Regeling informatiebeveiliging politie

BIZ, JU

«Politiewet 1993»

Ministerie van Binnenlandse Zaken
17 maart 1997/Nr. EIB96/U177
DGOOV/IB-OOV
Ministerie van Justitie
17 maart 1997/Nr. 569227/96 GBJ
Directie Strafrechtelijke Handhaving

De Minister van Binnenlandse Zaken en de Minister van Justitie,
Gelet op de artikelen 38, derde lid, artikel 46 en 48, eerste lid, van de Politiewet 1993;
Gezien het advies van de korpsbeheerders, kenmerk 0113\1235\EMd'H, d.d. 17 december 1996, en van de Raad voor het Korps landelijke politiediensten, d.d. 25 oktober 1996;

Besluiten:

Artikel 1
In deze regeling wordt verstaan onder:
a. *politiekorpsen:* de regionale politiekorpsen en het Korps landelijke politiediensten;
b. *afhankelijkheidsanalyse:* het vaststellen in hoeverre bedrijfsprocessen die door informatiesystemen ondersteund worden, afhankelijk zijn van de betrouwbaarheid van deze systemen en het vaststellen welke potentiële schades kunnen optreden als gevolg van het falen van deze informatiesystemen;
c. *betrouwbaarheid:* de mate waarin een politiekorps zich kan verlaten op een informatiesysteem voor zijn informatievoorziening.
d. *beschikbaarheid:* de mate waarin een informatiesysteem in bedrijf is op het moment dat een politiekorps het nodig heeft;
e. *integriteit:* de mate waarin een informatiesysteem zonder fouten is;
f. *exclusiviteit:* de mate waarin de toegang tot en de kennisname van een informatiesysteem en de informatie daarin beperkt is tot een gedefinieerde groep van gerechtigden;
g. *informatiesysteem:* een geheel van gegevensverzamelingen, personen, procedures, programmatuur en opslag-verwerkings- en communicatie-apparatuur;
h. *gemeenschappelijke IT-dienst:* een geheel van voorzieningen dat ter beschikking staat aan één of meerdere informatiesystemen binnen een politiekorps en waarvoor de verantwoordelijkheid eenduidig is toe te wijzen aan één organisatorische eenheid;
i. *kwetsbaarheidsanalyse:* het vaststellen van de invloed van het manifest worden van bedreigingen op het functioneren van een informatiesysteem of een gemeenschappelijke IT-dienst;
j. *informatiebeveiliging:* 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;
k. *informatiebeveiligingsplan:* de opsomming van alle beveiligingsmaatregelen of de vindplaatsen daarvan die voor een informatiesysteem of een gemeenschappelijke IT-dienst van kracht zijn;
l. *calamiteitenparagraaf:* de opsomming van alle maatregelen die tot uitvoering moeten komen als zich een situatie voordoet waarbij de beschikbaarheid, integriteit of exclusiviteit van een informatiesysteem in beduidende mate niet aan de eisen voldoen;
m. *kwaliteit:* de mate waarin het geheel van eigenschappen van een informatiesysteem voldoet aan de uit het gebruiksdoel voortvloeiende eisen;
n. *systeemexploitatie:* de zorg voor het functioneren van (een deel van) een informatiesysteem;
o. *systeemverwerving:* de zorg voor het ontwikkelen, kopen, huren en dergelijke en het uitvoeren van aanpassingen aan (delen van) een informatiesysteem zoals procedures, programmatuur of apparatuur.

Artikel 2
1. Deze regeling is van toepassing op het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.
2. De korpsbeheerder, en voor zover het betreft het Korps landelijke politiediensten, de Minister van Justitie, is verantwoordelijk voor informatiebeveiliging, hetgeen een onderdeel van de kwaliteitszorg voor bedrijfsprocessen en de ondersteunende informatiesystemen vormt.
3. Informatische relaties tussen een politiekorps en andere politiekorpsen gaan vergezeld van schriftelijke afspraken over de gehanteerde normen inzake de betrouwbaarheid van de informatiesystemen en de informatie daarin, op basis van de criteria en de bijbehorende normklassen, bedoeld in de bijlage die bij deze regeling is gevoegd, en de wijze waarop zekerheid wordt verkregen over de realisatie daarvan.
4. Informatische relaties tussen een politiekorps en andere instanties gaan vergezeld van schriftelijke afspraken over de betrouwbaarheid van de informatiesystemen en van de informatie daarin en de wijze waarop zekerheid wordt verkregen over de realisatie daarvan.

Artikel 3
1. De korpsbeheerder, en voor zover het betreft het Korps landelijke politiediensten, de Minister van Justitie, stelt het informatiebeveiligingsbeleid vast in een beleidsdocument en draagt dit beleid uit. Indien het informatiebeveiligingsbeleid mede betrekking heeft op informatiesystemen ten behoeve van de opsporing van strafbare feiten, stelt de korpsbeheerder dit beleidsdocument vast na overleg met de hoofdofficier van justitie.
2. Het document omvat tenminste:
a. de strategische uitgangspunten en randvoorwaarden die het politiekorps hanteert ten aanzien van informatiebeveiliging, met name de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid;
b. de organisatie van de beveiligingsfunctie, waaronder het toedelen van verantwoordelijkheden, taken en bevoegdheden;
c. de eenduidige en volledige indeling van informatievoorzieningsfaciliteiten in informatiesystemen en gemeenschappelijke IT-diensten en toewijzing

van de verantwoordelijkheden daarvoor aan leidinggevenden;
d. de wijze waarop het beleid wordt vertaald naar concrete maatregelen en de wijze waarop deze gefinancierd worden;
e. de gemeenschappelijke betrouwbaarheidseisen en maatregelen, vastgesteld met inachtneming van de bij deze regeling gevoegde bijlage, die voor het politiekorps van toepassing zijn;
f. de wijze waarop geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging door politieambtenaren gemeld worden, de politieambtenaar bij wie deze inbreuken worden gemeld en de wijze waarop deze worden afgehandeld;
g. de wijze waarop en de frequentie waarmee volgens een vastgesteld schema het informatiebeveiligingsbeleid geëvalueerd wordt en de toereikendheid van het informatiebeveiligingsbeleid alsmede de implementatie en de uitvoering daarvan wordt beoordeeld door een onafhankelijke deskundige en
h. de wijze waarop het beveiligingsbewustzijn wordt bevorderd.

Artikel 4
De korpsbeheerder, en voor zover het betreft het Korps landelijke politiediensten, de Minister van Justitie, draagt er zorg voor dat voor elk informatiesysteem en voor elke gemeenschappelijke IT-dienst op systematische wijze met inachtneming van de bij deze regeling gevoegde bijlage bepaald wordt welk stelsel van maatregelen uit hoofde van informatiebeveiliging getroffen dient te worden. Deze zorgplicht houdt tenminste in dat:
a. voor elk informatiesysteem een afhankelijkheidsanalyse wordt uitgevoerd, uitmondend in de aan het informatiesysteem te stellen betrouwbaarheidseisen;
b. voor elke gemeenschappelijke IT-dienst een afhankelijkheidsanalyse wordt uitgevoerd, uitmondend in de aan die IT-dienst te stellen betrouwbaarheidseisen;
c. voor elk informatiesysteem en voor elke gemeenschappelijke IT-dienst de bedreigingen worden geïdentificeerd en geanalyseerd;
d. voor elk informatiesysteem en voor elke gemeenschappelijke IT-dienst dusdanig maatregelen worden gekozen dat door middel van een kwetsbaarheidsanalyse aangetoond kan worden dat aan de gestelde betrouwbaarheidseisen wordt voldaan;
e. voor elk informatiesysteem en voor elke gemeenschappelijke IT-dienst een informatiebeveiligingsplan wordt vastgesteld. Hierin is in elk geval opgenomen:
1. een actieplan ter implementatie van alle beveiligingsmaatregelen;
2. een calamiteitenparagraaf waarvan de effectiviteit periodiek wordt getoetst.

Artikel 5
Met het oog op zo uniform mogelijke beveiligingsafspraken bij gegevensuitwisseling tussen politiekorpsen onderling en met andere instanties, bedoeld in artikel 2, derde en vierde lid, het bereiken van zo uniform mogelijke betrouwbaarheidseisen en maatregelen, bedoeld in artikel 3, onderdeel e, en het opstellen van zo uniform mogelijke informatiebeveiligingsplannen, bedoeld in artikel 4, onderdeel e, werken de politiekorpsen samen.

Artikel 6
De korpsbeheerder, en voor zover het betreft het Korps landelijke politiediensten, de Minister van Justitie, draagt er zorg voor dat voor elk bedrijfsproces de maatregelen die uit hoofde van de informatiebeveiliging van toepassing zijn op de ondersteunende informatiesystemen en dat de maatregelen die van toepassing zijn op elke gemeenschappelijke IT-dienst, worden vastgelegd, geïmplementeerd of uitgedragen en dat de werking volgens een vaststaand schema wordt gecontroleerd. Deze zorgplicht houdt tenminste in dat:
a. voor elk informatiesysteem en voor elke gemeenschappelijke IT-dienst de uit het informatiebeveiligingsplan voortvloeiende maatregelen voor de gebruikers worden vastgelegd en door de korpsbeheerder, en voor zover het betreft het Korps landelijke politiediensten,de Minister van Justitie, worden uitgedragen;
b. voor elk informatiesysteem en voor elke gemeenschappelijke IT-dienst de uit het informatiebeveiligingsplan voortvloeiende maatregelen voor systeemexploitatie schriftelijk worden vastgelegd;
c. volgens een vastgesteld schema een onafhankelijk oordeel over de kwaliteit van de getroffen informatiebeveiligingsmaatregelen en over het handhaven en naleven daarvan wordt verlangd;
d. voor elk informatiesysteem en voor elke gemeenschappelijke IT-dienst de uit het informatiebeveiligingsplan voortvloeiende maatregelen voor systeemmanagement door de korpsbeheerder, en voor zover het betreft het Korps landelijke politiediensten, de Minister van Justitie, schriftelijk worden vastgelegd;
e. de uit het informatiebeveiligingsplan voortvloeiende maatregelen voor systeemverwerving worden getoetst op hun implementatie en werking.

Artikel 7
Deze regeling treedt in werking op 1 april 1997.

Artikel 8
Deze regeling wordt aangehaald als Regeling informatiebeveiliging politie.
Deze regeling zal met de toelichting en de bijbehorende bijlage in de Staatscourant en het Algemeen Politieblad worden geplaatst.

's-Gravenhage, 17 maart 1997.
De Minister van Binnenlandse Zaken,
H.F. Dijkstal.
De Minister van Justitie,
W. Sorgdrager.

Toelichting

Algemeen

De noodzaak tot informatiebeveiliging
Het gebied van de politiële informatiebeveiliging is nog een bijna braakliggend terrein. Zo werd daarover in het rapport 'Beveiligingskader' dat op 12 oktober 1994 door het Beleidsadviescollege voor de politiële informatievoorziening (BPI) aan de Ministers van Binnenlandse Zaken en Justitie is uitgebracht, op pagina 22 opgemerkt: 'Uit het verrichte onderzoek beveiliging HKS/PODACS, uit de stand van zaken betreffende de ontwikkeling van beveiligingsplannen HKS en PODACS, en uit een onderzoek naar het bewust omgaan met beveiliging bij zeven politiekorpsen kan eenzelfde beeld worden geconstateerd. Beveiliging blijkt vooral in technische zin nagestreefd te worden waarbij eenduidig risicobeleid en beleidsplannen ontbreken.' Uit een enquête die begin 1996 in het kader van het Platform voor de Politiële Informatievoorziening (PPI)-project

'Implementatie informatiebeveiliging' onder de 25 regionale politiekorpsen en het Korps landelijke politiediensten is gehouden, blijkt dat het hiervoor geschetste beeld op hoofdlijnen nog weinig is veranderd. Onder meer gezien dit feit is het noodzakelijk dat de korpsbeheerders, en voor zover het betreft het Korps landelijke politiediensten, de Minister van Justitie, hun verantwoordelijkheid met betrekking tot informatiebeveiliging gaan invullen.

Verder is in het regeringsstandpunt ten aanzien van de adviezen van het BPI is op 7 juli 1995 aan de Voorzitter van de Tweede Kamer aangegeven dat door de Ministers van Binnenlandse Zaken en Justitie een stelsel van normen op het gebied van beveiliging wordt ontwikkeld waaraan de politiekorpsen moeten gaan voldoen (Kamerstukken II 1994/95, nr. 23 900 VI en VII, nr 31).

De politiekorpsen hebben een belangrijke inhaalslag uitgevoerd op het gebied van de geautomatiseerde informatievoorziening. Elk korps heeft in nog geen 10 jaar tijd een technische infrastructuur tot stand gebracht en zijn toepassingen ingevoerd voor de ondersteuning van bijna alle bedrijfsprocessen. Voor de uitvoering en besturing van het werk is de politie afhankelijk geworden van de informatievoorziening. Daarbij komt dat er niet alleen omvangrijke gegevensverzamelingen zijn aangelegd over gebeurtenissen, maar ook over natuurlijke personen. Verstoringen van de betrouwbaarheid (welk begrip bestaat uit de deelbegrippen beschikbaarheid, integriteit en exclusiviteit) hebben invloed op de uitvoering en besturing van het politiewerk en kunnen ook leiden tot schade aan de belangen van personen, politiekorpsen of andere instanties. Deze schade zal zijn weerslag hebben op het imago van de politie en kan aanzienlijke schadeclaims opleveren.

Een volgende belangrijke ontwikkeling is dat de politiekorpsen, net als andere organisaties, steeds minder zelfvoorzienend worden in hun informatievoorziening: zij maken gebruik van informatie die door anderen wordt geleverd en leveren zelf ook informatie aan anderen. Het gevolg is dat verstoringen van de betrouwbaarheid niet alleen invloed hebben op het eigen werk, maar ook op het werk van anderen. Wie onvoldoende aandacht besteedt aan de beveiliging van zijn informatievoorziening, wordt een risico voor anderen en loopt de kans dat hij daardoor geen gegevens meer van anderen ontvangt en in een isolement geraakt. Deze situatie, die het gevolg is van de introductie van de netwerktechnologie, maakt onderlinge afstemming noodzakelijk. Om deze reden is artikel 5 in de regeling opgenomen.

De complexiteit van het beveiligingsvraagstuk zal nog toenemen naarmate de technologie meer mogelijkheden biedt tot directe communicatie op elk gewenst moment en elke gewenste plaats. In de praktijk zal van deze mogelijkheden gebruik worden gemaakt. Het is daarom noodzakelijk voor de politie aandacht te besteden aan de beveiliging van de informatievoorziening en om de informatiebeveiliging aan te pakken op een gemeenschappelijke basis.

Ontwikkelingen

In dit verband kan worden vermeld dat begin 1995 in opdracht van het eerdergenoemde BPI het Handboek aanpak informatiebeveiliging politie en het daarbij behorende boek Hulpmiddelen zijn ontwikkeld. Deze stukken zijn inmiddels formeel geaccordeerd door de deelnemers aan het PPI, waarin vertegenwoordigers van de korpsbeheerders, korpschefs en hoofdofficieren van justitie zitting hebben.

In het Handboek aanpak informatiebeveiliging politie is aansluiting gezocht bij het Besluit voorschrift informatiebeveiliging rijksdienst 1994 (VIR) dat met ingang van 1 januari 1995 voor de rijksdienst geldt. Het VIR bevat een methode om te komen tot een systematische aanpak van informatiebeveiliging. Deze komt er voor de politie in het kort op neer dat het informatiebeveiligingsbeleid door de korpsbeheerder dan wel de Minister van Justitie wordt vastgelegd in een beleidsdocument. Hierin zijn onder meer opgenomen de gemeenschappelijke betrouwbaarheidseisen en maatregelen die voor het korps van toepassing zijn (het zgn. basisbeveiligingsniveau). Vervolgens wordt door het lijnmanagement een afhankelijkheids- en kwetsbaarheidsanalyse toegepast per informatiesysteem en per gemeenschappelijke IT-dienst: op basis daarvan worden beveiligingsmaatregelen vastgesteld die worden vastgelegd in beveiligingsplannen. Vervolgens worden deze maatregelen geïmplementeerd, gecontroleerd, geëvalueerd en zonodig bijgesteld.

Zowel in het VIR als in het eerdergenoemde rapport Beveiligingskader als in het Handboek Informatiebeveiliging rijksdienst wordt benadrukt dat het treffen van beveiligingsmaatregelen geen eenmalige zaak is maar dat hierbij sprake is van een iteratief proces.

Gezien de complexiteit van het informatiebeveiligingsbeleid binnen de rijksdienst is een termijn van twee jaar uitgetrokken voor de implementatie van het VIR.

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.

Inmiddels zal – parallel aan de oprichting van het ACIB – ten behoeve van de Nederlandse politie het Expertisecentrum Informatiebeveiliging Nederlandse Politie als steunpunt voor de politie worden ingericht. Daar waar het ACIB overheidsbreed werkt, heeft het expertisecentrum een functie specifiek ten behoeve van de sector politie. Voornoemd expertisecentrum 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.

De doelstellingen van het Expertisecentrum Informatiebeveiliging Nederlandse Politie zijn:

1. het vergroten van het bewustzijn van de noodzaak van informatiebeveiliging bij het management van de politiekorpsen.
2. het vergroten van de kennis, kunde en vaardigheden voor de aanpak van informatiebeveiliging bij het management en de ambtenaren die in de politiekorpsen zijn belast met de verantwoordelijkheid voor de uitvoering van of de advisering over informatiebeveiliging.
3. het stimuleren van de aanpak van informatiebeveiliging in de afzonderlijke politiekorpsen.
4. het stimuleren van een gezamenlijke

aanpak van de beveiliging van de informatievoorziening in de politiesector:
. strategisch, wat betreft gezamenlijke doelen, uitgangspunten en kaders.
. taktisch, wat betreft de in te zetten middelen en
. operationeel, wat betreft de aanpak van informatiebeveiliging in de politiekorpsen.

Juridisch kader
Eén van de aspecten die vallen onder het begrip 'beheer' dat op diverse plaatsen voorkomt in de Politiewet 1993, is de politiële informatiebeveiliging. Uitgaande van de toedeling van verantwoordelijkheden en bevoegdheden in deze wet, valt het beheer van de politiële informatiesystemen en daarmee ook de zorg voor de beveiliging van deze informatiesystemen en de informatie die daarin is opgeslagen, onder de verantwoordelijkheid van de korpsbeheerder (zie artikel 24 van de Politiewet 1993) respectievelijk de Minister van Justitie (zie artikel 38, derde lid, van de Politiewet 1993).

Andere wetgeving legt de beheerder in deze een zorgplicht op: op grond van artikel 7, tweede lid, juncto artikel 1, onderdeel f, sub 1 en 2 van de Wet politieregisters en op grond van artikel 8 juncto 1 van de Wet persoonsregistraties is de beheerder dan wel de houder (in praktijk de korpsbeheerder dan wel de Minister van Justitie) verplicht te zorgen voor de nodige voorzieningen van technische en organisatorische aard ter beveiliging van een persoonsregistratie tegen verlies of aantasting van gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking daarvan.

Overigens valt het Korps landelijke politiediensten ingevolge artikel 2 van het VIR onder de werking van dat besluit en is de Minister van Justitie gehouden te zorgen voor de beveiliging van de informatiesystemen die zich bij het Korps landelijke politiediensten bevinden en de informatie die daarin is opgeslagen.

Het voornemen van de Minister van Justitie om per 1 januari 1998 de agentschapsstatus te verlenen aan het Korps landelijke politiediensten, doet daaraan niet af.

Deze regeling verhoudt zich tot het VIR als een lex specialis ten opzichte van een lex generalis. Om deze reden en omdat het Korps landelijke politiediensten onderdeel uitmaakt van de Nederlandse politie, is de Regeling informatiebeveiliging politie van toepassing op het Korps landelijke politiediensten. Hierbij plaatsen wij de kanttekening dat deze regeling slechts op enkele punten verschilt van het VIR.

In de IT (informatietechnologie)-organisatie, thans operationeel als zesde divisie van het Korps landelijke politiediensten, zijn taken ondergebracht gericht op de informatie- en telecommunicatietechnologie bij de politie. Dit onderdeel dat onder meer is belast met het technisch beheer van het politiedatacommunicatiesysteem (PODACS) en de zogenaamde landelijke systemen (het Opsporingssysteem (OPS), het Nationaal Schengen Informatiesysteem (NSIS) en het Herkenningsdienstsysteem (HKS)/de Centrale Verwijzings index (CVI)) zal naar verwachting in de loop van het volgend jaar de status krijgen van zelfstandig bestuursorgaan en daarmee van het Korps landelijke politiediensten worden afgesplitst.

De informatiebeveiliging van de bovenregionale systemen zal dan geregeld worden op grond van de Wet Instituut informatie- en communicatietechnologie politie. De Regeling informatiebeveiliging politie zal van overeenkomstige toepassing worden verklaard op het Instituut informatie- en communicatietechnologie politie.

Uitgangspunten van deze regeling
Het Handboek aanpak informatiebeveiling politie en het VIR zijn de uitgangspunten van deze regeling. Met name van het VIR is deze regeling een afspiegeling. Waar mogelijk is aansluiting gezocht bij de methodiek van het VIR waarmee in het meergenoemde handboek rekening is gehouden. De in het VIR gehanteerde methodiek, de kernbegrippen van het VIR en de daarbij behorende toelichting zijn bij de politiekorpsen bekend. Het VIR is gepubliceerd in de Nederlandse Staatscourant (Stcrt. 1994, nr. 173) en de toelichting op het VIR is ter inzage gelegd bij de bibliotheek van het Ministerie van Binnenlandse Zaken.

Artikelsgewijs

Artikel 1
De volgorde van diverse definities is anders gekozen dan die van het VIR en wel op grond van de volgende argumenten: een afhankelijkheidsanalyse leidt tot een set betrouwbaarheidseisen, dus ligt het voor de hand eerst te definiëren wat een afhankelijkheidsanalyse en het begrip 'betrouwbaarheid' inhouden. Informatiebeveiliging is geen doel op zich, maar levert een bijdrage aan de kwaliteit van de informatievoorziening binnen een politiekorps en daarmee aan de betrouwbare uitvoering van de werkprocessen. Het begrip 'betrouwbaarheid' is onder te verdelen in drie deelbegrippen, te weten: beschikbaarheid, integriteit en exclusiviteit. Daarna volgt een omschrijving van het begrip 'informatiesysteem'. Voorbeelden van informatiesystemen zijn een bedrijfsprocessensysteem of een recherche-ondersteunend systeem. In plaats van het begrip 'verantwoordelijkheidsgebied' is in de regeling het begrip 'gemeenschappelijke IT-dienst' opgenomen omdat uit de inmiddels met het VIR opgedane ervaringen is gebleken dat met het begrip 'verantwoordelijkheidsgebied' in praktijk het begrip 'gemeenschappelijke IT-dienst' werd bedoeld. Gemeenschappelijke IT-diensten worden onderscheiden van informatiesystemen vanwege hun andersoortig karakter en omdat de verantwoordelijkheid voor deze diensten anders ligt dan bij de verantwoordelijkheid voor de beveiliging van informatiesystemen. Een voorbeeld van een gemeenschappelijke IT-dienst is een datacommunicatienetwerk binnen een regio waarvan onder meer het genoemde bedrijfsprocessensysteem en het recherche-informatiesysteem gebruik maken. De leidinggevenden die verantwoordelijk zijn voor het bedrijfsprocessensysteem of het recherche-ondersteunende systeem kunnen niet verantwoordelijk worden gehouden voor het realiseren van het gewenste niveau van beveiliging van het datacommunicatiesysteem. In de regeling is bepaald dat voor het beveiligingsniveau van de gemeenschappelijke IT-dienst verantwoordelijk is de organisatorische eenheid aan welke die verantwoordelijkheid eenduidig is toe te wijzen: in het gegeven voorbeeld de beheerder van het datacommunicatienetwerk. De eerdergenoemde leidinggevenden zijn wel degelijk verantwoordelijk voor het stellen van betrouwbaarheidseisen aan de IT-dienst.

Op basis van een kwetsbaarheidsanalyse worden maatregelen vastgesteld die worden vastgelegd in een informatiebeveiligingsplan. Onderdeel

van een dergelijk informatiebeveiligingsplan is een calamiteitenparagraaf.

Artikel 2
Binnen het proces van informatievoorziening kunnen zowel geautomatiseerde als niet geautomatiseerde informatiesystemen voorkomen. In veel systemen komen verschillende technologieën en informatiedragers naast elkaar voor, die tijdens de levenscyclus ook nog kunnen veranderen. De regeling is zodanig opgezet dat het daar onafhankelijk van is. Uiteraard wordt de keuze voor bepaalde maatregelen wel beïnvloed door de toegepaste technologie en door de vorm waarin de informatie wordt vastgelegd en gepresenteerd.

Eén van de aanleidingen tot deze regeling vormt het gegeven dat zowel voor de verwerking van gegevens als het transport daarvan steeds frequenter van elektronische media gebruik wordt gemaakt waarbij de menselijke factor geringer wordt en daarmee gebruikelijke controlemechanismen op bijvoorbeeld de juistheid en verwerking aangevuld dienen te worden met technische en procedurele maatregelen die de betrouwbaarheid verhogen. Omdat het traject van informatievoorziening waarbij gebruik wordt gemaakt van elektronische media veelal niet afdoende is af te scheiden van het traject waarbij conventionele media worden gebruikt, is de regeling van toepassing op het gehele proces van informatievoorziening.

In het juridisch kader is al tot uitdrukking gekomen dat de primaire verantwoordelijkheid voor de informatiebeveiliging een zaak is van de korpsbeheerder dan wel de Minister van Justitie. Deze kan zich door diverse leidinggevenden binnen zijn korps laten bijstaan (zie de toelichting op artikel 3, onderdeel b, de organisatie van de beveiligingsfunctie).

In het eerder genoemde rapport 'Beveiligingskader' wordt op pagina 15/16 opgemerkt; 'De politie is een belangrijke afnemer van informatie van derden, die noodzakelijk is om het politiewerk te ondersteunen (onder andere van de GBA, de RDW). Door de toeleverancier van de informatie kunnen eisen worden gesteld aan de bescherming van de toegeleverde informatie. Andersom is de politie een belangrijke toeleverancier van informatie die aan derden ter beschikking wordt gesteld. Het ligt in de rede aan de afnemer van de informatie beveiligingsmaatregelen te vragen die minimaal overeenkomen met het beveiligingsniveau dat de politie zelf heeft gedefinieerd'.

Het derde lid strekt ertoe dat politiekorpsen in hun onderlinge gegevensuitwisseling vastleggen welke afspraken zijn gemaakt over de zekerstelling van de betrouwbaarheid van uitgewisselde gegevens.

In de bij deze regeling gevoegde bijlage zijn diverse elementen van drie deelbegrippen van het begrip 'betrouwbaarheid' te weten beschikbaarheid, integriteit en exclusiviteit vermeld. Deze elementen, vermeld in de linkerkolom, worden aangeduid als criteria. In verband met een zorgvuldige gegevensuitwisseling is het van cruciaal belang dat de politie gebruik maakt van deze criteria en de bijbehorende normklassen, genoemd in de bijlage.

De waarden 'laag, gemiddeld, hoog, zeer hoog' rechtsboven worden aangeduid als 'normklassen'.

De in de matrix ingevulde normen zijn vermeld bij wijze van voorbeeld. Zo is voor het begrip 'beschikbaarheid' voor het criterium 'beschikbaarheidsperiode' in de normklasse laag of gemiddeld de norm 'kantoortijd' en is de norm in de normklasse hoog of zeer hoog: '7x24 uur'. Het is de bedoeling dat de in de matrix in te vullen normen door overleg binnen de diverse politiekorpsen worden vastgesteld.

Voor zover sprake is van uitwisseling van gegevens met andere politiekorpsen, worden de normen in overleg vastgesteld. Het spreekt voor zich dat bij de uitwisseling van gegevens tussen politiekorpsen onderling de bepalingen inzake het verstrekken van gegevens uit de privacywetgeving (Wet politieregisters, Wet persoonsregistraties en de op beide genoemde wetten genoemde uitvoeringsbepalingen) alsmede hetgeen bepaald wordt op grond van artikel 2 van het Besluit beheer regionale politiekorpsen in acht worden genomen.

Aangezien de competentie van de Ministers van Binnenlandse Zaken en Justitie niet verder reikt dan de korpsbeheerders respectievelijk de beheerder van het Korps landelijke politiediensten, kunnen geen normen op basis van de criteria en bijbehorende normklassen, bedoeld in de bijlage behorende bij deze regeling, aan derden waarmee de politie gegevens uitwisselt, worden opgelegd. In dit verband merken wij op dat het aanbeveling verdient dat ingeval van gegevensuitwisseling tussen politiekorpsen en derden op basis van de in de bijlage vermelde criteria en normklassen tot normering wordt gekomen.

Ook hier geldt dat de korpsbeheerders en de Minister van Justitie gebonden zijn aan de privacywetgeving en aan hetgeen wordt bepaald op grond van artikel 2 van het Besluit beheer regionale politiekorpsen.

Artikel 3
Informatiebeveiligingsbeleid staat niet op zich maar dient te worden afgestemd op de hieraan gerelateerde beleidsterreinen. Informatiebeveiliging kan worden beschouwd als een onderdeel van de kwaliteitszorg voor de informatievoorziening. Informatiebeveiliging vertoont een zekere overlap met de beveiliging van gebouwen en terreinen. Gegevens worden verwerkt met behulp van apparatuur die is opgesteld in een bepaalde locatie. De fysieke toegang tot deze apparatuur is veelal mede afhankelijk van de algemene toegangsbeveiligingsmaatregelen die voor die locatie zijn getroffen. Bovendien worden fysieke sleutels en sloten vervangen door geautomatiseerde toegangsbeheers- of geïntegreerde gebouwbeheerssystemen. Ook kan de beveiliging van personen afhankelijk zijn van de beveiliging van over hen in geautomatiseerde systemen opgeslagen gegevens. Daar waar gegevens over geld of goederen zijn opgeslagen in geautomatiseerde systemen, vertoont informatiebeveiliging raakvlakken met de beveiliging van deze activa. Alle beveiligingsvraagstukken dienen derhalve te worden gebaseerd op dezelfde beleidsuitgangspunten.

Het informatiebeveiligingsbeleid vertoont ook overlap met personeels (voorzienings) beleid en met het thema integriteit bij de politie. Aspecten die daarbij een belangrijke rol spelen, zijn het bevorderen van het beveiligingsbewustzijn en de procedures bij aanstelling van personeel op uit beveiligingsoogpunt kritische functies.

Voorts kan informatiebeveiliging afstemming noodzakelijk maken met de zorg voor arbeidsomstandigheden en de zorg voor het milieu, zowel op

het gebied van de toegepaste managementinstrumenten als inhoudelijk. Voorbeelden van overeenkomstige managementinstrumenten zijn beleidsdocumenten, procedures, plannen, opleidingen, bewustwordingsprogramma's en controles. Voorbeelden van inhoudelijke raakvlakken zijn toegangbeperkende maatregelen die onder bepaalde omstandigheden in strijd kunnen zijn met de (arbeids)veiligheid, klimaatbeheersingsmaatregelen voor computers die schadelijk kunnen zijn voor het milieu en geautomatiseerde productieprocessen en milieuzorgsystemen waarvan de kwaliteit afhankelijk is van de beschikbaarheid, integriteit en de exclusiviteit van de informatie en de informatievoorziening.

De vraag in welk beleidsdocument het informatiebeveiligingsbeleid moet worden vastgelegd, is in feite niet relevant. Het meest belangrijke is dat het informatiebeveiligingsbeleid wordt vastgelegd en bekrachtigd en uitgedragen door de korpsbeheerder dan wel de Minister van Justitie. De communicatie over informatiebeveiliging kan echter worden bevorderd door de beleidsuitgangspunten op te nemen in een afzonderlijk beleidsdocument.

Onderdeel b

Met de term 'informatiebeveiligingsfunctie' wordt bedoeld het geheel van voorwaarden in organisatorische zin dat binnen een politiekorps geregeld moet zijn om taken en verantwoordelijkheden op het gebied van informatiebeveiliging te kunnen invullen. Uitgangspunten voor de invulling van de informatiebeveiligingsfunctie zijn:

– informatiebeveiliging is de eindverantwoordelijkheid van de korpsbeheerder respectievelijk de Minister van Justitie. Deze zal leidinggevenden aanwijzen die verantwoordelijk zijn voor delen van de informatiebeveiliging van het complex van de korpsinformatiestructuur.
– informatiebeveiliging dient ingeweven te zijn in de bedrijfsprocessen;
– informatiebeveiliging is met name een kwestie van bewustwording;
– informatiebeveiliging vraagt nu om een inhaalslag met extra aandacht: gezien het vorige uitgangspunt zal deze extra aandacht tijdelijk kunnen zijn;
– informatiebeveiliging is een proces dat constante evaluatie en herziening vraagt;
– informatiebeveiliging raakt de totaliteit van de bedrijfsvoering van een korps.

De informatiebeveiligingsambtenaar zit dus niet in de eerste plaats in de I&A-hoek, maar benadert de problematiek vanuit de totaliteit van het functioneren van een politiekorps.

In deze zou aansluiting gezocht kunnen worden bij de structuur die door het eerder genoemde ACIB voor de rijksoverheid is ontwikkeld. Dit zou dan op korpsniveau betekenen dat de korpsbeheerder dan wel de Minister van Justitie formeel verantwoordelijk is voor het informatiebeveiligingsbeleid. Deze benoemt vervolgens een lid van de korpsleiding tot portefeuillehouder van het onderwerp informatiebeveiliging (bij de meeste departementen is dit een plv. SG of een directeur-generaal). Deze functionaris houdt zich op strategisch beleidsniveau inhoudelijk bezig met het onderwerp en communiceert daarover met zijn collega's van andere politiekorpsen.

Vervolgens is het raadzaam binnen de eigen organisatie een intern informatiebeveiligingsoverleg (IB-overleg) te creëren. In dit korpsbrede IB-overleg kunnen de volgende punten aan de orde worden gesteld:

– herziening van het informatiebeveiligingsbeleid en de toegekende verantwoordelijkheden;
– toezicht op de belangrijkste bedreigingen waaraan de informatie is blootgesteld;
– bespreking van en toezicht op beveiligingsincidenten;
– bespreken van initiatieven ter verbetering van de informatiebeveiliging;
– coördinatie van de implementatie voor nieuwe systemen of diensten.

Onder voorzitterschap van de portefeuillehouder zouden aan het IB-overleg onder meer de volgende functionarissen kunnen deelnemen: de chefs van de afdelingen personeel, facilitaire zaken en financiën. Secretaris van dit interne korpsoverleg zou een (de) informatiebeveiligingsfunctionaris kunnen zijn. De informatiebeveiligingsfunctionaris is deskundig op het gebied van IB en moet ook in staat zijn om als adviseur kennis over te dragen aan de korpsbeheerder dan wel de Minister van Justitie en diens leidinggevenden.

Onderdeel c

In afwijking van de terminologie van het VIR wordt in deze regeling gesproken van 'leidinggevenden' en niet van 'lijnmanagers' omdat dit recht doet aan de feitelijke situatie van een politie-organisatie. In een politiekorps wordt een chef I&A wel beschouwd als leidinggevende, maar niet als lijnmanager.

Onderdeel e

Teneinde het proces van het kiezen van maatregelen sterk te vereenvoudigen, kan een politiekorps ertoe overgaan voor één of meer informatiesystemen of gemeenschappelijke IT-diensten een basisbeveiligingsniveau te definiëren. Onder een basisbeveiligingsniveau wordt verstaan een stelsel van maatregelen dat als minimum wordt gehanteerd, soms ook wel het standaardbeveiligingsniveau of standaardbeveiligingsstelsel genoemd. In aanvulling op een basisbeveiligingsniveau kunnen voor sommige informatiesystemen of gemeenschappelijke IT-diensten aanvullende eisen/maatregelen geformuleerd worden. Om binnen de politie te komen tot uniformiteit, wordt voor het vaststellen van het basisbeveiligingsniveau het gebruik van de criteria en normklassen, bedoeld in de bijlage bij deze regeling, alsmede samenwerking tussen de korpsen voorgeschreven (zie wat dit laatste betreft artikel 5).

Het hanteren van een basisbeveiligingsniveau voor één of meer informatiesystemen of gemeenschappelijke IT-diensten is veelal een praktische aanpak van informatiebeveiliging en voorkomt dat door verschillende leidinggevenden dezelfde afwegingen moeten worden gemaakt bij het kiezen van de maatregelen. Het hanteren van een basisbeveiligingsniveau is aan te bevelen in de beginfase van informatiebeveiliging, omdat dan snel tot een behoorlijk niveau van beveiliging kan worden gekomen. In het bijzonder daar waar de homogeniteit van ondersteunende informatiesystemen in termen van beschikbaarheid, integriteit en exclusiviteit relatief groot is, kan verwacht worden dat een basisbeveiligingsniveau zijn nut zal hebben.

Wel dient onderkend te worden dat een basisbeveiligingsniveau frequenter aan verandering onderhevig zal zijn dan stelsels van maatregelen die op individuele informatiesystemen of gemeenschappelijke IT-diensten zijn

toegesneden omdat de vaak generieke maatregelen die ze bevatten toereikend dienen te blijven bij de introductie van nieuwe technologieën in slechts één of enkele van de informatiesystemen of gemeenschappelijke IT-diensten waarvoor de basisbeveiliging geldt.

Onderdeel f
Het uitgangspunt bij het melden van incidenten is dat elk incident gemeld moet worden bij de door de korpsbeheerder of de Minister van Justitie daarvoor aangewezen informatiebeveiligingsfunctionaris. Desgewenst kan hij incidenten melden aan een landelijk in te richten meldingsfaciliteit.

Onderdeel g
De evaluatie van het beleid en de beoordeling van implementatie en uitvoering ervan, hebben betrekking op de organisatie van de beveiligingsfunctie binnen het politiekorps, op alle informatiesystemen en op alle gemeenschappelijke IT-diensten. Door het opstellen van een schema kan zowel de volledigheid van het onderzoek naar de uitvoering van het beleid en de gemeenschappelijke eisen en maatregelen worden bewerkstelligd alsook differentiatie worden aangebracht in de frequentie waarmee bepaalde onderdelen worden onderzocht. Van het onderzoek wordt verslag uitgebracht aan de korpsbeheerder of de Minister van Justitie. De rol van de onafhankelijk deskundige kan naar keuze van het politiekorps – zowel volgens het VIR (zie pagina 38) als het rapport Beveiligingskader (zie pagina 7, punt 4) – vervuld worden door een accountant. Ook zou deze rol door een andere externe deskundige (een EDP-auditor) vervuld kunnen worden.

Onderdeel h
Beveiliging heeft, zoals eerder opgemerkt, raakvlakken met het thema integriteit bij de politie en impliceert gedragsregulering voor medewerkers en vergt discipline. Het is derhalve belangrijk dat beveiliging op natuurlijke wijze is ingebed in de normale gang van zaken en niet als iets aparts wordt ervaren. Het veranderen van de mentaliteit van medewerkers kan slechts geleidelijk gerealiseerd worden. Periodieke voorlichting (bijvoorbeeld via folders, brochures, posters, jaarverslagen, het personeelshandboek of de E-mail) is een manier waarmee een blijvend effect bewerkstelligd kan worden. Een meer blijvend effect kan echter gesorteerd worden door het aspect 'beveiliging' te integreren in het stelsel van functioneringsgesprekken en beoordelingen.

Artikel 4
Op grond van dit artikel wordt de informatiebeveiliging nader gepreciseerd en meer toegesneden op individuele informatiesystemen en gemeenschappelijke IT-diensten.

Informatiebeveiligingsmaatregelen moeten niet alleen vanuit een technische benadering worden getroffen maar vanuit diverse optieken. Zo valt bijvoorbeeld te denken aan:
1. fysieke maatregelen (toegangscontrole voor gebouwen, ruimten en installaties, omgevingsbescherming en -beheersing zoals onder andere klimaatregeling, brandbestrijdingsmiddelen en noodstroomvoorziening).
2. organisatorische en personele middelen (o.a. screening van personeel, functiescheiding, beperking van de tijdsduur voor het bekleden van bepaalde functies, registratie van inbreuken, het uitdragen van het informatiebeveiligingsbeleid door het korpsmanagement).
3. maatregelen in apparatuur en programmatuur (bijvoorbeeld het gebruik van regelmatig te wijzigen passwords, het werken met een bevoegdhedenmatrix, het registreren van aangebrachte wijzigingen en van pogingen tot ongeautoriseerde toegang en encryptie bij datacommunicatie).
4. juridische maatregelen (bijvoorbeeld contracten).

In het rapport Beveiligingskader worden als uitgangspunten voor het opstellen van beveiligingsplannen genoemd:
a. de bescherming van informatieverzamelingen bij de Nederlandse politie dient laagsgewijs te zijn opgebouwd. Dit houdt in dat er sprake is van een basisbeveiligingsniveau dat zonodig door middel van clusterbeveiliging op een hoger plan kan worden gebracht. Voor informatiesystemen die boven het basisniveau en de clusterbeveiliging extra beveiliging behoeven, kunnen specifieke beveiligingsmaatregelen worden getroffen.
b. Basis van de beveiliging vormen de primaire maatregelen die minimaal noodzakelijk zijn om gevoelige gegevens te beschermen.
De opbouw van de beveiliging voor meer gevoelige gegevensbestanden dient gradueel voort te bouwen op deze basisbeveiliging.

Bij het vaststellen van informatiebeveiligingsplannen dient gebruik gemaakt te worden van de criteria en de normklassen, bedoeld in de bijgevoegde bijlage, opdat communicatie tussen politiekorpsen over het niveau van beveiliging mogelijk is.

Artikel 5
Zoveel mogelijk uniformiteit op het gebied van afspraken inzake de zekerstelling van de betrouwbaarheid bij gegevensuitwisseling, basisbeveiligingsniveau en informatiebeveiligingsplannen is de gewenste eindsituatie.

Om deze te bereiken, is het noodzakelijk dat de politiekorpsen op de genoemde gebieden gaan samenwerken. Een hulpmiddel hierbij is de bijlage bij deze regeling. Door middel daarvan is het gebruik maken van de aangegeven criteria en normklassen verplicht. In hun onderlinge contacten zullen politiekorpsen in onderling overleg de normen vaststellen die bij wijze van voorbeeld in de bijgevoegde matrices zijn opgenomen. Het ligt bij deze samenwerking voor de hand dat gebruik wordt gemaakt van de bestaande overlegstructuren zoals bijvoorbeeld het Korpsbeheerdersberaad.

Artikel 6
Dit artikel heeft tot doel een aantal ijkpunten te omschrijven waarmee de werking van maatregelen tijdens het gebruik van een informatiesysteem of een gemeenschappelijke IT-dienst door de verantwoordelijke korpsbeheerder dan wel de Minister van Justitie en diens leidinggevenden bewerkstelligd en beheerst wordt. De laatstgenoemden moeten in staat zijn om het aspect beveiliging van informatievoorziening op een vanzelfsprekende wijze te integreren in het geheel van hun managementtaken. Daarbij is sprake van drie aandachtsgebieden:
1. de aansturing van de medewerkers die het informatiesysteem gebruiken.
2. de zorg voor het betrouwbaar (laten) exploiteren van het informatiesysteem.
3. de zorg voor het betrouwbaar (laten) verwerven van (componenten van) het informatiesysteem.
Het fundament voor het vastleggen,

uitdragen en controle van maatregelen wordt gevormd door het informatiebeveiligingsplan voor het informatiesysteem. Dit bevat minimaal een uitputtende opsomming van de vindplaatsen waar de maatregelen beschreven staan (zie artikel 4, onderdeel e). Het opstellen van het informatiebeveiligingsplan vormt de laatste stap in het methodologische proces om tot de keuze van een evenwichtig pakket van maatregelen voor de beveiliging te komen.

Artikel 7

Uit de ervaringen die tot op heden met het VIR zijn opgedaan, blijkt dat de termijn van twee jaar die voor de implementatie van het VIR is uitgetrokken, niet royaal is. Naar verwachting zal het nog enkele jaren na de inwerkingtreding van dit besluit duren voordat de politiële informatiebeveiliging op een bevredigend niveau is gerealiseerd. Wij zijn echter wel van mening dat eind 1998 in ieder politiekorps tenminste een basisbeveiligingsniveau moet zijn gerealiseerd.

De Minister van Binnenlandse Zaken,
H.F. Dijkstal.
De Minister van Justitie,
W. Sorgdrager.

Bijlage

Betrouwbaarheidscriteria en -normklassen

Inleiding

Artikel 2 van de regeling bepaalt dat bij gegevensuitwisseling tussen politiekorpsen onderling (lid 3) en met andere instanties (lid 4) schriftelijke afspraken gemaakt worden over de betrouwbaarheid van de informatiesystemen en de informatie daarin. Vanzelfsprekend kunnen (en dienen) dergelijke afspraken, al dan niet schriftelijk, ook gemaakt te worden bij gegevensuitwisseling binnen een politiekorps.

Deze betrouwbaarheidsafspraken kunnen op drie niveaus worden gemaakt:
– op het niveau van gevoeligheid, waarbij de afspraken betrekking hebben op de consequenties voor bedrijfsprocessen die van de informatie c.q. het informatiesysteem gebruik maken en voor de belangen van personen en instanties waarover gegevens worden uitgewisseld als er verstoring optreedt van de betrouwbaarheid van de informatie en de informatiesystemen;
– op het niveau van eisen, waarbij de afspraken betrekking hebben op de mate van betrouwbaarheid van de informatie en de informatiesystemen;
– op het niveau van maatregelen, waarbij de afspraken betrekking hebben op de realisatie van de betrouwbaarheid van de informatie en de informatiesystemen.

Duidelijk zal zijn dat afspraken op het niveau van gevoeligheid voor de partijen in uitwisseling weinig houvast biedt bij het invullen van de beveiliging (zekerstellen van de betrouwbaarheid) van de informatie en de informatiesystemen, terwijl afspraken op het niveau van maatregelen veel omvattend en complex zullen zijn en de geldigheidsduur van de afspraken ook beperkt zal zijn als gevolg van technologische en organisatorische ontwikkelingen. Afspraken over betrouwbaarheid van informatie en informatiesystemen moeten daarom gemaakt worden op het niveau van eisen. Bovendien is het zaak de eisen kwantitatief te formuleren, ten einde de afspraken meetbaar te maken.

In deze bijlage worden de criteria en -normklassen omschreven die door politiekorpsen dienen te worden gehanteerd bij het formuleren van eisen inzake de betrouwbaarheid van informatie en informatiesystemen.

Betrouwbaarheidscriteria

Beschikbaarheid wordt omschreven als: de mate waarin een informatiesysteem in bedrijf is op het moment dat een politiekorps het nodig heeft. Voor het formuleren van beschikbaarheidseisen zijn er de volgende criteria.
– Beschikbaarheidsperiode: de tijd dat de informatie en het informatiesysteem nodig is. De beschikbaarheidsperiode wordt uitgedrukt in tijdseenheden, bijvoorbeeld kantoortijd, 7x24 uur, etc.
– Bedrijfszekerheid: de mate waarin de gegevensverwerking vrij blijft van storingen of, anders gezegd, de gemiddelde tijd tussen het optreden van beschikbaarheidsstoringen. De bedrijfszekerheid wordt uitgedrukt in uren, bijvoorbeeld: 1 beschikbaarheidsstoring per 200 uur is acceptabel.
– Herstelbaarheid: de snelheid waarmee de gegevensverwerking hersteld kan worden na een storing. Daarbij kan onderscheid gemaakt worden in:
. de gemiddelde duur van een beschikbaarheidsstoring en
. de maximaal toegestane duur van een beschikbaarheidsstoring,
beide uitgedrukt in uren.
Beschikbaarheid wordt hier gespecificeerd in tijdafhankelijke criteria (het moment dat een politiekorps het informatiesysteem nodig heeft), niet in locatieafhankelijke criteria (de plaats waar het informatiesysteem nodig is). Indien ook locatieafhankelijke beschikbaarheidseisen moeten worden gesteld, dan kunnen de hierboven genoemde criteria nader worden gespecificeerd per werkplek, afdeling of gebouw of organisatie.

Integriteit wordt omschreven als: de mate waarin een informatiesysteem zonder fouten is. 'Zonder fouten' wil zeggen dat de informatieverwerking plaatsvindt volgens vooraf vastgestelde specificaties. De randvoorwaarde voor het maken van afspraken over de integriteit van informatiesystemen en de informatie daarin is dus de aanwezigheid van specificaties van de verwerking, zowel de geautomatiseerde als de handmatige. Voor het formuleren van integriteitseisen zijn er de volgende criteria.
– Juistheid: het percentage van de gegevensverzameling dat door het informatiesysteem juist, conform specificaties, wordt verwerkt. Bijvoorbeeld: 95% van de gegevens wordt juist verwerkt.
– Volledigheid: het percentage van de gegevensverzameling dat door het informatiesysteem volledig (zonder manco's) en enkelvoudig (zonder doublures) wordt verwerkt.
– Tijdigheid: het percentage van de gegevensverzameling dat door het informatiesysteem binnen de gespecificeerde termijn wordt verwerkt.
– Hersteltijd: het aantal uren na constatering van niet-integer verwerkte gegevens waarbinnen herstel dient plaatsgevonden te hebben.

In die gevallen waarin de vereiste juistheid, volledigheid en/of tijdigheid nagenoeg 100% moet zijn, is het soms praktischer de eisen te formuleren in faalkansen, bijvoorbeeld: 1 onjuist verwerkte transaktie per 1000 transakties is acceptabel.

Exclusiviteit wordt omschreven als: de mate waarin de toegang tot en kennisname van een informatiesysteem en de informatie daarin beperkt is tot een gedefinieerde groep van gerechtigden. Voor het formuleren

van eisen inzake exclusiviteit kunnen de volgende criteria van dienst zijn.
– Autorisatie: de aanduiding van de groep van personen die voor toegang tot en kennisname van een informatiesysteem en de informatie daarin gerechtigd is. Hoewel autorisatie feitelijk een specificatie is van exclusiviteit en niet van zekerstelling van exclusiviteit, wordt ervan uitgegaan dat naarmate de groep van geautoriseerde personen nauwkeuriger omschreven wordt de noodzakelijke zekerstelling van de exclusiviteit hoger wordt.
– Geoorloofdheid: de mate van zekerheid dat toegang tot en kennisname van een informatiesysteem en van de informatie daarin uitsluitend voor personen die daartoe gerechtigd zijn mogelijk is. Geoorloofdheid wordt uitgedrukt in het percentage van de feitelijke gebruik van het informatiesysteem. Bijvoorbeeld: 99% van het feitelijk gebruik van het systeem is geoorloofd gebruik. In die gevallen waarin de vereiste geoorloofdheid nagenoeg 100% moet zijn is het vaak praktischer de eis te formuleren in faalkansen, bijvoorbeeld: 1 ongeoorloofde toegang per 1000 toegangen is acceptabel.
– Braakbestendigheid: de tijd dat het kost om ongeoorloofd toegang tot een informatiesysteem te verkrijgen, uitgedrukt in uren.

Normklassen
Als voor elk informatiesysteem specifieke betrouwbaarheidsnormen worden geformuleerd, dan ontstaat een complex normenstelsel. Wat te doen als het ene systeem een bedrijfszekerheidsnorm stelt van 1 storing per 200 uur, het volgende systeem een norm stelt van 1 storing per 240 uur en het derde weer een norm stelt van 1 storing per 300 uur? Voor het maken van afspraken zal het op den duur handiger blijken om normklassen te hanteren. In deze regeling worden vier normklassen onderscheiden: 'laag', 'gemiddeld', 'hoog' en 'zeer hoog'.

Het is de bedoeling dat de normklassen worden ingevuld door overleg tussen de politiekorpsen. Hieronder volgt een voorbeeld van een mogelijke invulling van normklassen voor de onderscheiden betrouwbaarheidscriteria.

Normklasse à Criterium	Laag	Gemiddeld	Hoog	Zeer hoog
Beschikbaarheid				
Beschikbaarheids-periode	Kantoortijd	Kantoortijd	7x24 uur	7x24 uur
Bedrijfszekerheid	200 uur	400 uur	1500 uur	6000 uur
Herstelbaarheid	8 uur	4 uur	2 uur	1 uur
Integriteit				
Juistheid	< 90%	90-95%	95-99,9%	>99,9%
Volledigheid	< 90%	90-95%	95-99,9%	>99,9%
Tijdigheid	< 90%	90-95%	95-99,9%	>99,9%
Hersteltijd	> 24 uur	24-8 uur	8-1 uur	< 1 uur
Exclusiviteit				
Autorisatie	Iedereen in het korps	specifieke afdelingen	specifieke functies	specifieke personen
Geoorloofdheid	90%	99%	99,99%	99,99%
Braakbestendigheid	< 2 uur	2-4 uur	4-12 uur	> 12 uur

Tot slot
De in deze bijlage beschreven verzameling van betrouwbaarheidscriteria is niet volledig en vaststaand. Zoals elke taal is ook de 'informatiebeveiligingstaal' in ontwikkeling. Op basis van ervaringen met het toepassen van de betrouwbaarheidscriteria en van de normklassen zullen aanpassingen en uitbreidingen van de verzameling van criteria en invullingen van de normklassen kunnen worden verwacht.