Bijlage 1 – Reactie op de aanbevelingen

NCTV

Wat te doen?
- Richt het principe 'need to know' in voor systemen die staatsgeheime of vertrouwelijke informatie bevatten. De door ons onderzochte systemen bieden daar voor het merendeel goede mogelijkheden voor.
- Ga medewerkershandelingen monitoren om ongewenst gedrag eerder te kunnen signaleren. Zowel de NCTV Als de politie beschikken al over uitgebreide logging die monitoring mogelijk maakt.
- Richt binnen CTER (en mogelijk breder binnen de politie) voorzieningen in zodat rechercheurs en tolken veilig kunnen samenwerken.

- Toegang tot bijzondere informatie, waaronder in het bijzonder staatsgeheime informatie, op '*need to know'*-basis was binnen de NCTV altijd een uitgangspunt. Tegelijkertijd heeft het genoemde incident aangetoond dat een aanscherping van de getroffen maatregelen nodig was en dat de toegang tot het documentatiesysteem te ruim was ingericht.
- Per 1 november 2023 is dan ook direct het documentatiesysteem dichtgezet en wordt het archiveringssysteem niet langer gebruikt voor de verspreiding van inlichtingenproducten.
- Daarnaast zijn voor het documentatiesysteem procedures steviger ingericht conform het principe *'need to know'*. Dit betekent dat alleen die medewerkers de documenten te zien krijgen die dit ook echt nodig hebben voor hun werk. Ook het archief is nog maar beperkt toegankelijk, en inzage kan alleen na toestemming van een directeur op een specifieke vraag.
- Voor het archiveringssysteem waren reeds maatregelen ingericht in lijn met het '*need to know'* principe.
- Op dit proces is nu ook controle, logging en toezicht ingericht op wie wanneer welk stuk informatie inziet.
- Toezicht op medewerkershandelingen is versterkt o.a. door een afdeling in oprichting die toeziet op risicomanagement en compliance. Zo wordt onder andere meer toegezien op het gedrag van medewerkers rond het verwerken van staatsgeheime informatie en ook op het printgedrag van medewerkers. Hiermee wordt voortdurend gezien of de maatregelen in het kader van informatiebeveiliging op deze handelingen aanpassing behoeven, waarbij het VIR-BI en de BIO constant als uitgangspunt zullen gelden.

Wat te doen?
Actualiseer de risicoanalyse met aandacht voor bedreigingen die vanuit de eigen organisatie komen (insider threats).
Maak daarbij gebruik van de al uitgevoerde IB-quickscans. Maak risicoanalyse een vast onderdeel van het jaarplan informatiebeveiliging dat jaarlijks door het MT NCTV wordt vastgesteld en gemonitord.

- In *quickscans* informatiebeveiliging en risicoanalyses neemt de NCTV sinds 1 november 2023 *insider threat* nadrukkelijker mee als een belangrijk mogelijk risico. In de mitigerende maatregelen op de risico's worden hierbij altijd meerdere maatregelen meegenomen.
- Daarnaast onderzoekt de NCTV in de komende maanden hoe nog beter in processen het tegengaan van de *insider threat* kan worden meegenomen. Waar nodig zullen de processen verder aangescherpt worden.
- Periodiek wordt bezien in hoeverre mitigerende maatregelen die voortvloeien uit risicoanalyses aanpassing behoeven. Risicoanalyses zijn een vast onderdeel geworden van het jaarplan informatiebeveiliging dat jaarlijks door het MT NCTV wordt vastgesteld.

Wat te doen?
Er is veel aandacht voor het formuleren van nieuw IB-beleid maar dat heeft in onze ogen niet de hoogste prioriteit. Volgens ons moet de focus liggen op het treffen van de juiste maatregelen en de controle of gekozen maatregelen (blijven) werken. M.a.w. focus op de Do, Check en Act van de PDCA-cyclus en niet op de fase Plan.

- Het werken aan nieuw beleid en de implementatie daarvan gaan hand in hand en verloopt tegelijkertijd. De NCTV is begin 2023 al begonnen met het project digitale weerbaarheid om de informatiebeveiliging te verbeteren. Dit resulteerde er onder andere in dat het eerste geactualiseerde beleid in januari 2024 vastgesteld werd binnen de NCTV. De werking van het beleid en de maatregelen wordt vormgegeven in een PDCA (*Plan-Do-Check-Act*) cyclus (PCDA-cyclus).
- De afgelopen periode heeft de NCTV verschillende maatregelen en processen ingevoerd en op die manier de nadruk gelegd op de fases Do, Check, Act. Denk bijvoorbeeld aan de accreditatie van het digitale netwerk dat wordt gebruikt voor de verwerking van staatsgeheime informatie en strengere maatregelen op printen van bijzondere informatie en het toezicht hierop. Ook wordt er versneld op onderdelen in de implementatie, als dat noodzakelijk blijkt, bijvoorbeeld incidentmanagement.
- De eerste twee elementen van die cyclus, *Plan* en *Do*, zijn inmiddels uitgevoerd voor de processen rondom het werken met bijzondere informatie die binnen de NCTV weer werkend zijn. De laatste twee elementen, *Check* en *Act*, volgen in de komende periode.
- Bij die laatste twee elementen wordt voor de ingevoerde procedures en maatregelen getoetst of ze functioneren en nageleefd worden. Eventuele hiaten worden geïdentificeerd en opgelost.
- Zodra deze PDCA-cyclus continu kan worden doorlopen en verbeteringen worden gemaakt waar nodig, kan definitief worden gesteld dat het proces rondom de informatiebeveiliging, zoals die wordt vereist op basis van de BIO en het VIR-BI, op orde is en ook in de toekomst blijft.

Wat te doen?
- Voer de BIO in. Voorkom daarbij een papieren werkelijkheid. D.w.z. hanteer als uitgangspunt dat maatregelen pas zijn ingevoerd als ze aantoonbaar werken.
- Vul de maatregelen uit de BIO waar nodig aan met NCTV-specifieke maatregelen op basis van een actuele risicoanalyse en het VIRBI.
- Controleer periodiek de werking van maatregelen.

- Het beleid bij de NCTV t.a.v. informatiebeveiliging is geactualiseerd. In dit beleid zijn alle vereisten van het VIR, de BIO en het VIR-BI opgenomen.
- De uitwerking van dit beleid in concrete maatregelen is een doorlopend proces. Dat houdt in dat wordt getoetst of de praktijk aansluit bij het beleid of dat aanpassingen in de werking of de praktijk nodig zijn. Waar nodig worden aanvullende maatregelen getroffen.
- Jaarlijks staat een periodieke controle op de werking van de maatregelen gepland, waarbij in een cyclus van 3 jaar iedere maatregel aan bod komt. Een intern auditplan is hiertoe opgesteld.

Wat te doen?
- Ken toegangsrechten toe in het staatsgeheime DMS, het staatsgeheime digitale archiefsysteem en afdelingsmappen volgens het principe ‘need to know’.
- Verduidelijk de verantwoordelijkheid voor juiste toegangsrechten.
- Voer periodiek controle van toegangsrechten in.
- Pas toegangsrechten tijdig aan bij verandering van functie.

- Voor het documentatiesysteem zijn procedures steviger ingericht conform het principe *'need to know'*. Dit betekent dat alleen die medewerkers de documenten te zien krijgen die dit ook echt nodig hebben voor hun werk.
- Het archief is beperkt toegankelijk, en inzage kan alleen na toestemming van een directeur op een specifieke vraag.
- Binnen elke afdeling is bepaald welke functionaris welke rechten heeft. Zo zijn bijvoorbeeld de meest verstrekkende rechten zoals printen beperkt tot enkele medewerkers. Met elkaar wordt doorlopend scherp gekeken of gestelde regels worden gevolgd en of dit ordentelijk gebeurt.
- Middels logging wordt door de verantwoordelijke manager periodiek printopdrachten en toegangsrechten gecontroleerd.

Wat te doen?
Grip krijgen op verspreiding van staatsgeheime informatie door:
- Het beperken van het printen van informatie;
- Het verbeteren van het beheer van USB-sticks;
- Rubricering op te nemen in de naamgeving van bestanden zodat direct zichtbaar is dat het gaat om staatsgeheime informatie;
- Het periodiek schonen van kasten, kluizen en persoonlijke schrijven.

- De printrechten voor staatsgeheime informatie zijn ingeperkt, logging hierop wordt periodiek getoetst, het beheer van USB-sticks is verbeterd en persoonlijke schijven en mailboxen zijn opgeschoond:
    - Een beperkter aantal medewerkers heeft printrechten ten behoeve van het kunnen uitvoeren van een aantal specifieke taken. Hierop vindt periodiek controle plaats. Medewerkers die geen printrechten hebben kunnen dus geen prints maken. Medewerkers die wel printrechten hebben, mogen niet zomaar printen voor derden, maar moeten hier specifiek toestemming voor hebben van het verantwoordelijke afdelingshoofd.
    - De procedure rond gegevensdragers is aangepast, waardoor toestemming is vereist voor het verkrijgen – en het kunnen gebruiken – van de gegevensdragers. De administratie is verbeterd waarbij ontvangst, inname en vernietiging worden geregistreerd.
    - Daarnaast maakt ook duidelijkheid over en aandacht voor schonen en opruimen van gegevensdragers onderdeel uit van de procedure.
    - Voor staatsgeheime informatie is bepaald dat deze niet langer mag worden opgeslagen dan strikt noodzakelijk. Als voorbeeld hiervan geldt als uitgangspunt dat staatsgeheime informatie die vanuit derde partijen wordt ontvangen slechts dertig dagen mag worden ingezien.
    - Op fysieke werkplekken gold en geldt het *clean desk*-beleid, waarbij staatsgeheime informatie wordt behandeld conform de eisen gesteld in het VIR-BI. Dit betekent onder andere dat dergelijke informatie niet mag worden ingezien door daartoe niet gerechtigde personen en dat deze altijd op de juiste wijze moeten worden opgeslagen.
    - Ten aanzien van bestanden zijn andere maatregelen genomen waarmee het beoogde effect, namelijk alleen toegang voor personen die daartoe gerechtigd zijn, eveneens wordt bereikt.

Wat te doen?
Bepaal of achterstand in herhaalonderzoeken moet leiden tot acties. Bijvoorbeeld:
- Tijdelijk toegang tot staatsgeheime informatie beperken als een VGB ouder is dan vijf jaar.
- Voorrang geven aan medewerkers met bepaalde functies.

- Waar nodig zijn herhaalonderzoeken met spoed aangevraagd en mitigerende maatregelen getroffen op het gebied van toegang tot informatie.
- Er zijn maatregelen getroffen om het beleid ten aanzien van het tijdig aanvragen van herhaalonderzoeken en het melden van gewijzigde omstandigheden bij vertrouwensfunctionarissen aan de BVA aangescherpt na te leven.
- De lijst met vertrouwensfuncties wordt geactualiseerd.

Wat te doen?
De NCTV heeft met het logging- en monitoringssysteem een instrument in huis om gebeurtenissen binnen de systemen, activiteiten van beheerders en activiteiten van gebruikers te monitoren.
De NCTV heeft nog niet bepaald welk gedrag van medewerkers en welke gebeurtenissen moeten worden geregistreerd en gedetecteerd. In onze ogen is het de verantwoordelijkheid van het MT van de NCTV om op risicoanalyse gebaseerde keuzes te maken en uit te leggen aan medewerkers welk gedrag van beheerders en gebruikers wordt geregistreerd en hoe daarover wordt gerapporteerd.

- De wijze waarop wordt bepaald wat atypisch gedrag is moet worden ontwikkeld.
- In aanloop naar de vaststelling van dit beleid wordt elk gedrag in relatie tot de toegang tot staatsgeheime informatie gemonitord. Zo worden bijvoorbeeld printlogs voorgelegd aan verantwoordelijke managers en moet een manager besluiten over rechten voor het printen van staatsgeheime informatie. Deze rechten zijn sterk ingeperkt.

Wat te doen?
- Actualiseer het beleid voor het melden van inbreuken op beveiliging.
- Neem controle/bijstelling van de risicoanalyse op als stap in de afhandeling van grote incidenten.
- Besluit over het opnieuw introduceren van periodieke incidentrapportages aan het MT NCTV.

- Binnen de NCTV is aandacht voor misbruik onder andere verstevigd door veel duidelijkere kaders te stellen voor de individuele medewerkers waar zij op aangesproken worden. Daarmee moet duidelijk worden waar mededeling van moet worden gedaan bij de BVA.
- Momenteel wordt het incidentmanagement beleid, waaronder ook periodieke incidentrapportages vallen, herzien. Daarnaast worden beheer- en gebruikslogs bijgehouden van in gebruik zijnde systemen.

Wat te doen?
- Stel opnieuw vast wie welke taken heeft in het toezicht.
- Stel jaarlijks een toezichtplan op dat in het MT NCTV wordt vastgesteld.
- Bespreek jaarlijks de resultaten van het toezicht in het MT NCTV.

- Per werkproces of informatiesysteem van de NCTV wordt vastgesteld wie de rol als eigenaar heeft. De eigenaar is verantwoordelijk voor het doen van eerstelijns toezicht, op het goed inrichten van processen en systemen, op de uitvoering van processen en het gebruik van systemen.
- De toezichtstaken zijn versterkt langs het drielijnen model:
    - Eerste lijn: De eerstelijnsverantwoordelijkheid ligt hierbij nadrukkelijk bij de verschillende afdelingen binnen de NCTV. Binnen elke afdeling is bepaald welke functionaris welke rechten heeft. Zo zijn bijvoorbeeld de meest verstrekkende rechten zoals printen beperkt tot enkele medewerkers. Met elkaar wordt scherp gekeken of gestelde regels worden gevolgd en of dit ordentelijk gebeurt.
    - Tweede lijn: Is versterkt door een afdeling in oprichting die moet gaan toezien op Risicomanagement en Compliance binnen de NCTV. Ook wordt het beveiligingscoördinator (BVC)-cluster versterkt. Hoewel de afdeling nog in oprichting is, zijn onderdelen zoals het BVC-cluster, de Chief Information Security Officer (CISO) en privacy coördinator reeds operationeel. Deze nieuwe afdeling met BVC, CISO en privacy coördinator is binnen de NCTV actief in een ingevoerd *three lines* -model.
    - Derde lijn: Dit is voor wat het betreft het VIR-BI onder andere belegd bij de Beveiligingsautoriteit van JenV, die onafhankelijk toezichthouder en adviseur is namens de SG en voor de Wet veiligheidsonderzoeken namens de Minister. De samenwerking tussen deze organisatieonderdelen is en wordt verder versterkt.
    - Specifiek in het licht van onderhavige casus is de ADR reeds gevraagd om een jaar na het verschijnen van het rapport opnieuw te toetsen bij de NCTV wat de stand van zaken is. Doel is om de aanbevelingen en zelf geïdentificeerde verbeterpunten door te voeren, zodat de ADR bij de nieuwe toets kan constateren dat de informatiebeveiliging aanzienlijk is verbeterd in vergelijking met de peildatum van 1 oktober 2023. Daarnaast zal ook bezien worden hoe audits structureler kunnen worden ingevuld, zodat externe gezichtspunten kunnen worden meegenomen in het continue proces van verbetering van de informatiebeveiliging.
- Een toezichtsplan is opgesteld, dit zal jaarlijks opnieuw gebeuren. De taken in het toezicht worden daarin meegenomen.
- Een jaarlijkse bespreking van de resultaten van dit toezicht maakt hiervan onderdeel uit.

Wat te doen?
NCTV
- Stel vast dat het aspect insider threat met de gekozen aanpak voor risicoanalyse voldoende wordt meegenomen.
- Waarborg dat de casus maximaal wordt benut om ervan te leren.

- De NCTV neemt de *insider threat* al mee in de risicoanalyses. Daarnaast is een onderzoek gestart naar hoe de risico's van een *insider threat* nog beter in kaart gebracht kunnen worden en hoe deze risico's gemitigeerd kunnen worden.
- Het maximaal benutten van de ervaringen van de casus is een continu proces vanaf het moment dat dat de casus aan het licht kwam.
- De geleerde lessen worden voortdurend meegenomen, in het bijzonder ook in het incidentmanagement beleid dat momenteel wordt herzien.

Politie

Wat te doen?
- Richt het principe 'need to know' in voor systemen die staatsgeheime of vertrouwelijke informatie bevatten. De door ons onderzochte systemen bieden daar voor het merendeel goede mogelijkheden voor.
- Ga medewerkershandelingen monitoren om ongewenst gedrag eerder te kunnen signaleren. Zowel de NCTV Als de politie beschikken al over uitgebreide logging die monitoring mogelijk maakt.
- Richt binnen CTER (en mogelijk breder binnen de politie) voorzieningen in zodat rechercheurs en tolken veilig kunnen samenwerken.

- Bij de politie zijn de bestaande regels voor het raadplegen van politiesystemen reeds gebaseerd op het *need to know* principe. Het eerstelijns toezicht op het naleven hiervan wordt verscherpt. Het (lijn)management zal beter worden toegerust voor deze rol, bijvoorbeeld door een verplichte deelname aan een *awareness* training in 2025 voor teams die werken met bijzondere informatie. Daarnaast zal *protective monitoring* per 1 januari 2025 voor de gehele politieorganisatie worden ingericht.
- Per 1 januari 2025 wordt *protective monitoring* ingevoerd voor de gehele politieorganisatie.
- De politie heeft het geldende beleid voor veilige communicatie en veilig werken met tolken na de aanhoudingen hernieuwd onder de aandacht gebracht. Het gebruik van onveilige middelen is niet toegestaan. Daarnaast zijn er voorzieningen om veilig te werken met tolken. Tolken beschikken over een eigen basispolitieaccount met zeer beperkte toegangsrechten. Dit account kan worden gebruikt voor het veilig beluisteren van audiobestanden en het opstellen van vertalingen. Tolken hebben voor hun werkzaamheden toegang tot faciliteiten om veilig te werken op politielocaties en bij hoge uitzondering op afstand. Het eerstelijns toezicht van leidinggevenden op de naleving van het geldende beleid is verscherpt.

Wat te doen?
- Communiceer over alle initiatieven op het gebied van risicoanalyse en deel de uitkomsten van de analyses.
- Actualiseer de beschrijving van het proces Risicomanagement Informatievoorziening.
- Voer binnen het CTER periodiek een risicoanalyse uit rekening houdend met dreiging vanuit statelijke actoren en criminele organisaties en insider threat.

- De politie heeft vastgesteld dat het bewustzijn van hedendaagse veiligheidsrisico's rondom informatiebeveiliging moet worden vergroot. Dat geldt met voorrang voor het CTER-cluster, maar ook voor de bredere politieorganisatie. Om de risico's op het vlak van de omgang met bijzondere informatie alsook de bredere (veiligheid)risico's nader onder de aandacht te brengen, zullen de teams van de politie die met bijzondere informatie werken in 2025 verplicht deelnemen aan een *awareness* training. Deze training zal ook gericht zijn op handelingsperspectieven voor de politiemensen die in de meest risicovolle contexten werken. De politie zal deze training structureel borgen.
- Politie gaat het proces Risicomanagement Informatievoorziening updaten en zal daarin onder de aandacht voor *insider threat* en dreigingen door statelijke actoren en georganiseerde misdaad meenemen.
- De politie maakt geen risicoanalyses voor individuele organisatieonderdelen, omdat de veiligheid van politiesystemen niet op het niveau van organisatieonderdelen wordt geborgd. De politie maakt derhalve risicoanalyses op organisatieniveau. Afwijking hiervan is niet doelmatig. Wel zal er in de *awareness* training worden stilgestaan bij de risico's voor het CTER-cluster en vergelijkbare organisatieonderdelen. *Insider threat* en dreigingen door statelijke actoren en georganiseerde misdaad worden meegenomen in de organisatie-brede update van het proces Risicomanagement Informatievoorziening.

Wat te doen?
- Maak afspraken over de beveiliging van de door CTER zelf beheerde applicaties, controle en toezicht.
- We bevelen de organisatie nadrukkelijk niet aan om de focus te leggen op het bijstellen van het gehele IB-beleid. De fasen Do, Check en Act vragen wat ons betreft op dit moment meer aandacht.

- Voor de gehele IV-infrastructuur van de politie zijn generieke beveiligingsmaatregelen van kracht. De politie zal onderzoeken of, en zo ja welke, aanvullende afspraken nodig zijn voor het de eigen beheerde omgeving van het CTER-cluster.
- De politie zal naar aanleiding van het ADR-rapport maatregelen treffen om de PDCA-cyclus sluitend te maken. De nadruk ligt daarbij op *Do, Check, Act*. Bij het sluitend maken van de PDCA-cyclus zal worden ingezet op het versterken en beter toerusten van alle drie lijnen uit het *three lines* model. Het betreft het (lijn)management (eerste lijn), interne controle (tweede lijn) en audit (derde lijn).
- Het (lijn)management zal beter worden toegerust om uitvoering te geven aan zijn verantwoordelijkheid op het vlak van informatiebeveiliging, waaronder toezicht en controle in de werkpraktijk. Als deel van de transitie van de landelijke eenheden wordt de *span of control* (het aantal medewerkers per leidinggevende) bij het CTER-cluster reeds verkleind, waardoor er naar verwachting meer ruimte ontstaat voor aandacht voor informatiebeveiliging naast het de operationele werkzaamheden. Daarnaast zal het (lijn)management van het CTER-cluster en andere teams die met bijzondere informatie werken in 2025 verplicht deelnemen aan een *awareness* training, die vervolgens geborgd zal worden. De politie zal eveneens de beveiligingsautoriteit en concernaudit versterken.

Wat te doen?
- Maak een realistisch tijdspad voor de invoering van de baseline.
- Richt de terugkoppeling in vanuit de organisatie over de implementatie.
- Wacht binnen CTER niet op het centrale traject om de baseline in te voeren. Start op basis van de uitkomsten van intern onderzoek n.a.v. de casus en het onderzoek door de ADR met het treffen van maatregelen uit de baseline.

- De politie gaat een realistisch tijdspad opstellen voor de invoering van de baseline in de gehele politieorganisatie. Het invoeren van de baseline is een zeer omvangrijke opgave, gezien de omvang van de politieorganisatie (meer dan 60.000 politiemedewerkers). De invoering zal dus stap voor stap plaatsvinden. Binnen het Politiedienstencentrum wordt de invoering van de baseline eind 2024 voltooid.
- De concern audit zal de invoering van de baseline volgen en hierover terugkoppeling verzorgen binnen de organisatie.
- De baseline zal binnen de bredere uitrol met voorrang worden ingevoerd bij het CTER-cluster.

Wat te doen?

- Beperk het aantal personen per zaak in Summ-IT dat gemachtigd is om anderen toegang te geven tot de zaak.
- Controleer periodiek de toegang tot een zaak en trek overbodige toegangsrechten in.
- Onderzoek de mogelijkheid om tijdelijk rechten toe te kennen in Summ-IT die automatisch vervallen.

- De politie zal onderzoeken of het nodig is om het aantal personen te beperken dat in Summ-IT gemachtigd is om andere toegang te geven. Het feit alleen dat een relatief groot aantal personele hiertoe gemachtigd is hoeft niet in strijd te zijn met het *need to know* principe. In de operationele werkpraktijk van de politie bestaat dikwijls de noodzaak nieuwe personen bij een zaak te betrekken, bijvoorbeeld omdat een (grootschalig) onderzoek 24/7 doorgaat en/of bij een onderzoek verschillende specialismes moeten worden betrokken.
- De politie had reeds ingeregeld dat Summ-IT accounts na verloop van tijd automatisch op niet-actief worden gezet, waardoor het account niet langer bruikbaar is en er geen toegang meer kan worden verkregen tot zaken in Summ-IT. Daarmee is er sprake van een geautomatiseerde periodieke controle. De politie zal onderzoeken of een meer fijnmazige aanpak nodig is, bijvoorbeeld het mogelijk maken van variatie in de periode waarna een account op non-actief wordt gesteld.

Wat te doen?

- Geef tolken passende faciliteiten om hun werk te doen: laptop en account voor het beluisteren en vertalen van via opname- en afluisterapparatuur verzamelde audiobestanden, een voorziening voor het ontvangen van vertrouwelijke stukken via mail en een voorziening om te printen. Zorg dat deze faciliteiten in de praktijk ook gebruikt worden.
- Verbied de verspreiding van vertrouwelijke informatie via [onveilige communicatiemiddelen].
- Verduidelijk de relatie tussen de rubriceringsrichtlijn en de Wpg. Kies daarbij voor een vuistregel die bruikbaar is bij risicoanalyse, rubricering van informatie en de selectie van maatregelen. Bijvoorbeeld: Wpg artikel 8 – Politie vertrouwelijk; Wpg artikel 9 – Politie Confidentieel; Wpg artikel 10 en 12 – Politie Geheim.
- Vertaal "onder embargo", "paars" en "hoog beveiligd" naar Wpg-artikelen en rubricering.

- De politie heeft reeds maatregelen getroffen om te verzekeren dat tolken passende faciliteiten hebben om hun werk te doen. Tolken hebben een eigen basispolitieaccount met zeer beperkte toegangsrechten. Er zijn faciliteiten om veilig te werken op politielocaties en er zijn veilige digitale middelen beschikbaar om bij hoge uitzondering werkzaamheden vanaf afstand uit te voeren. De politie inventariseert momenteel of er voldoende veilige faciliteiten zijn voor tolken op politielocaties. Zo niet, dan zal het aantal faciliteiten worden uitgebreid.
- Verder is de politie reeds gestart met het opstellen van een gedetailleerd werkproces op basis van het geldende beleid, zodat relevante teams en personen eenvoudig praktische informatie voorhanden hebben inzake het veilig werken met tolken.
- Het gebruik van onveilige communicatiemiddelen is niet in lijn met het geldende beleid en derhalve reeds verboden. Binnen het CTER-cluster is hiervoor (nogmaals) expliciet aandacht gevraagd.
- De politie gaat onderzoeken of het mogelijk is om een relatie te leggen tussen de rubriceringrichtlijn (die ziet op te beschermen belangen van de politie) en de Wpg-artikelen (die zien op het beschermen van privacy van burgers). Tevens zal de politie onderzoeken in welke mate het mogelijk is om 'onder embargo, 'paars' en 'hoog beveiligd' naar Wpg-artikelen en rubricering.

Wat te doen?
- Schoon het beleid over screening op.
- Schep duidelijkheid over de vereiste screening voor CTER-medewerkers.
- Geef richting aan het maatwerk om te bepalen wanneer een AIVD A-veiligheidsonderzoek nodig is voor een tolk die werkzaam is voor CTER.

- Het beleid voor de screening van tolken is reeds verduidelijkt. De politie werkt uitsluitend met door de politie gescreende tolken en vertalers die ingeschreven staan bij het Register beëdigde tolken en vertalers. Als er geen tolk beschikbaar is uit de database die kan voorzien in de gevraagde expertise, kan alleen om zwaarwegende operationele redenen en met toestemming van een leidinggevende gebruik worden gemaakt van een tolk die niet is opgenomen in de database. In de praktijk gebeurt dit als er sprake is van een taal die niet of nauwelijks voorkomt of als er unieke kennis van een bepaald context nodig is om goed te vertalen. De politie heeft besloten dat alle tolken op een hoger niveau dan voorheen door de politie gescreend moeten zijn. Dit proces is na de aanhoudingen onmiddellijk in gang gezet. De politie heeft hiervoor capaciteit vrijgemaakt, zodat met de realisatie van deze maatregelen direct een aanvang gemaakt kon worden. Al eerder was de database van het tolkenbureau opgeschoond en waren alle tolken waarvan de registratie in het Register Beëdigde Tolken en Vertalers niet op orde was, verwijderd.
- De politie heeft reeds verduidelijkt voor welke functies binnen het CTER-cluster een AIVD-A screening nodig is.
- De politie zal concretiseren in welke gevallen tolken die bij het CTER-cluster werken bovenop hun politie screening (op een hoger niveau dan voorheen) een AIVD-A screening nodig hebben.

Wat te doen?
- Richt structurele monitoring in op basis van de in het tapsysteem en Summ-IT gelogde gebruikershandelingen.
- Maak een begin met protective monitoring door in beeld te brengen wat de atypische signalen zijn bij CTER die via protective monitoring naar voren moeten komen.
- Ga na welke faciliteiten de logging van Summ-IT en het tapsysteem nu al bieden om die atypische signalen te rapporteren.

- De mogelijkheid om gebruikershandelingen in verschillende politiesystemen te monitoren bestond al. Met *protective monitoring* kunnen deze gebruikershandelingen proactief en geautomatiseerd worden geanalyseerd op atypische signalen om onrechtmatig gebruik van systemen te detecteren. Momenteel wordt met pilots in twee eenheden ervaring opgedaan in het gebruik van dit instrument. Ten behoeve van deze pilots is vastgelegd welke handelingen als atypisch signaal moeten worden beschouwd.
- Per 1 januari 2025 wordt *protective monitoring* ingevoerd voor de gehele politieorganisatie. Dit is een zeer omvangrijke ingreep, waarmee de politie een belangrijk technisch hulpmiddel in handen krijgt om ongeautoriseerde toegang en risicovol en onrechtmatig gebruik van informatie te detecteren. Het CTER-cluster maakt deel uit van de landelijke uitrol van *protective monitoring*.
- De concretisering van atypische signalen maakt deel uit van de lopende pilots.

Wat te doen?
- Richt de registratie en afhandeling in van inbreuken op de beveiliging van Eigen beheerde omgevingen.
- Richt een incidentenrapportage in van alle incidenten met systemen en informatie die zich bij de politie hebben voorgedaan.

- Voor de gehele IV-infrastructuur van de politie zijn generieke beveiligingsmaatregelen van kracht. De politie zal onderzoeken of, en zo ja welke, aanvullende afspraken nodig zijn voor de eigen beheerde omgevingen, waaronder die van het CTER-cluster. De mogelijkheid om een aparte registratie van inbreuken in te richten voor deze eigen beheerde omgevingen loopt hierin mee.
- Het inrichten van een incidentenrapportage van alle incidenten met systemen en informatie die zich bij de politie hebben voorgedaan bij de politie betekent een zeer grote opgave, gelet op de omvang van de politieorganisatie en de hoeveelheid informatie die wordt verwerkt. De politie zal in kaart brengen of, en zo ja hoe, incidentenrapportages binnen de organisatie kunnen worden opgesteld die werkelijk bijdragen aan overzicht en inzicht, met als uiteindelijk doel dat de (organisatieonderdelen van) de politie lessen kunnen trekken uit deze incidentenrapportages. Daarbij wordt voorrang gegeven aan het CTER-cluster.

Wat te doen?
Stel een beveiligingscoördinator aan bij de eenheid Landelijke Opsporing en Interventies die toezicht houdt op de beveiliging van informatie bij CTER.

- De politie heeft besloten om fulltime beveiligingscoördinatoren aan te stellen bij beide landelijke eenheden. Daarmee wil de politie het tweedelijns toezicht versterken. De tweede lijn kan specifieke expertise leveren aan de eerste lijn, het (lijn)management. Ook is het aan de tweede lijn om leidinggevende te wijzen op risico's en hen tegenspraak te bieden.

Wat te doen?
- Bij langdurige inzet van een tolk periodiek een bewuste afweging maken (door het management van CTER) of de inzet voortgezet moet worden.
- Screening van tolken periodiek controleren.

- Leidinggevenden maken in hun dagelijkse werk een afweging tussen mogelijke risico's enerzijds en operationeel belang anderzijds. Er wordt bij leidinggevenden extra aandacht gevraagd voor deze afweging, als onderdeel van de verplichte *awareness training* voor teams die met bijzondere informatie werken.
- De politie werkt uitsluitend met door de politie gescreende tolken en vertalers die ingeschreven staan bij het Register beëdigde tolken en vertalers. Dit register wordt doorlopend bijgewerkt. Het tolkenbureau van de politie beheert de database met daarin alle beëdigde tolken en vertalers en wijst op aanvraag tolken toe. Als er geen tolk die kan voorzien in de gevraagde expertise beschikbaar is uit de database, kan alleen om zwaarwegende operationele redenen en met toestemming van een leidinggevende gebruik worden gemaakt van een tolk die niet is opgenomen in de database. In de praktijk gebeurt dit als er sprake is van een taal die niet of nauwelijks voorkomt of als er unieke kennis van een bepaald context nodig is om goed te vertalen.
- Op het huidige screeningsniveau van tolken wordt periodiek een herhaalonderzoek uitgevoerd. Verder kan een incidenteel herhaalonderzoek worden uitgevoerd als er een wijziging is in de persoonlijke situatie die van invloed kan zijn op de betrouwbaarheid van de tolk in kwestie.

Wat te doen?
Politie

- Zorg dat maatregelen die zijn/worden ingevoerd rondom de inzet van tolken breed bekend worden.

- De tolkenliaisons van alle politie-eenheden komen periodiek bijeen om (nieuwe) maatregelen en mogelijke knelpunten te bespreken. De tolkenliaisons zorgen voor de communicatie binnen de eigen eenheid. Waar nodig wordt op onderwerpen (landelijk) geëscaleerd.