de (externe) systemen. ToetsingOnline is het belangrijkste systeem en ook het meest kwetsbare systeem, waarop geen doorontwikkeling meer zal gaan plaatsvinden. De focus voor dit systeem zal in het komende jaar daarom ook liggen op het in stand houden van en het alert blijven op de beveiliging van deze website.

Het komende jaar zal in het teken staan van het werken met CTIS en het vervangen van de basisfunctionaliteiten van ToetsingOnline en het realiseren van een werkend LTR. Eveneens zal aandacht gegeven worden aan het maken van nieuwe risicoanalyses van alle systemen om de afhankelijkheid en kwetsbaarheid te (her)bepalen.

De aandacht zal worden gelegd op het plan van aanpak van de BIO en de daaruit vloeiende acties. De huidige openstaande punten voor het implementeren van de maatregelen van de BIO hebben betrekking op:

- Het documenteren van beleidsdocumenten van de CCMO op het gebied van informatiebeveiliging, privacy en integriteit (aanvullend op het VWS-beleid).
- Het wijzigen van bestaande (verouderde) of het schrijven van nieuwe Standard Operating Procedures (SOP's).
- Het wijzigen van bestaande of het schrijven van nieuwe werkbeschrijvingen voor support of beheer van systemen.
- Het verbeteren van de emailbeveiliging voor (en het monitoring hiervan op) de domeinen ccmo.nl, romero.nl en toetsingonline.nl (SPF/DKIM/DMARC).
- Het verbeteren van de toegangsbeveiliging voor (en het monitoring hiervan op) de domeinen ccmo.nl, romero.nl en toetsingonline.nl (DNSSEC, STARTTLS, DANE, IPv6).
- Alle websites van de CCMO conformeren aan de wet GDI en de Europese standaard EN 301549, welke van kracht is medio 2018. Daarnaast de nieuwe websites voorzien van een toegankelijkheidsverklaring en privacy-verklaring.
- De nieuwe websites van de CCMO voorbereiden op de wet eIDAS verordening 910/2014/EG, welke van kracht is per september 2018.

Ondertekening:

5.1.2.e
algemeen secretaris

Centrale Commissie Mensgebonden Onderzoek (CCMO)
Parnassusplein 5 | 2511 VX Den Haag
Postbus 16302 | 2500 BH Den Haag
T 070 340 6700 | E ccmo@ccmo.nl | I http://www.ccmo.nl

5. IB-plan

In dit hoofdstuk komen de plannen voor het komende jaar over Informatiebeveiliging. Hierin worden de bijstellingen doorgevoerd die zijn voorgesteld in de vooruitblik.

5.1 Activiteiten in het kader informatiebeveiliging en eigenaarschap informatiesystemen

Het uitvoeren geplande acties en/of onderzoeken van aanbevelingen voor alle systemen genoemd in hoofdstuk 3.1 en 4.1.

5.2 Beveiligingsbewustzijn medewerkers

Er vindt jaarlijks voorlichting plaats binnen de organisatie over beleid, procedures, maatregelen, naleving en evt. incidenten op het gebied van informatiebeveiliging, privacy en integriteit. Het komende jaar zullen de volgende acties worden ondernomen om het beveiligingsbewustzijn van de medewerkers te verbeteren:

Het uitvoeren van het plan beveiligingsbewustzijn 2021 waar het volgende in wordt opgenomen:.

- Het bespreken van actuele onderwerpen op het CCMO bureauoverleg.
- Het verplicht volgen van online modules “Informatiebeveiliging” en “Privacy en AVG” op het opleidingspaspoort-platform van VWS voor de nieuwe mensne die dat nogf niet gedaan hebben.
- Het verspreiden van actuele informatie aangeleverd door de CISO en Privacy Officer kerndepartement aan de medewerkers van de CCMO.
- E-mailberichten ter bewustwording van dreigende zaken op de werkvloer of het digitale werken aan de medewerkers van de CCMO.
- Blijven werken aan de bewustwording van informatiebeveiliging bij medewerkers en commissieleden van de CCMO en METC’s.

5.3 Controle autorisaties

De CCMO controleert tweemaal per jaar de toegangsrechten van alle systemen die door SSC-ICT worden verleend, i.p.v. het advies om dit eenmaal per jaar uit te voeren. Als leidraad wordt hiervoor het CCMO autorisatiemodel gebruikt.
Aanbeveling is om dit komende jaar voort te zetten, gezien het aantal fouten dat wordt geconstateerd. Daarnaast is het aan te bevelen om de lijst ICT middelen van de directie regelmatig te controleren. Bij wijzigingen van medewerkers klopt de registratie van deze middelen vaak niet. Bij eventuele calamiteiten zal deze lijst correct moeten zijn, om de toegang tot deze middelen direct te kunnen ontzeggen.

Er wordt een controle uitgevoerd op de toegangsrechten van:

Extern:
Website ToetsingOnline
Website CCMO
Viadesk samenwerkingsruimte
European Medicines Agency (VPN koppeling Londen)

Intern:
Outlook dienstpostbussen
Rechten netwerkschijven
Marjolein
3F
GMI
DigiInkoop

IDM
TEM
P-Direkt
ICT middelen medewerkers CCMO (SSC-ICT)

De geplande acties zijn:

Doorlopende controle op registratie van ICT middelen medewerkers
Doorlopende controle op email en websites beveiligingen (internet.nl, cookiechecker.nl etc.)

December 2021:	Periodieke controle autorisaties bedrijfsvoeringapplicaties (2e controle) Check opgave van belangen en (nevenfuncties) commissieleden (2e controle)
Januari 2022:	Check toegang alle systemen (1e controle) Check geheimhoudingsverklaringen / bewerkersovereenkomsten (1e controle)
Mei 2022:	Jaarlijkse check op geldigheid compliances (ISO / NEN certificaten) van externe leveranciers
Juni 2022:	Check opgave van belangen en (nevenfuncties) commissieleden (1e controle) Periodieke controle autorisaties bedrijfsvoeringapplicaties (1e controle)
Juli 2022:	Check toegang alle systemen (2e controle) Check geheimhoudingsverklaringen / bewerkersovereenkomsten (2e controle)
December 2022:	Periodieke controle autorisaties bedrijfsvoeringapplicaties (2e controle) Check opgave van belangen en (nevenfuncties) commissieleden (2e controle)

Sleutelbeheer
De CCMO heeft een aantal archiefkasten op de 15e etage. Deze kasten worden enerzijds gebruikt voor de opslag van het dynamische archief en anderzijds gebruikt door de medewerkers (persoonlijke één-meter plank). Alle genoemde kasten zijn altijd afgesloten.

[redacted]
5.1.2.h

6. Verwijzingen

- CCMO autorisatiemodel
- CCMO informatiebeveiligingsbeleid
- CCMO privacy beleid
- CCMO integriteitsbeleid

7. Referenties

- Een veilig VWS

8. Bijlage 1: Overzicht processen en systemen

Informatie systeem	Beleidsprocessen	Classificatie proces	BEI eisen proces	Belang IS voor proces	Risico analyse aanwezig
Website www.toetsingonline.nl	- Het registreren van protocollen van medisch-wetenschappelijk onderzoek met mensen. - Het toetsen van protocollen van medisch-wetenschappelijk onderzoek met mensen.	S	L,L,ZL	N	Ja, d.d. februari en maart 2013. Q3 2019 planning van nieuwe risicoanalyse.
Website www.ccmo.nl	- Geven van voorlichting over de uitvoering en toepassing van de Wet medisch-wetenschappelijk onderzoek met mensen.	O	ZL,ZL,ZL	O	Nee
Marjolein	- Het toetsen van protcollen van medisch-wetenschappelijk onderzoek met mensen. - Bevoegde instantie van geneesmiddelenonderzoek. - Erkennen van medisch-ethische toetsingscommissies. - Toezicht op de werkzaamheden van erkende METC's. - Administratief beroeps- en bezwaarorgaan.	S	L,L,ZL	N	Nee
Viadesk	- Het toetsen van protocollen van medisch-wetenschappelijk onderzoek met mensen. - Bevoegde instantie	S	L,L,ZL	O	Ja, quickscan BIR uitgevoerd op 11-12-2017

	van geneesmiddelenonderzoek (VHP).				
ROMERO	- alle bovengenoemde	S	L,L,ZL	N	Ja, quickscan AVG uitgevoerd op 29-01-2019 en DPIA uitgevoerd op 24-05-2019
Archief (papier)	- alle bovengenoemde	O	L,L,ZL	O	Nee

Legenda:

Kolom classificatie van het proces

K = kritisch strategisch (Bij afwezigheid van het proces of het niet goed functioneren loopt de haalbaarheid van de hoofddoelstelling van de organisatie direct gevaar op)
S = strategisch (Bij afwezigheid van het proces of het niet goed functioneren van het proces kan het halen van de hoofddoelstelling van de organisatie in gevaar komen)
B = bijdragend (Bij afwezigheid van het proces of het niet goed functioneren komt het halen van de hoofddoelstelling niet direct in gevaar)
O = ondersteunend (Bij afwezigheid van het proces of het niet goed functioneren komt het halen van de hoofddoelstelling niet in gevaar)

Kolom BEI eisen van het proces (B = beschikbaarheid, E= exclusiviteit, I= integriteit)

ZH = zeer hoog
H = hoog
L = laag
ZL = zeer laag

Kolom belang informatiesysteem voor het proces

V = Vitaal systeem (Het proces kan niet meer voortbestaan zonder de aanwezigheid van het informatiesysteem. Zonder informatiesysteem werkt het proces niet)
N = Nuttig systeem (Bij niet goed functioneren van het systeem wordt het proces ondoelmatig of niet efficiënt)
O = Ondersteunend systeem (Het proces kan voor een bepaalde periode zonder systeem)
G = Geen relatie (In voortgang en kwaliteit van het proces speelt het informatiesysteem geen rol)

9. *Bijlage 2: Overzicht AVG-verwerkingen*

Dit overzicht is gesorteerd op meldingsnummer

Nummer	Naam	Doel verwerking	Type verwerking	Status
M1004	6 Verzending van nieuwsbrieven	Verzending van de CCMO nieuwsbrief aan belangstellenden die zich hiervoor hebben aangemeld via de CCMO-website. De verwerking is een onderdeel van het proces: Geven van voorlichting over de uitvoering en toepassing van de Wet medisch-wetenschappelijk onderzoek met mensen.	Secundair	Definitief
M4921	6 Analyse van webstatistieken van bezoekers websites	De CCMO gebruikt webstatistieken om te begrijpen hoe bezoekers de websites gebruiken. Deze informatie helpt de websites te verbeteren, bijvoorbeeld door informatie aan te vullen of door het gebruikersgemak te verbeteren.	Secundair	Definitief
M4922	6 Publicaties op CCMO website	De CCMO publiceert de samenstelling van de CCMO commissie, secretariaat CCMO en de lokale erkende medisch-ethische toetsingscommissies op de website van de CCMO. Deze informatie is noodzakelijk voor de goede vervulling van de publiekrechtelijke taak, namelijk het creëren en bevorderen van transparantie naar en vertrouwen bij organisaties, burgers en communicatie met derden.	Secundair	Definitief
M4926	1a Beoordeling van protocollen medisch-wetenschappelijk onderzoek met mensen	De toetsingscommissie beoordeelt onderzoeksvoorstellen in specifieke onderzoeksgebieden zoals in de wet vastgelegd. Het betreft de wetten: Wet medisch-wetenschappelijk onderzoek met mensen (WMO) en de Embryowet. Deze verwerking is onderdeel van het proces: Beoordelen van protocollen van medisch-wetenschappelijk onderzoek met mensen.	Primair	Definitief
M4929	1b Beoordeling veiligheidsinformatie goedgekeurde, lopende onderzoeken	De toetsingscommissie beoordeelt veiligheidsinformatie (SAE's en SUSAR's) van goedgekeurd, lopend onderzoek. Deze verwerking is onderdeel van het proces: Beoordelen van protocollen van medisch-wetenschappelijk onderzoek met mensen.	Primair	Definitief
M4930	3b Toezicht functioneren van METC's	De CCMO houdt toezicht (naar aanleiding van incidenten, meldingen, signalen en dergelijke) en doorlopend toezicht (monitoring van de	Primair	Definitief

		kwaliteit). Hierbij staat het continue verbeterproces van de erkende METC's centraal. Deze verwerking is onderdeel van het proces: Toezicht.		
M4932	4 Behandelen administratief beroep tegen besluit lokale METC	De CCMO behandelt het administratief beroepschrift van een belanghebbende indien deze een administratief bezwaar instelt tegen een besluit van de lokale toetsingscommissie. Deze verwerking is onderdeel van het proces: Behandelen van administratief beroep op een beslissing door een toetsingscommissie.	Primair	Definitief
M4933	4 Behandelen bezwaar tegen besluit CCMO	De CCMO behandelt het bezwaarschrift van een belanghebbende indien deze een bezwaar indient tegen het besluit van de CCMO. Deze verwerking is onderdeel van het proces: Behandelen van bezwaar op een beslissing door een toetsingscommissie.	Primair	Definitief
M4934	6 Vergaderingen met externen	De CCMO heeft regelmatig overleg met externen, zoals ketenpartners, commissieleden, voorzitters en secretarissen en andere belanghebbenden over praktische en juridische aspecten m.b.t. toetsing van medisch-wetenschappelijk onderzoek met mensen.	Secundair	Definitief
M4935	2 Marginale toets onderzoek met geneesmiddelen als Bevoegde Instantie	Toetsing en afgifte verklaring van geen bezwaar als bevoegde instantie. De CCMO is de bevoegde instantie wanneer een andere medisch-ethische toetsingscommissie een onderzoeksvoorstel met geneesmiddelen beoordeelt. Deze verwerking is onderdeel van het proces: Uitvoeren van een marginale toets op onderzoek met geneesmiddelen.	Primair	Definitief
M5030	3a Toezicht METC en erkenning leden	De CCMO houdt toezicht vooraf, zoals de beoordeling van reglementen, de deskundigheid en onafhankelijkheid van de leden van erkende METC's. Deze verwerking is onderdeel van het proces: Toezicht.	Primair	Definitief
M7440	1 Beoordeling van protocollen pilot EU-verordening 536/2014	Pilot voor het beoordelen van voorstellen voor geneesmiddelenonderzoek zoals in de aankomende EU-verordening 536/2014 is vastgelegd. De CCMO of de lokale METC's werken in samenwerking met andere EU-lidstaten aan de beoordeling van het VHP onderzoeksvoorstel en amendementen. Deze verwerking is onderdeel van het proces:	Primair	Definitief

		Beoordelen van protocollen van medisch-wetenschappelijk onderzoek met mensen.		
M7442	6 Afhandeling vragen via dienstpostbussen	De CCMO heeft als uitvoeringsorgaan een spilfunctie als (inter)nationale vraagbaak over medisch-wetenschappelijk onderzoek met mensen dat (mede) in Nederland wordt uitgevoerd. Vragen van correspondenten komen binnen via verschillende dienstpostbussen. Deze verwerking is onderdeel van het proces: Geven van voorlichting over de uitvoering en toepassing van de Wet medisch-wetenschappelijk onderzoek met mensen.	Secundair	Definitief
M7443	1 Beoordeling van protocollen pilot EU-verordening 2017/745 en 2017/746	Pilot voor het beoordelen van voorstellen voor onderzoek met medische hulpmiddelen en in-vitrodiagnostica zoals in de aankomende EU-verordeningen 2017/745 en 2017/746 is vastgelegd. De CCMO (validatie) en de lokale METC's (beoordeling) werken in samenwerking met IGJ (marktoezicht op product of opdrachtgever) aan de beoordeling van het onderzoeksvoorstel en amendementen. Deze verwerking is onderdeel van het proces: Beoordelen van protocollen van medisch-wetenschappelijk onderzoek met mensen.	Primair	Definitief
M7454	1 Werving, selectie en (her)benoeming van commissieleden	De leden en de plaatsvervangende leden van de CCMO worden benoemd bij ministerieel besluit. Werving en selectie van een nieuw commissielid gaat volgens het coöptatiesysteem, waar het vertrekkende lid kandidaten aandraagt binnen zijn/haar eigen discipline. Deze verwerking is onderdeel van het proces: Beoordelen van protocollen van medisch-wetenschappelijk onderzoek met mensen.	Primair	Definitief
M7463	4 Behandeling van klachten over het handelen van de CCMO	De CCMO behandelt klachten over het handelen van de CCMO overeenkomstig de Klachtenregeling CCMO.	Primair	Definitief
M7464	4 Behandeling van bezwaar tegen openbaarmaking CCMO-register	Kerngegevens van mensgebonden medisch-wetenschappelijk onderzoek dat in Nederland is beoordeeld door een erkende METC of de CCMO worden in het openbare CCMO-register geplaatst. Een jaar na einde	Primair	Definitief

		onderzoek dienen de onderzoeksresultaten eveneens openbaar gemaakt worden. De CCMO behandelt bezwaren tegen de openbaarmaking van deze onderzoeksinformatie van medisch-wetenschappelijk onderzoek met mensen in het CCMO-register.		
M7465	1 Wetenschappelijk advies aan het CBG	De CCMO brengt wetenschappelijk advies uit in voorkomende gevallen op verzoek van het CBG.	Primair	Definitief
M7466	7 Personele administratie	De verwerking van personele gegevens van medewerkers van de CCMO. Voor werving, selectie en indiensttreding (M5494); aanvraag ARBO-middelen (M4586); Formatie en bezetting & personeelsplanning (M3457); Personeelsbeheer (ambtenaren) (M2090, 2112); Ontwikkeling medewerkers (M2109); Ziekteverzuim, reintegratie, herstel (M4557, M4558, M4559, M4567); IDM rijkspas (M1177); Rijksadresgids (M1007); Rijksdirectory (M988); Rijksportaal (M845); BvRIN (M1010); Single Sign On (M1008).	Secundair	Definitief
M7468	7 Financiële administratie	Het verwerken van salarissen, facturen, vaste vergoedingen, binnen- en buitenlandse dienstreizen en overige declaraties.	Secundair	Definitief
M7470	4 Behandeling van Wob-verzoeken	De CCMO behandelt verzoeken om informatie op grond van de Wet openbaarheid van bestuur (Wob).	Primair	Definitief
M7479	6 Research en monitoring van rapportages Social Media	De CCMO ontvangt wekelijkse rapportages van berichten op sociale media die worden verzameld op basis van vooraf gekozen steekwoorden. De verzamelde informatie helpt de publieke opinie te achterhalen over medisch-wetenschappelijk onderzoek en biedt inzicht in wat er in de buitenwereld speelt. Dit inzicht kan gebruikt worden om bijvoorbeeld de informatievoorziening op de website verder te optimaliseren of om via de eigen sociale-mediakanalen te reageren op berichten van sociale-mediagebruikers.	Secundair	Definitief
M7564	7 Administratie van toegang tot IT-middelen en systemen	De CCMO registreert de uitgifte en inname van IT-middelen en verleent toegang tot verschillende systemen aan medewerkers en commissieleden aan de hand van het CCMO autorisatiemodel. Elk half jaar worden de	Secundair	Definitief

		autorisaties op alle systemen gecontroleerd aan de hand van functie of rollen. Voor dit proces worden gebruikersovereenkomsten, verklaringen, controlelijsten en managementoverzichten bewaard in het informatiebeveiligingsdossier van de CCMO.		
M7566	7 Registratie van geheimhoudings verklaringen	De CCMO bewaart geheimhoudingsverklaringen van externe personen en samenwerkingsovereenkomsten met ketenpartners in het informatiebeveiligingsdossier van de CCMO.	Secundair	Definitief
M7573	6 Relatiebeheer externe contacten	De CCMO onderhoudt contacten en communiceert met externe relaties, zoals ketenpartners, METC's, branche-organisaties, patiëntverenigingen, instellingen, andere (overheids) organisaties, leveranciers etc.	Secundair	Definitief
	7 Behandelen verzoeken AVG		Secundair	Nog niet gestart
	7 Check compliance leveranciers (intern en extern)		Secundair	Nog niet gestart
	7 Behandelen verzoeken AVG		Secundair	Nog niet gestart
	7 Leveranciers Incident/changes etc (Jira, Topdesk enzo)		Secundair	Nog niet gestart
	7 IB / AVG / Integriteit incidenten (anoniem en info beveiligd voor MT)		Secundair	Nog niet gestart
	7 Accountbeheer (ToetsingOnline, Viadesk)		Secundair	Nog niet gestart
	7 Bezoekers gebouw (FMH)		Secundair	Nog niet gestart
	7 AVG-register verwerkingen		Secundair	Nog niet gestart

10. Bijlage 3: Overzicht Te Beschermen Belangen / EU en NATO informatie

Formulier 1: Invulinstructie Te Beschermen Belangen (TBB)

1. Welke spionagegevoelige Te Beschermen Belangen (TBB) zijn in uw organisatie aanwezig?

   - ○ **staatsgeheim** (nationaal) gerubriceerde informatie
   - **X** **EU** of **NAVO** (internationaal) gerubriceerde informatie (*Zo ja, vul formulier 2 ook in*)
   - ○ **Spionagegevoelige** informatie, gerubriceerd of niet-gerubriceerd

2. Vermeld bij ieder TBB de **opslag**(locatie), zoals de ICT-systemen.
3. Vermeld bij ieder TBB de **verantwoordelijke** persoon.
4. Houden de **beveiligingsmaatregelen** rekening met spionagedreiging?
5. Zijn de beveiligingsmaatregelen **op orde**?
6. Zijn er **restrisico's** voor een kernbelang.
   Zo ja, zijn die geaccepteerd door de eindverantwoordelijke binnen uw organisatie?

Datum:

Naam: [redacted]

Functie: Algemeen Secretaris

Directie / organisatie: CCMO

Formulier 2: Invulinstructie EU en NAVO informatie
Inventarisatie ten behoeve van de National Security Authority-Nederland (NSA-NL)

AFDELING/DIRECTIE/DIENSTEN/INSTELLINGEN	EU INFORMATIE	NAVO INFORMATIE
CCMO	**X** Ja ○ Nee	○ Ja **X** Nee

Indien JA geantwoord:

1. Wat zijn de EU en/of NAVO **rubriceringsniveaus** van de informatie waarmee gewerkt wordt?
   Departementaal Vertrouwelijk

2. Hoe wordt deze informatie **verwerkt**/behandeld? (fysiek/digitaal)
   Digitaal

   Hoe komt deze informatie binnen?
   Via Eudralink of CIRCABC. Een enkele keer via email.

   Hoe wordt dit (i.e. binnenkomende EU/NAVO-gerubriceerde informatie) zichtbaar gemaakt en gedistribueerd?
   In afdelingsmappen op het netwerk van SSC-ICT

   Hoe wordt opgeslagen/bewaard?
   In afdelingsmappen op het netwerk van SSC-ICT

   Indien digitaal: welke systeem wordt hiervoor gebruikt (vb.: eigen netwerk/stand alone)?
   Marjolein, netwerk SSC-ICT

3. Zijn de medewerkers op de hoogte hoe om te gaan met EU en/of NAVO gerubriceerde gegevens?
   Ja

4. Zijn er medewerkers die deel uit maken van EU en/of NAVO **werkgroepen**?
   Zo ja, welke welkgroepen?

- CTFG (Clinical Trial Faciliation Group)
- EU clinical trial information systems expert group
- Expert group on clinical trials
- Commission Working Group (onder Medical Devices Coördination Group (MDCG))
- Ad hoc working group on the interplay between the GMO and the pharmaceuticals legislation

   Krijgen zij na een EU of NAVO vergadering/bijeenkomst informatie in handen mee?
   Nee

5. Zijn er ook **externen** (niet-VWS medewerkers) die voor/namens VWS werkzaamheden uitvoeren en met EU en/of NAVO informatie werken?

   Ja

6. Zijn er medewerkers die kennis moeten nemen van EU en/of NAVO informatie in het bezit van een juiste en geldige **clearance**[1]?

   Ja

7. Zijn er VWS medewerkers die **<u>buiten</u> VWS om** in aanraking komen met EU en/of NAVO informatie? (bijvoorbeeld: deel uit maken van werkgroepen onder verantwoordelijkheid van andere ministeries, niet overheidsinstanties?)

   Nee

Datum:

Naam: 5.1.2.e

Functie: Algemeen Secretaris

Directie / organisatie CCMO

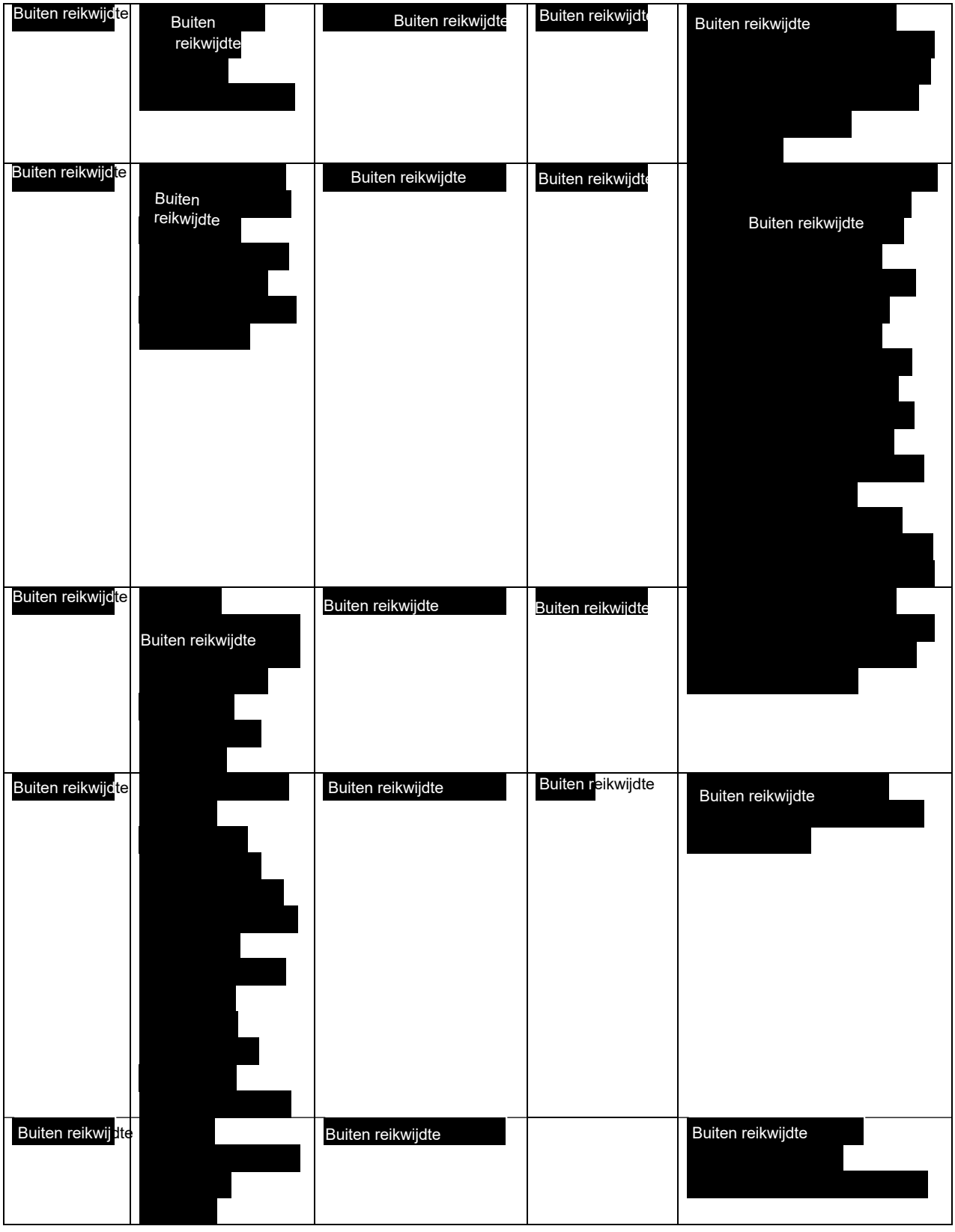
[1] *A security clearance is a status granted to individuals allowing them access to classified information (state or organizational secrets) or to restricted areas, after completion of a thorough background check.*
NL: Een status met verklaring dat - uit het oogpunt van de nationale en/of internationale veiligheid - geen bezwaar bestaat tegen toegang tot geclassificeerde of gerubriceerde informatie.

11. Bijlage 4: Overzicht beveiligingsincidenten

Dit overzicht is geanonimiseerd!

Datum	Omschrijving incident	Categorie Informatiebeveiliging. AVG Fysieke beveiliging Personele /persoonsbeveiliging Integriteit	Status	Omschrijving Afhandeling
Buiten reikwijdte	Buiten reikwijdte	Buiten reikwijdte	Buiten reikwijdte	Buiten reikwijdte
Buiten reikwijdte	Buiten reikwijdte	Buiten reikwijdte	Buiten reikwijdte	
Buiten reikwijdte	Buiten reikwijdte	Buiten reikwijdte	Buiten reikwijdte	
Buiten reikwijdte	Buiten reikwijdte	Buiten reikwijdte	Buiten reikwijdte	
Buiten reikwijdte	Buiten reikwijdte	Buiten reikwijdte	Buiten reikwijdte	

Buiten reikwijdte	Buiten reikwijdte [redacted]	Buiten reikwijdte	Buiten reikwijdte	Buiten reikwijdte [redacted]
Buiten reikwijdte	Buiten reikwijdte [redacted]	Buiten reikwijdte	Buiten reikwijdte	[redacted]
Buiten reikwijdte	Buiten reikwijdte [redacted]	Buiten reikwijdte	Buiten reikwijdte	[redacted]
Buiten reikwijdte	Buiten reikwijdte [redacted]	Buiten reikwijdte	Buiten reikwijdte	[redacted]
Buiten reikwijdte	[redacted]	Buiten reikwijdte	Buiten reikwijdte	[redacted]
Buiten reikwijdte	[redacted] Buiten reikwijdte [redacted]	Buiten reikwijdte	Buiten reikwijdte	[redacted]
Buiten reikwijdte	Buiten reikwijdte [redacted]	Buiten reikwijdte	Buiten reikwijdte	[redacted]


Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte
Buiten reikwijdte

	Buiten reikwijdte			Buiten reikwijdte

Melden bij 5.1.2.e @minvws.nl en iig phishing bij SSC-ICT en ciso kern (CC)