

## **Basisnormen Beveiliging en Beheer ICT-infrastructuur**



# Basisnormen Beveiliging en Beheer ICT-infrastructuur

PI/DO  
Platform Informatiebeveiliging  
B. Bokhorst  
R. Kuiper  
S. Mekking  
P. Mercera  
R. Torabkhani



Uitgeverij LEMMA BV – Utrecht – 2003

Aan de totstandkoming van deze uitgave is de uiterste zorg besteed. Voor informatie die nochtans onvolledig of onjuist is opgenomen, aanvaarden auteur(s), redactie en uitgever geen aansprakelijkheid. Voor eventuele verbeteringen van de opgenomen gegevens houden zij zich gaarne aanbevolen.

ISBN 90-5931-228-7

NUR 980

<http://www.lemma.nl>

[infodesk@lemma.nl](mailto:infodesk@lemma.nl)

© 2003 Uitgeverij LEMMA BV, Postbus 3320, 3502 GH UTRECHT

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

Voor zover het maken van kopieën uit deze uitgave is toegestaan op grond van artikel 16b Auteurswet 1912 j° het Besluit van 20 juni 1974, Stb. 351 zoals gewijzigd bij Besluit van 23 augustus 1985, Stb. 471 en artikel 17 Auteurswet 1912, dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht, Postbus 3060, 2130 KB Hoofddorp. Voor het overnemen van één of meer gedeelten uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (artikel 16 Auteurswet 1912) dient men zich tot de uitgever te wenden.

Omslagontwerp en typografie: Twin Design BV, Culemborg

# Voorwoord

Het Platform Informatiebeveiliging (PI) heeft als doel 'het bevorderen van de beveiliging van alle belangen betreffende gegevensverwerking, -opslag en -transport, alles in de ruimste zin van het woord'. Binnen deze doelstelling wordt het ontwikkelen van aanvaardbare richtlijnen voor de praktische inrichting van informatiebeveiliging als essentieel onderwerp gezien. Door het gezamenlijk opstellen van dergelijke richtlijnen kan worden gebruikgemaakt van praktijkervaringen, zodat een doeltreffende richtlijn ontstaat die ook uitvoerbaar is.

De PI-richtlijnen worden in werkgroepverband ontwikkeld onder auspiciën van een bestuurslid in de rol van projectleider. Deze ziet er onder meer op toe dat de PI-kwaliteitsrichtlijnen door de werkgroep worden gehandhaafd. De deelnemers van de werkgroepen zijn primair afkomstig uit de organisaties die aangesloten zijn bij PI, maar niet uitsluitend. Het betreft beveiligingsfunctionarissen en ICT-auditors van uiteenlopende bedrijven en instellingen, die zich kenmerken door de hoge eisen die zij in hun advies- en controlewerkzaamheden aan organisaties moeten stellen in verband met de sterke automatiseringsgraad en de belangen die met de geautomatiseerde informatievoorziening zijn gemoeid. Door deze achtergrond vormen de deelnemers een representatieve afspiegeling van de aanwezige ICT-beveiligingsexpertise in Nederland en bieden zij een draagvlak om gezag te verlenen aan de ontwikkelde richtlijnen, hetgeen bevorderlijk is voor de acceptatie door het algemene en het ICT-management.

De PI-beveiligingsrichtlijnen zijn primair bedoeld voor functionarissen die zijn belast met het implementeren van ICT-systemen, zoals systeembeheerders en technische ontwerpers en bouwers.

Daarnaast zijn de richtlijnen van betekenis voor de volgende doelgroepen.

- ICT-beveiligingsfunctionarissen (security officers en administrators). De ICT-beveiligingsfunctie binnen een organisatie is verantwoordelijk voor het (doen) treffen van beveiligingsmaatregelen. De richtlijnen bieden hierbij ondersteuning.
- ICT-management. Het ICT-management is (eind)verantwoordelijk voor de informatiebeveiliging binnen zijn competentiegebied en geeft hieraan invulling door het (doen) analyseren van risico's en het bepalen van (globale) beveiligingsdoelstellingen. De beargumenteerde keuzen in de richtlijnen zijn hierbij een handvat.
- ICT-auditors. De richtlijnen kunnen worden gehanteerd als toetsingsnorm bij ICT-audits.

Aldus bieden de richtlijnen enerzijds een handreiking aan beveiligingsfunctionarissen en het ICT-management om een toereikende en evenwichtige beveiliging van de informatievoorziening te implementeren en bieden zij anderzijds een basis aan ICT-auditors voor de normstelling bij de beoordeling van de beveiliging van een ICT-systeem.

Aan deze PI-studie hebben de volgende personen en organisaties hun medewerking verleend:

B. Bokhorst <sup>RE RA</sup>, Belastingdienst/Centrum voor ICT

R. Kuiper, Logica <sup>CMG</sup>

S. Mekking, Kadaster

Drs. P. Mercera, Hewlett Packard

Ir. J. Schapink <sup>RE</sup>, EDP Audit Pool

Drs. R. Torabkhani, UWV

Dank voor hun constructieve bijdragen in de reviewfase van de PI-studie is verschuldigd aan:

H. Luijff, <sup>TNO-FEL</sup>

W. Tewarie, Defensie Accountantsdienst

B. de Backker, Atos/Origin

L. van Rij en J. Speckkamp, <sup>KPMG-IRM</sup>

M. Huijbers, PinkRocade

# Inhoud

<b>1</b>	<b>Inleiding</b>	<b>9</b>
1.1	PI-beveiligingsrichtlijnen	12
1.2	Uitgangspunten voor deze PI-studie	13
<b>2</b>	<b>Beschrijving objectgebieden</b>	<b>19</b>
2.1	Hoofdingeling	19
2.2	ICT-infrastructuur	21
2.3	Beheerprocessen	28
2.4	Samenhang normen voor techniek en processen	29
<b>3</b>	<b>Basisnormen ICT-infrastructuur</b>	<b>31</b>
3.1	Inrichting ICT-infrastructuur	31
3.2	Servers	37
3.3	Netwerk infrastructuur	38
3.4	Clients	39
3.5	Filterende netwerkkoppelingen	41
3.6	Identificatie	44
3.7	Authenticatie	45
3.8	Autorisatie	47
3.9	Encryptie	49
3.10	Monitoren/loggen	50

<b>4</b>	<b>Basisnormen beheerprocessen</b>	<b>53</b>
4.1	Inrichting processen	53
4.2	Service Level Management	57
4.3	Availability Management	61
4.4	Capacity Management	66
4.5	ICT Service Continuity Management	71
4.6	Security Management	79
4.7	Configuration Management	86
4.8	Service desk	90
4.9	Incident Management	92
4.10	Problem Management	99
4.11	Change Management	102
4.12	Release Management	110
4.13	Operations	114
4.14	Supply Management	127
	<b>Bijlage 1</b> Overzicht relatie Code voor Informatiebeveiliging met Basisnormen Beveiliging en Beheer ICT-infrastructuur	<b>133</b>
	<b>Bijlage 2</b> Overzicht relatie CobiT met Basisnormen Beveiliging en Beheer ICT-infrastructuur	<b>141</b>
	<b>Bijlage 3</b> Begrippen	<b>143</b>
	<b>Literatuur</b>	<b>145</b>
	<b>Register</b>	<b>147</b>
	<b>Over de auteurs</b>	<b>149</b>