Auditdienst Rijk
Ministerie van Financiën

-

Onderzoeksrapport
Afnemers CIS 2016, ISZW, FIOD, KMAR

Definitief

Colofon

Titel	Afnemers CIS 2016 , ISZW FIOD KMAR
Uitgebracht aan	dgRR
Datum	19 juni 2017
Kenmerk	2017-0000118209

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Aanleiding opdracht **4**

Maatregelen grotendeels geïmplementeerd, aanscherping op details ingezet **5**

1 Bevindingen algemeen **6**
1.1 De autorisatieprocedure is niet bij alle diensten formeel en actueel 6
1.2 De afnemers zijn positief over de dienstverlening van IBO 6
1.3 De werkplek is overeenkomstig de omgeving van de opsporing ingericht als kritisch, expliciete rubricering CIS niet opgenomen 6

2 Bevindingen bevragingsproces **7**
2.1 Voor het benaderen van CIS is een kritisch ruimte ingericht 7
2.2 De CIS gebruikers zijn interne medewerkers en hebben kennis van het proces 7
2.3 De toetsing van verzoeken vindt plaats conform de afspraken en de norm op volledigheid en juistheid en niet op de inhoud 8
2.4 De 'no hits' bevragingen volgen een specifieke procedure 8
2.5 Bij 96% van de deelwaarneming is de rechtmatigheid aangetoond 8

3 Bevinding lokaal beheer **9**
3.1 Er zijn interne afspraken voor het benaderen van CIS vanaf een andere locatie 9
3.2 De lokale beheerders hebben ruime gebruikservaring 9
3.3 De begeleiding van nieuwe gebruikers is specifiek per dienst 9
3.4 Er is periodieke controle op het autorisatiebeheer en van de rechtmatigheid van de bevragingen 9

4 Verantwoording onderzoek **11**
4.1 Werkzaamheden en afbakening 11
4.2 Gehanteerde Standaard 11
4.3 Verspreiding rapport 11

5 Ondertekening **12**

Bijlage 1 Reactie van opdrachtgever **13**

Bijlage 2 Toetskader bevraging CIS 2016 **15**

Aanleiding opdracht

De minister van Veiligheid en Justitie is conform artikel 8 tweede lid van het Besluit Verstrekking Gegevens Telecommunicatie gehouden jaarlijks een verslag op te stellen van een audit naar de goede uitvoering van het besluit door aanbieders van openbare telecommunicatiediensten of van openbare telecommunicatienetwerken, het informatiepunt, de arrondissementsparketten en de politiekorpsen, of andere (bijzondere) opsporingsdiensten.
Per brief van 29 september 2016, met kenmerk 803747 heeft de directeur-generaal Rechtspleging en Rechtshandhaving, mw. mr J.G. Vegter, de Auditdienst Rijk (ADR) gevraagd onderzoek te doen naar de rechtmatigheid van de bevraging bij de afnemers FIOD, ISZW en KMaR.
In deze rapportage zijn de bevindingen van dit onderzoek opgenomen.

Maatregelen grotendeels geïmplementeerd, aanscherping op details ingezet

Alle drie onderzochte (bijzondere) Opsporingsdiensten (hierna (B)OD's) hebben maatregelen getroffen zodat de gemaakte afspraken, waaronder het rechtmatig bevragen in het CIOT Informatie Systeem (CIS), worden nagekomen. Deze maatregelen zijn ingericht en worden nageleefd. Verbeteringen hebben beperkt betrekking op het formaliseren van de procedure of werkinstructie dan wel het expliciet opnemen van de werkzaamheden.
In tweeënzeventig van de vijfenzeventig bevragingen van de uitgevoerde deelwaarneming is de rechtmatigheid aantoonbaar. Op de door de ADR teruggekoppelde bevindingen zijn door de diensten een aantal verbeteracties ingezet.

Wij merken op dat, in tegenstelling tot de afspraak in het SLA, het technisch mogelijk is het CIS van buiten de kritisch ingerichte locatie te benaderen, bijvoorbeeld bij het "thuis werken". Door alle drie diensten zijn hiervoor specifieke mondelinge werkafspraken gemaakt.
Het maken van overeenstemmende afspraken over het gebruik van het CIS buiten de specifiek ingerichte locatie en het afstemmen van randvoorwaarden waaronder dit kan plaatsvinden, kan bijdragen aan het beperken van het risico van ongewilde en grote diversiteit van lokale afspraken.

1 Bevindingen algemeen

1.1 De autorisatieprocedure is niet bij alle diensten formeel en actueel

Eén van de drie diensten heeft geen formeel vastgestelde procedure voor de toekenning van autorisaties. Deze dienst gebruikt een werkinstructie waarin het overgrote deel van de eisen conform het Service Level Agreement (SLA) zijn opgenomen. Deze werkinstructie wordt gevolgd, maar is niet formeel vastgesteld en bevat niet alle taken (w.o. autorisatiebeheer) van de lokale beheerder. Hoewel de werkinstructie niet expliciet formeel is vastgelegd, wordt de werkinstructie, indien nodig, door de lokale beheerder geactualiseerd en besproken. Uit de werkzaamheden die deze lokale beheerder uitvoert kan de ADR ook afgeleiden dat autorisatiebeheer plaatsvindt.

Hoewel het actueel houden van de procedure/werkinstructie bij geen van de drie diensten geformaliseerd is, wordt bij twee diensten de procedure/werkinstructie periodiek getoetst. Bij deze diensten worden op initiatief van de lokale beheerder de documenten geactualiseerd, zoals recentelijk in 2017 heeft plaatsgevonden. Bij de derde dienst dateert de procedure uit 2014 en zijn een aantal aspecten van de procedure en werkinstructie niet meer actueel. Dit komt door invoering van een ander systeem en een reorganisatie. Bij deze dienst worden de wijzigingen van de procedure tijdens de werkbespreking met de medewerkers besproken. De dienst heeft in reactie op de constateringen van de ADR aangegeven de procedure en werkinstructie aan te passen om het volledig en actueel te maken, bijvoorbeeld door het uitvoeren van een periodieke toets.

1.2 De afnemers zijn positief over de dienstverlening van IBO

Alle drie de diensten geven aan dat ze geen aanmerkingen hebben op de dienstverlening van IBO en dat zij in het bevragingsproces geen beperkingen ondervinden. De (B)OD'S's hebben onderling afspraken gemaakt in geval dat uitwijk nodig is. Dit is bij geen van deze diensten nog noodzakelijk geweest. Om die reden hebben geen van de drie diensten heeft een specifieke incidenten-/klachtenprocedure ingericht.
Eén van de diensten geeft aan dat problemen voorkomen met de geldigheid van certificaten. Een voorbeeld is dat eind 2016 de geldige certificaten plotseling ten onrechte waren 'verlopen' door een wijziging op het CIS. Hierover was door IBO vooraf onvoldoende gecommuniceerd.

1.3 De werkplek is overeenkomstig de omgeving van de opsporing ingericht als kritisch, expliciete rubricering CIS niet opgenomen

Binnen de opsporing wordt alle informatie aangemerkt als Staatsgeheim Confidentieel (STGC). Daarom is de werkplek waar CIS bevragingen worden uitgevoerd, ingericht als een kritische ruimte (gezoneerd en beperkt toegankelijk). Hoewel dit het geval is, heeft geen van de drie onderzochte diensten expliciet een rubriceringniveau aangegeven in de werkinstructie/procedure.
Naar aanleiding van dit onderzoek heeft één dienst aangegeven inmiddels de rubricering expliciet aan de werkinstructie te hebben toegevoegd.

2 Bevindingen bevragingsproces

2.1 Voor het benaderen van CIS is een kritisch ruimte ingericht

Het CIS is voor de infodesk medewerkers bij alle drie diensten toegankelijk in een specifieke, als kritische gedefinieerde, ruimte. Deze ruimte is bij twee diensten conform het beleid naast voor medewerkers van de infodesk ook toegankelijk voor andere medewerkers. De specifieke ruimte waar de CIS bevragingen worden uitgevoerd is afgeschermd, maar niet afgesloten. Bij één van deze diensten wordt deze infodesk-ruimte buiten kantoortijd wel fysiek afgesloten. En bij twee diensten kan de lokale beheerder ook bevragingen uitvoeren op een werkplek in de gezoneerde omgeving maar buiten de specifiek ingerichte ruimte.
Bij de derde dienst was in tegenstelling tot het beleid de toegang niet beperkt tot infodesk medewerkers. De teamleider heeft maatregelen genomen om deze toegangsautorisaties in te trekken.
Het CIS is technisch bij alle drie de diensten ook buiten de specifiek ingerichte infodesk ruimte te benaderen, bijvoorbeeld thuis of op een andere organisatielocatie. De locatie waarvan het CIS wordt benadert kan niet worden afgeleid uit het rapport 'CIOT Auditdetails'. Bij alle diensten zijn specifieke aanvullende maatregelen getroffen. In 3.1 zijn de bevindingen hieromtrent opgenomen.

2.2 De CIS gebruikers zijn interne medewerkers en hebben kennis van het proces

Alle medewerkers die bevragingen mogen doen in CIS zijn door de lokale beheerder geautoriseerd. Deze medewerkers hebben zowel een persoonlijk gebruikersaccount en wachtwoord op de KA-omgeving als een persoonlijk certificaat /CIS account en wachtwoord.

Externe medewerkers zijn bij geen van de diensten betrokken bij het bevragingsproces in CIS. Eén dienst geeft aan indien externe medewerkers in aanraking komen met het CIS, zij gescreend zijn en een geheimhoudingsverklaring hebben getekend. Bij één dienst is de screening van externe medewerkers een standaard procedure, ongeacht waar zij worden ingezet. Bij geen enkele dienst is in de werkinstructies een richtlijn of een verwijzing opgenomen naar andere beleidstukken.

Alle geautoriseerde Infodesk medewerkers moeten een gebruikerscursus volgen. Bij één dienst wordt een medewerker, die hiervoor nog niet in de gelegenheid is geweest begeleid door de lokale beheerder of een ervaren infodesk medewerker met ruime kennis van het proces. Bij één dienst hebben, op het moment van onderzoek, alle geautoriseerde medewerkers de gebruikerscursus gevolgd. Bij één dienst wordt pas na het volgen van de gebruikerscursus de autorisatie aangevraagd.

Verdere begeleiding van de nieuwe medewerker gebeurt intern. Bij twee van de drie diensten wordt een nieuwe medewerker door de lokale beheerder begeleid bij het gebruik van CIS. Bij één dienst is de begeleiding voor het installeren van het certificaat overgedragen aan de IT beheer organisatie.

2.3 De toetsing van verzoeken vindt plaats conform de afspraken en de norm op volledigheid en juistheid en niet op de inhoud

Geen van de drie diensten maakt de vordering zelf op. In alle procesbeschrijvingen en/of werkinstructies is aangegeven dat de vordering gecontroleerd wordt op volledigheid en juistheid (bevoegde autoriteit en geldige grondslag). Eén dienst heeft een aanvullende voorwaarde gesteld van een tweede handtekening van de teamleider. De controle hiervan wordt ook door de geautoriseerde infodesk medewerker meegenomen tijdens het uitvoeren van een bevraging. Conform de norm wordt door alle diensten geen inhoudelijke toetsing uitgevoerd.
De bevoegde autoriteit, kenmerk en rechtsgrondslag wordt door allen in het CIS ingevuld. In één geval kon de vordering door het gebruik van een ongebruikelijk kenmerk pas na veel inspanning worden teruggevonden.
De documenten om de rechtmatigheid van de bevraging aan te tonen worden bij de diensten opgeslagen. Ze hebben alle drie een eigen systematiek/archiveringswijze (in Planon of op een lokale netwerkschijf) van deze documenten.

2.4 De 'no hits' bevragingen volgen een specifieke procedure

Voor het behandelen van 'no hits' hebben alle diensten een specifieke procedure opgesteld. De voorbereiding voor de doorbevraging van de 'no hits' wordt door de infodesk medewerker voorbereid, en na retour ontvangst van de geautoriseerde, wordt de bevraging doorgestuurd naar de afdeling Interceptie.

2.5 Bij 96% van de deelwaarneming is de rechtmatigheid aangetoond

De ADR heeft een deelwaarneming uitgevoerd van totaal vijfenzeventig CIS bevragingen (vijfentwintig posten per dienst). Deze zijn geselecteerd uit het 'Rapport Audit CIS' in de periode van 1 juli 2016 – 31 december 2016. Hieronder volgt een opsomming van de bevindingen van deze deelwaarneming:

- alle bevragingen zijn uitgevoerd door geautoriseerde infodesk medewerkers;
- bij drie bevragingen kon de rechtmatigheid van de bevraging niet worden aangetoond:
    - bij twee bevragingen kon de vordering niet worden getoond;
    - bij één bevraging ontbrak een handtekening van bevoegde autoriteit op de vordering;
- overige:
    - bij één bevraging is sprake van een foutieve registratie in het CIS van het wetsartikel, de vordering is met behulp van het kenmerk gevonden;
    - bij één bevraging is een ongebruikelijk CIS kenmerk geregistreerd, waardoor extra inspanning nodig was om de vordering in het lokale archief te vinden;
    - bij één bevraging is sprake van een tijdissue, omdat naar aanleiding van de eerste beoordeling aanvullende informatie is opgevraagd die na het tussenliggende weekend is ontvangen en verwerkt;
    - bij één bevraging is de vordering niet in het gebruikelijke lokale archief gevonden, maar in de mailbox van de infodesk.

3 Bevinding lokaal beheer

3.1 Er zijn interne afspraken voor het benaderen van CIS vanaf een andere locatie

Zoals in 2.1 is beschreven is het CIS technisch bij alle drie de diensten ook buiten de specifiek ingerichte infodesk ruimte te benaderen.
De diensten hebben allen interne werkafspraken gemaakt voor het benaderen van CIS vanaf een andere locatie. Bijvoorbeeld thuiswerken is pas toegestaan als er een specifiek certificaat door de medewerker is behaald. Een ander voorbeeld is dat thuiswerken alleen met medeweten van de leidinggevende mag.
De lokale beheerders geven aan dat thuiswerken door de organisatie niet wordt gestimuleerd en dat de afspraken met leidinggevende voornamelijk mondelinge zijn gemaakt, en niet zijn opgenomen in de werkinstructie / procedure van het CIS.

3.2 De lokale beheerders hebben ruime gebruikservaring

De lokale beheerder zijn bij alle drie de diensten ervaren CIS gebruikers. De lokale beheerders moeten ook een beheercursus volgen. In een aantal gevallen heeft de plaatsvervangende lokale beheerder nog niet de benodigde beheercursus gevolgd, omdat deze niet frequent wordt georganiseerd. Bij twee diensten wordt deze op de werkvloer begeleid en bij de derde heeft de plaatsvervanger nog geen toegang tot het beheerdeel van het CIS.

3.3 De begeleiding van nieuwe gebruikers is specifiek per dienst

Alle medewerkers die bevragingen in CIS uitvoeren zijn bij alle drie de diensten geautoriseerd. Alle informatie over het installeren van het certificaat en het uitvoeren van de bevraging is voor de medewerkers beschikbaar. Bij één van de diensten is niet de lokale beheerder, maar de IT beheer organisatie betrokken bij de begeleiding van het installeren van het certificaat. Bij alle drie diensten worden nieuwe CIS gebruiker op de werkvloer begeleid.

3.4 Er is periodieke controle op het autorisatiebeheer en van de rechtmatigheid van de bevragingen

Na aanvraag door de lokale beheerder verstrekt IBO het CIS-account aan de geautoriseerde medewerkers van de infodesk afdeling. Op locaties is bij alle diensten een administratie van deze aanvragen aangetroffen. Naar aanleiding van het onderzoek is bij één dienst het certificaten overzicht geactualiseerd.
Voor de autorisatie beheertaak maakt de lokale beheerder ook gebruik van het overzicht van de gebruikersaccounts dat periodiek door IBO wordt verstuurd. De lokale beheerder voert een periodieke controle uit op deze accounts. Lokale beheerders hebben via e-mail correspondentie laten zien welke acties hierop worden ondernomen.
Bij één dienst is vastgesteld dat de opheffing van voormalig plv. beheerder meer dan twee maanden na datum van vertrek heeft plaatsgevonden. De laatste login datum toont aan dat in de tussenliggende periode geen gebruik is gemaakt van dit gebruikeraccount.

Bij geen van de diensten wordt het maximaal aantal toegestane certificaten overschreden.

Bij één dienst zijn de toegewezen certificaten met geldigheiddatum als bijlage bij de werkinstructie opgenomen. De exclusieve toegang is bij alle diensten ook gerelateerd aan toegang tot het (verbijzonderde) netwerk of eigen werkplek met ICT voorziening.

Bij geen van de diensten wordt het BOB middel intern opgemaakt. Alle diensten geven aan dat alle infodesk medewerkers Opsporingsambtenaar (OA) of Bijzondere Opsporingsambtenaar (BOA) zijn. Daarnaast zijn deze medewerkers AIVD of MIVD gescreend. Hiervan houden de lokale beheerders geen expliciete administratie bij, omdat dit in het personeeldossier van de medewerkers is opgenomen. Bij één dienst is het de verantwoordelijkheid van de medewerkers hun OA/BOA status actueel te houden.

Alle lokale beheerders voeren een periodieke controle uit op de uitgevoerde bevragingen. Deze controle is zichtbaar gemaakt en de bevindingen worden genoteerd. Geconstateerde tekortkomingen worden bij alle diensten met de betrokken medewerker en/of teamleider besproken.
De periodieke controle wordt niet overal op dezelfde wijze uitgevoerd. De periodiciteit bij één dienst is maandelijks, terwijl de andere dienst per kwartaal aanhoudt. Daarnaast verschilt het uitgangspunt bij deze controle. De ene beheerder gebruikt uitsluitend de informatie uit het 'Rapport CIOT Auditdetails' terwijl de andere beheerder afwisselend ook de ingekomen verzoeken in het infodesk registratiesysteem/dossier als uitgangspunt neemt. Deze laatste dienst heeft in 2017 voor de toets door de interne IV afdeling in de toekomst een breed CIS toetskader opgesteld. Thema's die hierin voorkomen zijn o.a. informatiebeveiliging, autorisatieproces en rechtmatigheid.

4 Verantwoording onderzoek

4.1 Werkzaamheden en afbakening

Het onderzoek is uitgevoerd bij de FIOD[1], de KMAR[2] en de ISZW[3] en heeft betrekking op de rechtmatige bevraging van het CIS conform de wet –en regelgeving, de SLA en DAP bij deze drie opsporingsdiensten.
Het onderzoek is uitgevoerd in de periode van december 2016 – maart 2017. De werkzaamheden hebben o.a. betrekking op het bestuderen van wet- en regelgeving, de diverse SLA's en beschikbare procesbeschrijvingen, werkinstructies en afspraken. Daarnaast heeft de ADR interviews gehouden met sleutelfiguren, waaronder de portefeuillehouder, het lokale functioneel beheer en een medewerker/gebruiker CIS. Verder is op basis van een overzicht uit het CIS een deelwaarneming met en omvang van vijfentwintig posten per dienst uitgevoerd.

De centrale vraag bij de audit is:
Welke maatregelen zijn door de opsporingsdiensten getroffen zodat de bevragingen in het CIOT Informatie Systeem (CIS) door de medewerkers rechtmatig plaatsvinden? En in welke mate worden deze nageleefd?

Het veldonderzoek is afgerond op 28 maart 2017. De resultaten zijn opgenomen in het toetskader en afgestemd met de betreffende dienst. Hierbij hebben de diensten in hun reactie aangegeven welke verbeterpunten zij inzetten. Waar van toepassing, is dit in het rapport overgenomen. Het rapport is met de opdrachtgever besproken op 4 mei 2017.

4.2 Gehanteerde Standaard

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing.

In dit rapport wordt geen zekerheid verschaft, omdat er geen assurance-opdracht is uitgevoerd.

4.3 Verspreiding rapport

De opdrachtgever, mw. Mr. J.G. Vegter, is eigenaar van dit rapport.

De ADR is de interne Auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie de ADR deze opdracht is overeengekomen. In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de ADR een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van door de ADR uitgebrachte rapporten en plaatst dit overzicht op de website.

1 Fiscale Inlichtingen en Opsporingsdienst
2 Koninklijke Marechaussee
3 Inspectie van het ministerie Sociale Zaken en Werkgelegenheid

5 Ondertekening

Den Haag, 22 juni 2017

w.g.

mw. mr. J.T.N.J. Tjin-A-Tsoi

projectleider Auditdienst Rijk

Bijlage 1 Reactie van opdrachtgever

Ministerie van Veiligheid en Justitie

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
FO

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/venj

Ons kenmerk
2088350

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

> Retouradres Postbus 20301 2500 EH Den Haag

Auditdienst Rijk
T.a.v. Dhr. J.P. Looman
Postbus 20201
2500 EE Den Haag

Datum 9 juni 2017
Onderwerp Onderzoeksrapport "Afnemers CIS 2016, ISZW, FIOD, KMAR"

Geachte heer Looman,

De minister van Veiligheid en Justitie is conform artikel 8 tweede lid van het Besluit Verstrekking Gegevens Telecommunicatie gehouden jaarlijks een verslag op te stellen van een audit naar de goede uitvoering van het besluit door aanbieders van openbare telecommunicatiediensten of van openbare telecommunicatienetwerken, het informatiepunt, de arrondissementsparketten en de politiekorpsen, of andere opsporingsdiensten. Ik heb u derhalve gevraagd onderzoek te doen naar de rechtmatigheid van de bevraging bij de afnemers FIOD, ISZW en KMaR.

Ik heb kennisgenomen van het onderzoeksrapport "Afnemers CIS 2016, ISZW, FIOD, KMAR", opgesteld door de ADR in opdracht van DGRR. In de rapportage zijn de bevindingen van dit onderzoek opgenomen. Ik stel met tevredenheid vast dat u met succes inzicht heeft kunnen verschaffen in de rechtmatigheid van de bevragingen bij de afnemers FIOD, ISZW en KMaR, en u onder meer vaststelt dat maatregelen getroffen zijn en waar nodig reeds verbeteracties zijn ingezet, zodat de gemaakte afspraken worden nagekomen.

Uw bevindingen uit dit onderzoek zullen betrokken worden bij het brede verslag dat opgesteld zal worden naar aanleiding van dit onderzoeksrapport, waarin tevens de bevindingen uit de overige lopende onderzoeken, zoals naar CIOT beheer, betrokken zullen worden, opdat een integrale beoordeling gemaakt kan worden.

Met vriendelijke groet,

J.G. Vegter
Directeur Generaal Rechtshandhaving en Rechtspleging

Bijlage 2 Toetskader bevraging CIS 2016

Nr	Norm	Bron
A	**ALGEMEEN**	
1a	De (B)OD heeft voor de toekenning en intrekking van autorisaties aan medewerkers t.b.v. de bevraging CIOT (inclusief spoedprocedure) en de daaruit voortvloeiende verwerking van gegevens een (formele) procedure **vastgesteld**. Deze is gedocumenteerd en wordt onder de aandacht gebracht van de gebruikers. In deze procedure zijn conform de SLA: • de verantwoordelijkheden van de gebruiker opgenomen. • Het inrichten van de werkpek waar CIS wordt benadert • Het aanwijzen van een lokale beheerder en plaatsvervanger door de Inspecteur / directeur • de beheersing en toewijzing van toegangsrechten, waarin alle fasen in de levenscyclus van gebruikerstoegang worden vastgelegd (inclusief afmeldingen).	SLA/DAP
1b	Periodiek (minimaal 1 x per jaar) wordt getoetst of de procedure en werkwijze wordt toegepast en/of moet worden geactualiseerd. Bijvoorbeeld op basis van nieuwe procedures, afspraken of wet- en regelgeving. Deze toets is onderdeel van de procedure CIS en de audittrail is vastgelegd.	SLA/ DAP
2	De dienstverlening van IBO heeft geen invloed op het bevragingsproces bij de (B)OD. Denk aan: -Beschikbaarheid -Uitwijk bij uitval -Performance (antwoord snelheid) -Gebruikersondersteuning / opleiding -afhandeling van Incidenten / klachten	SLA/ DAP
3	Incidenten / klachten bij de (B)OD die van invloed zijn op het bevragingsproces worden bij de (B)OD (centraal) geregistreerd. Indien deze van invloed zijn op de beschikbaarheid en/of exclusiviteit van CIS wordt dit gemeld bij de Servicedesk IBO (voorheen CIOT). De lokale beheerder monitort de afloop. Hiervoor is een procedure vastgesteld en deze wordt nageleefd.	SLA/ DAP
4	De (B)OD heeft voor de bevragingenproces een rubriceringsniveau gedefineerd4 en hierop beveiligingsmaatregelen ingericht en de implementatie hiervan kan worden aangetoond. Beveiligingsmaatregelen kunnen generiek maar ook specifiek betrekking hebben op de CIS bevragingsproces	SLA / DAP

4 CIOT Gebruikersvoorwaarden vermeld in punt 3 dat het CIOT informatiesysteem gerubriceerd is als Staatsgeheim – Geheim. WBP klasse 3.

Nr	Norm	Bron
B	**BEVRAGINGSPROCES**	
1	Voor het opvragen van gegevens bij de providers wordt **alleen de CIOT-cliënt** gebruikt. Alleen in geval van een calamiteit wordt de calamiteiten procedure gevolgd. De CIOT client is alleen te benaderen op de specifiek ingerichte ruimte. Als via andere lokatie (bijvoorbeeld vanuit thuiswerkplek) de CIOT client te benaderen is zijn daarvoor maatregelen getroffen. Welke?	DAP / Gebruikershandleiding
2	De technische voorziening (CIOT webtoepassing) is alleen toegankelijk voor personen die door de lokale beheerder zijn geautoriseerd.	DAP / Gebruikershandleiding
3	Een nieuwe gebruiker wordt door de beheerder bij het gebruik van de CIOT cliënt begeleid. Relatie met norm C 6	DAP / Gebruikershandleiding
4	Alle documenten die nodig zijn om het verband te kunnen vaststellen dienen voorafgaand aan de CIS bevraging ter plaatse beschikbaar te zijn	DAP / Gebruikershandleiding
5	Het vragen van gebruiksgegevens van de aanbieders **via een bevel5** is alleen toegestaan **door de bevoegde autoriteit** en een **geldige grondslag**6. Bevoegde autoriteit zijn: - de rechter-commissaris in strafzaken, - de officier van justitie, - de beheerder van een politiekorps, of - het hoofd van een opsporingsdienst, dan wel - de door de beheerder voor zijn korps of door het hoofd voor zijn dienst aangewezen opsporingsambtenaar - het hoofd van de Binnenlandse Veiligheidsdienst, of de door hem aangewezen ambtenaar. Uit het bevel7 blijkt op basis van welke rechtsgrondslag de gevraagde gegevens worden gevorderd.	DAP / Gebruikershandleiding
6a	Aanvragen worden alleen door een **geautoriseerde ambtenaar8** uitgevoerd. Aangewezen door eindverantwoordelijke bij de (B)OD en/of lokaal beheerder. **Externen** die in aanraking komen met het CIOT informatiesysteem zijn gescreend en hebben een geheimhoudingsverklaring getekend. Art.5 lid 1 Besluit verstrekking gegevens telecommunicatie: *Een verzoek van een bevoegde autoriteit kan slechts worden gedaan door een door Onze Minister van Justitie (in praktijk de directeur van het CIOT) geautoriseerde ambtenaar die daartoe gebruik*	SLA/DAP / Gebruikershandleiding

5 *Het verzoek van de bevoegde autoriteit is op papier (in handen of fax) of elektronisch (e-mail) bij de geautoriseerde ambtenaar bezorgd bijvoorbeeld Proces verbaa, OA voor 126 na, 126 ua en 126 zi ; OvJ voor 126n, 126 u, 126 ii en 126 zi WvSv*
6 126 na, 126 ua, 126 zi, 126n, 126 u, 126 ii en 126 zi WvSv (zie toelichting)
7 Een bevel is een vordering van een bevoegde autoriteit om een verzoek te doen in het kader van een onderzoek van telecommunicatie, met daarbij bepaald op welke rechtsgrondslag die bevel toepassing heeft.
8 alleen Opsporingsambtenaar of Bijzondere Opsporingsambtenaar

Nr	Norm	Bron
	maakt van een hem toegekende toegangscode.	
6b	Als de geautoriseerde ambtenaar het BOB (bijzondere opsporingsbevoegdheid) middel (het proces verbaal vordering verstrekking gegevens en/ of het proces verbaal verstrekking gegevens) opmaakt is hij/zij OA / BOA.	SLA/DAP / Gebruikershandleiding
6c	De geautoriseerde ambtenaar heeft kennis van het proces en de daarbij horende eisen, hetgeen ondermeer blijkt uit de gevolgde gebruikerscursus.	SLA/DAP / Gebruikershandleiding
7	Een aanvrager/geautoriseerde ambtenaar is in het bezit van een **eigen CIOT-account en password**. Een toegewezen certificaten zijn exclusief en worden niet met collega's gedeeld.	SLA/DAP / Gebruikershandleiding
8	Een CIOT bevraging dient **rechtmatig** te zijn. De geautoriseerde ambtenaar checkt de rechtmatigheid van verzoeken. Hierbij dienen de volgende gegevens beschikbaar te zijn: - naam en handtekening bevoegde autoriteit; - geldigheid machtiging; - rechtsgrondslag*; - feitelijke aanvrager / onderzoeksteam; - dossierkenmerk. *)Bij het checken van de rechtsgrondslag wordt door de geautoriseerde ambtenaar nagegaan: • of de rechtsgrondslag is ingevuld (komt overeen met de toegestane wetsartikelen) • of het wetsartikel de bevraging rechtvaardigt (toetsen van rechtsgrondslag) • of de autoriteit bevoegd is voor het betreffende artikel onderzoek te doen (mandatering) • of de periode van machtiging niet is verstreken. *In spoedeisende situaties komt het voor dat de vereiste machtiging niet tijdig kan worden aangeleverd. Lokaal worden afspraken gemaakt over het binnen 3* 24 uur naleveren van de vereiste machtiging.* De geautoriseerde ambtenaar onthoudt zich van een inhoudelijke beoordeling, dat wil zeggen van een beoordeling of er voldoende feiten en omstandigheden zijn om onderzoek naar het vermelde strafbare feit te rechtvaardigen.	Besluit/ DAP/ Gebruikershandleiding
9	Bij een verzoek dient altijd een identificerend kenmerk (bijv. onderzoeksnummer, proces-verbaalnummer of parketnummer) te worden meegeven, op basis waarvan een eenduidige relatie kan worden gelegd naar het onderliggende (straf)dossier.	DAP/ Gebruikershandleiding

Nr	Norm	Bron
10	Van een verzoek worden de volgende gegevens verplicht in CIOT informatiesysteem vastgelegd: • bevoegde autoriteit; • kenmerk; • organisatie eenheid / opsporingsteam; • rechtsgrondslag.	DAP/ Gebruikershandleiding
11	De geautoriseerde ambtenaar houdt dossier, zodanig dat te allen tijde rechtmatigheid van de uitgevoerde bevragingen tot op dossierniveau kan worden aangetoond.	DAP/ Gebruikershandleiding
12	'No hits' worden via de speciale procedure verder behandeld. *Momenteel kan je een no-hit aanmaken, deze gaat naar een overzicht no-hit en hier kan je een provider bij zoeken (selecteren). Vervolgens kan je een no-hit formulier aan laten maken en gaan de pdf's maar de provider. De registratie gaat nu handmatig en dit zal in de toekomst geautomatiseerd worden.*	SLA/DAP / Gebruikershandleiding
13	Voor de audit worden 25 random posten getrokken die betrekking hebben op de bevragingen over een periode van de 6 maanden. Van alle posten moet de rechtmatigheid van de bevraging door de (B)OD binnen 2 uur na de selectie van de posten aangetoond kunnen worden.	Opdracht bevestiging

Nr	Norm	Bron
C	**BEHEER CIOT WEB-TOEPASSING**	
1	De ruimte waarin de webvoorziening is geplaatst is alleen toegankelijk voor aangewezen bevoegd personeel en is geclassificeerd als zijnde een kritische ruimte. De beveiligingsmaatregelen die betrekking hebben op een kritische ruimte worden nageleefd. De webvoorziening is niet te benaderen buiten deze ruimte. Als dit mogelijk is zijn hier specifieke maatregelen voor getroffen. De naleving van de maatregelen is aantoonbaar en wordt periodiek getoetst.	DAP/ Gebruikershandleiding
2	De aangewezen beheerder en zijn plaatsvervanger hebben kennis van het proces en de daarbij behorende eisen hetgeen ondermeer blijkt uit de gevolgde beheercursus.	DAP/ Gebruikershandleiding
3	Alleen de lokale beheerder of zijn plaatsvervanger mogen user-accounts CIOT aanvragen of laten intrekken. De lokale beheerder houdt hiervan administratie en communiceert hierover met het CIOT. Aanvraagformulieren voor toegang tot CIOT informatiesysteem zijn ondertekend door de portefeuillehouder en/of lokale beheerder. De lokale beheerder beoordeeld aantoonbaar periodieke of de verleende autorisaties nog	DAP/ Gebruikershandleiding

Nr	Norm	Bron
	actueel zijn. Bij het intrekken van een user-account deactiveert de lokale beheerder de gebruikersID binnen de CIOT Web-client en meldt de intrekking schriftelijk (E-mail) aan de Servicedesk CIOT. De beheerder ontvangt van CIOT/IBO periodiek een overzicht van gebruikers ter afstemming.	
4	Per (B)OD zijn niet meer dan 3 * 15 bevragerscertificaten uitgereikt. Totaal maximaal 47 (inclusief 2 beheerderscertificaten)	DAP/ Gebruikershandleiding
5	Uit de administratie van de beheerder blijkt dat: - Autorisatie tot het doen van bevragingen in de CIOT cliënt is slechts verleend aan een aangewezen OA / BOA. Voorzover hij/zij het BOB middel opmaakt (het proces verbaal vordering verstrekking gegevens en/ of het proces verbaal verstrekking gegevens). - Externen die in aanraking komen met het CIOT informatiesysteem zijn gescreend en hebben een geheimhoudingsverklaring getekend	DAP/ Gebruikershandleiding
6	Na ontvangst van het certificaat, user id en wachtwoord begeleidt de lokale beheerder de nieuwe gebruiker bij het installeren en gebruik van de CIOT cliënt. De lokale beheerder, laat deze de nieuwe gebruiker aanloggen en het wachtwoord wijzigen	DAP/ Gebruikershandleiding
7	De lokale beheerder monitort dat toegewezen certificaten exclusief zijn en niet met collega's worden gedeeld.	DAP/ Gebruikershandleiding
8	De lokale beheerder beoordeelt steekproefsgewijs de uitgevoerde bevragingen en gebruikt hiervoor de monitoring module. Van de controle wordt aantekening gemaakt (o.a. datum en de bevindingen, acties, follow up)	DAP/ Gebruikershandleiding
9	De lokale beheerder registreert, meldt en monitort incidenten tav CIS.	DAP/ Gebruikershandleiding

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00