

ONDERZOEK TELEWERKEN

# BZK POLITIE

Deelrapport 3:  
Beveiligingsaspecten



Auteur: ing. N. Oussoren MCM  
Ref: g:../BZK Politie/Stap 3 Beveiligingsaspecten/Beveiligingsaspecten definitief.doc  
Uitgave: 17 juni 2002

# Inhoudsopgave

<b>1</b>	<b>SAMENVATTING</b> .....	<b>4</b>
<b>2</b>	<b>INLEIDING</b> .....	<b>5</b>
<b>3</b>	<b>REGELING INFORMATIEBEVEILIGING POLITIE</b> .....	<b>7</b>
<b>3.1</b>	<b>Algemeen</b> .....	<b>7</b>
<b>3.2</b>	<b>Verantwoordelijkheid voor informatiebeveiliging</b> .....	<b>7</b>
<b>3.3</b>	<b>Informatiebeveiligingsbeleid</b> .....	<b>7</b>
<b>3.4</b>	<b>Invulling</b> .....	<b>8</b>
<b>4</b>	<b>STATUS VAN DE BELEIDSVOORBEREIDING</b> .....	<b>9</b>
<b>4.1</b>	<b>Status van de Organisatie van de informatiehuishouding</b> .....	<b>9</b>
4.1.1	Ontwikkeling.....	9
4.1.2	Consequenties voor telewerken.....	9
4.1.3	Standaardisatie van de werkplek.....	10
<b>4.3</b>	<b>Status: PODACS regeling</b> .....	<b>11</b>
4.3.1	Algemeen.....	11
4.3.2	Aanpassing PODACS-Regeling.....	12
<b>4.4</b>	<b>Verantwoordelijkheid Informatiebeveiliging</b> .....	<b>12</b>
4.4.1	Controle op handhaving PODACS-regeling .....	12
<b>4.5</b>	<b>Relatie met het juridisch onderzoek</b> .....	<b>12</b>
<b>4.5</b>	<b>Conclusie</b> .....	<b>13</b>
<b>5</b>	<b>RAPPORTAGE VEILIG THUISWERKEN</b> .....	<b>14</b>
<b>5.1</b>	<b>Algemeen</b> .....	<b>14</b>
<b>5.2</b>	<b>Afspraken met telewerkers</b> .....	<b>14</b>
<b>5.3</b>	<b>Conclusie</b> .....	<b>14</b>
5.3.1	Aanbevelingen uit het rapport.....	15
5.3.2	Invulling aanbevelingen.....	15
<b>6</b>	<b>ONTWIKKELINGEN: LOPENDE PROJECTEN</b> .....	<b>16</b>
<b>6.1</b>	<b>P-Info</b> .....	<b>16</b>
6.1.1	De functionaliteiten van P-info .....	16
6.1.2	Beveiligingsvoorwaarde P-info.....	16
6.1.3	Projectaanpak P-Info.....	17
6.1.4	Conclusie.....	17
<b>6.2</b>	<b>IPOS</b> .....	<b>17</b>
6.2.1	Doel van het project.....	17
6.2.2	Resultaten tot nu toe.....	17

<b>7</b>	<b>ONTWIKKELING: TECHNOLOGIE .....</b>	<b>19</b>
<b>8</b>	<b>ADVIEZEN EN AANBEVELINGEN.....</b>	<b>20</b>

# 1 Samenvatting

Dit onderzoek betreft een inventarisatie van de opvattingen over beveiliging van informatiesystemen voor zover deze relevant zijn voor de telewerkpraktijk binnen de Nederlandse politie. Door documentenstudie, door het onderzoeken van pilots en door gerichte interviews is een beeld ontstaan van de stand van zaken m.b.t. het beveiligingsbeleid.

Gebleken is dat door het ontbreken van een korpsoverschrijdend informatiebeveiligingsbeleid voor telewerken momenteel gekozen is voor de meest veilige ICT omgeving. De rapportage "Veilig thuiswerken", ontwikkeld door het ITO, wordt gepresenteerd als een formulering van landelijk beleid voor veilig telewerken op de thuiswerkplek. Dit is dit een goede ontwikkeling maar kent ook beperkingen. Impliciet wordt in de genoemde rapportage gekozen voor een beperking van de telewerkmogelijkheden omdat – vanwege de hoge veiligheidseisen - niet alle kantoorfunctionaliteiten op de telewerkplek gerealiseerd kunnen worden. Dit hoeft voor het implementeren van telewerken geen belemmering te vormen maar het betekent wel dat de werkprocessen kritisch beoordeeld moeten worden op telewerkbaarheid. Dit zal tot gevolg kunnen hebben dat werkprocessen anders georganiseerd, zo mogelijk zelfs gereorganiseerd moeten worden.

Tijdens dit onderzoek is niet duidelijk geworden in hoeverre – naast bovengenoemde centrale ontwikkelingen - de korpsen op het vlak van telewerken reeds zelf beleid op dit terrein hebben ontwikkeld. Uit ons veldonderzoek (zie deelrapportage 1) is gebleken dat het formuleren van beleid vaak niet als startpunt maar als sluitstuk van telewerkpilots wordt gezien. De telewerkpilot levert als het ware de input voor het te formuleren beleid. Een dergelijke meer incrementele aanpak is wel praktisch maar heeft zeker risico's (gevaren worden an pas tijdens de rit zichtbaar).

De praktische keuze voor het kiezen van de meest veilige ICT omgeving is verklaarbaar vanuit de hoge eisen die wet- en regelgeving stelt aan de kwaliteit van de informatiehuishouding binnen de politiesector. In Deelrapportage 2 "Juridische aspecten van telewerken" wordt aangegeven dat ook de Arboverplichtingen leiden tot een hoog beveiligingsniveau.. Dit heeft in het bijzonder betrekking op processen en functies waar de veiligheids- en vertrouwelijkheidsaspecten een belangrijke rol spelen.

De belangrijkste adviezen van dit deelrapport over beveiligingsaspecten van telewerken zijn weergegeven in het laatste hoofdstuk. Belangrijke aanbevelingen zijn:

- *Ontwikkel met ondersteuning van het Expertisecentrum of haar rechtsopvolger een landelijk informatiebeveiligingsbeleid voor de politiesector die als leidraad voor de korpsen kan dienen bij het opstellen van hun eigen beleid.*
- *Stimuleer of initieer projecten die tot doel hebben werkplekken te standaardiseren en die voldoen aan alle Arbo-eisen. Daarbij kan het helpen Arbowerkplekken te certificeren*
- *Ontwikkel de beveiligingsbewakingsfunctie met het doel beveiligingsaudits uit te voeren en richt de daarbij behorende organisatie in op ministerieel- en op korpsniveau.*
- *Ontwikkel telewerkbeleid op ministerieel- en korpsniveau (uitwerking bijvoorbeeld in een telewerkconvenant). Stel op centraal en op korpsniveau een telewerkregeling op waarin gedragslijnen zijn opgenomen m.b.t. informatiebeveiliging.*

## 2 Inleiding

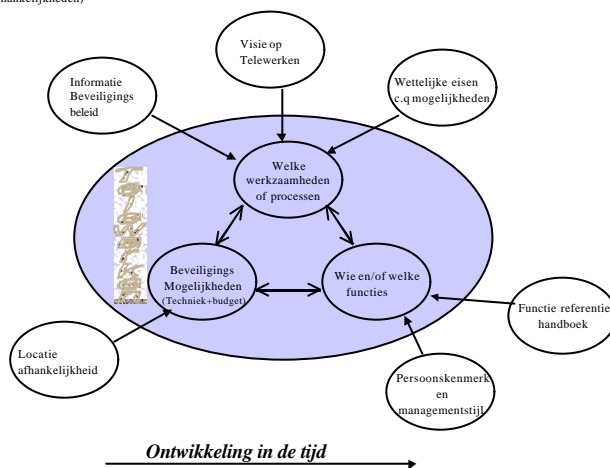
Uit het deelrapport 1 "Verkenning van de mogelijkheden" komt naar voren dat bij de verschillende telewerkpilots binnen de politieorganisatie het aspect beveiliging als een belangrijk item wordt gezien. Daarbij wordt vaak geworsteld tussen voldoende beveiligde en voldoende functionele mogelijkheden op de telewerkplek. (zie verslag over de KLPD, deelrapport 1). De korpsen zijn voor de beveiliging van de informatiesystemen gehouden aan de PODACS-regeling. Omgang met vertrouwelijke informatie is voor de telewerksituatie niet anders dan voor de kantoor situatie. *Beveiliging krijgt meer aandacht op het technische niveau dan op het organisatorisch/ gedragsniveau. (beveiligingsbewustzijn.)*

Uit het oriënterend onderzoek van telewerkprojecten buiten de politiesector komt naar voren dat het bewaken van het beveiligingsniveau als een kwetsbaar onderdeel gezien wordt (zie o.a. de opmerking van de accountantsdienst van het Ministerie van Sociale Zaken en Werkgelegenheid in verslag van de Arbeidsinspectie regio Zuid). Bij het Ministerie van Defensie (DTO) gaat men zelfs zover dat men de verschillende thuiswerkoplossingen door de Defensie Accountantsdienst laat beoordelen alvorens men overgaat tot implementatie.

Deze rapportage gaat met name in op telewerkafhankelijkheden: informatiebeveiligingsbeleid en de organisatorische aspecten daarvan.

### De telewerk thema's

(afhankelijkheden)



Dit document beschrijft eerst de formele verantwoordelijkheden en de formele eisen die gesteld worden aan het **informatiebeveiligingsbeleid** en wie daar verantwoordelijk voor is. (Onderzoek naar de feitelijke stand van zaken binnen de korpsen maakt geen onderdeel uit van onze opdracht.) Daarna wordt ingegaan op de status van de beleidsvoorbereiding en de (mogelijke) consequenties voor het invoeren van telewerken. Met name wordt aangegeven dat de organisatie van de informatiehuishouding betekenis heeft voor telewerken. Daarna wordt naar de status van de rapportage "Veilig thuiswerken" en de PODACS-regeling gekeken. Tenslotte wordt in dit hoofdstuk ingegaan op hoe de verantwoordelijkheid voor de informatiebeveiliging is geregeld.

Verder wordt inhoudelijk de rapportage 'Veilig thuiswerken' beschouwd en worden globaal de projecten P-Info en IPOS in het licht van telewerken behandeld. Afsluitend wordt een beeld gegeven van de technologische ontwikkelingen en aangegeven dat het adviseren over de mogelijkheden of onmogelijkheden van het realiseren van telewerken binnen de politieorganisatie tijdsafhankelijk is. Immers de technische mogelijkheden nemen toe waardoor het uitvoeren van plaatsafhankelijk werken steeds eenvoudiger wordt en beveiligingseisen steeds beter te realiseren zijn.

De activiteiten die in dit kader ondernomen zijn, zijn de volgende:

- Deskonderzoek van o.a. de documenten genoemd in de voetnoten en van de technologische ontwikkelingen in relatie met telewerken
- Interview bij ITO over inhoudelijke aspecten nota "Veilig thuiswerken"

- Navraag bij de secretaris van het I & A Beraad over besluitvorming in deze Raad
- Interview bij BZK DGOOV afdeling VIP over procedure en status van document "Veilig thuiswerken, beveiligingsbeleid en het project P-info
- Navraag bij ITO over de beveiligingsvoorwaarden van het Project P-info
- Navraag bij de Regieraad over de operationele invulling van P-info.
- Interview met de heer Kool, projectleider van het project IPOS

## 3 Regeling informatiebeveiliging Politie

### 3.1 Algemeen

Omdat de regeling informatiebeveiliging Politie de randvoorwaarden aangeeft die gesteld worden aan het gebruik en de beveiliging van politie informatie die ook voor de werkvorm telewerken geldt, is eerst onderzocht hoe de formele verantwoordelijkheid voor het ontwikkelen van dit informatiebeleid binnen de politieorganisatie is belegd. Tevens is gekeken in hoeverre telewerken specifiek genoemd zou moeten worden. Dit geeft een beeld van welke werkzaamheden nog opgepakt dienen te worden voordat telewerken formeel gerealiseerd kan worden. Een onderzoek naar de reeds gerealiseerde plannen binnen de korpsen valt buiten deze opdracht.

### 3.2 Verantwoordelijkheid voor informatiebeveiliging

De regeling informatiebeveiliging politie<sup>1</sup> geeft aan dat de korpsbeheerders verantwoordelijk zijn voor de informatiebeveiliging binnen hun korps. Dit houdt in (art 1 punt J) dat het volgende beschreven en binnen het korps ingericht dient te worden:

*“het treffen en onderhouden van een samenhangend pakket van maatregelen ter waarborging van de beschikbaarheid, integriteit en exclusiviteit van een informatiesysteem en daarmee van de informatie daarin “*

Deze regeling is van toepassing op het gehele proces van informatievoorziening (art 2 punt 1). Flexibel werken en Telewerken worden niet als aparte processen genoemd en vallen derhalve volledig onder de regeling. Dat door Telewerken werkprocessen kwetsbaarder kunnen worden, immers deze processen komen buiten de kantooromgeving in de thuisomgeving waardoor de mogelijkheden tot adequate beveiliging een ander karakter krijgen, wordt verder in de regeling niet gesignaleerd. Onder andere kan het onbevoegd gebruik of het meekijken van onbevoegde een extra veiligheidsrisico inhouden.

### 3.3 Informatiebeveiligingsbeleid

De regeling geeft aan dat de korpsbeheerder het informatiebeveiligingsbeleid vast stelt in een **beleidsdocument**. Dit document omvat onder andere:

- De strategische uitgangspunten en randvoorwaarden
- De organisatie van de beveiligingsfunctie
- De indeling van informatievoorzieningsfaciliteiten
- De vertaling naar concrete maatregelen

Er worden verder geen voorwaarden gesteld aan het tot stand komen van de concrete maatregelen en aan de eisen waar deze aan moeten voldoen. De rol van het ITO en de BZK beleidsrapportage (bijvoorbeeld de rapportage “Veilig thuiswerken”) worden niet nader genoemd. Dit betekent dat de korpsen hierin een eigen verantwoordelijkheid hebben. Dit geldt niet voor het gebruik van korpsoverschrijdende informatiesystemen. In art 3 wordt aangegeven dat BZK daar verantwoordelijk voor is.

Voor het invoeren van Telewerken is het noodzakelijk dat deze vorm van werken een onderdeel uitmaakt van het informatiebeveiligingsbeleid. Tevens zullen er uitvoeringsregels moeten worden geïntroduceerd of worden ontwikkeld die adequaat en toegesneden zijn op de plaatselijke situatie.

---

<sup>1</sup> Gepubliceerd in de Staatscourant 1997, nr. 60 / pagina 18

### **3.4 Invulling**

*De voorbereiding om vanuit het beveiligingsaspect telewerken mogelijk te maken zijn de volgende. Als eerste zou het informatiebeveiligingsbeleid getoetst moeten worden op het aspect Telewerken; zijn de eisen vanuit het beveiligingsbeleid voor telewerken voldoende duidelijk?*

*Daarna dienen er concrete uitvoeringsregels voor een beveiligde werkomgeving worden geformuleerd. Het rapport "Veilig thuiswerken" geeft hiervoor een aanzet.*

*Ook is het verkrijgen van toestemming voor het gebruik van de korpsoverschrijdende informatiesystemen op straat of thuis een onderdeel van de voorbereiding. Tenslotte zal de ICT infrastructuur beoordeeld moeten worden, met name of deze voldoet aan de gestelde beveiligingseisen en de specifieke eisen van de eigenaren van informatiesystemen.*

## 4 Status van de beleidsvoorbereiding

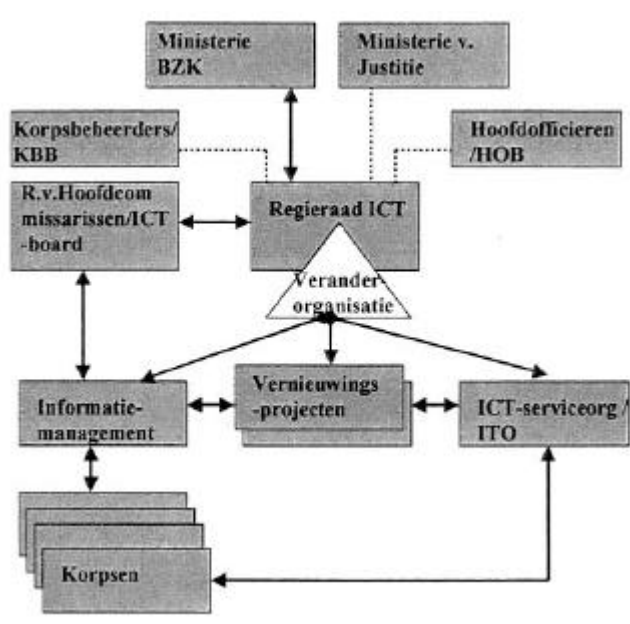
### 4.1 Status van de Organisatie van de informatiehuishouding

De organisatie wijziging voor het aansturen van "informatiehuishouding" binnen de politie kan ook consequenties hebben voor het formuleren van telewerkbeleid. Telewerken zal een vast onderdeel moeten uitmaken van de informatiehuishouding. Dit geldt met name voor het gebruik en de beveiliging van korpsoverschrijdende informatiesystemen.

#### 4.1.1 Ontwikkeling

De organisatieverandering voor het aansturen van de informatiehuishouding wordt voorbereid door Regieraad ICT Politie<sup>2</sup>. Deze raad heeft zich gebogen over de wijze waarop de vernieuwing van de informatiehuishouding van de politie en de ICT-infrastructuur in en tussen de korpsen kan worden vormgegeven. In de rapportage Bestek 2001-2005<sup>3</sup> wordt een nieuwe ICT-sturingsrelatie geschetst en aangegeven hoe de overgangperiode ingevuld en aangestuurd dient te worden.

De sturing in de transitiefase zit er als volgt uit:



Onder de verantwoordelijkheid van deze organisatie zal de komende jaren een revitalisering en vernieuwing van de informatiehuishouding gerealiseerd gaan worden. Dit betekent dat de regionale opzet en sturing zal afnemen en de infrastructuur en bedrijfsapplicaties korpsoverschrijdende ingevuld zullen gaan worden.

#### 4.1.2 Consequenties voor telewerken

Voor het telewerkbeleid van de korpsen betekent dit dat er

- meer afstemming plaats zal gaan vinden. (beveiligings- en telewerkbeleid).
- voor meer applicaties toestemming moet worden verkregen voor gebruik in de telewerkomgeving.

Het geeft ook mogelijkheden ten aanzien van het beheer van de telewerkplek en de daarvoor benodigde infrastructuur. In de nieuwe situatie zal een centrale service organisatie op dit vlak kunnen ontstaan

<sup>2</sup> Uitvoeringsplan voortkomend uit het Masterplan van de Regieraad ICT Politie. Behandeling in de Tweede kamer op 23 augustus 2000. Tweede Kamer, vergaderjaar 1999-2000, 26 345, nr. 41

<sup>3</sup> Regieraad ICT Politie Bestek 2001-2005 voor de vernieuwing van de informatiehuishouding van de Nederlandse politie. 16 februari 2001.

waarmee de korpsen schaalvoordelen kunnen realiseren. Te denken valt aan een helpdesk voor de Telewerker ook voor de uren na kantoor tijd.

#### **4.1.3 Standaardisatie van de werkplek**

In het document van de Regieraad wordt ook aangegeven dat standaardisatie van de werkplek opgepakt dient te worden (hoofdstuk 7: Vernieuwen van de infrastructuur) *Het realiseren van dit voornemen zal de invoering van Telewerken vereenvoudigen.*

Bij de standaardisatie van de werkplek (werkgebonden) wordt uitgegaan van drie basis werkplekconcepten namelijk:

- 1 *Politie op straat.* Behoeft aan het onderhouden van contacten en verkrijgen van gegevens uit bestanden. Ondersteuning middels een handheld
- 2 *Medewerkers op de politiebureaus* voor het verrichten van gestructureerde taken. Ondersteuning middels een thin-client werkplek.
- 3 *Medewerkers met onderzoeks-, analyse- of researchwerkzaamheden.* Ondersteuning middels een zwaarder type werkplek.

NB: Een concrete invulling van werkplekconcept 1 is het project P-info.

Een andere werkplekindeling die gemaakt kan worden is op basis van de locatie. In het document van de Regieraad wordt in dit kader een verwijzing gemaakt naar het einddocument van het project Basis Netwerk Infrastructuur Politie – 2000. Hier heeft men werkplekken en gebruikerslocatie als volgt onderscheiden:

- Vast
- Wissel
- Flexibel
- Thuis
- Tijdelijk
- Voer- of vaartuig
- Straat

Afhankelijk van het gebruik kan de ondersteuning voor deze werkplekken als volgt getypeerd worden.

- PC-zwaar
- PC-licht
- Windows Based Terminal (WTB)
- Laptop
- Handheld

Welke ondersteuning nodig is op welke werkplek is afhankelijk van het gewenste gebruik. Dit kan dus per korps of per functie anders worden ingevuld.

Voor het invoeren van telewerken is het van belang te weten welke werkprocessen op welke locaties ondersteund dienen te worden. Beveiligingseisen zullen de verschillende mogelijkheden waarschijnlijk beperken.

Het grote voordeel van het standaardiseren van de werkplek is het vereenvoudigen van het beheer van de (tele)werkplek. Door standaardisatie kan daardoor een lager beheer- en exploitatiekosten worden gerealiseerd.

## **4.2 STATUS: RAPPORTAGE “VEILIG THUISWERKEN”**

De rapportage “Veilig thuiswerken” is onder verantwoordelijkheid van BZK DG00V afdeling VIP gemaakt. Het ITO, met medewerking vanuit de zuidelijke regio's heeft deze rapportage opgesteld. Uitgangspunt voor deze rapportage was de geldende regelgeving, het beleid van de zuidelijke regio's en de leidraden van het Expertisecentrum informatiebeveiliging Nederlandse Politie<sup>4</sup>.

---

<sup>4</sup> BZK richtlijn “De Regeling Informatiebeveiliging Politie DG00V/IB-00V nr. EI96/U177

Om inzicht te krijgen over de status van dit document (besluitvorming binnen de politie organisatie) heeft een gesprek plaats gevonden met de opdrachtgever van deze rapportage de heer Terpsta van BZK DGOOV. Als belangrijke punten kwam het volgende naar voren:

- De korpsen (als ZBO's) zijn zelf verantwoordelijk voor het formuleren en realiseren van een veilige telewerkomgeving. De rapportage is een voorzet, gemaakt door het ITO, om op een verantwoorde wijze veilig thuiswerken binnen de regio's te kunnen realiseren.
- De rapportage is gereed maar dient nog binnen BZK vastgesteld te worden. Daarna gaat deze met een begeleidend schrijven, waarin ook melding gemaakt wordt van het onderzoek van BZK Arbeidsvoorwaardenbeleid, naar de Korpschefs en hoofden I&A binnen de korpsen.
- In het najaar zal deze rapportage op de agenda van het Korpsbeheerdersberaad en van het I&A beraad<sup>6</sup> geplaatst worden.

## 4.3 Status: PODACS regeling

### 4.3.1 Algemeen

De PODACS-regeling is een regeling van de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Justitie en bevat aanwijzingen en regels over het gebruik van het politie-datacommunicatiesysteem.

In de huidige regeling staan in artikel 8 de voorwaarden die gesteld worden aan kiesverbindingen.

#### *Artikel 8:*

Indien bij verbindingen gebruik wordt gemaakt van kiesverbindingen worden er voorzieningen getroffen ter beveiliging van deze netwerktoegang tot het datacommunicatienetwerk van het politiekorps dat is gekoppeld aan het PODACS.<sup>6</sup>

Deze voorzieningen houden ten minste in:

- a) adequate verificatie van de kiesverbinding;
- b) sterke wederzijdse authenticatie tussen de op de kiesverbinding aangesloten netwerkapparatuur van de communicerende partijen;
- c) uitgebreide vastlegging van netwerkhandelingen en
- d) jaarlijkse analyse van de vastgelegde netwerkhandelingen als bedoeld onder c).

#### *De toelichting op dit artikel is de volgende:*

Kiesverbindingen mogen binnen en met het datacommunicatienetwerk van het politiekorps worden toegepast mits deze adequaat worden beveiligd. Door middel van een kiesverbinding creëert men feitelijk een toegang tot het regionale netwerk vanaf een openbaar netwerk. Deze toegang dient van een adequate toegangsbeveiliging te worden voorzien:

Vastgesteld dient te worden waarvandaan de verbinding tot stand wordt gebracht. Dit dient heden te geschieden door middel van de implementatie van een terugbelsysteem.

Er dient op netwerkniveau door middel van een authenticatiemechanisme de authenticiteit van de communicerende netwerkcomponenten te worden vastgesteld. Momenteel dient dit te gebeuren door middel van bijvoorbeeld het Challenge Handshake Authentication Protocol.

Er dient een uitgebreide logging van gebruik van de kiesverbinding plaats te vinden. Deze vastlegging dient periodiek te worden gecontroleerd op beveiligingsincidenten. De logging omvat tenminste vastlegging van alle geslaagde en niet geslaagde inkiespogingen, de tijdstippen (van toegang en verbreken), en waar mogelijk de actualiteit van de gebruikte inbelnummers en alle beheeractiviteiten van de inkiesvoorziening.

Het beheersysteem dient bij voorkeur te zijn voorzien van directe signalering van iedere potentiële aanval.

---

De leidraad "Algemene Beveiligingsmaatregelen" van het Expertisecentrum

<sup>5</sup> Het concept is binnen het I&A beraad besproken op 31 aug 2002.

<sup>6</sup> Het politiedatacommunicatiesysteem (PODACS): het geheel van verbindingen, knooppunten en netwerkaansluitingen tot en met de koppelvlakken dat bestemd is voor de geautomatiseerde uitwisseling van gegevens door middel van draadgebonden telecommunicatievoorzieningen tussen uitsluitend:

- i) politiekorpsen onderling;
- ii) politiekorpsen en organisaties en instanties

De logging dient wekelijks te worden gecontroleerd op gebruikersactiviteiten, beheeractiviteiten en mogelijke aanvallen op de inkiesvoorziening. De logging bestanden zijn dermate beveiligd dat operationeel beheerders de logging niet kunnen wijzigen (alleen security administrators). De loggingbestanden dienen drie maanden lang te worden bewaard opdat reconstructie van gebeurtenissen gedurende deze periode mogelijk is.

Teneinde te kunnen garanderen dat daadwerkelijk alleen op een gecontroleerde wijze wordt ingelogd dient periodiek een controle plaats te vinden op de aanwezigheid van niet-geautoriseerde modemverbindingen.

Tot zover de bestaande regeling voor zoverre deze betrekking heeft op de voorwaarde die bij telewerken aan de orde zijn.

#### **4.3.2 Aanpassing PODACS-Regeling**

In de tijd van het opstellen van deze regeling was dit de toegestane mogelijkheid om aansluiting te realiseren met het politienet. Door de technologische ontwikkelingen o.a. Internet en de nieuwe organisatie ICT-gaat BZK deze regeling vernieuwen. Het voornemen is om regionale inbediensten niet meer toe te staan en het inbellen (de connectie met het politienet) onder verantwoordelijkheid van het ITO te brengen. Binnen welke tijdsspanne deze regeling aangepast zal worden is nog niet duidelijk.

### **4.4 Verantwoordelijkheid Informatiebeveiliging**

De verantwoordelijkheid voor het realiseren van een adequate informatiebeveiligingsbeleid ligt bij de korpsbeheerder. Hoe deze verantwoordelijkheid organisatorisch, procedureel en technisch bij de korpsen is ingevuld, is in dit onderzoek niet verder onderzocht. Voor de snelheid van invoeren van telewerken is de status van invulling van deze functie van grote betekenis omdat dit feitelijk de eerste stap is bij het realiseren van telewerk oplossingen. Dit geldt ook voor de ondersteuning van de diender op straat (in de auto e.d) middels de ICT-middelen.

#### **4.4.1 Controle op handhaving PODACS-regeling**

De controle op de uitvoering van de wettelijke regelgeving ligt bij BZK. Het ministerie is op basis van artikel 11<sup>7</sup> verantwoordelijk voor het bewaken van de uitvoering van de regeling. In de praktijk laat BZK deze controle door een extern accountantskantoor middels audits uitvoeren. Deze audits zijn voor het eerst recentelijk gehouden.

Bij het grootschalig invoeren van flexibel werken middels ondersteuning van ICT-middelen zou de informatiebeveiligingsorganisatie versterkt moeten worden. Deze organisatie zou tevens ondersteuning kunnen verlenen bij het geven van adviezen en ondersteunen van het handhaven van het beveiligingsniveau. Of deze rol door het Expertisecentrum<sup>8</sup> uitgevoerd zou kunnen is niet waarschijnlijk omdat het Expertisecentrum een ondersteunde rol naar de korpsen heeft, hetgeen strijdig kan zijn met de controlerende rol die hier aan de orde is. Deze mogelijkheden dienen nader onderzocht te worden.

### **4.5 Relatie met het juridisch onderzoek**

In deelrapport 2 "Juridische aspecten van telewerken" wordt aangegeven dat de Wet politieregisters een open beveiligingseis kent. Iedere beheerder kan deze eis naar eigen wens invullen. Als conclusie wordt gesteld dat met de invoering van telewerken de beveiliging verzaamd c.q. aangepast moet worden waarbij het treffen van voorzieningen complexer zal worden. Ook wordt aangegeven dat de Europol Overeenkomst "open" beveiligingseisen stelt. Het advies is dan ook om landelijke beveiligingsnomen in

---

<sup>7</sup> Artikel 11 Indien de korpsbeheerder niet of niet volledig toepassing geeft aan deze regeling, waardoor het beveiligingsniveau van het PODACS wordt of kan worden aangetast, kan de minister beveiligingsmaatregelen nemen.

<sup>8</sup> Ten behoeve van de rijksdienst is het Advies- en Coördinatiepunt Informatiebeveiliging (ACIB) ingesteld. Het ACIB adviseert, ondersteunt en begeleidt de ministeries bij hun activiteiten op het terrein van de informatiebeveiliging. Het ACIB fungeert als kennis en expertisecentrum en geeft voorlichting over informatiebeveiliging. Voor de Nederlandse politie heeft het Expertisecentrum Informatiebeveiliging Nederlandse Politie deze rol en heeft eenzelfde faciliterend karakter als het ACIB: het adviseert, ondersteunt en begeleidt de regionale politiekorpsen bij hun activiteiten op het terrein van de informatiebeveiliging. De missie van het expertisecentrum is het bevorderen van de beveiliging van de informatievoorziening in de politiesector op een gemeenschappelijke basis.

te voeren. Deze rol zou op basis van haar opdracht door het expertisecentrum uitgevoerd kunnen worden.

## **4.5 Conclusie**

Pas na de besluitvorming zal duidelijk worden in hoeverre er draagvlak is voor de maatregelen die in de rapportage Veilig thuiswerken genoemd worden. De ontwikkeling op het gebied van de informatiehuishouding is positief omdat het verkrijgen van toestemming voor het gebruik van informatiesystemen, buiten de kantooromgeving, eenvoudiger zal worden. Het standaardiseren van de werkplekken zal invoering van telewerken vereenvoudigen en de beheerkosten positief beïnvloeden. Ook zal de aangekondigde aanpassing van de PODACS-regeling mogelijkheden geven om de exploitatie van telewerken goedkoper te regelen door onderbrenging van deze taak bij een centraal orgaan. Deze werkwijze zal voor BKZ kunnen betekenen dat het auditen van de beveiliging (uitvoerings)maatregelen eenvoudiger plaats zal kunnen vinden.

Er zal nadere aandacht gegeven moeten worden aan het bewaken van de kwaliteit van de (telewerk)beveiliging binnen de korpsen voor zover dit de korps specifieke toepassingen en organisatorische invulling betreffen. Tevens zal er op centraal niveau de beveiligingscontrole functie versterkt moeten worden.

## 5 Rapportage veilig thuiswerken

In dit hoofdstuk wordt de rapportage “Veilig thuiswerken Nederlandse Politie” inhoudelijk bekeken en aangegeven hoe deze richtlijn door de korpsen gebruikt kan worden bij het realiseren van telewerkprojecten.

### 5.1 Algemeen

De rapportage wordt gepresenteerd als zijnde het formuleren van landelijk beleid voor veilig thuiswerken en behandeld vanuit de technologie de wijze waarop telewerken, passend binnen de beveiligingsrandvoorwaarden gerealiseerd kan worden.

Bij het opstellen is uitgegaan van een baseline beveiliging dit wil zeggen dat uitgegaan is van het beveiligingsniveau Gemiddeld<sup>9</sup>. Dit betekent dat voor informatiesystemen die een classificatie “Hoog” heeft, aanvullende maatregelen genomen moeten worden. Dit zou kunnen betekenen dat zo'n informatiesysteem niet in een telewerksituatie gebruikt kan worden.

*Dit kan betekenen dat voor bepaalde functies waar die processen aan de orde zijn, telewerken niet tot de mogelijkheden behoort of maar beperkt mogelijk is.*

*Ook stelt deze rapportage dat in de thuissituatie geen printmogelijkheden geboden moeten worden. Onderzocht moet worden of deze restrictie nog meer functies uitsluit voor uitvoering in telewerkverband.*

### 5.2 Afspraken met telewerkers

De rapportage geeft een checklist voor het opstellen van een thuiswerkovereenkomst. Deze checklist gaat uit van de volgende opbouw van afspraken:



Bovenstaande afsprakenstructuur zal op korpsniveau mogelijk aangepast dienen te worden.

### 5.3 Conclusie

*De rapportage is een prima hulpmiddel voor het nader definiëren van op het korps toegespitst telewerkbeleid. Dit is ook de opzet van de makers geweest. Wel wordt in de managementsamenvatting aangegeven dat er op verschillende gebieden nader onderzoek en uitwerking nodig is. Afhankelijk van hoe breed telewerken binnen het korps opgezet gaat worden (telewerken voor een beperkte groep of voor de hele organisatie) zullen deze aanbevelingen consequenties hebben voor de snelheid waarmee telewerkprojecten gerealiseerd kunnen worden.*

<sup>9</sup> De Regeling Informatiebeveiliging Politie (RIP) gaat uit van drie niveaus: hoog, gemiddeld en laag.

### 5.3.1 Aanbevelingen uit het rapport

Volledigheidshalve worden de aanbevelingen hieronder worden samengevat:

**Aanbeveling 1** gaat over het formuleren van een eenduidig begrip telewerken en luidt: *Verder uitwerken van de begrippen telewerken, mobiel werken en beschrijven van de gewenste functionaliteit.*

Deze aanbeveling geeft aan dat het veelal onduidelijk is welke functionaliteiten op welke (werk) locatie uitgevoerd moeten worden.

**Aanbeveling 2** gaat over het ontwikkelen van een samenhangend beleid dat voor alle vormen van flexibel werken moet gelden. De aanbeveling luidt: *Uitwerken van het beleid rond telewerken en mobiel werken.*

**Aanbeveling 3** gaat over dat in dit beleidskader een benadering is gekozen waarin het beheer en de beveiliging maximaal geregeld en gecontroleerd zijn waardoor de mogelijkheden van de telewerker sterk zijn afgebakend. Deze keuze zijn gedaan vanuit de huidige voorzieningen. Deze voorzieningen zijn nog niet geschikt voor de telewerksituatie. De aanbeveling luidt: *Maak een implementatieplan voor de ICT voorzieningen voor veilig thuiswerken.*

**Aanbeveling 4** gaat over het verder uitwerken van de managementchecklist en luidt: *Maak een handreiking veilig thuiswerken voor de organisatie*

**Aanbeveling 5** gaat over het verbreden van telewerken. De beleidsnotie "Veilig thuiswerken" doet geen uitspraken over mobielwerken op variabele locaties. De uitkomsten van deze aanbeveling zou dit wel moeten opleveren. De aanbeveling luidt: *Onderzoek welke pakketten en mechanismen nu beschikbaar zijn voor het beveiligen van laptops voor de mobiele telewerker voor kleinschalig gebruik. Onderzoek tevens de mogelijke inzet en de rest-risico's van de oplossing.*

### 5.3.2 Invulling aanbevelingen

Bij het invoeren van telewerken binnen de korpsen is het zeker noodzakelijk de functionaliteiten (onderdeel van aanbeveling 1) uit te werken, een implementatieplan te ontwikkelen (aanbeveling 3) en thuiswerkbeleid en telewerkovereenkomsten te ontwikkelen (aanbeveling 4). Het project P-info en de telewerkontwikkeling bij de KLPD kunnen worden gezien als een eerste invulling van aanbeveling 5. Ook zijn er ontwikkelingen bij de korpsen (zie rapportage "Inventarisatie telewerkprojecten bij de Politie") en wel bij de korpsen Groningen, Amsterdam-Amstelland en Brabant Zuid-oost die mogelijk geheel of gedeeltelijk invulling geven aan de aanbevelingen.

## 6 Ontwikkelingen: Lopende Projecten

### 6.1 P-Info

Als voorbeeld voor het invoering van flexibel werken (= een uitgebreidere vorm van telewerken omdat er geen sprake is van een vaste locatie) kan het project P-info van de politieregio Gelderland-Midden genoemd worden.

In dit project zijn, vooruitlopend op het vaststellen van het beleidsdocument "Veilig thuiswerken", beveiligingsvoorwaarden vastgesteld en gerealiseerd. Deze praktische invulling met name voor de informatiebeveiliging zal na evaluatie als voorbeeld kunnen dienen voor de wijze waarop informatiebeveiliging bij Telewerkprojecten gerealiseerd kan worden.

#### 6.1.1 De functionaliteiten van P-info

P-info maakt het mogelijk voor de gebiedsagenten om op ieder gewenst moment via hun mobiele WAP telefoon regionale politiedatabases en landelijke opsporingsregisters te kunnen bevragen. In de toekomst zal het mogelijk zijn locaties van incidenten weer te geven op kaartjes (wat heeft in mijn plaatselijke omgeving plaats gevonden en wat zijn de lopende zaken in mijn regio), te e-mailen, afspraken te plannen in een agenda, en adressen en telefoonnummers op te vragen en te bewaren. De positiebepaling (de meldkamer weet waar de diender zich bevindt) heeft voordelen voor de persoonlijke veiligheid van de diender en maakt het mogelijk een snelle opvolging van de hulpvraag te realiseren.



#### Functionaliteit

Met P-Info kunnen agenten altijd en overal via hun mobiele WAP telefoon:

- regionale politiedatabases (o.a. informatie over incidenten, betrokken personen en goederen, burgers en ondernemingen) en landelijke opsporingsregisters (voertuigen, gezochte personen) raadplegen;
- locaties weergeven op kaartjes;
- beschikken over centrale kantoorfuncties (e-mail, agenda, adressenlijst) van het bedrijfsnetwerk.

#### 6.1.2 Beveiligingsvoorwaarde P-info

Bij het project P-info is veel aandacht besteed aan beveiliging van de informatie. Er wordt gesproken van een end-to-end beveiligingsaanpak waarbij de hele keten onderdeel uitmaakt van de beveiligingsmaatregelen. Voordat informatie uit (politie)bestanden op straat gebruikt mag worden, moet aan de volgende eisen worden voldaan:

- De eigenaar van de gegevens (informatiesysteem) moet schriftelijke toestemming geven. Dit zijn bijvoorbeeld RDW, GBA, Politie-opsporingsregister. Voor het verkrijgen van toestemming moet aan hoge beveiligingseisen worden voldaan.
- Van de eigenaars van de informatiesystemen is toestemming verkregen voor gebruik van de informatie op straat. Bij navraag onder welke (beveiligings)condities deze toestemming is verkregen werd door betrokkene hier geen nadere informatie over gegeven<sup>10</sup>.

<sup>10</sup> Later is meegedeeld dat nadere informatie over de voorwaarden waaronder toestemming voor het gebruik van de informatie op straat is verkregen, voor de korpsen te verkrijgen is bij de heer Terpstra van BZK

- De toegang naar het netwerk moet op het niveau van en geënt zijn op de ITD (Internet toegangsdiens) voorwaarden. De koppeling met het politienetwerk moet gecertificeerd zijn. (encryptie-procedure<sup>11</sup>)
- Beveiligingsmaatregelen zijn onder andere het toepassen van een redelijk “zware” encryptie en een inlogprocedure met een uitgebreide authenticatie en autorisatie procedure om toegang te verkrijgen tot het netwerk én om toegang te verkrijgen tot het betreffende informatiesysteem. Authenticatie voor toegang tot het netwerk vindt plaats op basis van secure ID middels een persoonlijke kaart van de gebruiker die in het toestel is geplaatst
- De gebruiker kan alleen bij de informatie komen op systemen die voor de betreffende persoon ontsloten is.

### 6.1.3 Projectaanpak P-Info

Om goed zicht te krijgen op het gebruik in de praktijk maar ook op de veiligheidsaspecten kent dit project vier invoeringsfases:

- De pilot (deze is afgerond)
- Invoering van de 1.0 versie voor 100 gebruikers
- Invoering van de 1.1 versie voor 1000 gebruikers
- Invoering van de 2.0 versie, beschikbaar stellen voor landelijk gebruik. Volgens planning zal dit eind 2002 plaats gaan vinden.

### 6.1.4 Conclusie

*Voor het P-info project is een eerste praktische invulling aan de beveiligingsvoorwaarde gegeven. Deze invulling kan als voorbeeld voor telewerken situaties gebruikt worden. Echter de beveiligingsmaatregelen zouden minder “zwaar” ingevuld behoeven te worden omdat telewerken plaatsgebonden is. Bij telewerken is het mogelijk aanvullende afspraken te maken over bijvoorbeeld de objectbeveiliging en te eisen dat het woonhuis (telewerklocatie) moet voldoen aan de eisen van “Veilig wonen”.*

## 6.2 IPOS

In opdracht van de Regieraad loopt het project **IPOS** ( Informatievoorziening voor politiewerk op straat) dit is de opvolger van het project Kantoor Op Straat, waarbij de verschillende activiteiten die op dit moment met betrekking tot de mobiele werkplek in het veld lopen, zoveel mogelijk betrokken worden.

### 6.2.1 Doel van het project

Het project heeft tot doel een betere informatievoorziening voor de politie te realiseren die onafhankelijk is van plaats en tijd. Het project richt zich op basispolitiezorg, de Diender op straat en heeft tot doel de hoofdprocessen (informatietechnisch) beter te ondersteunen. Dit zijn de processen:

- Noodhulp
- Wijkwerk

Het project is gestart in november 2001 en loopt tot december 2002.

### 6.2.2 Resultaten tot nu toe

De resultaten van dit project zijn:

- Een implementatie leidraad voor de korpsen
- Het ontwikkelen van een beheerorganisatie

---

<sup>11</sup> Cryptografie is een versleuteling die in feite niets meer dan een geavanceerde vorm van geheimschrift is waarmee leesbare tekst door middel van een formule wordt omgezet in een onleesbare, versleutelde tekst. Encryptie wordt gebruikt om documenten onleesbaar te maken tijdens transport over het Internet. Alleen de verzender en/of de ontvanger hebben een sleutel waarmee de onleesbare tekst kan worden omgezet in begrijpelijke taal.

De implementatie leidraad zal het volgende gaan bevatten:

- Procesmodel politiestraatwerk;
- Referentiekader;
- Eisen aan Politie-applicaties
- Implementatiescenario's
- Model regionale beheerorganisatie.

Uit het Interview met de projectleider de heer Kool bleek dat er behoefte bestaat het onderzoeksresultaat van dit telewerkonderzoek te betrekken en zomogelijk in te brengen in het IPOS project.

## 7 Ontwikkeling: technologie

De techniek ontwikkelt zich razend snel waardoor de mogelijkheden om plaatsonafhankelijk te gaan werken steeds eenvoudiger worden. Ook wordt hard gewerkt om het beveiligen van informatie te verbeteren en voor de gebruiker eenvoudiger te maken. De volgende ontwikkelingen maken het invoeren van telewerken eenvoudiger en (informatietechnisch) veiliger:

- Computers (waaronder Laptop's en PDA's)
- Kleinere en handzamer ICT middelen
- Internet (waaronder VPN's, ASDL)
- Meer capaciteit en betere beveiliging
- Encryptie technieken (waaronder PKI<sup>12</sup>)
- Betere informatiebeveiliging
- Chipcards (autorisatie en authenticatie mogelijkheden)
- Verhogen van de gebruiksvriendelijkheid; opslag biometrische informatie
- Draadloze communicatie technieken (GSM, GPRS)
- Locatie onafhankelijk worden
- Software (nieuwe applicaties)
- betere beveiliging en gebruiksvriendelijkheid.

Kortom te veel om op te noemen. Deze ontwikkelingen geven aan dat een advies over de mogelijkheden of onmogelijkheden van het realiseren van telewerken binnen de politieorganisatie tijdsafhankelijk is omdat de technische mogelijkheden toenemen waardoor het uitvoeren van plaatsonafhankelijk werken steeds eenvoudiger wordt en beveiligingseisen steeds beter te realiseren zijn.

Naarmate meer gebruik wordt gemaakt van openbaar toegankelijke oplossingen, is het beveiligingsrisico groter en moet het beveiligingsniveau hoger zijn. Op dit punt kan geen risico worden geaccepteerd. Het toepassen van landelijke standaarden op het terrein van de informatiebeveiliging zal ertoe leiden dat de Minister van BZK landelijke aanwijzingen moet geven.

*Opmerking: Binnen BZK heeft Public Key Infrastructuur (PKI) prioriteit gekregen. Het beleid is erop gericht om het derden moeilijk te maken om berichten te onderscheppen of er een andere identiteit aan te geven. In 2002 zal daarom in versneld tempo worden gewerkt aan de PKI.*

---

<sup>12</sup> **Public Key Infrastructuur.** Als uitgangspunt voor de beveiliging wordt gekozen voor een universeel geaccepteerde methodiek met gebruikmaking van encryptie-technieken (versleutelingstechnieken), culminerend in een zogeheten Public Key Infrastructuur (PKI). In zo'n infrastructuur wordt gewerkt met een publieke sleutel (public key) en een privé sleutel (private key). Een bericht kan alleen dan worden ontcijferd als de ontvanger beschikt over de juiste sleutel. De zender van het versleutelde bericht weet dat uitsluitend de beoogde ontvanger het kan lezen. Ook is de zender ervan verzekerd dat het bericht onderweg niet veranderd is. Aan de andere kant weet de ontvanger dat de zender is wie hij zegt te zijn en dat het ontvangen bericht inderdaad zo en niet anders is bedoeld en verzonden.

In feite kan met deze methodiek een elektronische handtekening worden gezet, waarbij onafhankelijke derde partijen borg staan voor de versleuteling en voor de uitgifte van persoonlijke sleutels gekoppeld aan identiteiten in de vorm van certificaten. Dergelijke certificaten bevatten een aantal gegevens van de houder, inclusief de publieke sleutels waarmee een elektronische handtekening kan worden gezet, en waarmee te verzenden informatie onleesbaar kan worden gemaakt.

## 8 Adviezen en aanbevelingen

Samenvattend zijn de volgende adviezen te geven:

1. *Ontwikkel met ondersteuning van het Expertisecentrum Informatiebeveiliging Nederlandse Politie (of haar rechtsopvolger) een landelijk informatiebeveiligingsbeleid dat als leidraad voor de korpsen kan fungeren.*
2. *Het niveau van de openbaarheid van het datatransport is bepalend voor het beveiligingsniveau. De Minister van BZK dient landelijke aanwijzingen te geven m.b.t. de toepassing van een beveiligingsinstrumentarium daar waar gebruik wordt gemaakt van openbare voorzieningen voor datatransport.*
3. *Onderzoek binnen de korpsen in hoeverre telewerken in het bestaande informatiebeleid is opgenomen en qua beveiliging is afgedekt.*
4. *Formuleer uitvoeringsregels voor informatiebeveiliging voor de niet locatiegebonden werkomgeving (te weten de flexplek of buurtbureau, op straat, in de auto en voor de thuissituatie). Het rapport Veilig thuiswerken zal - afhankelijk van de besluitvorming binnen het korpsoverleg - hierbij de leidraad zijn. Ook zal - wederom afhankelijk van de uitkomsten van dat overleg - landelijk danwel per korps een projectgroep worden ingesteld die voor de uitwerking van de uitvoeringsregels zorgdraagt.*
5. *Onderzoek in hoeverre de ICT-infrastructuur binnen het korps en de PODACS-regeling voldoen om invulling te kunnen geven aan de geformuleerde uitvoeringsregels voor flexibel werken.*
6. *Herijk de PODACS-regeling zodat op het gebied van ICT-beheer ITO een ondersteunende rol bij de invoering en ontwikkeling van telewerken kan spelen.*
7. *Standaardiseer - door middel van gerichte projecten - de voorkomende werkplekken in de politieorganisatie. Werkplekken (dus ook mobiele werkplekken) moeten ARBO gecertificeerd zijn. Deze taak kan worden toegedeeld aan het Expertisecentrum Informatiebeveiliging Nederlandse Politie (of aan haar rechtsopvolger).*
8. *Ontwikkel de beveiligingsbewakingsfunctie met het doel beveiligingsaudits uit te voeren en richt de daarbij behorende organisatie op ministerieel- en korpsniveau in.*
9. *Ontwikkel telewerkbeleid op ministerieel- en korpsniveau (uitwerking telewerkconvenant) en stel een telewerkregeling op centraal en korpsniveau op met gedragsregels op het terrein van informatiebeveiliging.*
10. *Inventariseer de beveiligingsvoorwaarden zoals deze door de informatie-eigenaren is gesteld voor lopende projecten (o.a. P-Info).*
11. *Maak bij het opstarten van initiatieven op het telewerkgebied gebruik van de resultaten van het lopende project IPOS. Werk zo mogelijk gezamenlijk vervolgstappen uit om snel te komen tot de implementatieleidraad voor de korpsen.*