Centrale
Commissie
Mensgebonden
Onderzoek

Informatiebeveilingsplan

Titel Verantwoording & Vooruitblik CCMO 2018
Ingangsdatum 1 januari 2019
Versie 1.0
Status Definitief

Verantwoordelijken

Opgesteld door	*Functie*	*Handtekening*
5.1.2.e	5.1.2.e	5.1.2.e 14/1/2019
Beoordeeld door	*Functie*	*Handtekening*
5.1.2.e	5.1.2.e	5.1.2.e 14 01 2019
Geautoriseerd door	*Functie*	*Handtekening*
5.1.2.e	Algemeen secretaris	5.1.2.e 14/1/2019

Versiebeheer

Versie	*Datum*	*Omschrijving*	*Naam*	*Status*
0.1	11-10-2018	Eerste versie document	5.1.2.e 5.1.2.e	concept
1.0	14-01-2019	Wijzigingen doorgevoerd op verzoek management / goedkeuring document	5.1.2.e 5.1.2.e	definitief

Inhoudsopgave

1. Inleiding 3
2. Informatiesystemen, AVG-registraties en TBB 3
   2.1 Eigenaarschap systemen 3
   2.2 Overzicht processen en systemen 4
   2.3 Overzicht registraties persoonsgegevens 4
   2.4 Vertrouwensfuncties 4
   2.5 Te beschermen belangen (TBB) en EU / NATO informatie 4
3. Verantwoording 4
   3.1 Voortgang van de te implementeren maatregelen 5
   3.2 Incidenten 9
   3.3 Conclusie 9
4. Vooruitblik 10
   4.1 Aanbevelingen 10
5. IB-plan 12
   5.1 Activiteiten in het kader informatiebeveiliging en eigenaarschap informatiesystemen 12
   5.2 Beveiligingsbewustzijn medewerkers 12
   5.3 Controle autorisaties 12
6. Verwijzingen 13
7. Referenties 13
8. Bijlage 1: Overzicht processen en systemen 14
9. Bijlage 2: Overzicht AVG-verwerkingen 16
10. Bijlage 3: Overzicht Te Beschermen Belangen / EU en NATO informatie 19
11. Bijlage 4: Overzicht beveiligingsincidenten 22

1. *Inleiding*

Het management van de Centrale Commissie Mensgebonden Onderzoek (CCMO) is verantwoordelijkheid 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 Te Beschermen Belangen.

2.1 Eigenaarschap systemen

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

Website CCMO	https://www.ccmo.nl
Website ToetsingOnline	https://www.toetsingonline.nl
Website Onderzoekswijs	https://www.onderzoekswijs.nl

Marjolein (document management systeem VWS)
Bedrijfsvoeringapplicaties VWS (IDM, GMI, 3F, HIS, DigiInkoop, TEM, SSC-ICT netwerk en applicaties, Planon, AVG-register, ISMS),
P-Direkt (personeel management systeem VWS)
Viadesk (samenwerkingsruimte voor commissieleden en METC's)
VWS-Flex (samenwerkingsruimte voor projectgroep EU-verordening)
Formdesk (online formulieren management systeem voor commissieleden)

* De CCMO is alleen verantwoordelijk voor de data-gegevens in Marjolein, bedrijfsvoeringapplicaties VWS, P-Direkt, Viadesk, VWS-Flex en Formdesk; 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 Rijksdienst valt (BIR).

De volgende systemen vallen boven de Baseline:

Geen (alle systemen zijn gerubriceerd op vertrouwelijkheidsniveau Departementaal Vertrouwelijk)

Het afgelopen jaar is het volgende gewijzigd:
Er is in het afgelopen jaar geen risicoanalyse uitgevoerd op bovenstaande systemen. Er zijn daarnaast geen wijzigingen in bovenstaande systemen doorgevoerd zodat deze boven de Baseline zouden kunnen vallen.

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 in het afgelopen jaar nog geen risicoanalyses uitgevoerd. Er zijn wijzigingen in het beschermingsniveau van de 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 gepland staat per 1 januari 2019 van kracht te zijn.

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:
Alle bestaande WBP-registraties zijn opnieuw geanalyseerd en onderverdeeld in de hoofdprocessen van de CCMO. De nieuwe verwerkingen zijn ingevoerd in het AVG-register van het Ministerie van VWS.

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 Verantwoording & Vooruitblik CCMO 2017 bevat een overzicht van openstaande aanbevelingen van de auditresultaten voor ToetsingOnline (www.toetsingonline.nl) om de risico's te verlagen. Deze maatregelen waren verwerkt in de laatst ontwikkelde release 4.0. Recentelijk is door het management besloten om de doorontwikkeling van ToetsingOnline per direct te stoppen en deze release niet meer uit te brengen. Er is aan de hand van een pentest in november 2018 een inventarisatie gemaakt op de huidige versie van het systeem om het beveiligingsniveau zo hoog mogelijk te krijgen en te houden. Deze resultaten worden zo snel mogelijk verwerkt in een nieuwe release van het systeem.

Website CCMO

De huidige website van de CCMO (www.ccmo.nl) voldoet niet aan de open standaarden voor rijkswebsites. Daarnaast voldoet de leverancier niet volledig aan de vereiste compliances aan de hand van de BIR richtlijn 10.2.2 (risicofactor 16). Dit jaar is een project gestart om de website onder te brengen bij Platform Rijksoverheid (PRO). De nieuwe website is in november 2018 live gegaan. De contracten van de leverancier zijn opgezegd, de oude websites zijn opgeheven en de domeinnaam is ondergebracht bij het Ministerie van Algemene Zaken. Voor deze website wordt om deze reden dit jaar geen risicoanalyse of AVG quickscan uitgevoerd.

Website CCMO jaarverslag

De huidige website van de CCMO (www.ccmo-jaarverslag.nl) voldoet niet aan de open standaarden voor rijkswebsites. Daarnaast voldoet de leverancier niet volledig aan de vereiste compliances aan de hand van de BIR richtlijn 10.2.2 (risicofactor 16). Dit jaar is een project gestart om de website onder te brengen bij Platform Rijksoverheid (PRO). De jaarverslagen pagina's zijn ondergebracht in de nieuwe PRO website van de CCMO (www.ccmo.nl). De contracten van de leverancier zijn opgezegd, de oude websites zijn opgeheven en de domeinnaam is ondergebracht bij het Ministerie van Algemene Zaken. Voor deze website wordt om deze reden dit jaar geen risicoanalyse of AVG quickscan uitgevoerd.

Website Onderzoekswijs

De huidige website Onderzoekswijs (www.onderzoekswijs.nl) voldoet niet aan de open standaarden voor rijkswebsites. Daarnaast voldoet de leverancier niet volledig aan de vereiste compliances aan de hand van de BIR richtlijn 10.2.2 (risicofactor 16). Dit jaar is een project gestart om deze website over te dragen naar een andere (externe) organisatie. Deze website wordt op dit moment gebouwd ter vervanging van onze website. De verwachting is dat deze nieuwe website in het eerste halfjaar van 2019 live gaat. De website Onderzoekswijs wordt dan vervolgens opgeheven.
Voor deze website wordt om deze reden dit jaar geen risicoanalyse of AVG quickscan uitgevoerd.

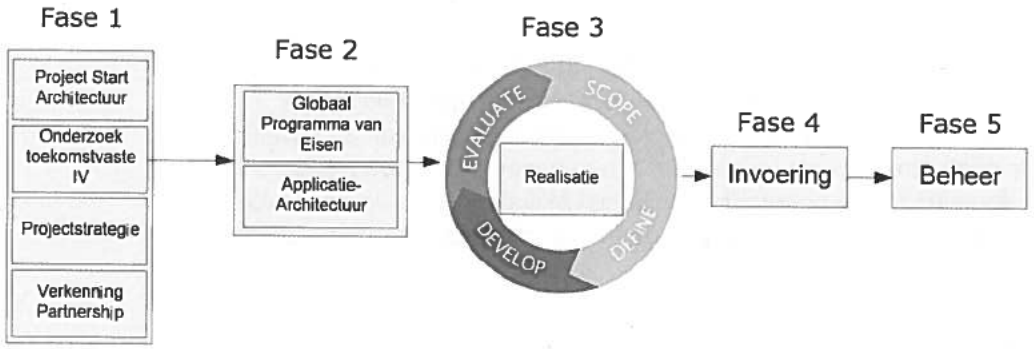
Webapplicatie Formdesk

Het online formulieren management systeem Formdesk is recentelijk in gebruik genomen om de verklaringen van belangen van de commissieleden, sneller en eenvoudiger te laten

invullen. Deze verklaringen worden op de website van de CCMO gepubliceerd. De verklaring zal digitaal worden ondertekend, i.p.v. de natte handtekening om identiteitsfraude te voorkomen. Een risicoanalyse staat op de planning om uitgevoerd te worden.

IV vernieuwing
De CCMO maakt gebruik van verschillende ICT-systemen, zowel intern als extern, om haar wettelijke taken te kunnen uitvoeren. Naar aanleiding van de EU-verordening: EU nr 536/2014 wordt op dit moment een EU-portaal gebouwd, dat in samenwerking met de lidstaten en de Europese Geneesmiddelen Agentschap (EMA) wordt opgezet. Het EU-portaal fungeert als centraal punt voor de indiening van gegevens en informatie over klinische proeven met geneesmiddelen in EU-lidstaten. De CCMO zal als Landelijk Bureau gaan fungeren en ondergaat hierdoor een grote organisatorische verandering.
Het 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. Na inwerkingtreding van de EU Verordening, moet toetsing van de overige mensgebonden onderzoeken (NB: Zo'n 70% van het totaal aantal WMO onderzoeken) door dezelfde organisatiestructuur uitgevoerd worden als de geneesmiddelenonderzoeken, maar mag daarvoor geen gebruik maken van het EU-Portaal. Hiervoor is een aparte (reeds bestaande) ICT ondersteuning nodig. Het IV vernieuwingstraject en de aansluiting op het EU-portaal zal een geüniformeerd platform gaan bieden. In oktober 2018 wordt gestart met fase 2:

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 BIR richtlijn 10.2.2 (risicofactor 16). Deze maatregel is uitgevoerd (Q2 2018).
- Voor het technisch beheer en de doorontwikkeling van ToetsingOnline is het contract met de leverancier is verlengd en de verwerkersovereenkomst (Arvodi 2016) getekend. Deze maatregel is uitgevoerd (Q4 2017).
- Nieuwe risicoanalyse & AVG quickscan uitvoeren ivm het in stand houden van de huidige versie van ToetsingOnline. Deze maatregel is ingepland (Q1 2019).

- Aanbeveling om de mogelijkheden te onderzoeken voor verhuizen van de website ccmo.nl en ccmo-jaarverslag.nl naar Platform Rijksoverheid (PRO) of een leverancier met compliances (ISO / NEN certificaten) aan de hand van de BIR richtlijn 10.2.2 (risicofactor 16). Deze maatregel is uitgevoerd (Q2 2018).

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

Website ToetsingOnline
- Nieuwe risicoanalyse & AVG quickscan uitvoeren. Deze maatregel is ingepland (Q1 2019).
- Uitvoeren van pentest op huidige release van ToetsingOnline. Deze maatregels is uitgevoerd (Q4 2018).
- Het verhuizen van het eigenaarschap van de domeinnaam naar Dienst Publiek en Communicatie van het Ministerie van Algemene Zaken. Deze maatregel is ingepland (Q1 2019).
- Jaarlijkse check op geldigheid compliances (ISO / NEN certificaten) van de leverancier aan de hand van de BIR richtlijn 10.2.2 (risicofactor 16). Deze maatregel is ingepland (Q2 2019).

Website CCMO
- Het verhuizen van het eigenaarschap van de domeinnaam naar Dienst Publiek en Communicatie van het Ministerie van Algemene Zaken. Deze maatregel is uitgevoerd (Q2 2018).
- Het verhuizen van deze website naar Platform Rijksoverheid (PRO).Deze maatregel is uitgevoerd (Q4 2018).
- Het opvragen van risicoanalyses / ICV van Platform Rijksoverheid. Deze maatregel is ingepland (Q1 2019).

Website CCMO jaarverslag
- Het verhuizen van het eigenaarschap van de domeinnaam naar Dienst Publiek en Communicatie van het Ministerie van Algemene Zaken. Deze maatregel is uitgevoerd (Q3 2018).
- Het verhuizen van deze website naar Platform Rijksoverheid (PRO).Deze maatregel is uitgevoerd (Q4 2018).
- Het opvragen van risicoanalyses / ICV van Platform Rijksoverheid. Deze maatregel is ingepland (Q1 2019).

Website Onderzoekswijs
- Het opheffen van deze website door nieuwe website van een andere organisatie; (Q2 of Q3 2019).
- Jaarlijkse check op geldigheid compliances (ISO / NEN certificaten) van de leverancier aan de hand van de BIR richtlijn 10.2.2 (risicofactor 16). Deze maatregel is ingepland (Q1 2019).

Webapplicatie Formdesk
- Nieuwe risicoanalyse & AVG quickscan uitvoeren. Deze maatregel is ingepland (Q1 2019).

IV vernieuwing
- Het uitvoeren van een Privacy Impact Assessment (PIA) & BIR 2017 quickscan voor het bepalen van de te nemen maatregelen. Deze maatregel is op dit moment in uitvoering (Q1 2019).

- Het maken van een overzicht van verplichte webrichtlijnen en andere kaders waar de nieuwe omgeving aan moet voldoen(Q1 2019).

Document management systeem Marjolein

- Nieuwe risicoanalyse en AVG quickscan uitvoeren. Deze maatregel is ingepland (Q1 2019).
- Het opvragen van risicoanalyses / ICV van Ministerie van VWS. Deze maatregel is ingepland (Q1 2019).
- Het schrijven van een procedure m.b.t. de wettelijke richtlijnen digitale archivering. Deze maatregel is ingepland (Q1 2019).
- 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.

Bedrijfsapplicaties VWS

- Nieuwe risicoanalyses en AVG quickscans uitvoeren. Deze maatregel is ingepland (Q1 2019).
- Het opvragen van risicoanalyses / ICV van Ministerie van VWS en SSC-ICT. Deze maatregel is ingepland (Q1 2019).
- Verwerkersovereenkomsten afsluiten indien nodig met de betreffende aanbieders van verschillende ministeries (Q1 2019).

Digitale samenwerkingsruimte Viadesk

- TBB en AVG quickscan uitvoeren om de BIR quickscan te completeren. Deze maatregel is ingepland (Q1 2019).
- Mogelijkheden onderzoeken voor overstappen naar de samenwerkingsruimte Rijksoverheid.
- Jaarlijkse controle op compliances (ISO / NEN certificaten) van de leverancier aan de hand van de BIR richtlijn 10.2.2 (risicofactor 16).). Deze maatregel is uitgevoerd (Q2 2018).

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.

Papieren & digitale archief

- Nieuwe risicoanalyse en AVG quickscan uitvoeren.
- Er is nog één kast met een dynamisch archief over die na registratie naar DocDirekt verhuist. 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 ingepland (Q1 2019).
- Er is nog een deel archief bij een externe leverancier opgeslagen. Er is een project met het Ministerie van VWS gestart om dit archief zsm naar DocDirekt te verplaatsen (Q2 2019).
- De externe harde schijf met alle data van het document management systeem DocsOpen en oude omgeving van ToetsingOnline wordt op een nog nader te bepalen veilige plaats opgeslagen. De mogelijkheden voor opslag hiervoor is opgevraagd bij mogelijke partijen.

Algemeen

- Het maken van een plan van aanpak voor het implementeren van de BIR 2017 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 (Q2 2019).

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 BVA en CISO 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 2019.
- 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 BIR 2017 op alle systemen.
- Het uitvoeren van risicoanalyses en AVG / BIR / TBB quickscans voor alle systemen is gewenst.
- Het finaliseren van verwerkingen in het AVG register van VWS.
- Het gebruik gaan maken van het ISMS van VWS voor opslag IB-documenten en het bewaken van de voortgang van alle IB-activiteiten.
- Het beheer van overige domeinen van de CCMO overdragen aan het Ministerie van Algemene Zaken.
- Alle websites van de CCMO voorbereiden op de wet GDI en de Europese standaard EN 301549, welke van kracht zijn per medio 2018. Daarnaast alle websites voorzien van een toegankelijkheidsverklaring en privacy-verklaring.
- Alle websites 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, ccmo-jaarverslag.nl en toetsingonline.nl (SPF/DKIM/DMARC).
- Het verbeteren van de toegangsbeveiliging voor (en het monitoring hiervan op) de domeinen ccmo.nl, ccmo-jaarverslag.nl en toetsingonline.nl (DNSSEC, STARTTLS, DANE, IPv6). Voor ccmo.nl ligt een actie bij VWS om de beveiliging bij SSC-ICT te verbeteren.

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 de IV vernieuwing en de integratie met het toekomstige EU-portaal. In 2019 zal eveneens 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 BIR 2017 en de daaruit vloeiende acties. De huidige openstaande punten voor het implementeren van de maatregelen van de BIR (2012) 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 verhuizen van ccmo.nl en ccmo-jaarverslag.nl naar het Platform Rijksoverheid.
- Het overdragen en opheffen van onderzoekswijs.nl bij oplevering van de nieuwe voorziening.
- Het verbeteren van de emailbeveiliging voor (en het monitoring hiervan op) de domeinen ccmo.nl, ccmo-jaarverslag.nl en toetsingonline.nl (SPF/DKIM/DMARC).
- Het verbeteren van de toegangsbeveiliging voor (en het monitoring hiervan op) de domeinen ccmo.nl, ccmo-jaarverslag.nl en toetsingonline.nl (DNSSEC, STARTTLS, DANE, IPv6).
- Alle websites van de CCMO voorbereiden op de wet GDI en de Europese standaard EN 301549, welke van kracht is medio 2018. Daarnaast alle websites voorzien van een toegankelijkheidsverklaring en privacy-verklaring.
- Alle websites van de CCMO voorbereiden op de wet eIDAS verordening 910/2014/EG, welke van kracht is per september 2018.

Ondertekening: [redacted]

5.1.2.e

5.1.2.e

algemeen sec[redacted]ris

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 maken van het plan beveiligingsbewustzijn 2019 waar het volgende in wordt opgenomen:.

- Het bespreken van actuele onderwerpen op het CCMO bureauoverleg.
- Het verspreiden van actuele informatie aangeleverd door de CISO, FG of IBX-overleg van VWS 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
Website Onderzoekswijs
Viadesk samenwerkingsruimte
Formdesk
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

December 2018:	Periodieke controle autorisaties bedrijfsvoeringapplicaties (2e controle) Check opgave van belangen en (nevenfuncties) commissieleden (2e controle) Pentest toetsingonline.nl
Januari 2019:	Check toegang alle systemen (1e controle) Check geheimhoudingsverklaringen / bewerkersovereenkomsten (1e controle)
Mei 2019:	Jaarlijkse check op geldigheid compliances (ISO / NEN certificaten) van externe leveranciers
Juni 2019:	Check opgave van belangen en (nevenfuncties) commissieleden (1e controle) Periodieke controle autorisaties bedrijfsvoeringapplicaties (1e controle)
Juli 2019:	Check toegang alle systemen (2e controle) Check geheimhoudingsverklaringen / bewerkersovereenkomsten (2e controle)
December 2019:	Check opgave van belangen en (nevenfuncties) commissieleden (2e controle)

Sleutelbeheer
De CCMO heeft een aantal archiefkasten op de 7e 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 [redacted]

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
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
Website www.onderzoekswijs.nl	- Geven van voorlichting over de uitvoering en toepassing van de Wet medisch-wetenschappelijk onderzoek met mensen.	O	ZL,ZL,ZL	G	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	S	L,L,ZL	N	Nee

	bezwaarorgaan.				
Viadesk	- Het toetsen van protocollen van medisch-wetenschappelijk onderzoek met mensen. - Bevoegde instantie van geneesmiddelenonderzoek (VHP).	S	L,L,ZL	O	Ja, quickscan BIR uitgevoerd op 11-12-2017
Formdesk	- Het toetsen van protocollen van medisch-wetenschappelijk onderzoek met mensen.	O	L,L,ZL	O	Nee
IV vernieuwing	- alle bovengenoemde	S	L,L,ZL	N	Nee
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	6a Voorlichting - Contactgegevens ontvangers nieuwsbrief	Verzending nieuwsbrief CCMO aan geïnteresseerden die zich hiervoor hebben aangemeld via 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.	Primair	Concept
M4921	6b Voorlichting - IP-gegevens bezoekers website	Verstrekken van informatie over toetsing van medisch wetenschappelijk onderzoek met mensen en geldende wetgeving aan diverse betrokken partijen.	Primair	In bewerking
M4922	6c Voorlichting - Beantwoording vragen (algemeen)	Beantwoording van vragen over de toetsing van medisch wetenschappelijk onderzoek met mensen en daarop van toepassing zijnde wetgeving.	Primair	Concept
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	Primair	Definitief

		medisch-wetenschappelijk onderzoek met mensen.		
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 kwaliteit). Hierbij staat het continue verbeterproces van de erkende METC's centraal. Deze verwerking is onderdeel van het proces: Toezicht.	Primair	Definitief
M4932	4a Behandelen administratief beroep tegen oordeel lokale METC	De CCMO behandelt het administratief beroepschrift van een belanghebbende indien deze een administratief bezwaar instelt tegen het oordeel van de lokale toetsingscommissie. Deze verwerking is onderdeel van het proces: Behandelen van administratief beroep op een beslissing door een toetsingscommissie.	Primair	Ter review
M4933	4b Behandelen bezwaar tegen oordeel CCMO	De CCMO behandelt het bezwaarschrift van een belanghebbende indien deze een bezwaar indient tegen het oordeel van de CCMO. Deze verwerking is onderdeel van het proces: Behandelen van bezwaar op een beslissing door een toetsingscommissie.	Primair	Ter review
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
Bijlage	Overzicht gemeenschappelijke verwerkingen VWS	De CCMO maakt gebruik van de standaard kantoorautomatisering van VWS. De in de bijlage genoemde verwerkingen zijn ook van toepassing op de CCMO.	Primair	Definitief

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?

   - o **staatsgeheim** (nationaal) gerubriceerde informatie
   - X **EU** of **NAVO** (internationaal) gerubriceerde informatie (*Zo ja, vul formulier 2 ook in*)
   - o **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: 14/1/2019

Naam: 5.1.2.e

Functie: Algemeen Secretaris

Directie / organisatie: CCMO

5.1.2.e

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
   - 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 **buiten 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:	14-1-2019
Naam:	[redacted] 5.1.2.e
Functie:	Algemeen Secretaris
Directie / organisatie	CCMO

[redacted] 5.1.2.e

[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. WBP Fysieke beveiliging Personele /persoonsbeveiliging Integriteit	Status	Omschrijving Afhandeling
buiten reikwijdte	buiten reikwijdte	buiten reikwijdte	buiten reikwijdte	buiten reikwijdte verzoek
buiten reikwijdte	buiten reikwijdte	buiten reikwijdte	buiten reikwijdte	buiten reikwijdte verzoek
buiten reikwijdte	buiten reikwijdte	buiten reikwijdte	buiten reikwijdte	buiten reikwijdte verzoek
buiten reikwijdte	buiten reikwijdte	buiten reikwijdte	buiten reikwijdte	buiten reikwijdte verzoek

buiten reikwijdte	buiten reikwijdte	buiten reikwijdte	buiten reikwijdte	buiten reikwijdte verzoek
buiten reikwijdte	buiten reikwijdte	buiten reikwijdte verzoek	buiten reikwijdte	buiten reikwijdte verzoek
buiten reikwijdte	buiten reikwijdte	buiten reikwijdte verzoek	buiten reikwijdte	buiten reikwijdte verzoek
buiten reikwijdte	buiten reikwijdte	buiten reikwijdte	buiten reikwijdte	buiten reikwijdte verzoek
buiten reikwijdte	buiten reikwijdte	buiten reikwijdte verzoek	buiten reikwijdte	buiten reikwijdte verzoek

				buiten reikwijdte verzoek [redacted]

Bijlage

5.1.2.e @VWS
AVG-Verwerkingenregister
Overzicht 'Gemeenschappelijke Verwerkingen VWS'

versie 07 januari 2019

Voor een aantal verwerkingen geldt dat veel directies en VWS-onderdelen ermee te maken hebben. Denk aan burgerbrieven, sollicitaties en het bijhouden van verzendlijsten voor bijvoorbeeld nieuwsbrieven. Om te voorkomen dat er '25 keer min of meer dezelfde verwerking' in het register staat, faciliteert 5.1.2.e @VWS een set met 'Gemeenschappelijke Verwerkingen VWS, kortweg GVV'.
In een aantal gevallen valt een verwerking formeel onder een bepaalde directie - zoals Wob-verzoeken en bezwaar- en beroepschriften onder WJZ - en vind je de verwerking ook daar terug. Elk onderdeel dat gebruik maakt van deze verwerkingen kan verwijzen naar deze verwerkingen in het centrale (VWS-)register op www.avgregisterrijksoverheid.nl.

Verwerkingen VWS		AVG-register	No.
1.	buiten reikwijdte verzoek	buiten reikwijdte	
2.	buiten reikwijdte verzoek	buiten reikwijdte	
3.	buiten reikwijdte ver	buiten reikwijdte	
4.	buiten reikwijdte verzoek	buiten reikwijdte	
5.	buiten reikwijdte verzoek	buiten reikwijdte	
6.	buiten reikwijdte verzoek	buiten reikwijdte	
7.	buiten reikwijdte verzoek	buiten	buiten
	buiten reikwijdte verzoek	reikwijdte	reikwijdte
8.	buiten reikwijdte verzoek	buiten	reikwijdt
9.	buiten reikwijdte verzoek	buiten reikwijdte	buiten reik-wijdte verzoek
	buiten reikwijdte verzoek		
	buiten reikwijdte verzoek		
	buiten reikwijdte verzoek		buiten reik-wijdte verzoek
	buiten reikwijdte verzoek		
	buiten reikwijdte verzoek		
	buiten reikwijdte verzoek		

10.	buiten reikwijdte verzoek	buiten reikwijdte	buiten reikwijdte
11.	buiten reikwijdte verzoek		
12.	buiten reikwijdte verzoek	buiten reikwijdte	buiten reikwijdte
13.	buiten reikwijdte verzoek		

Verwerkingen Rijksbreed	AVG-register	No.
1.	buiten reikwijdte verzoek	
	buiten reikwijdte verzoek	buiten reik-wijdte verzoek
	buiten reikwijdte verzoek	buiten reik-wijdte verzoek
	buiten reikwijdte verzoek	buiten reik-wijdte verzoek
	buiten reikwijdte verzoek	buiten reik-wijdte verzoek
	buiten reikwijdte verzoek	buiten reik-wijdte verzoek
	buiten reikwijdte verzoek	buiten reik-wijdte verzoek
	buiten reikwijdte verzoek	buiten reik-wijdte
	buiten reikwijdte	
2.	buiten reikwijdte	
	buiten reikwijdte verzoek	buiten reikwijdte buiten reikwijdte
	buiten reikwijdte verzoek	
	buiten reikwijdte verzoek	buiten reikwijdte
	buiten reikwijdte verzoek	
	buiten reikwijdte verzoek	buiten reikwijdte

*) (Nog) niet gepubliceerd op www.avgregisterrijksoverheid.nl, beschikbaar via link naar Rijksportaal.