Besluit voorschrift informatiebeveiliging rijksdienst 2007

20 juni 2007

De Minister-President, Minister van Algemene Zaken,
Handelend in overeenstemming met het gevoelen van de Ministerraad;

Besluit:

Artikel 1. Begripsbepalingen
In dit besluit wordt verstaan onder:
a. Informatiebeveiliging: het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen;
b. Informatiesysteem: een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.

Artikel 2. Plaatsbepaling en reikwijdte
1. Dit voorschrift geldt voor de Rijksdienst waartoe gerekend worden de Ministeries met de daaronder ressorterende diensten, bedrijven en instellingen.
2. Dit voorschrift geldt voor het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.
3. Informatiebeveiliging is een lijnverantwoordelijkheid en vormt een onderdeel van de kwaliteitszorg voor bedrijfs- en bestuursprocessen en de ondersteunende informatiesystemen.

Artikel 3. Informatiebeveiligingsbeleid
De secretaris-generaal van een Ministerie stelt het informatiebeveiligingsbeleid vast, draagt dit uit en legt verantwoording hierover af. Het beleid omvat ten minste:
a. De strategische uitgangspunten en randvoorwaarden die het Ministerie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid;
b. De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden;
c. De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers;
d. De gemeenschappelijke betrouwbaarheidseisen en normen die op het Ministerie van toepassing zijn;
e. De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd;
f. De bevordering van het beveiligingsbewustzijn;

Artikel 4. Verantwoordelijkheden lijnmanagement
Het lijnmanagement is verantwoordelijk voor de beveiliging van zijn informatiesystemen. Het lijnmanagement:
a. Stelt op basis van een expliciete risico afweging de betrouwbaarheidseisen voor zijn informatiesystemen vast;
b. Is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
c. Stelt vast dat de getroffen maatregelen aantoonbaar overeenstemmen met de betrouwbaarheidseisen en dat deze maatregelen worden nageleefd;
d. Evalueert periodiek het geheel van betrouwbaarheidseisen en beveiligingsmaatregelen en stelt deze waar nodig bij.

Artikel 5. Slotbepaling
1. Het Besluit voorschrift informatiebeveiliging rijksdienst 1994 wordt ingetrokken.
2. Dit besluit treedt in werking met ingang van 1 juli 2007.
3. Dit besluit wordt aangehaald als het Besluit voorschrift informatiebeveiliging rijksdienst 2007.

Dit besluit zal met toelichting in de Staatscourant worden geplaatst.

Den Haag, 20 juni 2007.
De Minister-President, Minister van Algemene Zaken,
J.P. Balkenende.

Toelichting

Voorwoord
De Algemene Rekenkamer rapporteerde in het Rechtmatigheidonderzoek 2003 dat zeven van de negen onderzochte Ministeries – deels al jaren – niet voldeden aan het Voorschrift Informatiebeveiliging Rijksdienst 1994 (hierna VIR). De Algemene Rekenkamer drong er daarom bij de Minister van BZK (voluit Binnenlandse Zaken en Koninkrijksrelaties) op aan het toezicht op het VIR te verbeteren of het voorschrift nog eens goed te beoordelen op uitvoerbaarheid en eventueel te herzien.

Het Interdepartementaal Overleg Directeuren Informatievoorziening (IODI) heeft naar aanleiding daarvan een werkgroep bestaande uit vertegenwoordigers van een aantal Ministeries de opdracht gegeven nog eens kritisch naar (de ervaringen met) het VIR te kijken. De opdracht van de werkgroep was als volgt geformuleerd:
1. Onderzoek of de constateringen van de Algemene Rekenkamer binnen de Ministeries breed worden gedeeld.
2. Voer een onderzoek / quick scan uit naar de ervaringen binnen de Ministeries met de uitvoering van het VIR.
3. Doe aanbevelingen voor de verbetering/vereenvoudiging van de uitvoering van het VIR onder het motto ‘meer eenvoud, meer focus’.

De volgende bevindingen van de werkgroep zijn door het pSG beraad vastgesteld:
– De meeste Ministeries waren redelijk tevreden over de wijze waarop intern het VIR wordt uitgevoerd. Dit terwijl de Algemene Rekenkamer constateerde dat zeven van de negen onderzochte Ministeries niet voldoen aan de eisen van het VIR.
– De Ministeries waren ontevreden over de actualiteit en toepasbaarheid van het VIR aangezien enkele onderdelen van het VIR 1994 een vlotte en optimale uitvoering in de weg stonden.
– De Ministeries sloten zich aan bij de aanbeveling van de Algemene Rekenkamer om het voorschrift nog eens goed te beoordelen op uitvoerbaarheid en eventueel te herzien.

Het pSG beraad heeft besloten tot aanpassing van het VIR 1994 Vastgesteld werd dat:
– de verplichting om voor elk informatiesysteem een Afhankelijkheids- & Kwetsbaarheidsanalyse te maken als niet wenselijk wordt beschouwd;
– de samenhang tussen de wet- en regelgeving wat betreft informatiebeveiliging als onvoldoende wordt beoordeeld;
– managers te weinig oog en aandacht hebben voor informatiebeveiliging;
– informatiebeveiliging in veel gevallen onvoldoende is geïntegreerd in de bedrijfsvoering.

Het nieuwe VIR richt zich op het feitelijk aantoonbare niveau van informatiebeveiliging. De grondgedachte is dat informatiebeveiliging op meerdere manieren tot stand kan komen, zolang dit maar middels bewuste keuzes gebeurt. Daarom zijn veel vormvoor-

schriften (A&K analyse, IBP) uit het VIR 1994 verdwenen. In feite hoort informatiebeveiliging iets te zijn wat standaard tussen de oren van managers en medewerkers zit, niet iets waar ze door een voorschrift op gewezen moeten worden. Het Ministerie van BZK zal deze circulaire vijf jaar na invoering evalueren.

Hieronder een opsomming van de belangrijkste veranderingen in het voorliggende VIR.
– Bij het aanpassen van het VIR is gestreefd naar een toekomstvaste regeling.
– De onderlinge afhankelijkheid tussen systemen is een belangrijke risicofactor voor de informatiebeveiliging. Hiervoor wordt in het nieuwe VIR ketenverantwoordelijkheid geïntroduceerd en vervalt het begrip verantwoordelijkheidsgebied.
– Informatiebeveiliging vormt een integraal onderdeel van de bedrijfsvoering en is daarmee een managementverantwoordelijkheid. Daarom wordt de aandacht én verantwoordelijkheid van lijnmanagement en organisatie voor de informatiebeveiliging nog meer benadrukt.
– Het dwingende voorschrift om voor élk informatiesysteem en voor élk verantwoordelijkheidsgebied een afhankelijkheids- en kwetsbaarheidanalyse (A&K analyse) uit te voeren, is zodanig aangepast, dat voor elk systeem op basis van een risico afweging bepaald wordt welke specifieke beveiligingsmaatregelen de organisatie treft. Deze meer pragmatische werkwijze versterkt het VIR en maakt de inzet van middelen voor informatiebeveiliging effectiever en efficiënter. Hierbij wordt het motto 'van onbewust risico's lopen naar bewust risico's nemen' gevolgd.
– Het VIR gaat niet meer uit van één voorgeschreven methodiek, zoals risicoanalyse of A&K analyse. De kern is niet zozeer het hanteren van een methodiek, maar het bewust komen tot betrouwbaarheidseisen en maatregelen. Ministeries kunnen op deze wijze kiezen voor een methode of systematiek die past bij de interne risico afweging methodiek en daarmee dus aansluit op het risicodenken binnen het betreffende Ministerie. Daarmee is er in het VIR geen noodzaak voor het element 'comply or explain'. In feite wordt aan het management een managementverantwoording (in control statement) wat betreft de informatiebeveiliging gevraagd.
– Doordat het VIR integraal onderdeel is van de bedrijfsvoering sluit het aan bij de Planning en Control cyclus.
– Om het VIR te effectueren wordt gebruik gemaakt van de kwaliteitscirkel van Deming (Plan Do Check Act cyclus).
– De artikelen en de toelichting hebben hetzelfde gewicht en geldingskracht.
– Het begrippenkader van de Code van Informatiebeveiliging (ISO17799:2005) is in dit voorschrift overgenomen.

Inleiding
Bestuurs- en bedrijfsprocessen in moderne organisaties zijn in belangrijke mate afhankelijk van goed functionerende informatiesystemen. Veel processen zijn nagenoeg onmogelijk zonder de toepassing van geautomatiseerde gegevensverwerking. Uitval van computers of telecommunicatiesystemen, het in ongerede raken van gegevensbestanden of het door onbevoegden kennisnemen dan wel manipuleren van bepaalde gegevens kan ernstige gevolgen hebben voor de beleids- en bedrijfsvoering. Dit heeft mogelijk negatieve gevolgen voor burger, bedrijf of overheid. Het is niet ondenkbaar dat hieraan ook politieke consequenties verbonden zijn of dat het imago van de overheid in het algemeen en van een Ministerie in het bijzonder wordt geschaad.

De genoemde afhankelijkheid wordt mede beïnvloed door technologische ontwikkelingen op het gebied van de informatievoorziening. Ketens en de koppeling van voorheen losstaande informatiesystemen leiden tot complexe situaties met diffuse verantwoordelijkheden. Enerzijds komen gegevens steeds gemakkelijker beschikbaar, anderzijds zijn gegevensstromen steeds moeilijker beheersbaar. Geautomatiseerde informatievoorziening vindt plaats op alle werkplekken van overheidsorganisaties. Het gebruik van informatievoorzieningen neemt daarbij een veelheid aan verschijningsvormen aan: kantoorautomatisering, e-mail, networking, plaats- en tijdonafhankelijk werken, de integratie van spraak, beeld en conventionele data en soortgelijke trends. De wijze waarop deze geautomatiseerde hulpmiddelen ter beschikking gesteld en geëxploiteerd worden, is aan verandering onderhevig. Veel meer dan voorheen is er sprake van gedecentraliseerde beslissingsbevoegdheden binnen een Ministerie, belangrijke delen van de programmatuur worden kant-en-klaar gekocht in plaats van zelf ontwikkeld en exploitatie/beheer wordt regelmatig uitbesteed. Dit alles verandert de mogelijkheden op controle en toezicht.

Daarnaast streeft de overheid naar meer transparantie en naar een betere dienstverlening door de inzet van geautomatiseerde zelfbediening door de burger.

Informatiebeveiliging is daarbij een absolute randvoorwaarde voor:
– het garanderen van de betrouwbaarheid van de informatie van de Ministeries en hun uitvoeringsorganisaties;
– de samenwerking en gegevensuitwisseling tussen overheden;
– het vertrouwen van de burger in de overheid.

In het nieuwe VIR is gestreefd naar een stelsel van regels dat een hoge mate van toekomstvastheid bezit.

Keuzes
De levenscyclus van informatietechnologieën is divers en steeds vaker kort: een nieuwe technologie kan zijn intrede doen zonder dat daarover nu uitspraken mogelijk zijn en bestaande technologieën kunnen binnen een paar jaar verouderd zijn. Het is daarom niet wenselijk om op het niveau van technische maatregelen regels op te stellen voor informatiebeveiliging.

Datzelfde geldt ook voor de meeste organisatorische maatregelen die in het kader van informatiebeveiliging gesteld zouden kunnen worden. Informatievoorziening neemt een dusdanig belangrijke plaats in bij het functioneren van de overheid dat beveiliging daarvan in integraal verband specifieke aandacht vereist. Voor zover het gaat om de interne informatievoorziening van afzonderlijke Ministeries is dat de verantwoordelijkheid van de Ministeries zelf. Uit dien hoofde is volstaan met globale regels voor wat minimaal Ministeriebreed geregeld dient te worden, op de wijze waarop dat in artikel 3 van dit voorschrift is gebeurd. De afzonderlijke Ministers zijn immers verantwoordelijk voor de beveiliging van de informatie en de informatievoorziening binnen de eigen Ministeries.

Een belangrijk kenmerk van het nieuwe voorschrift is de globaliteit, hetgeen echter niet betekent dat het vrijblijvend is. In het voorschrift zijn de 'spelregels' vastgelegd waaraan elk Ministerie zich te houden heeft en als zodanig biedt het voorschrift steun en houvast bij het voeren van beleid terzake.

Veel informatievoorzieningprocessen hebben niet alleen betrekking op het interne functioneren van overheidsorganisaties maar staan ten dienste van informatieverwerking en transport ten behoeve van derden (zoals andere Ministeries, uitvoeringsorganisaties, lagere overheden, bedrijfsleven en burgers). Het ligt daarom voor de hand om minimale eisen te stellen aan de wijze waarop met informatiebeveiliging wordt omgegaan bij informatie uitwisseling tussen of binnen een Ministerie en andere instanties.

Er is bewust gekozen om artikel 4 in termen van de Planning en Control cyclus, conform reguliere bedrijfsvoering, te formuleren. Informatiebeveiliging is daarmee een managementonderwerp. In de regeling zelf is de gewenste aandacht van het management voor informatiebeveiliging ingebouwd. Informatiebeveiliging zelf vindt plaats via de kwaliteitscirkel van Deming (PDCA cyclus). Zo staat handhaven en verbeteren van de informatiebeveiliging telkens op de (management)agenda.

Zoals eerder opgemerkt is niet gekozen om een vaste methodiek voor te schrijven, zoals een A&K of risico analyse. Het gevaar daarvan zou zijn dat een dergelijk begrip een eigen betekenis gaat krijgen en afleidt van de kern: het identificeren van de betrouwbaarheidseisen en nemen van passende maatregelen daarbij. Er bestaan verschillende gangbare methoden en technieken (zoals de Code voor Informatiebeveiliging en Cobit) en het is de verantwoordelijkheid van het lijnmanagement om daaruit een toegesneden keuze te maken en daarover vervolgens verantwoording af te leggen.

De betrouwbaarheidseisen en de daaruit voortvloeiende maatregelen vormen het uitgangspunt voor lijnmanagers die de verantwoordelijkheid hebben voor een informatiesysteem tijdens de levenscyclus ervan. Hiermee zijn de spelregels vastgelegd waarmee binnen overheidsorganisaties aan informatiebeveiliging inhoud gegeven wordt met het oog op een efficiënt samenwerkende overheid die betrouwbaar omgaat met de haar toevertrouwde informatie.

Relatie met andere regelgeving
De regels over informatiebeveiliging zijn terug te vinden in onder meer het Beveiligingsvoorschrift Rijksdienst 2005, het Voorschrift informatiebeveiliging – bijzondere informatie (Vir-bi). Ook de Wet bescherming persoonsgegevens (Wbp) en het Algemeen Rijksambtenarenreglement (ARAR) geven binnen hun werkingsgebied aanwijzingen voor informatiebeveiliging bij de Rijksdienst.

Het Beveiligingsvoorschrift Rijksdienst 2005 (BVR) kan gezien worden als een 'kapstok' waaraan vele elementen van beveiliging opgehangen kunnen worden. Centraal in het BVR staat de Beveiligingsambtenaar (BVA) die namens de secretaris-generaal belast is met de beveiliging van het Ministerie. Dit omvat ook de zorgplicht voor het VIR en Vir-bi. Het Vir-bi benadrukt de zorgplicht van ieder Ministerie en van diens lijnmanagement voor de beveiliging van bijzondere informatie bij de rijksdienst. Het Vir-bi is te beschouwen als een aanvulling op het VIR.

Elk Ministerie kan ingevolge de Wbp een functionaris gegevensbescherming aanstellen. Waar mogelijk en nodig trekken de informatiebeveiliging- en gegevensbescherming functionarissen gezamenlijk op. Informatiebeveiliging en bescherming van persoonsgegevens zijn, hoewel verschillend, onlosmakelijk met elkaar verbonden. De Wbp regelt in artikel 13 (aangevuld met CBP Achtergrondstudie en verkenning 23) welke maatregelen in het kader van informatiebeveiliging organisaties moeten treffen om op een adequate manier persoonsgegevens te beschermen. Deze maatregelen maken deel uit van het informatiebeveiligingsbeleid van een Ministerie.

Het ARAR bepaalt de rechten en plichten van rijksambtenaren. Informatiebeveiligingseisen bevinden zich in het bijzonder aan de plichtenkant, waarbij de rol van de ambtenaar in de beveiliging wordt toegelicht. Het gaat daarbij onder andere om de geheimhoudingsplicht.

Vervangen voorschriften
Het onderhavige voorschrift vervangt het VIR 1994, vastgesteld bij besluit van de Minister-president van 22 juli 1994, nr. 94/M004882, Staatscourant 173.

Artikelsgewijs

Artikel 1. Begripsbepalingen
Artikel 1 definieert de begrippen informatiebeveiliging en informatiesystemen in het kader van dit voorschrift. Dit zijn de kernbegrippen voor het VIR.

In dit besluit wordt verstaan onder:

a. Informatiebeveiliging: het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen;

Het kernbegrip voor dit voorschrift is het woord informatiebeveiliging zelf. Dit wordt gedefinieerd door gebruik te maken van de drie algemeen geaccepteerde aspecten van beveiliging: vertrouwelijkheid, beschikbaarheid en integriteit.

Naast informatiebeveiliging, wordt het begrip betrouwbaarheid gehanteerd: de mate waarin de organisatie zich voor de informatievoorziening kan verlaten op een informatiesysteem. De betrouwbaarheid van een informatiesysteem is daarmee de verzamelterm voor de begrippen beschikbaarheid, integriteit en vertrouwelijkheid. Het aspect controleerbaarheid speelt een belangrijke rol bij het afleggen van verantwoording over alle aspecten van informatiebeveiliging.

Vertrouwelijkheid
Met vertrouwelijkheid wordt gedoeld op het waarborgen dat informatie alleen toegankelijk is voor degenen, die hiertoe zijn geautoriseerd. Het gaat hier onder andere om het beveiligen van de toegang tot de gebouwen, informatiesystemen en de ICT-infrastructuur tegen onbevoegden (hackers en andere indringers) en malafide software (virussen, trojan horses). Maar ook om maatregelen om te voorkomen dat de eigen medewerkers toegang krijgen tot informatie die niet voor hen is bedoeld. Techniek speelt bij dit aspect een grote rol in de randvoorwaardelijke sfeer.

Beschikbaarheid
Beschikbaarheid betreft het waarborgen, dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen). Voor de beschikbaarheid van geautomatiseerde of handmatige (papieren archief) informatiesystemen worden tegenwoordig meestal Service Level Agreements (SLA) – of vergelijkbare overeenkomsten met een andere benaming – afgesloten tussen de eigenaar van het informatiesysteem (uiteindelijk lijnmanagement) en de ICT dienstenleverancier.

Beschikbaarheid is meer en meer het werkterrein van de beheerder en wordt vooral met techniek gerealiseerd. De beheerder is verantwoordelijk voor het correct en beheerst uitvoeren van de afspraken uit de SLA en rapporteert hierover aan de opdrachtgever. Voor de informatiebeveiligingsfunctie rest vooral het toezicht op de maatregelen die waarborgen, dat informatie niet verloren gaat, indien zich ernstige problemen voordoen.

Integriteit
Integriteit omhelst het waarborgen van de juistheid en volledigheid van informatie en de verwerking ervan. De juistheid en volledigheid van de informatie is een directe verantwoordelijkheid van de eigenaar van het systeem en de hem ondersteunende managers en medewerkers.

b. Informatiesysteem: een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.

Een informatiesysteem is een samenhangende (logische) groepering van gegevensverwerkende processen en gegevensverzamelingen. Componenten van een informatiesysteem kunnen zijn: gegevensverzamelingen, gegevensstromen, gegevensverwerkende activiteiten, de bij het systeem betrokken mensen, technische middelen, processen, procedures en programma's. Het begrip informatiesysteem omvat nadrukkelijk ook gemeenschappelijke voorzieningen als ICT-infrastructuur, die als basisvoorziening voor (delen van) een Ministerie gelden.

Het informatiesysteem is niet per definitie een geautomatiseerd (digitaal) systeem. Papieren systemen of dossiers vallen tevens onder de reikwijdte van deze definitie. Informatiebeveiliging brengt met zich mee dat deze gegevensverzamelingen ook in ogenschouw worden genomen.

De organisatie benoemt voor ieder informatiesysteem een eigenaar. Deze is verantwoordelijk voor de inbedding van informatiebeveiligende maatregelen in

dit systeem. Daar waar het systeem onderdeel uit maakt van een keten, voegt het informatiesysteem zich naar de eisen die vanuit de keten worden gesteld waarbij de eigenaar zorg draagt voor de aansluiting met het eigen beveiligingsbeleid.

Informatiesystemen kenmerken zich door het feit dat gegevens of worden opgeslagen of worden verwerkt. Via de beveiligingsmaatregelen en het gedefinieerde beveiligingsniveau wordt de opgeslagen of te verwerken informatie beschermd. Er ligt hier ook een belangrijk verband met de Wbp en het Vir-bi. Deze wet- en regelgeving kan aanvullende eisen stellen en wordt verondersteld meegenomen te zijn in de aan het systeem gestelde betrouwbaarheidseisen.

Artikel 2. Plaatsbepaling en reikwijdte
Dit artikel omschrijft de reikwijdte van het voorschrift, zowel in de zin van de overheidsorganisaties die het aangaat als van het onderwerp informatiebeveiliging. Voorts positioneert dit artikel het aspect informatiebeveiliging als een 'gewone' lijnverantwoordelijkheid. Daaraan inhoud geven gebeurt zowel op basis van interne overwegingen betreffende de betrouwbaarheid van de werkprocessen van een organisatie als op basis van externe randvoorwaarden zoals bestaande wet- en regelgeving. Uitgangspunt daarbij vormt de noodzaak om tot een integrale benadering van informatiebeveiliging te komen.

1. Dit voorschrift geldt voor de Rijksdienst waartoe gerekend worden de Ministeries met de daaronder ressorterende diensten, bedrijven en instellingen.

Tot de Rijksdienst behoren de Ministeries met hun directoraten-generaal, centrale en stafdirecties en intern verzelfstandigde dienstonderdelen (zoals agentschappen). Dat wil zeggen alle organisatieonderdelen op rijksniveau waarvoor de Ministeriële verantwoordelijkheid onverkort geldt. Er is vooralsnog niet voor gekozen om de regelgeving op het gebied van informatiebeveiliging rechtstreeks van toepassing te laten zijn op extern verzelfstandigde onderdelen van de rijksoverheid.

Het blijft daarmee de verantwoordelijkheid van de individuele Ministers om ervoor te zorgen dat het onderhavige voorschrift zelf of een gemotiveerd ander stelsel van bepalingen betreffende informatiebeveiliging op individuele zelfstandige bestuursorganen van toepassing wordt. Als gekozen wordt voor het van toepassing laten zijn van het voorschrift op zelfstandige bestuursorganen dan dienen in het volgende voor 'Ministerie' en 'secretaris-generaal' analoge begrippen te worden gekozen.

De verantwoordelijkheid van de Minister voor informatiebeveiliging bij zelfstandige bestuursorganen brengt met zich mee dat het zelfstandige bestuursorgaan jaarlijks moet rapporteren in haar jaarverslag wat de stand van zaken omtrent informatiebeveiliging is. En indien aan de orde welke de verbetermaatregelen, alsmede belangrijke wijzigingen, in het informatiebeveiligingsbeleid zijn. In het jaarverslag wordt het oordeel over de situatie van de informatiebeveiliging vermeld, evenals hoe en door wie dit oordeel tot stand gekomen is.

2. Dit voorschrift geldt voor het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.

Binnen het proces van informatievoorziening kunnen zowel geautomatiseerde als niet geautomatiseerde informatiesystemen (zie 1b) voorkomen. In veel systemen komen verschillende technologieën en informatiedragers naast elkaar voor, die tijdens de levenscyclus ook nog kunnen veranderen. Het voorschrift 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.

3. Informatiebeveiliging is een lijnverantwoordelijkheid en vormt een onderdeel van de kwaliteitszorg voor bedrijfs- en bestuursprocessen en de ondersteunende informatiesystemen.

Informatiebeveiliging is geen doel op zich, maar levert een bijdrage aan de kwaliteit van de informatievoorziening binnen een organisatie en daarmee aan de betrouwbaarheid van de bedrijfs- en bestuursprocessen.

De kwaliteit van de bedrijfsvoering van een Ministerie wordt geborgd door te werken volgens een Planning en Control cyclus (P&C cyclus). Dit is de jaarlijkse terugkerende beleid-, begroting- en verantwoordingcyclus waarbinnen alle relevante bedrijfsvoeringaspecten in samenhang een plaats hebben. Om tot een evenwichtig, samenhangend en afdoend stelsel van beveiligingsmaatregelen voor een informatiesysteem te komen, wordt informatiebeveiliging geïncorporeerd in die cyclus.

Door het beveiligingsbeleid op te nemen in de P&C cyclus en hierover door de organisatieonderdelen verantwoording af te laten leggen door reguliere voortgangsrapportages, heeft beveiliging een duidelijke rol in de verticale sturingskolom van een Ministerie. Een P&C cyclus is veelal vastgelegd in de Ministeriële begrotingsaanschrijving. Aansluiting hierbij voorkomt dat informatiebeveiliging als een eigenstandig onderwerp wordt behandeld en daardoor laag geprioriteerd wordt. Over de begroting en de uitvoering daarvan is het verplicht onder VBTB wetgeving (van beleidsbegroting tot beleidsverantwoording) verantwoording af te leggen.

Over het functioneren van de informatiebeveiliging (dus de kwaliteitscirkel) wordt conform de P&C cyclus zowel binnen het Ministerie als extern in de bedrijfsvoeringparagraaf richting Tweede Kamer en Algemene Rekenkamer verantwoording afgelegd door de Ministeriële leiding.

Artikel 3. Informatiebeveiligingsbeleid
Dit artikel bepaalt dat voor een Ministerie het beleid voor informatiebeveiliging wordt vastgesteld èn uitgedragen door de hoogst verantwoordelijke ambtenaar. In de praktijk is dit, vanwege zijn verantwoordelijkheid voor de bedrijfsvoering, vaak de pSG (of een vergelijkbare functie). Op grond van die verantwoordelijkheid ligt het in de rede dat deze het beleid vaststelt en uitdraagt.

De afzonderlijke leden van dit artikel bevatten de minimale inhoud van het beleid. Het beleid vormt de basis voor diverse vormen van communicatie richting de medewerkers, mede in het kader van bewustwordingsprogramma's, en geeft aan welk informatiebeveiligingsbeleid wordt gevoerd.

De secretaris-generaal van een Ministerie stelt het informatiebeveiligingsbeleid vast, draagt dit uit en legt verantwoording hierover af. Het beleid omvat ten minste:

a. De strategische uitgangspunten en randvoorwaarden die het Ministerie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid;

Het Ministeriële integrale beveiligingsbeleid (op basis van het Beveiligingsvoorschrift Rijksdienst 2005) heeft naast informatiebeveiliging tevens betrekking op de beveiliging van materieel en personen. De maatregelen die uit dien hoofde worden getroffen kunnen tevens van belang zijn voor de beveiliging van de informatievoorziening van een Ministerie. Ook voor de aspecten bewustzijn, melding van incidenten en vooral voor de inrichting van de informatiebeveiligingsfunctie is afstemming van belang teneinde wederzijdse versterking te bereiken en overlappingen en tegenstrijdigheden te vermijden.

Informatiebeveiliging is één van de aspecten van informatievoorziening. Het ligt voor de hand om de activiteiten ten behoeve van beveiliging in te bedden in het geheel van activiteiten voor informatievoorziening. Op beleidsmatig niveau geldt dit in het bijzonder voor het vaststellen van de strategische uitgangspunten en randvoorwaarden, de verdeling van de verantwoordelijkheden (zie lid c) en de financiering.

b. De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden;

De term informatiebeveiligingsfunctie dient niet te worden opgevat in de betekenis van een afzonderlijke functie binnen een organisatie die aan een persoon is opgedragen. De term omvat het geheel aan functies binnen een organisatie en de taken die bij die functies horen, voorzover ze betrekking hebben op informatiebeveiliging.

In het Beveiligingsvoorschrift Rijksdienst 2005 zijn in de artikelen 5 en 6 de taken van respectievelijk de beveiligingsambtenaar en de beveiligingscoördinator vastgelegd. De aldaar beschreven taken hebben ook betrekking op informatiebeveiliging.

Informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Het uitvoeren van activiteiten ten einde tot een evenwichtig pakket aan maatregelen te komen, noodzaakt tot het inzetten van andere disciplines die bijvoorbeeld in staf- en ondersteunende diensten (zoals ict, personeel, organisatie en facilitaire zaken) gebundeld zijn. Het is van belang helderheid te hebben over de randvoorwaarden van het gebruik van deze deskundigen ten opzichte van de eindverantwoordelijkheid van het lijnmanagement. Dit geldt in het bijzonder voor die maatregelen die voor het Ministerie als geheel vastgesteld worden, voor de wijze waarop de melding en registratie van incidenten plaatsvindt en voor de wijze waarop evaluatie van het informatiebeveiligingsbeleid wordt uitgevoerd.

Uitgangspunt bij het optreden van incidenten is dat deze door medewerkers gemeld worden. Bij welke functionaris een dergelijk signaal moet worden afgegeven en hoe daarmee binnen een Ministerie wordt omgegaan, wordt vastgelegd in het beleidsdocument inzake informatiebeveiliging.

c. De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers;

Lijnmanagers zijn verantwoordelijk voor de informatiesystemen waarmee de aan hen toevertrouwde bedrijfsprocessen worden ondersteund. Omdat binnen een organisatie de verschillende informatiesystemen veelal niet onafhankelijk van elkaar kunnen worden beschouwd is de toewijzing van ketens van informatiesystemen aan lijnmanagers evenzeer nodig. Deze ketens kunnen voor een deel ook buiten de eigen organisatie liggen, dit ontslaat het lijnmanagement niet van hun verantwoordelijkheid. De lijnmanager maakt in dat geval met partijen buiten de organisatie sluitende afspraken over informatiebeveiliging.

In het beleid moet vastgelegd worden op welke wijze deze ketenverantwoordelijkheid wordt belegd binnen de organisatie teneinde zeker te stellen dat het lijnmanagement verantwoordelijk gesteld kan worden voor het realiseren van het vereiste betrouwbaarheidsniveau van de gehele keten. Voor het realiseren van het door hem gewenste niveau van informatiebeveiliging is een lijnmanager aangewezen op afspraken met anderen binnen deze keten. In deze situatie moet duidelijk vastliggen onder wiens verantwoordelijkheid het gebruik plaatsvindt en wie daarmee de verantwoordelijkheid draagt voor het vastleggen, uitdragen en controleren van de van toepassing zijnde maatregelen.

d. De gemeenschappelijke betrouwbaarheidseisen en normen die op het Ministerie van toepassing zijn;

Een Ministerie kan er voor kiezen om een gemeenschappelijk stelsel van betrouwbaarheidseisen, normen en/of maatregelen af te spreken. Zo'n stelsel zal in het algemeen betrekking hebben op het merendeel van de informatiesystemen dat gebruikt wordt en ontlast tot op zekere hoogte de individuele lijnmanagers van hun taak om informatiebeveiliging gedetailleerd inhoud te geven. Dit houdt bijvoorbeeld in de wijze waarop de logische en/of fysieke toegangsbeveiliging binnen (delen van) het Ministerie gerealiseerd wordt. Of het bestaat uit een pakket aan betrouwbaarheidseisen die aan de 'normale' processen en ondersteunende informatiesystemen worden gesteld (daarbij kunnen indien nodig aanvullend per informatiesysteem specifieke eisen worden gesteld). Een dergelijk stelsel wordt veelal aangeduid met de term baseline.

De eisen kunnen ook het karakter hebben van een classificatie van informatie (en daarmee van de informatiesystemen waarin deze informatie potentieel optreedt). Hiermee wordt een indeling in gevoeligheidsklassen bedoeld waaraan veelal in oplopende volgorde steeds zwaardere eisen worden gesteld voor een of meerdere aspecten van beveiliging. Er is in dit voorschrift gekozen om het hanteren van een vast stramien van klasse indelingen niet voor te schrijven. Hiervoor kan worden teruggegrepen naar voorhanden zijnde wet- en regelgeving zoals Vir-bi en Wbp.

e. De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd;

De evaluatie van het beleid heeft betrekking op de organisatie en uitvoering van informatiebeveiliging binnen het Ministerie en wordt beoordeeld door een onafhankelijke deskundige. Het ligt voor de hand de frequentie af te laten hangen van het abstractieniveau van het beleid en de mate waarin de organisatie aan veranderingen en ook incidenten onderhevig is. De resultaten van de evaluatie worden gebruikt voor de bijstelling van het informatiebeveiligingsbeleid.

Conform het BVR is de beveiligingsambtenaar, namens de secretaris-generaal, verantwoordelijk voor het toezicht op de uitvoering van het beveiligingsbeleid. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door of vanwege de beveiligingsambtenaar dan wel door interne of externe auditteams.

f. De bevordering van het beveiligingsbewustzijn.

De naleving van de beveiligingsvoorschriften blijft mensenwerk en vereist de voortdurende aandacht. Deugdelijke procedures en technische maatregelen zijn niet voldoende. Beveiliging is vooral een kwestie van mentaliteit waarbij lering trekken uit fouten essentieel is. Het is 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, bijvoorbeeld door middel van periodieke voorlichting

Er is een duidelijk verband met integer handelen door ambtenaren en de activiteiten die het Ministerie op dat terrein ontplooid. Waar mogelijk zal het management relaties tussen beide onderwerpen moeten leggen. Voordeel daarbij is, dat de medewerker informatiebeveiliging én integriteit niet als losstaande onderwerpen zien maar als communicerende vaten. Daarnaast zal het management medewerkers moeten faciliteren om mee te kunnen werken aan een beveiligde omgeving. Aandacht is nodig voor het onderscheid tussen beheerders en gebruikers.

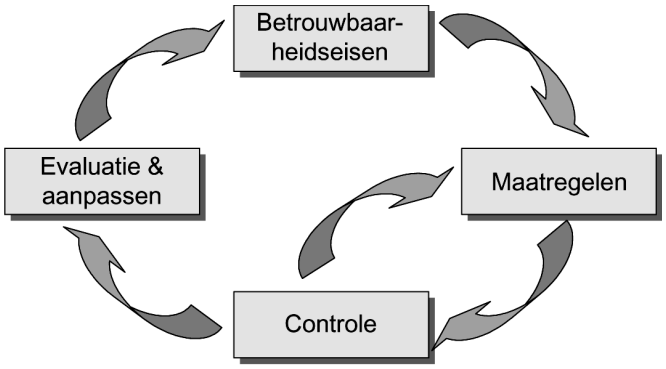
Artikel 4. Verantwoordelijkheden lijnmanagement

Het lijnmanagement is verantwoordelijk voor de kwaliteit van bedrijfsvoering. Die verantwoordelijkheid wordt verticaal in de lijn verdeeld, van organisatietop tot afdelingshoofd. Informatiebeveiliging geldt als een integraal onderdeel van de bedrijfsvoering. Zo is het lijnmanagement ook eindverantwoordelijk voor informatiebeveiliging. Het begrip lijnmanagement wordt hierbij ruim opgevat. In voorkomende gevallen kan ook een afdelingshoofd of een manager van een stafafdeling onder het lijnmanagement worden verstaan.

Het lijnmanagement kan besluiten om (delen van) de ontwikkeling, exploitatie of het onderhoud van het systeem uit te besteden. Ook in deze gevallen blijft het lijnmanagement eindverantwoordelijk voor de beveiliging van het systeem. Het lijnmanagement communiceert de betrouwbaarheidseisen van het systeem aan de derde partij. Via een schriftelijke overeenkomst (bijvoorbeeld een Service Level Agreement) wordt vastgelegd hoe de derde partij aan deze eisen gaat voldoen en tevens worden er consequenties verbonden aan het niet naleven van deze afspraken. Vanuit zijn hoedanigheid als verantwoordelijke partij, controleert het lijnmanagement of de werkzaamheden van de derde partij het vereiste betrouwbaarheidsniveau realiseren.

Voor het effectueren van informatiebeveiliging wordt gewerkt via de Plan Do Check Act cyclus (zie figuur). Na het vaststellen wat nodig is (betrouw-

baarheidseisen), worden maatregelen getroffen en gecontroleerd of die maatregelen het gewenste effect sorteren (controle). Deze controle kan direct aanleiding geven tot bijsturing in de maatregelen. Ook kan het totaal van eisen, maatregelen en controle aan revisie toe zijn (evaluatie). Het goed doorlopen van deze kwaliteitscirkel zorgt op elk moment voor het adequate beveiligingsniveau.



Figuur: PDCA cyclus voor Informatiebeveiliging

Het lijnmanagement is verantwoordelijk voor de beveiliging van zijn informatiesystemen. Het lijnmanagement:

a. Stelt op basis van een expliciete risico afweging de betrouwbaarheidseisen voor zijn informatiesystemen vast;

De lijnmanager bepaalt op systematische wijze wat de betrouwbaarheidseisen zijn voor (de keten van) informatiesystemen waarvoor hij verantwoordelijk is. Hieraan ligt een expliciete risico afweging ten grondslag. Er is niet voor gekozen een methodiek voor te schrijven. Veeleer kan de lijnmanager op basis van zijn eigen situatie beoordelen welke methode het meest effectief is. Het belang en de kwaliteit van beleids- en bedrijfsvoering staan bij risico afwegingen voorop.

Uitgaande van kwaliteitseisen die aan de producten en diensten van een organisatie worden gesteld, zullen de werkprocessen adequaat moeten worden ingericht. De eisen die informatiebeveiliging stelt nemen een belangrijke plaats in bij de inrichting van werkprocessen en trachten tegelijkertijd zo min mogelijk afbreuk te doen aan een doelmatige en doeltreffende uitvoering van werkprocessen.

Methodes om eisen vast te stellen waaraan kan worden gedacht zijn:
– afhankelijkheid & kwetsbaarheid analyse;
– risicoanalyse;
– baseline toets;
– certificering (bijvoorbeeld ISO/NEN) met bijbehorende toets

De baseline toets komt in aanmerking als een organisatie of organisatieonderdeel een baseline benadering voor informatiebeveiliging wenst toe te passen die op de meeste ‘gewone’ informatiesystemen van toepassing wordt verklaard.

De betrouwbaarheidseisen die op Ministerieel niveau zijn vastgesteld hebben rechtstreekse werking op individuele informatiesystemen. In al deze gevallen dient gestreefd te worden naar het samenstellen van een pakket betrouwbaarheidseisen van gelijksoortige aard en detaillering.

Een andere methode is certificering. Hierbij valt bijvoorbeeld te denken aan certificering op basis van de Code voor Informatiebeveiliging (ISO27001). Hierbij onderzoekt een externe partij of de betrouwbaarheidseisen en maatregelen overeenkomen met de Code voor informatiebeveiliging.

Om te voldoen aan het VIR wordt in het systeemontwikkelingtraject de vaststelling van betrouwbaarheidseisen zo vroeg mogelijk uitgevoerd, bij voorkeur tijdens de fase ‘definitiestudie’, eventuele detailleringen passen in de fasen ‘basisontwerp’ en ‘detailontwerp’. Het veronachtzamen van beveiliging in ontwikkel- en implementatietrajecten heeft tot gevolg dat achteraf gerepareerd of veranderd moet worden. Daarmee lopen organisaties het gevaar dat de beveiliging niet optimaal is ingericht en bovendien het traject duurder wordt door reparaties achteraf. In beide gevallen ongewenste effecten.

Naast het ontwikkelen en implementeren kunnen informatiesystemen ook worden verworven en/of geëxploiteerd. In deze gevallen draagt de lijnmanager de zorg voor het betrouwbaar (laten) exploiteren van het informatiesysteem en de zorg voor het betrouwbaar (laten) verwerven van (componenten van) het informatiesysteem.

Bij het verwerven van een nieuw informatiesysteem en/of het exploiteren hiervan is het de verantwoordelijkheid van de lijnmanager om er voor te zorgen dat tijdens het selectieproces de betrouwbaarheidseisen die aan het informatiesysteem gesteld worden, als randvoorwaarden gelden. Heeft de verwerving niet betrekking op een nieuw informatiesysteem maar betreft het onderhoud op een bestaand informatiesysteem (dat geen deel uitmaakt van de systeemexploitatie) dan geldt onverkort dat de betrouwbaarheidseisen (met de daaraan gerelateerde maatregelen) van een informatiesysteem één van de randvoorwaarden vormen voor de onderhoudsactiviteiten.

In sommige situaties kunnen betrouwbaarheidseisen rechtstreeks worden afgeleid uit de relevante wet- en regelgeving. Voor persoonsgegevens kan in dit verband aan de Wbp worden gedacht; voor bijzondere informatie aan het VIR-BI. Voor informatiesystemen die een keten ondersteunen stelt de aangewezen lijnmanager van de organisatie de betrouwbaarheidseisen vast.

b. Is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;

Uitgaande van de vastgestelde betrouwbaarheidseisen en de in beschouwing genomen bedreigingen stelt de lijnmanager een evenwichtig pakket van maatregelen vast. Evenwichtig betekent dat er een balans bestaat tussen de kosten en lasten van (extra) maatregelen enerzijds en de afgedekte risico’s anderzijds. Hierbij maakt de lijnmanager een keuze uit een combinatie van zowel personele, procedurele, organisatorische, fysieke, juridische als technische maatregelen.

Bij het kiezen van (informatiebeveiliging)maatregelen wordt zoveel mogelijk gebruik gemaakt van maatregelen die binnen de organisatie al zijn getroffen, zoals de maatregelen die voortvloeien uit een baseline. Het kiezen van deze maatregelen is voor een belangrijk deel te positioneren in het proces van systeemontwikkeling, -onderhoud en -verwerving. Dit geldt overigens ook voor de implementatie van de technische maatregelen.

Nadat een keuze is gemaakt voor de te treffen maatregelen, worden deze maatregelen aantoonbaar vastgelegd en

geïmplementeerd. Dit gebeurt deels in de technische specificaties van een informatiesysteem, zoals bij integriteitcontroles en maatregelen op het gebied van de beschikbaarheid van hardware. Het geheel van alle maatregelen, dus inclusief de specifieke beveiligingsmaatregelen, maakt óf onderdeel uit van de contracten (bij verwerving) en/of van de systeemdocumentatie (bij eigen systeemontwikkeling). Gelijktijdig zijn er maatregelen voor de te hanteren procedures bij het gebruik van het informatiesysteem. In veel gevallen is het niet zinvol om te streven naar een apart document waarin alle maatregelen zijn opgesomd. Dit zou slechts tot administratieve ballast leiden gezien de verschillende aard (bijvoorbeeld technisch, procedureel) en de verwevenheid van de maatregelen. Zij vormen vaak niet één direct identificeerbare afzonderlijke categorie.

Bij systemen die onderdeel zijn van een keten, maakt het lijnmanagement via een Service Level Agreement (SLA) of een andere vorm van een dienstenovereenkomst, afspraken over de normen waaraan de keten moet voldoen. Daarnaast kan gebruik gemaakt worden van een Third Party Mededeling (TPM) waarin een onafhankelijke partij een verklaring afgeeft over het niveau van beveiliging binnen een organisatie. Hiermee wordt een garantie afgegeven dat de andere organisatie in de keten voldoet aan een vooraf vastgesteld beveiligingsniveau.

Naast het vastleggen en implementeren van maatregelen, is het ook van belang dat bepaalde maatregelen uitgedragen worden. Dit kan worden bereikt via opleidingen, werkinstructies of een gebruikershandleiding, maar ook door een helpfunctie in de betreffende toepassingsprogrammatuur. In dit kader is continue aandacht voor het bevorderen van het beveiligingsbewustzijn belangrijk.

c. Stelt vast dat de getroffen maatregelen aantoonbaar overeenstemmen met de betrouwbaarheidseisen en dat deze maatregelen worden nageleefd;

De vaststelling heeft de aard van een controle op de werking van informatiebeveiliging. Het doel van controle is na te gaan of het gehele pakket van maatregelen de gewenste betrouwbaarheid geeft. Deze controle kan aanleiding geven tot bijstelling of intensivering van de maatregelen.

De leidinggevende heeft de taak/verantwoordelijkheid na te gaan of het gehele pakket aan maatregelen nog steeds voldoet, dat wil zeggen de gewenste betrouwbaarheid geeft. Doordat er continu (o.a. organisatorische en technische) veranderingen plaatsvinden, is het noodzakelijk periodiek na te gaan of de getroffen maatregelen nog steeds het gewenste betrouwbaarheidsniveau garanderen. Indien niet, dan bepaalt de lijnmanager welke maatregelen additioneel worden genomen en/of welke maatregelen vervallen.

Bij majeure veranderingen van organisatie of informatiesystemen wordt direct gecontroleerd of het pakket van maatregelen nog voldoet aan de gewenste betrouwbaarheid. Indien nodig wordt het pakket aan maatregelen aangepast.

Voor de controle op de uitvoering en naleving van de maatregelen heeft de manager verschillende mogelijkheden. Zo kan bijvoorbeeld een baseline toets, self assessment, certificering of externe controle door een deskundige en onafhankelijke partner worden uitgevoerd.

De controlefrequentie kan verschillen, afhankelijk het belang van de naleving van de betrouwbaarheidseisen voor de organisatie.

d. Evalueert periodiek het geheel van betrouwbaarheidseisen en beveiligingsmaatregelen en stelt deze waar nodig bij.

Het doel van deze periodieke evaluatie is na te gaan of het geheel van betrouwbaarheidseisen en beveiligingsmaatregelen nog steeds het juiste niveau van informatiebeveiliging bewerkstelligt. De evaluatie kan aanleiding geven tot het bijstellen van de betrouwbaarheidseisen en/of de maatregelen.

De Minister-President, Minister van Algemene Zaken,
J.P. Balkenende.