STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 5393
21 maart
2012

Beleidsregels van de Minister van Veiligheid en Justitie van 11 januari 2012, nr DGP/DPV/VIT, over de beveiliging van het radiocommunicatienetwerk C2000

De Minister van Veiligheid en Justitie,

Gelet op artikel 2 Regeling C2000 en GMS;

Vanwege het belang van het C2000-netwerk voor de handhaving van de openbare orde, veiligheid en hulpverlening worden er regels gesteld aan de informatiebeveiliging daarvan;

Gehoord het advies van het Veiligheidsberaad;

Besluit:

Artikel 1 Begrippen

In deze regeling wordt verstaan onder:
a) *het C2000-netwerk:* het communicatienetwerk ten behoeve van de Openbare Orde en Veiligheid(OOV) diensten binnen Nederland, zoals bedoeld in artikel 1 van de Regeling C2000 en GMS;
b) *de eigenaar van het C2000-netwerk:* de staat der Nederlanden, de minister van Veiligheid en Justitie. De eigenaar van het C2000-netwerk vertegenwoordigt mede namens de Minister Defensie en de Minister van Volksgezondheid, Welzijn en Sport de staat der Nederlanden;
c) *strategisch beheerder:* de minister van Veiligheid en Justitie
d) *tactisch en operationeel beheerder:* de beheerorganisatie van C2000, Voorziening tot samenwerking Politie Nederland/Unit Meldkamer Systemen;
e) *gebruikers:* een organisatie die voor OOV-taken gebruik maakt van het C2000- communicatienetwerk. Dit kan een aangewezen gebruiker, een gelieerde of een bijzondere gebruiker zijn;
f) *aangewezen gebruiker:* een organisatie die op het terrein van openbare orde, veiligheid en hulpverlening een wettelijk opgedragen taak heeft en ten behoeve van haar operationele processen gebruik maakt van C2000;
g) *gelieerde:* een organisatie die de aangewezen gebruiker ondersteunt bij de uitvoering van zijn taken op het terrein van openbare orde, veiligheid en hulpverlening en die daarbij met behulp van mobiele communicatie door de aangewezen gebruiker wordt aangestuurd.
h) *adviesorgaan C2000:* :et overleg van gebruikers dat de strategisch beheerder adviseert over C2000. De adviestaak met betrekking tot C2000 wordt ingevuld door de Bestuurscommissie Informatievoorziening van het Veiligheidsberaad. Ten aanzien van C2000 wordt dit gedaan in afstemming met het korpsbeheerdersberaad;
i) *een bijzondere gebruiker:* een organisatie die naar het oordeel van de Minister van Veiligheid en Justitie uit het oogpunt van openbare orde, veiligheid en hulpverlening onder reguliere omstandigheden en bij crisis en rampen in contact moeten kunnen treden met een of meer aangewezen gebruikers en daartoe gebruik maakt van C2000.
j) *C2000-randapparatuur:* een apparaat dat via de air-interface met het C2000-netwerk is verbonden. Dit zijn T2000 handsets, P2000 handsets of mobiele data terminals;
k) *beschikbaarheid:* de mate waarin (gegevens in) een informatiesysteem beschikbaar is voor een eindgebruiker;
l) *beveiligingsincident:* een gebeurtenis die opgetreden is, of die kan optreden en die negatieve effecten heeft op de informatiebeveiliging van het C2000-communicatienetwerk of in de controleerbaarheid van deze eigenschappen;
m) *integriteit:* de mate waarin (gegevens in) een informatiesysteem foutenvrij is;
n) *vertrouwelijkheid:* de mate waarin de gegevens ineen informatiesysteem slechts toegankelijk is voor geautoriseerde personen;
o) *(C2000-) Infrastructuur:* alle middelen die binnen het verantwoordelijkheidsgebied van de eigenaar van het C2000-communicatienetwerk vallen en fysiek zijn verbonden met het C2000- communicatienetwerk. Hieronder vallen schakelpunten, paging routers, netwerkinfrastructuur, opstelpunten, vitale SCL's, C2000-meldkamerapparatuur, netwerkmanagement systeem en diverse gateways.

Artikel 2 Doelstelling en reikwijdte

- De informatiebeveiliging van het C2000-netwerk wordt gedefinieerd in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

- De doelstelling van het informatiebeveiligingsbeleid is de realisatie en het behoud van informatiebeveiliging van het C2000-netwerk. Dit informatiebeveiligingsbeleid stelt de grondslagen en richtlijnen vast voor de informatiebeveiliging van het C2000 communicatienetwerk en de taken, verantwoordelijkheden en bevoegdheden van de daarbij betrokken partijen.
- De reikwijdte van dit beleid is gelimiteerd tot aspecten die gerelateerd zijn aan de
- Informatiebeveiliging van het C2000 communicatienetwerk. Het Informatiebeveiligingsbeleid is van toepassing op alle personen en organisaties die het C2000 communicatienetwerk gebruiken, beheren of onderhouden in dienst van, gelieerd aan, of werkend in opdracht van één van de OOV-diensten, de beheerders of de eigenaar.
- Taken kunnen worden uitbesteed aan leveranciers of een andere partij, echter de verantwoordelijkheden van partijen, zoals deze in dit beleid zijn belegd, zijn niet overdraagbaar. Daarnaast is het de verantwoordelijkheid van de uitbestedende partij dat de leverancier formeel is geaccrediteerd en alle uit dit beleid voortvloeiende maatregelen, behorend bij de uitbestede taak, heeft geïmplementeerd.

Artikel 3 Implementatie en beveiligingsincidenten

1. De implementatie en naleving van de beveiligingsmaatregelen bij de gebruikers worden jaarlijks getoetst door de eigenaar.

2. De gebruiker implementeert in beginsel de maatregelen (zie Bijlage 2). De gebruiker mag alleen hiervan afwijken indien hij voldoende kan motiveren dat een vergelijkbaar basis beveiligingsniveau wordt gerealiseerd.

3. De beheerder gebruikt de vastgelegde beveiligingseisen als richtsnoer voor zijn eigen risicobeheersingproces om zo te waarborgen dat aan de eisen wordt voldaan.

4. Door te voldoen aan de beveiligingseisen, zijn de gebruikers en de beheerder in overeenstemming met dit beleid.

5. Partijen zijn verplicht jaarlijks te rapporteren aan de beheerder over de status van de implementatie van de voor hen verplichte beveiligingsmaatregelen.

6. Alle C2000 eindgebruikers en personen werkzaam voor het C2000 communicatienetwerk of binnen een betrokken partij worden op de hoogte gebracht over hun verantwoordelijkheden rond informatiebeveiliging en hebben daarvoor training gekregen.

7. Door middel van formele afspraken met partijen betrokken bij het C2000 communicatienetwerk is geborgd dat dit informatiebeveiligingsbeleid en de daaruit voorvloeiende beheersmaatregelen van toepassing zijn op de medewerkers werkzaam binnen deze partijen.

8. Het gebruik van leveranciers of het overdragen van taken aan overige partijen ontslaat de partij niet van de bij hem belegde verantwoordelijkheid: In het geval dat een leverancier een verplichte beveiligingsmaatregel niet implementeert, is de partij die gebruik maakt van de leverancier hier direct verantwoordelijk voor.

9. Alle personen die het C2000 communicatienetwerk gebruiken, beheren of onderhouden (waaronder leveranciers), melden via de binnen de eigen organisatie aangewezen beveiligingsfunctionaris, de beveiligingsincidenten bij het operationeel-beveiligingsbeheer.

Artikel 4 Gebruik en beheer door aangewezen gebruikers

1. De aangewezen gebruiker is verantwoordelijk voor beveiligd gebruik van C2000-netwerk.

2. De aangewezen gebruiker is verantwoordelijk voor de implementatie van de beveiligingsmaatregelen (Bijlage 2).

Artikel 5 Verantwoordelijkheid aangewezen gebruiker voor gelieerde en leverancier

1. De aangewezen gebruiker is verantwoordelijk voor het voldoen van haar gelieerden aan dit informatiebeveiligingsbeleid.

2. De aangewezen gebruiker legt met de gelieerde contractueel vast dat de gelieerde de set maatregelen in Bijlage 2 implementeert. Hierbij is de aangewezen gebruiker ervoor verantwoordelijk dat de gelieerde deze maatregelen daadwerkelijk implementeert en rapporteert de aangewezen gebruiker over de status van implementatie aan de beheerder.

3. De aangewezen gebruiker voert de taken en voortvloeiende verantwoordelijkheden beheer C2000 randapparatuur en gebruik C2000 beheer- en meldkamersystemen voor de gelieerde uit. Het is de gelieerde niet toegestaan deze taken zelfstandig uit te voeren.

4. De aangewezen gebruiker mag twee C2000 beveiligingsgerelateerde taken uitbesteden aan leveranciers.

Artikel 6 Gebruik en beheer bijzondere gebruikers

1. Zoals alle partijen binnen het C2000-communicatienetwerk implementeert de bijzondere gebruiker de algemene maatregelen uit Bijlage 2.

2. Om te worden toegelaten als bijzondere gebruiker tot het C2000-communicatienetwerk, is de bijzondere gebruiker geaccrediteerd door de eigenaar.

Artikel 7 Gebruik en beheer randapparatuur door tactisch en operationeel beheerder

1. De beheerder is verantwoordelijk voor beveiligd gebruik van C2000-randapparatuur.

2. De beheerder is verantwoordelijk voor de implementatie van de beveiligingsmaatregelen (Bijlage 2).

Artikel 8 Gebruik en beheer C2000 meldkamer -en beheersystemen door tactisch en operationeel beheerder

1. De eigenaar is verantwoordelijk voor het formeel vaststellen van de accreditatiecriteria en de uiteindelijke accreditatiebeslissing. Hiernaast is de beheerder verantwoordelijk voor het laden en verwijderen van cryptografische sleutels in randapparatuur van bijzondere gebruikers.

2. De beheerder is verantwoordelijk voor het onderhouden van de accreditatiecriteria aan de hand van voortschrijdend inzicht en het uitvoeren van toetsingen bij gebruikers en leveranciers en op externe koppelingen, SCL's en randapparatuur.

Artikel 9 Operationeel beveiligingsbeheer

1. Het operationeel beveiligingsbeheer is verantwoordelijk voor het beperken van de impact van beveiligingsincidenten.

2. Het operationeel beveiligingsbeheer is verantwoordelijk voor het signaleren van ontwikkelingen aan strategisch beveiligingsbeheer.

3. Het operationeel beveiligingsbeheer is belegd bij de tactisch en operationeel beheerder.

Artikel 10 Strategisch beveiligingsbeheer

1. Het strategisch beveiligingsbeheer wordt ondersteund door en ziet toe op het operationeel beveiligingsbeheer. Daarnaast is strategisch beveiligingsbeheer verantwoordelijk voor de toetsing op naleving door middel van periodieke audits. De rol van het strategisch beveiligingsbeheer is belegd bij de eigenaar.

Artikel 11 Toezicht en controle

1. De verantwoordelijkheid voor uitvoering van toezicht, controle en herziening is belegd bij de eigenaar.

Artikel 12 Controle en audits

1. Controle heeft als doel vast te stellen of de beveiligingsmaatregelen geïmplementeerd zijn en of zij het gewenste effect bereiken (namelijk een C2000 communicatienetwerk met voldoende beschikbaarheid, integriteit en vertrouwelijkheid).

2. De controles vinden plaats in de vorm van audits.

Artikel 13 Herziening

1. In de Herziening (van het informatiebeveiligingsbeleid) wordt de informatiebeveiliging van het C2000-communicatienetwerk geëvalueerd door strategisch beveiligingsbeheer.

2. De herziening vindt jaarlijks plaats door strategisch beveiligingsbeheer.

3. Indien de herziening hier aanleiding toe geeft, wordt dit informatiebeveiligingsbeleid aangepast en opnieuw vastgesteld.

4. In het geval van ernstige incidenten kan strategisch beveiligingsbeheer deze herziening vervroegd plaats laten vinden.

Artikel 14 Naleving

1. De effectiviteit van het beveiligingsbeleid wordt bepaald door de mate waarin betrokken partijen de beveiligingsmaatregelen naleven.

Artikel 15 Inwerkingtreding

Deze regeling treedt in werking met ingang van de tweede dag na de dagtekening van de Staatscourant waarin zij wordt geplaatst.

Artikel 16

Deze beleidsregels worden aangehaald als: Beleidsregels Informatiebeveiligingsbeleid C2000

Den Haag, 11 januari 2012

De Minister van Veiligheid en Justitie
I.W. Opstelten.

BIJLAGE 1: TOETSINGSOVERZICHT

In de onderstaande label is de periodiciteit van de in dit beleid genoemde toetsingsmomenten kort weergegeven:
Audit strategisch beveiligingsbeheer
Jaarlijkse stelselevaluatie met betrekking tot informatiebeveiliging voor het C2000- communicatienetwerk.
Deze evaluatie is de input voor wijzigingen in dit beleid. De eigenaar in overleg met strategisch beveiligingsbeheer plant om de twee jaar de stelselevaluatie.

Audit beheerder
Jaarlijks
Hoewel dit jaarlijks plaatsvindt, zal per jaar een aandachtsgebied (bijvoorbeeld één taak) worden gekozen. Strategisch beveiligingsbeheer stelt jaarlijks deze aandachtsgebieden vast.

Audit gebruiker
Jaarlijks.
Deze audit zal niet jaarlijks voor alle gebruikers plaatsvinden, maar slechts voor zes (6) gebruikers per jaar. Strategisch beveiligingsbeheer stelt jaarlijks vast welke gebruikers worden geaudit en kan daarbij ook aandachtspunten aangeven.

Herhalingsaccreditatie Steekproefsgewijs.
Jaarlijks vastgesteld.
Dit omvat herhalingsonderzoeken bij reeds geaccrediteerde partijen, apparaten of koppelingen.
Dit vindt steekproefsgewijs plaats, in het bijzonder bij een directe aanleiding. Bijvoorbeeld: beveiligingsincidenten en (grote) veranderingen. Strategisch beveiligingsbeheer stelt jaarlijks vast welke herhalingsaccreditaties worden uitgevoerd. De herhalingsonderzoeken voor gebruikers vinden plaats door middel van de gebruiker audits.

BIJLAGE 2: BEVEILIGINGSMAATREGELEN GEBRUIKERS

Deze bijlagebevat de beveiligingsmaatregelen per rol, welke zijn gerelateerd aan de NEN-ISO/IEC 27002:2007. De partijen waarbij de rol is belegd zijn verantwoordelijk voor de implementatie van de beveiligingsmaatregelen.

2.0 Algemene beveiligingsmaatregelen

2.0.1 De gebruiker richt een documentatiesysteem in voor het centrale beheer van documentatie relevant voor de informatiebeveiliging van het C2000-communicatienetwerk. Onderdeel van het documentatiesysteem moet ten minste zijn: versiebeheer en traceerbaarheid.
Dit systeem is onderdeel van het kwaliteitssysteem van de gebruiker.
Indien in deze bijlage gedocumenteerd staat dan is het betreffende gedeelte in dit documentatiesysteem zijn opgenomen.

2.0.2 De taken, verantwoordelijkheden en bevoegdheden van werknemers, ingehuurd personeel en externe eindgebruikers ten aanzien van de informatiebeveiliging van C2000 moeten worden vastgesteld en gedocumenteerd.

2.0.3 Elke gebruiker stelt een C2000-beveiligingsfunctionaris aan, die als centraal aanspreekpunt voor en naar de beheerder en eigenaar fungeert op het gebied van informatiebeveiliging. Deze functionaris geeft tevens uitvoering aan de beveiligingsincidenten- en implementatierapportage naar de beheerder.

2.0.4 De toegangsrechten (zowel logisch als fysiek) van alle werknemers, ingehuurd personeel en externe eindgebruikers tot C2000-voorzieningen worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of wordt na wijziging van zijn/haar taak aangepast.

2.0.5 De toegangsrechten (zowel logisch als fysiek) van alle werknemers, ingehuurd personeel en eindgebruikers tot C2000-voorzieningen worden minimaal halfjaarlijks door of in opdracht van het lijnmanagement gecontroleerd. Het resultaat van deze controle wordt gedocumenteerd.

2.0.6 Er is een procedure vastgesteld en beschikbaar voor alle werknemers, ingehuurd personeel en externe eindgebruikers om beveiligingsincidenten onverwijld bij operationeel beveiligingsbeheer te melden.

2.0.7 Beveiligingsincidenten en reacties hierop dienen te worden geregistreerd, daarnaast dient een procedure tot onverwijlde opvolging door de beveiligingsfunctionaris te zijn vastgesteld.

2.0.8 Er is een disciplinair proces van toepassing op werknemers, ingehuurd personeel en eindgebruikers die inbreuk op de informatiebeveiliging van het C2000-communicatienetwerk hebben gepleegd.

2.0.9 Relevante handboeken, werkinstructies en gedragscodes rond informatiebeveiliging zijn voor elke eindgebruiker en beheerder beschikbaar.

2.0.10 Elke gebruiker controleert de implementatie van de voor hem en zijn gelieerden verplichte beveiligingsmaatregelen en rapporteert hierover jaarlijks aan operationeel beveiligingsbeheer volgens een format vastgesteld door operationeel beveiligingsbeheer.

2.0.11 Elke gebruiker controleert de implementatie van de voor zijn leveranciers verplichte beveiligingsmaatregelen en rapporteert hierover jaarlijks aan operationeel beveiligingsbeheer volgens een format vastgesteld door operationeel beveiligingsbeheer.
Leveranciers die crypto gerelateerde handelingen uitvoeren (zogenaamd type 2 leveranciers) dienen te zijn geaccrediteerd door de eigenaar. De implementatie van de verplichte beveiligingsmaatregelen en volledige medewerking van de leverancier bij een controle op deze implementatie dient in het contract met de leverancier te worden opgenomen.

2.0.12 Alle logische en fysieke koppelingen tussen de C2000-infrastructuur en andere componenten die niet onderdeel zijn van de standaard C2000 dienstverlening (dit ter beoordeling van de beheerder) zijn geaccrediteerd door de eigenaar.

2.0.13 De locatie(s) waar C2000 middelen staan opgesteld zijn beveiligd. Het totaal aan inbraakwerende en vertragende maatregelen dient te voldoen aan de maatregelen behorend bij het risiconiveau 3 volgens de verbeterde risicoklasse indeling (VRKI) van het Nationaal Centrum voor Preventie.

2.1 Gebruik C2000 randapparatuur

2.1.1 Alle C2000-randapparatuur wordt geregistreerd in een actuele inventaris. Hierin is te allen tijde inzichtelijk aan welke functionaris en aan welk voertuig het randapparaat is toegewezen.

2.1.2 De C2000-randapparatuur wordt tenminste één keer per week gecontroleerd op juistheid en volledigheid. Ontbrekende randapparaten dienen onverwijld aan operationeel beveiligingsbeheer te worden gemeld.

2.1.3 Er behoren regels te worden vastgesteld voor aanvaardbaar gebruik van C2000- randapparatuur.

Deze gedragsregels bevatten ten minste dat:
- C2000-randapparatuur is bestemd voor persoonlijk gebruik.
- C2000-randapparatuur niet onnodig onbeheerd wordt achtergelaten.
- De C2000-randapparatuur voor zakelijk gebruik is en niet bestemd is voor privé doeleinden.
- Alle pogingen tot het misbruik van de apparatuur, zoals het (trachten van) herprogrammeren, openbreken en anderszins manipuleren van het apparaat of de (cryptografische) informatie hierin, strikt verboden is.
- De instructies van de fabrikant ter bescherming van de apparatuur worden opgevolgd (bijvoorbeeld bescherming legen het blootstellen aan elektromagnetische velden).
- De instructies van de beheerder die betrekking hebben op de beveiliging van het C2000-netwerk worden opgevolgd.

Verder bevatten de gedragsregels instructies voor eindgebruikers hoe te handelen in het geval van vermissing van C2000-randapparatuur alsmede de regels voortkomend uit het Landelijk Kader Fleetmap.

2.1.4 De bovenstaande gedragsregels zijn gecommuniceerd naar en voor akkoord verklaard door personen bij eerste ontvangst van C2000-randapparatuur. Daarna zijn zij eenvoudig voor deze personen beschikbaar.

2.1.5 Er is een procedure ingericht die het melden van vermissing, verlies en diefstal van randapparatuur beschrijft. Hierin zijn de contactpersonen en escalatiepaden uitgeschreven. De procedure voorziet in het uitschakelen door de beheerder van vermiste, verloren en gestolen randapparatuur.

2.1.6 Alle personen die C2000-randapparatuur gebruiken krijgen geschikte training en regelmatige bijscholing met betrekking tot informatiebeveiliging en procedures van de organisatie.

2.1.7 De (tijdelijk) niet in gebruik zijnde C2000-randapparatuur (i.e. voorraad, defect) is ondergebracht in afgesloten kasten in een beveiligde ruimte(n). Toegang tot deze ruimte is beperkt tot hiervoor bevoegde personen.

2.2 Beheer C2000 randapparatuur (lokaal beheer)

2.2.1. Alle beheerde C2000-randapparatuur wordt geregistreerd in een actuele inventaris. Hieruit is inzichtelijk welke randapparaten aan welke functionaris en aan welk voertuig is uitgegeven en in welke gespreksgroepen het randapparaat actief kan zijn.

2.2.2 Er wordt geregistreerd welke randapparatuur zich buiten de directe controle van de gebruiker (bijvoorbeeld in het geval van onderhoud, inbouw en reparatie) bevindt.

2.2.3 Wijzigingen in de configuratie (template) van de randapparatuur worden geregistreerd.

2.2.4 Alleen gespreksgroepen waarvoor de gebruiker geautoriseerd is middels het Landelijk Kader Fleetmap of schriftelijke toestemming heeft van de gespreksgroepeigenaar, mogen in een randapparaat van de gebruiker worden geprogrammeerd.

2.2.5 Alle C2000-randapparatuur heeft binnen de organisatie een formele eigenaar die managementverantwoordelijkheid heeft voor het gebruik en informatiebeveiliging van de randapparatuur en die optreedt als centraal aanspreekpunt voor de C2000-apparatuur.

2.2.6 De (tijdelijk) niet in gebruik zijnde C2000-randapparatuur (i.e. voorraad, defect) is ondergebracht in afgesloten kasten in een beveiligde ruimte(n). Toegang tot deze ruimte is beperkt tot hiervoor bevoegde personen.

2.2.7 De toegang tot de beveiligde ruimte(n) wordt geregistreerd.

2.2.8 Datum en tijdstip van aankomst en vertrek van bezoekers worden geregistreerd en bezoekers van de beveiligde ruimte(n) behoren gedurende de gehele periode waarin zij zich in deze ruimte(n) bevinden te worden begeleid en er wordt toezicht gehouden op de uitvoer van werkzaamheden. Aan hen mag alleen toegang worden verleend voor geautoriseerde doeleinden zoals reparatie en onderhoud.

2.2.9 Toegangsrechten tot de beveiligde ruimte(n) worden halfjaarlijks beoordeeld, geactualiseerd en wanneer nodig ingetrokken. Het resultaat van deze controle wordt gedocumenteerd.

2.2.10 De achtergrond van alle lokale beheerders is geverifieerd via een screening equivalent met die voor een Vertrouwensfunctie niveau C, in de zin van de wet Veiligheidsonderzoeken van 10 oktober 1996.

2.2.11 Alle personen die C2000-randapparatuur beheren krijgen geschikte training en regelmatige bijscholing met betrekking tot informatiebeveiliging en procedures van de organisatie, relevant voor hun werkgebied.

2.2.12 Slechts C2000 geaccrediteerde randapparatuur mag worden gebruikt. Randapparatuur mag alleen worden aangeschaft van een geaccrediteerde leverancier, met een TEA2 supplier licentie.

2.2.13 Er is een procedure aanwezig voor de in- en uitbouw van randapparatuur uit voer-, vaar- en vliegtuigen. In- en uitbouw geschiedt enkel bij geaccrediteerde bedrijven.

2.2.14 Randapparaten die aan een organisatie of persoon worden verstrekt die niet geautoriseerd is

voor het gebruik van C2000, zijn uitgeschakeld in het netwerk of bevatten geen geldige cryptosleutel.

2.2.15 Het (tijdelijk) blokkeren van het C200- randapparaat vindt volgens de door de beheerder gespecificeerde procedure plaats te vinden.

2.2.16 Het uitvoeren van cryptografische handelingen aan C2000-randapparatuur (laden/verwijderen van sleutels en het programmeren van C2000-randapparatuur) is in overeenstemming met de instructies, in de Documentatieset Lokaal Cryptomanagement.

2.2.17 Programmeermiddelen voor het laden van sleutels in C2000 randapparatuur worden dagelijks, wanneer deze niet direct in gebruik zijn, opgeborgen in kluizen.

2.3 Gebruik C2000 meldkamer- en beheersystemen (lokaal beheer)

2.3.1 De achtergrond van alle lokale beheerders is geverifieerd via een screening equivalent met die voor een Vertrouwensfunctie niveau C, in de zin van de wet Veiligheidsonderzoeken van 10 oktober 1996.

2.3.2 Alle personen die C2000-apparatuur gebruiken en beheren krijgen geschikte training en regelmatige bijscholing met betrekking tot de beveiliging en procedures van het C2000-communicatienetwerk.

2.3.3 De apparatuurruimte(n) waarin C2000-systeemapparatuur is ondergebracht (exclusief de radio bedienterminals en -werkplekken) dienen te voldoen aan de eisen gesteld in het document Programma van eisen apparatuurruimtes t.b.v. C2000 radiobediensystemen.

2.3.4 De toegang tot de beveiligde ruimte(n) wordt geregistreerd.

2.3.5 Er is een bezoekersregeling waarin datum en tijdstip van aankomst en vertrek van bezoekers worden geregistreerd. Bezoekers van de meldkamer en apparatuurruimte(n) behoren gedurende de gehele periode waarin zij zich in deze ruimte(n) bevinden te worden begeleid.

2.3.6 Toegangsrechten tot de beveiligde ruimte(n) worden halfjaarlijks beoordeeld, geactualiseerd en als nodig ingetrokken. Het resultaat van deze controle wordt gedocumenteerd.

2.3.7 De meldkamer- en apparatuurruimte(n) zijn 7 dagen per week, 24 uur per dag voor de beheerder toegankelijk conform de bezoekersregeling van de aangewezen gebruiker.

2.3.8 Het radiobediensysteem en de hierbij behorende servers en netwerkcomponenten zijn aangesloten op een UPS en noodstroomgenerator met een autonomietijd van 8 uur om de C2000-functionaliteiten te beschermen tegen storingen ten gevolge van uitval van de stroomvoorziening.

2.3.9 De C2000 apparatuur is beveiligd tegen blikseminslag en spanningspieken.

2.3.10 Op de beheersystemen wordt gebruik gemaakt van unieke identificaties (ID) zodat lokale beheerders kunnen worden gekoppeld aan en verantwoordelijk kunnen worden gesteld voor hun handelingen. Lokale beheerders dienen te allen tijde gebruik te maken van hun eigen identificatie.

2.3.11 Wireless Dispatch Systemen die ook gekoppeld zijn aan het C2000 communicatienetwerk anders dan via de TETRA air-interface mogen slechts in ruimten worden opgesteld die voldoen aan de eisen voor apparatuurruimten (zie punt 2.3.3).

2.3.12 Wireless Dispatch Systemen die alleen gekoppeld zijn aan hel C2000 communicatienetwerk via de TETRA air-interface dienen te worden behandeld als C2000 randapparatuur.

2.4 Algemene maatregelen voor leveranciers van gebruikers (Type I)

2.4.1 Indien de leverancier een private rechtspersoon is, dan toont deze zijn integriteit aan door de overhandiging van een geldige Verklaring Omtrent het Gedrag Rechtspersonen (VOGR) aan de gebruiker. Als de geldigheid van de VOGR verloopt, is de leverancier verplicht een nieuwe te overhandigen aan de gebruiker. Deze verplichting wordt contractueel geborgd.

2.4.2 De locatie(s) waar C2000 middelen (al dan niet in een voertuig) worden opgeslagen zijn beveiligd.
Het totaal aan inbraakwerende en vertragende maatregelen dient te voldoen aan de maatregelen behorend bij het risiconiveau 3 volgens de verbeterde risicoklasse indeling (VRKI) van hel Nationaal Centrum voor Preventie.

2.4.3 De leverancier overlegt op verzoek van de gebruiker een actuele lijst die de namen bevat van alle medewerkers die door de leverancier geautoriseerd zijn werkzaamheden in het kader van het afgesloten onderhoudscontract uit te voeren. Hieronder vallen ook tijdelijke medewerkers en medewerkers van onderaannemers.

TOELICHTING

Algemeen

Artikelsgewijze toelichting

Artikel 1

Het C2000 communicatienetwerk bestaat uit twee netwerken; het T2000 en het P2000 netwerk.

In hoofdlijn zijn drie partijen betrokken bij het C2000-communicatienetwerk:
- De beheerder van het communicatienetwerk, een rol die belegd is bij het onderdeel Unit Meldkamer Systemen (UMS) van de voorziening tot samenwerking Politie Nederland (vtsPN);
- De gebruikers van het communicatienetwerk;
- De eigenaar van het communicatienetwerk die de Staat der Nederlanden vertegenwoordigt mede namens de Minister Defensie en de Minister van Volksgezondheid, Welzijn en Sport. Deze rol is belegd is bij het ministerie van Veiligheid en Justitie (VenJ).

Artikel 2

Dit beleid geeft nadrukkelijk geen invulling voor de beveiliging van bijzondere informatie (departementaal vertrouwelijke informatie en staatsgeheimen), zoals gedefinieerd in het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI)uit 2004. Dit betekent dat gebruikers die van het C2000-communicatienetwerk gebruik willen maken voor het communiceren van bijzondere informatie, de vereisten, opgelegd vanuit het VIR-BI, additioneel implementeren.
Voor dit beleid is gekozen de methodiek van de norm NEN-ISO/IEC 27001:2005 (Managementsystemen voor informatiebeveiliging) te volgen, zoals ook is geadopteerd in het Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR2007).
Behalve de eisen voortvloeiend uit dit informatiebeveiligingsbeleid, zijn er wettelijke eisen gesteld aan de beveiliging van gegevens en informatiesystemen. Het informatiebeveiligingsbeleid C2000 beoogt in lijn te zijn met deze wetten, in het bijzonder de Wet Bescherming persoonsgegevens, de Wet politiegegevens, de Wet op de Geneeskundige Behandelingsovereenkomst, de Wet computercriminaliteit, het Burgerlijk Wetboek, de Telecommunicatiewet, de Wet justitiële en strafvorderlijke gegevens, de Archiefwet en het Wetboek van Strafvordering.

De strategisch beheerder stelt beveiligingsmaatregelen op die voor alle gebruikers van toepassing zijn.
De vanuit dit beleid gestelde, beveiligingsmaatregelen voor gebruikers hebben in beginsel ten doel om gebruikeroverschrijdende risico's te beheersen.
Het is de eigen verantwoordelijkheid van gebruikers om een afweging te maken of naast de maatregelen uit het informatiebeveiligingsbeleid C2000 additionele beveiligingsmaatregelen benodigd zijn.
De beheerder wordt door de strategisch beheerder beveiligingseisen opgelegd waaraan de informatiebeveiliging van het C2000-communicatienetwerk moet voldoen.
Voor zover de beheerder zelf gebruikerstaken uitvoert (bijvoorbeeld het beheer van randapparatuur voor zichzelf en bijzondere gebruikers), is de beheerder gebonden aan dezelfde beveiligingsmaatregelen als die van toepassing zijn op de gebruikers. De beheerder vertaalt middels zijn eigen risicobeheersingproces deze beveiligingseisen in concrete beveiligingsmaatregelen. De effectiviteit van dit risicobeheersingproces wordt jaarlijks getoetst door de eigenaar.

Artikel 4

Het gebruik van randapparatuur omvat voor de aangewezen gebruikers minimaal de volgende taak:
- ontvangst en retournering van randapparatuur.
  Beveiligingsdoelstellingen ten aanzien van het gebruik van C2000 randapparatuur:
- het C2000 communicatienetwerk mag niet worden verstoord door verkeerd gebruik;
- toegang van ongeautoriseerde personen; toegang tot de randapparatuur wordt voorkomen, zowel tijdens werkzaamheden, als bij transport en opslag;
- de beheerder beschikt over een actuele inventarisatie van verloren of gestolen randapparatuur.

Uit pragmatische overwegingen is het een regionale aangewezen gebruiker toegestaan deze taak in zijn geheel over te dragen aan een andere aangewezen gebruiker uit dezelfde regio. Er is hiertoe goedkeuring van beide partijen nodig; de verantwoordelijkheden voor informatiebeveiliging zijn evenwel niet overdraagbaar.

Het beheer van C2000- randapparatuur omvat voor de aangewezen gebruikers de volgende taken:
- de uitgifte, inname en reparatie van randapparatuur;
- in- en uitbouw van C2000 randapparatuur in voertuigen;
- het bekend maken van randapparatuur aan het netwerk ten behoeve van eindgebruikers;
- het instrueren van de eindgebruikers;
- het voeren van een administratie van randapparatuur;
- het fysiek beschermen van nog niet uitgegeven of niet in gebruik zijnde randapparatuur;
- het programmeren van randapparatuur;
- het melden van vermiste en gestolen randapparatuur aan de beheerder.
- het aanschaffen en vernietigen van randapparatuur;
- het aanvragen, transporteren, opslaan, laden en verwijderen van cryptografische sleutels (lokaal cryptomanagement);
- het terugmelden van TEI en TEA2 sleutel combinaties aan de beheerder.

Deze taken maken deel uit van het lokaal beheer van de aangewezen gebruiker.

Beveiligingsdoelstellingen ten aanzien van het beheer van C2000-randapparatuur:
- alleen geautoriseerde personen wordt toegang verschaft tot randapparatuur.
- de geautoriseerde eindgebruikers worden voorzien van foutenvrije randapparatuur;
- de geautoriseerde personen communiceren uitsluitend binnen die gespreksgroepen waarvoor zij geautoriseerd zijn;
- het C2000 communicatienetwerk mag niet worden verstoord door (onopzettelijk) verkeerd gebruik;
- toegang tot randapparatuur door ongeautoriseerde personen wordt voorkomen;
- het lokaal cryptomanagement vindt plaats in overeenstemming met de Documentatieset Lokaal Cryptomanagement.

Het gebruik van C2000 meldkamer- en beheersystemen omvat voor de aangewezen gebruikers de volgende taken:
- de communicatie met en aansturing van eindgebruikers in het veld via spraak, data (T2000) en alarmeringen (P2000);
- de communicatie met de overige OOV meldkamers;
- hosten van C2000 meldkamersystemen voor de Beheerder in een veilige en betrouwbare omgeving;
- het beheer van de eigen gespreksgroepen (naamgeving);
- het beheer van gebruiksinstellingen in het systeem;
- het inrichten van veilige externe koppelingen.

Deze taken maken deel uit van het lokaal beheer van de aangewezen gebruiker.

Beveiligingsdoelstellingen ten aanzien van het gebruik van C2000-meldkamer- en beheersystemen:
- alleen geautoriseerde personen hebben toegang tot de C2000 meldkamer- en beheersystemen;
- alleen de eigen gespreksgroepen en instellingen worden beheerd;
- het C2000-communicatienetwerk wordt niet verstoord door verkeerd gebruik;
- de C2000-meldkamer- en beheersystemen bevinden zich in een fysiek veilige omgeving;
- de integriteit en continuïteit van de gebruiksinstellingen is gewaarborgd.

De beheerder is verantwoordelijk voor het beheer van de C2000 meldkamersystemen bij de aangewezen gebruiker maar is hierbij wel afhankelijk van de aangewezen gebruiker voor het nemen van bepaalde beveiligingsmaatregelen, met name fysieke. Deze beveiligingsmaatregelen maken daarom deel uit van de beveiligingsmaatregelen opgelegd aan de aangewezen gebruiker beschreven in Bijlage 2.
Wijzigingen in de netwerkomgeving van de C2000-meldkamer- en beheersystemen (bijvoorbeeld externe koppelingen) worden door de beheerder geaccrediteerd.

Uit pragmatische ovenwegingen is het een regionale aangewezen gebruiker toegestaan deze taak in zijn geheel over te dragen aan een andere aangewezen gebruiker uit dezelfde regio. Hiertoe is de goedkeuring van beide partijen nodig en is het slechts toegestaan in het geval van een gedeelde (gecolokeerde) meldkamer; de verantwoordelijkheden voor informatiebeveiliging zijn evenwel niet overdraagbaar.

Artikel 5

Vanuit informatiebeveiliging kunnen twee typen leveranciers worden onderscheiden:
I. In- en uitbouw van C2000 randapparatuur in voertuigen.
II. Uitgifte, inname en reparatie van C2000 randapparatuur in combinatie met het programmeren en het uitvoeren van lokaal cryptomanagement van de betreffende randapparatuur.

In het geval van een leverancier type I controleert de aangewezen gebruiker dat de leverancier voldoet aan de algemene leverancierseisen uit Bijlage 2. De aangewezen gebruiker meldt daarnaast aan de beheerder welke leverancier wordt gebruikt voor in- en uitbouw van C2000-randapparatuur en het resultaat van de door de aangewezen gebruiker uitgevoerde controle tegen de maatregelen in Bijlage 2.

Leveranciers type II dienen geaccrediteerd te worden door de eigenaar.

De type I leverancierseisen uit Bijlage 2 vormen de eerste basis voor de accreditatie eisen. Daarnaast worden aan deze leveranciers die taken met betrekking tot lokaal cryptomanagement het programmeren van C2000-randapparatuur uitvoeren, additionele eisen gesteld conform de Documentatieset Lokaal Cryptomanagement en de beveiligingseisen voor het laden van cryptosleutels.

De aangewezen gebruiker dwingt in contracten met leveranciers voor het uitvoeren van bovengenoemde taken de implementatie van de hier genoemde maatregelen af en verzekert medewerking van de leverancier bij een mogelijke periodieke controle.

Artikel 6

Voor de accreditatie wordt de aspirant bijzondere gebruiker door de beheerder getoetst op naleving van de uit dit beleid verplichte beveiligingsmaatregelen (in Bijlage 2). Na een succesvol doorlopen toets zal de beheerder de toetsingsrapportage met een positief advies aan de eigenaar voorleggen. De eigenaar beslist vervolgens de bijzondere gebruiker al dan niet te accrediteren en dientengevolge toe te laten. Zodra de bijzondere gebruiker is toegelaten dient hij te voldoen aan alle verplichtingen uit dit beleid, waaronder implementatie van beveiligingsmaatregelen, rapportage en controle.

Het gebruik van randapparatuur omvat voor de bijzondere gebruikers de volgende taken:
- dagelijks gebruik van C2000-randapparatuur tijdens werkzaamheden;
- (korte termijn) opslag van toegelaten randapparatuur, bijvoorbeeld op de momenten dat de medewerker geen dienst heeft;
- ontvangst en retournering van randapparatuur.

Beveiligingsdoelstellingen ten aanzien van het gebruik van C2000-randapparatuur door de bijzondere gebruiker:
- het C2000-communicatienetwerk mag niet worden verstoord door (onopzettelijk) verkeerd gebruik;
- voorkomen moet worden dat ongeautoriseerde personen toegang krijgen tot randapparatuur, zowel tijdens werkzaamheden, als transport en opslag;
- de beheerder dient te beschikken over een actuele inventarisatie van verloren of gestolen randapparatuur.

In Bijlage 2 zijn deze beveiligingsdoelstellingen vertaald naar concrete maatregelen, die de bijzondere gebruikers implementeren.

Het beheer van randapparatuur voor de bijzondere gebruikers wordt uitgevoerd door de beheerder. Dit omvat de volgende taken:
- de uitgifte, inname en reparatie van randapparatuur;
- het bekend maken van randapparatuur aan het netwerk ten behoeve van eindgebruikers (subscriberbeheer);
- het voeren van een administratie van randapparatuur;
- het programmeren van randapparatuur;
- het aanschaffen en vernietigen van randapparatuur.

De volgende taken zijn belegd bij de bijzondere gebruiker zelf:
- in- en uitbouw van C2000-randapparatuur in voertuigen;
- het instrueren van de eindgebruikers;
- het voeren van een administratie van randapparatuur;
- het fysiek beschermen van nog niet uitgegeven of niet in gebruik zijnde randapparatuur;
- het melden van vermiste en gestolen randapparatuur aan de beheerder.

Beveiligingsdoelstellingen ten aanzien van het beheer van randapparatuur voor de bijzondere gebruiker:
- alleen geautoriseerde personen wordt toegang verschaft tot randapparatuur;
- de geautoriseerde eindgebruikers worden voorzien van foutenvrije randapparatuur;
- de geautoriseerde personen kunnen uitsluitend communiceren binnen die gespreksgroepen waarvoor zij geautoriseerd zijn;
- het C2000-communicatienetwerk mag niet worden verstoord door (onopzettelijk) verkeerd gebruik;

- voorkomen moet worden dat ongeautoriseerde personen toegang krijgen tot randapparatuur.

In Bijlage 2 zijn deze beveiligingsdoelstellingen vertaald naar concrete maatregelen, die de bijzondere gebruikers implementeren.

De bijzondere gebruiker mag één C2000 beveiligingsgerelateerde taak uitbesteden aan leveranciers. Het betreft de volgende taak:
- in- en uitbouw van C2000 randapparatuur in voertuigen.

De bijzondere gebruiker controleert dat de leverancier voldoet aan de algemene leverancierseisen uit Bijlage 2. De bijzondere gebruiker meldt daarnaast aan de beheerder welke leverancier wordt gebruikt voor in- en uitbouw van C2000-randapparatuur en het resultaat van de door de bijzondere gebruiker uitgevoerde controle tegen de maatregelen in Bijlage 2.

De bijzondere gebruiker dwingt in contracten met leveranciers voor het uitvoeren van bovengenoemde taak de implementatie van de hier genoemde maatregelen af en verzekert medewerking van de leverancier bij een mogelijke periodieke controle.

De bijzondere gebruiker belegt het beheer van zijn randapparatuur en het beheer van zijn gespreksgroepen bij de beheerder.

Anders dan voor aangewezen gebruikers is het de bijzondere gebruiker niet toegestaan zelf lokaal cryptomanagement uit te voeren. Dit wordt door de beheerder uitgevoerd in opdracht van de eigenaar.

Artikel 7

Het gebruik van randapparatuur omvat voor de beheerder de volgende taak:
- ontvangst en retournering van randapparatuur.

Beveiligingsdoelstellingen ten aanzien van het gebruik van randapparatuur door de beheerder:
- het C2000-communicatienetwerk mag niet worden verstoord door verkeerd gebruik;
- voorkomen moet worden dat ongeautoriseerde personen toegang krijgen tot randapparatuur, zowel tijdens werkzaamheden, als transport en opslag;
- de beheerder dient te beschikken over een actuele inventarisatie van verloren of gestolen randapparatuur.

In Bijlage 2 zijn deze beveiligingsdoelstellingen vertaald naar concrete maatregelen, die ook voor de beheerder van toepassing zijn.

De beheerder maakt als onderdeel van zijn beheertaken ook zelf gebruik van randapparatuur.

Het beheer van randapparatuur omvat voor de beheerder de volgende taken:
- de uitgifte, inname en reparatie van randapparatuur;
- in- en uitbouw van C2000-randapparatuur In voertuigen;
- het bekend maken van randapparatuur aan het netwerk ten behoeve van eindgebruikers;
- het instrueren van de eindgebruikers;
- het voeren van een administratie van randapparatuur;
- het fysiek beschermen van nog niet uitgegeven of niet in gebruik zijnde randapparatuur;
- het programmeren van randapparatuur;
- het melden van vermiste en gestolen randapparatuur;
- het aanschaffen en vernietigen van randapparatuur;
- het aanvragen, transporteren, opslaan, laden en verwijderen van cryptografische sleutels (ook lokaal cryptomanagement voor bijzondere gebruikers).

Beveiligingsdoelstellingen ten aanzien van het gebruik van randapparatuur door de beheerder:
- alleen geautoriseerde personen wordt toegang verschaft tot randapparatuur;
- de geautoriseerde eindgebruikers worden voorzien van foutenvrije randapparatuur;
- de geautoriseerde personen kunnen uitsluitend communiceren binnen die gespreksgroepen waarvoor zij geautoriseerd zijn;
- het C2000-communicatienetwerk mag niet worden verstoord door (verkeerd gebruik;
- voorkomen wordt dat ongeautoriseerde personen toegang krijgen tot randapparatuur.

Het lokaal cryptomanagement vindt plaats in overeenstemming met de Documentatieset Lokaal Cryptomanagement.

In Bijlage 2 zijn deze beveiligingsdoelstellingen vertaald naar concrete maatregelen, die ook voor de beheerder van toepassing zijn.

Zoals alle partijen binnen het C2000-communicatienetwerk dient ook de beheerder de algemene maatregelen uit Bijlage 2 te implementeren.

Het gebruik van randapparatuur omvat voor de beheerder de volgende taken:
- dagelijks gebruik van C2000-randapparatuur tijdens werkzaamheden.
- (korte termijn) opslag van toegelaten randapparatuur, bijvoorbeeld op de momenten dat de medewerker geen dienst heeft.
- ontvangst en retournering van randapparatuur.

Beveiligingsdoelstellingen ten aanzien van het gebruik van randapparatuur door de beheerder:
- het C2000-communicatienetwerk mag niet worden verstoord door verkeerd gebruik;
- voorkomen moet worden dat ongeautoriseerde personen toegang krijgen tot randapparatuur, zowel tijdens werkzaamheden, als transport en opslag;
- de beheerder beschikt over een actuele inventarisatie van verloren en gestolen randapparatuur.

In Bijlage 2 zijn deze beveiligingsdoelstellingen vertaald naar concrete maatregelen, die ook voor de beheerder van toepassing zijn.

De beheerder maakt als onderdeel van zijn beheertaken ook zelf gebruik van randapparatuur.

Het beheer van randapparatuur omvat voor de beheerder de volgende taken:
- de uitgifte, inname en reparatie van randapparatuur;
- in- en uitbouw van C2000-randapparatuur In voertuigen;
- het bekend maken van randapparatuur aan het netwerk ten behoeve van eindgebruikers;
- het instrueren van de eindgebruikers;
- het voeren van een administratie van randapparatuur;
- het fysiek beschermen van nog niet uitgegeven en niet in gebruik zijnde randapparatuur;
- het programmeren van randapparatuur;
- het melden van vermiste en gestolen randapparatuur;
- het aanschaffen en vernietigen van randapparatuur;
- het aanvragen, transporteren, opslaan, laden en verwijderen van cryptografische sleutels (ook lokaal cryptomanagement voor bijzondere gebruikers).

Beveiligingsdoelstellingen ten aanzien van het gebruik van randapparatuur door de beheerder:
- alleen geautoriseerde personen wordt toegang verschaft tot randapparatuur;
- de geautoriseerde eindgebruikers worden voorzien van foutenvrije randapparatuur;
- de geautoriseerde personen kunnen uitsluitend communiceren binnen die gespreksgroepen waarvoor zij geautoriseerd zijn;
- het C2000-communicatienetwerk mag niet worden verstoord door verkeerd gebruik;
- voorkomen moet worden dal ongeautoriseerde personen toegang krijgen tot randapparatuur.

Het lokaal cryptomanagement vindt plaats in overeenstemming met de Documentatieset Lokaal Cryptomanagement.
In Bijlage 2 zijn deze beveiligingsdoelstellingen vertaald naar concrete maatregelen, die ook voor de beheerder van toepassing zijn.

Het voeren van cryptomanagement behelst de volgende taken:
- beheer van sleutelmateriaal voor C2000-randapparatuur;
- het genereren en leveren van TEA2 sleutelmateriaal aan partijen die C2000- randapparatuur beheren;
- het toelaten van het randapparaat op het C2000-communicatienetwerk nadat gebruiker gemeld heeft dat de betreffende sleutel geladen is;
- het uitsluiten van randapparatuur van het C2000-communicatienetwerk op aanwijzen van operationeel beveiligingsbeheer;
- het voeren van een sluitende administratie voor teruggemelde en geactiveerde TEI -TEA2 sleutel combinaties voor randapparatuur;
- het beheer en toezicht op naleving van TEA2 fabrikant, leverancier en gebruikers licenties.

Beveiligingsdoelstellingen ten aanzien van cryptomanagement:
- de juistheid van verstrekt sleutelmateriaal is verzekerd, daarnaast wordt sleutelmateriaal slechts aan geautoriseerde personen verstrekt;

- verzoeken tot toelating of uitsluiting van een randapparaat dienen door de beheerder te worden uitgevoerd. Het verzoek kan alleen worden gedaan door een daartoe geautoriseerde persoon. Dit dient door de beheerder te worden gecontroleerd.

De beheerder vervult deze taak voor zichzelf (de beheerder is zelf ook een beperkte C2000 gebruiker) en gedeeltelijk voor de bijzondere gebruikers (het laden en verwijderen van cryptografische sleutels). Voor bijzondere gebruikers wordt dit gedaan in opdracht van de eigenaar.

Gezien de technische complexiteit en het groot aantal middelen is er voor gekozen om de beheerder zijn eigen risicobeheersingproces te laten opstellen. Aan het uitvoeren van deze taken worden daarom beveiligingseisen gesteld. Deze zijn in een separaat document vastgelegd. De beheerder vertaalt zelf deze beveiligingseisen in beveiligingsmaatregelen. Hierbij wordt rekening gehouden met de verplichte beveiligingsmaatregelen voor gebruikers in Bijlage 2 van dit beleid, zodat er geen overlap en hiaten ontstaan.

De beveiligingsmaatregelen van de beheerder en de onderbouwing hiervan ('Verklaring van Toepasselijkheid' in de terminologie van NEN-ISO/IEC 27001:2005) worden ter goedkeuring aan de eigenaar voorgelegd. Bij akkoord worden deze maatregelen geïmplementeerd en rapporteert de beheerder hierover.

Zoals alle partijen binnen het C2000-communicatienetwerk dient ook de beheerder de algemene maatregelen uit Bijlage 2 te implementeren.

Artikel 8

Leidend voor de verantwoordelijkheden aangaande beheertaken, is de geldende demarcatie tussen lokaal en centraal beheer.

Het gebruik van C2000-beheersystemen omvat voor de beheerder de volgende taken:
- het beheer van de gespreksgroepen;
- het beheer van de gebruiksinstellingen in het systeem;
- het inrichten van een veilige en betrouwbare netwerkomgeving voor de beheersystemen inclusief veilige externe koppelingen.

Beveiligingsdoelstellingen ten aanzien van het gebruik van C2000-beheersystemen:
- slechts geautoriseerde personen hebben toegang tot de C2000 beheer- en meldkamersystemen;
- slechts de eigen gespreksgroepen en instellingen mogen worden beheerd;
- het C2000-communicatienetwerk mag niet worden verstoord door verkeerd gebruik;
- de integriteit en continuïteit van de gebruiksinstellingen is gewaarborgd.

In Bijlage 2 zijn deze beveiligingsdoelstellingen vertaald naar concrete maatregelen, die voor zover relevant voor C2000-beheersystemen ook voor de beheerder van toepassing zijn.

Het beheer van C2000-meldkamersystemen behelst voor de beheerder de volgende taken:
- onderhoud van hardware en software van de C2000-meldkamersystemen;
- testen en toepassen van patches;
- testen en toepassen van upgrades;
- testen en vervangen van componenten;
- ondersteuning bij incidenten;
- functioneel beheer C2000-meldkamersystemen;
- afstemming met en toezicht op leveranciers.

Beveiligingsdoelstellingen ten aanzien van het beheer van C2000-meldkamersystemen:
- slechts geautoriseerde personen hebben logische toegang tot de C2000- meldkamer- en beheersystemen;
- de achtergrond van deze personen is geverifieerd en ze zijn afdoende opgeleid;
- de systemen zijn betrouwbaar (redundantie, virusbescherming);
- de continuïteit van de systemen is gewaarborgd;
- de hard- en software is getest en wordt adequaat onderhouden.

Het beheer van C2000-infrastructuur behelst de volgende taken:
- onderhoud van hardware en software van de C2000-infrastructuur;
- testen en toepassen van patches;
- testen en toepassen van upgrades ;
- testen en vervangen van componenten;
- ondersteuning bij incidenten;

- beheer energievoorziening;
- beheer datalijnen;
- beheer van gerelateerd vastgoed;
- afstemming met en toezicht op leveranciers;
- het hebben en uitvoeren van back-up en herstel procedures;
- het borgen van de kwaliteit van deze taken middels een kwaliteitssysteem.

Beveiligingsdoelstellingen ten aanzien van het beheer van het C2000-infrastructuur:
- slechts geautoriseerde personen hebben fysieke of logische toegang tot (componenten van) de C2000-infrastructuur;
- de achtergrond van deze personen is geverifieerd en ze zijn afdoende opgeleid;
- de systemen zijn betrouwbaar (redundantie, virusbescherming);
- de continuïteit van de systemen is gewaarborgd;
- de hard- en software is getest en wordt adequaat onderhouden;
- C2000-communicatie mag niet worden afgeluisterd, onderschept of verstoord.

Het voeren van netwerk beheer behelst de volgende taken:
- beheer configuratiegegevens;
- monitoring en controle van het netwerk en applicaties;
- het optimaliseren van netwerkparameters.

Beveiligingsdoelstellingen ten aanzien van het netwerkbeheer:
- slechts geautoriseerde wijzigingen op de fleetmap en overige componenten dienen te worden uitgevoerd;
- beveiligingsincidenten dienen vroegtijdig gesignaleerd en geadresseerd te worden. De beheerder stemt beveiligingsincidenten, maatregelen en verbetervoorstellen af in het gebruikers beveiligings-overzicht.

De beheerder vervult deze taak voor zichzelf (de beheerder is zelf ook een beperkte C2000 gebruiker) en voor de bijzondere gebruikers. Voor bijzondere gebruikers wordt dit gedaan in opdracht van de eigenaar.

De beheerder voert deze taak uit voor de aangewezen gebruikers die de enigen zijn die beschikking hebben over een C2000-meldkamer.

Ten aanzien van accreditatie-eisen en het uitvoeren van de accreditatietoetsing gelden de volgende taken:
- uitvoeren van accreditatietoetsingen voor externe koppelingen, SCL's, randapparatuur gebruikers en leveranciers;
- actueel houden van accreditatievoorwaarden voor externe koppelingen, SCL's, randapparatuur, gebruikers en leveranciers, door het doen van wijzigingsvoorstellen naar de eigenaar.

Beveiligingsdoelstellingen ten aanzien van accreditatie:
- slechts externe koppelingen, randapparatuur, SCL's, leveranciers en gebruikers, die de informatie-beveiliging van het C2000-communicatienetwerk niet negatief beïnvloeden, worden toegelaten;
- slechts partijen met een geschikte TEA2 licentie mogen gebruik maken van en/of beheervoeren over C2000-randapparatuur.

Het uitgangpunt van accreditatie is dat de informatiebeveiliging van het C2000- communicatienetwerk niet negatief mag worden beïnvloed bij toelating van een nieuwe partij, apparaat en koppeling. Het accreditatie proces is als volgt opgebouwd:
Het stellen van voorwaarden voor de toelating van nieuwe partijen, apparaten en koppelingen binnen het C2000 communicatienetwerk:
- o externe koppelingen;
- o SCL's;
- o randapparatuur (namelijk de CTK);
- o gebruikers;
- o leveranciers.

Het proces kent een toetsende organisatie (de beheerder) die partijen, apparaten en koppelingen toetst aan de toelatingsvoorwaarden en hierover rapporteert aan de beslissende organisatie (eigenaar) die op basis hiervan een beslissing neemt omtrent toelating.

Bij reeds geaccrediteerde partijen, apparaten en koppelingen worden periodiek ook herhalingsonder-zoeken uitgevoerd. Reeds toegelaten randapparatuur en SCL's worden in beginsel alleen opnieuw

getoetst als sprake is van significante veranderingen, dit ter beoordeling van de beheerder, op basis van de beschrijving van de veranderingen.

De herhalingsonderzoeken voor gebruikers vinden plaats door middel van de implementatieaudits. Externe koppelingen en leveranciers worden periodiek onderworpen aan een nieuwe toetsing. Hierbij ligt de nadruk op wijzigingen sinds de vorige toetsing en beveiligingsincidenten in de afgelopen periode. Door de toetsende organisatie wordt gerapporteerd aan de eigenaar die op basis hiervan een beslissing neemt omtrent de continuering van de toelating.

De C2000 ToelatingsKeuring (CTK) maakt onderdeel uit van het accrediteren van randapparatuur. De eigenaar herziet de toelatingsvoorwaarden op basis van voortschrijdend inzicht. De periodieke controle van geaccrediteerde leveranciers en koppelingen vindt steekproefsgewijs plaats, in beginsel om de drie jaar.
De beheerder adviseert over de accreditatievoorwaarden aan de eigenaar en voert de accreditatietoetsing uit na vaststelling van deze voorwaarden door de eigenaar.

Artikel 9

Het Operationeel Beveiligingsbeheer omhelst de volgende taken:
- het opzetten en implementeren van een raamwerk voor het vastleggen van beveiligingsrelevante gebeurtenissen binnen het C2000- communicatienetwerk en op basis daarvan het vroegtijdig signaleren van beveiligingsincidenten;
- het verzamelen en analyseren van beveiligingsincidenten van partijen betrokken bij het C2000 communicatienetwerk, met name de gebruikers en de beheerder;
- het reageren op beveiligingsincidenten, om zo de schade van deze incidenten zo veel mogelijk te beperken;
- de aggregatie van beveiligingsincidenten en rapportages daarover aan de eigenaar;
- het voorbereiden van wijzigingen in dit beleid in de vorm van nieuwe maatregelen;
- het opzetten van een gebruikers beveiligingsoverleg waar zij hun ervaringen en zorgen kunnen uitspreken en dat minimaal jaarlijks bijeenkomt. Het voorzitterschap van dit overleg en de notulering daarvan is belegd bij Operationeel Beveiligingsbeheer.

Beveiligingsdoelstellingen ten aanzien van Operationeel Beveiligingsbeheer:
- de impact op het C2000-communicatienetwerk van beveiligingsincidenten door middel van adequaat incidentenbeheer dient beperkt te blijven.
- het proactief en reactief signaleren van ontwikkelingen aan Strategisch Beveiligingsbeheer in de informatiebeveiliging van het C2000- communicatienetwerk, waardoor adequate bijsturing mogelijk is.

Taken en verantwoordelijkheden van de eigenaar:
- nemen van accreditatiebeslissingen voor externe koppelingen, SCL's, randapparatuur, gebruikers en leveranciers;
- vaststellen van accreditatievoorwaarden voor externe koppelingen, SCL's, randapparatuur, gebruikers en leveranciers.

Beveiligingsdoelstelling ten aanzien van taken en verantwoordelijkheden van de eigenaar:
- slechts externe koppelingen, randapparatuur, SCL's, leveranciers en gebruikers, die de informatiebeveiliging van het C2000-communicatienetwerk niet negatief beïnvloeden, worden toegelaten.

Operationeel beveiligingsbeheer analyseert de beschikbare beveiligingsincidenten en rapporteert hier maandelijks over aan het strategisch beveiligingsbeheer. Deze analyse omvat ook een analyse van de beveiligingsincidenten relevant voor C2000 beschreven in de literatuur en de media.
Kritische beveiligingsincidenten van het C2000 communicatienetwerk worden direct gemeld bij strategisch beveiligingsbeheer.

Het uitgangpunt van accreditatie is dat de informatiebeveiliging van het C2000- communicatienetwerk niet negatief mag worden beïnvloed bij toelating van een nieuwe partij, apparaat of koppeling.

Het accreditatieproces is als volgt opgebouwd:
Het stellen van toelatingsvoorwaarden voor de toelating van nieuwe partijen, apparaten en koppelingen binnen het C2000-communicatienetwerk:
- externe koppelingen
- SCL's
- randapparatuur (namelijk de CTK)
- gebruikers
- leveranciers

Het proces kent een toetsende organisatie die partijen, apparaten en koppelingen toetst aan de toelatingsvoorwaarden en hierover rapporteert aan de beslissende organisatie (eigenaar) die op basis hiervan een beslissing neemt omtrent toelating.
Bij reeds geaccrediteerde partijen, apparaten of koppelingen worden periodiek ook herhalingsonderzoeken uitgevoerd. Reeds toegelaten randapparatuur en SCL's worden in beginsel alleen opnieuw getoetst als sprake is van significante veranderingen, dit ter beoordeling van de beheerder, op basis van de beschrijving van de veranderingen.

De diepgang van de hernieuwde toetsing is afhankelijk van de omvang van deze veranderingen. De herhalingsonderzoeken voor gebruikers vinden plaats door middel van de implementatieaudits. Externe koppelingen en leveranciers worden periodiek onderworpen aan een nieuwe toetsing. Hierbij ligt de nadruk op wijzigingen sinds de vorige toetsing en beveiligingsincidenten in de afgelopen periode, Door de toetsende organisatie wordt gerapporteerd aan de eigenaar die op basis hiervan een beslissing neemt omtrent de continuering van de toelating.

De C2000 ToelatingsKeuring (CTK) maakt onderdeel uit van het accrediteren van randapparatuur. De eigenaar herziet de toelatingsvoorwaarden op basis van voortschrijdend inzicht. De periodieke controle van geaccrediteerde leveranciers en koppelingen vindt steekproefsgewijs plaats, in beginsel om de drie jaar.
De eigenaar neemt hierbij de accreditatiebeslissing en stelt de accreditatievoorwaarden vast.

Artikel 10

De informatiebeveiliging van het C2000-communicatienetwerk blijft op langere termijn gewaarborgd. Dit wordt bereikt door middel van het strategisch beveiligingsbeheer dat door de eigenaar wordt uitgevoerd. In dit proces wordt toegezien op de effectiviteit en implementatie van de beveiligingsmaatregelen en -eisen, met als doel bijsturing in het geval van tekortkomingen.

Het strategisch beveiligingsbeheer onderhoudt daartoe:
- de gestelde beveiligingsmaatregelen opgelegd aan de gebruikers (zie Bijlage 2);
- de beveiligingseisen waaraan de beheerder voldoet en levert daarmee de richtsnoer voor het risicobeheersingproces van de beheerder.

Voor de invulling van het strategisch beveiligingsbeheer is gekozen voor de norm NEN-ISO/IEC 27001:2005 (Managementsystemen voor informatiebeveiliging) die ook geadopteerd is in het Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR2007). Deze norm schrijft voor dat het beveiligingsmanagement in een PDCA (Plan, Do, Check, Act) cyclus is omvat die wordt aangestuurd vanuit een Information Security Management System (ISMS). Het Strategisch Beveiligingsbeheer vervult de rol van dit ISMS.

Artikel 11

Om de informatiebeveiliging van het C2000-communicatienetwerk op de langere termijn te waarborgen is alleen het beleggen van taken en het eisen van beveiligingsmaatregelen niet voldoende. Er moet ook op de implementatie en effectiviteit van de beveiligingsmaatregelen bij de gebruikers worden toegezien.

Daarnaast wordt vastgesteld dat de beheerder voldoet aan de aan hem gestelde beveiligingseisen. Dit wordt bereikt door aan de ene kant toezicht te houden en aan de andere kant regelmatig controles te laten plaatsvinden. Primair zijn de gebruikers zelf verantwoordelijk voor toezicht en controle op de implementatie van de voor hen verplichte beveiligingsmaatregelen en rapportage daarover aan de beheerder.

Daarnaast bestaat er de centrale functie Toezicht, Controle.en Herziening. Binnen de eerste twee onderdelen wordt getoetst of partijen (met name gebruikers en de beheerder) conform zijn met dit informatiebeveiligingsbeleid. Binnen het laatste onderdeel worden gesignaleerde hiaten in informatiebeveiligingsbeleid geadresseerd door herziening daarvan.
Toezicht heeft tot doel dat de eigenaar een correct en actueel beeld heeft van het totale niveau van informatiebeveiliging van het C2000-communicatienetwerk. Een belangrijk instrument dat de eigenaar heeft zijn de maandrapportages van Operationeel Beveiligingsbeheer betreffende beveiligingsincidenten.
Deze rapportages dienen ten minste te bevatten:
- Overzicht van nieuw gemelde beveiligingsincidenten en reactie op die incidenten.
- Overzicht van nog onopgeloste beveiligingsincidenten en huidige status.

Aangezien de maandrapportages van Operationeel Beveiligingsbeheer voor een groot deel zijn

gebaseerd op de melding van deze beveiligingsincidenten door gebruikers, is het essentieel dat gebruikers snel en volledig hun beveiligingsincidenten melden.

Naast de incidentenrapportages stellen zowel de gebruikers als de beheerder een jaarlijkse rapportage op met daarin de status van de implementatie van de voor hen verplichte, dan wel door hen voorgestelde beveiligingsmaatregelen.

Aangezien Strategisch Beveiligingsbeheer deze rapportages mede gebruikt voor het selecteren van de te controleren gebruikers, is deze rapportage voor het begin van de controle beschikbaar. De rapportages bevatten de volgende gegevens;
- Status van implementatie (verplichte) beveiligingsmaatregelen (aangewezen en bijzondere gebruikers).
- Status van implementatie (verplichte) beveiligingsmaatregelen bij gelieerde gebruikers (aangewezen gebruikers, wanneer van toepassing).

Hieruit blijkt dat dus dat gelieerde gebruikers niet rechtstreeks rapporteren aan Strategisch Beveiligingsbeheer maar via de aangewezen gebruiker waar zij bij horen. Voor de status zijn drie mogelijkheden: genomen, gedeeltelijk genomen en niet genomen.

Bij de statussen gedeeltelijk genomen en iet genomen wordt aangegeven in welk opzicht er nog niet wordt voldaan aan de maatregel, wat hiervan de oorzaak is, eventueel mitigerende omstandigheden en een planning voor de correcte implementatie van de maatregel. De gebruiker mag alleen afwijken van de voorgeschreven beveiligingsmaatregelen indien hij voldoende kan motiveren dat een vergelijkbaar basis beveiligingsniveau wordt gerealiseerd (‘comply or explain’).

Artikel 12

In het kader van dit beleid kunnen drie typen audits worden onderscheiden:

I. Audit op effectiviteit en implementatie strategisch beveiligingsbeheer. Deze audit heeft tot doel om dit beleid en de hierin gestelde eisen en beveiligingsmaatregelen te toetsen.
Speciale aandacht wordt ook gegeven aan het toetsen van het proces waarin het beleid en de eisen en beveiligingsmaatregelen zijn opgesteld. De Inspectie OOV vervult als onafhankelijke deskundige een belangrijke taak in dit zogenaamde metatoezicht.

II. Audit op effectiviteit en implementatie risicobeheersingproces van de beheerder. Deze audit heeft tot doel vast te stellen of de beheerder voldoet aan de door de
Eigenaar gestelde eisen en doelstellingen. Dit omvat ook de toetsing dat de beheerder die beveiligingsmaatregelen uit Bijlage 2 heeft geïmplementeerd verbonden met de gebruikerstaken die de beheerder uitvoert (bijvoorbeeld het beheer van randapparatuur voor zichzelf en bijzondere gebruikers).

III. Audit op implementatie van beveiligingsmaatregelen aangewezen gebruikers (inclusief gelieerden) en bijzondere gebruikers, aan de hand van de voor de gebruikers verplichte beveiligingsmaatregelen (zie Bijlage 2). Deze audit heeft tot doel vast te stellen of de gebruiker alle, vanuit zijn taken verplichte, beveiligingsmaatregelen heeft geïmplementeerd.
Audit type I en II vinden jaarlijks plaats. Audit type III vindt meerdere malen per jaar (minstens 6 keer per jaar) plaats, maar dan wel bij verschillende gebruikers. De hier beschreven periodieke audits worden geïnitieerd door strategisch beveiligingsbeheer.

Artikel 13

Voor de herziening wordt ten minste als input gebruikt:
- voortgang rapportages van de beheerder en gebruikers;
- audit rapportages met betrekking tot ISMS, beheerder en gebruikers;
- accreditatie rapportages;
- beveiligingsincident rapportages, die zijn opgeleverd aan Strategisch Beveiligingsbeheer;
- reeds voorziene wijzigingen in het C2000-communicatienetwerk en zijn omgeving;
- klachten en suggesties van aangesloten partijen.

Hieruit kunnen de volgende typen aanpassingen voortvloeien:
- in dit informatiebeveiligingsbeleid;
- in de gestelde beveiligingsmaatregelen opgelegd aan gebruikers (Bijlage 2);
- in de beveiligingseisen voor hel risicobeheersingproces van de beheerder.

Artikel 14

Voor toezicht en controle is het van belang dat partijen ook worden aangesproken op het niet naleven van beveiligingseisen.

Hiervoor is de volgende procedure van toepassing:
Het operationeel beveiligingsbeheer stemt met gebruikers af over de naleving van het beveiligingsbeleid.

Bij een ernstige en/of meer dan incidentele niet-naleving van het informatiebeveiligingsbeleid informeert het operationeel beveiligingsbeheer het strategische beveiligingsbeheer. Daarbij overlegt operationeel beveiligingsbeheer:
- een onderbouwde beschrijving van de niet-conformiteiten;
- een duiding van de ernst van deze niet-conformiteiten;
- een voorstel voor de noodzakelijk geachte maatregelen.

Bij een constatering door het strategisch beveiligingsbeheer van een ernstige en/of meer dan incidentele niet-naleving van het informatiebeveiligingsbeleid vindt vervolgens overleg plaats tussen het strategisch beveiligingsbeheer, operationeel beveiligingsbeheer en het management van de betrokken verantwoordelijke organisatie. Dit kan leiden tot een waarschuwing en het dringende verzoek om de noodzakelijk geachte beveiligingsmaatregelen te effectueren.

Indien de waarschuwing geen of onvoldoende effect sorteert, zullen verdergaande maatregelen worden genomen:
bij een structurele niet naleving van het informatiebeveiligingsbeleid C2000 door een
- Aangewezen gebruiker, adviseert het Strategisch Beveiligingsbeheer de Minister van VenJ een aanwijzing te geven;
- bij een structurele niet naleving van het informatiebeveiligingsbeleid C2000 door een bijzondere gebruiker, zegt de Minister van VenJ de gebruiksovereenkomst op;
- bij een structurele niet naleving van het informatiebeveiligingsbeleid C2000 door een gelieerde beëindigt de aangewezen gebruiker de gebruiksovereenkomst met de gelieerde;
- bij een structurele niet naleving van het informatiebeveiligingsbeleid C2000 door een leverancier beëindigt de opdrachtgevende organisatie (de aangewezen gebruiker, de beheerder of de bijzondere gebruiker) de overeenkomst met de leverancier.