

BIO

Versie 1



Inhoudsopgave

Wijzigingshistorie:	2
Voorwoord	3
DEEL 1 Achtergrond BIO	
7	
1. Informatiebeveiliging bij de overheid	9
1.1 Inleiding	9
1.2 Informatiebeveiligingskaders en uitgangspunten overheid	9
1.3 ISO 27002	10
1.4 Evaluatie en bijstelling	11
1.5 Forum Standardisatie	11
2. Opzet van de BIO	13
2.1 Opzet BBN's	13
2.2 Controls	13
2.3 Implementatierichtlijnen	13
2.4 Overheidsmaatregelen	14
2.5 Addendum	14
2.6 Operationalisering in handreikingen	14
2.7 Rollen	14
3. Basisbeveiligingsniveaus	17
3.1 BBN1	17
3.2 BBN2	17
3.3 BBN3	18
4. Verantwoording over de BIO	19
4.1 Verantwoordelijkheid afhankelijk van basisbeveiligingsniveau	19
4.2 Explains op overheidsmaatregelen	19
4.3 Ketensamenwerking	20
4.4 Dienstenleveranciers	20
DEEL 2 Kader BIO	
23	
Inleiding	24
BBN-toets	25
Controls en overheidsmaatregelen	26
5. Informatiebeveiligingsbeleid	27
5.1 Aansturing door de directie van de informatiebeveiliging	27
6. Organiseren van informatiebeveiliging	29
6.1 Interne organisatie	29
6.2 Mobiele apparatuur en telewerken	30
7. Veilig personeel	31
7.1 Voorafgaand aan het dienstverband	31
7.2 Tijdens het dienstverband	31
7.3 Beëindiging en wijziging van dienstverband	32
8. Beheer van bedrijfsmiddelen	33
8.1 Verantwoordelijkheid voor bedrijfsmiddelen	33
8.2 Informatieclassificatie	34
8.3 Behandelen van media	35
9. Toegangsbeveiliging	37
9.1 Bedrijfseisen voor toegangsbeveiliging	37
9.2 Beheer van toegangsrechten van gebruikers	37
9.3 Verantwoordelijkheden van gebruikers	39
9.4 Toegangsbeveiliging van systeem en toepassing	39
10. Cryptografie	41
10.1 Cryptografische beheersmaatregelen	41
11. Fysieke beveiliging en beveiliging van de omgeving	43
11.1 Beveiligde gebieden	43
11.2 Apparatuur	44
12. Beveiliging bedrijfsvoering	47
12.1 Bedieningsprocedures en verantwoordelijkheden	47
12.2 Bescherming tegen malware	48
12.3 Back-up	49
12.4 Verslaglegging en monitoren	50
12.5 Beheersing van operationele software	51
12.6 Beheer van technische kwetsbaarheden	51
12.7 Overwegingen betreffende audits van informatiesystemen	51
13. Communicatiebeveiliging	53
13.1 Beheer van netwerkbeveiliging	53
13.2 Informatietransport	54
14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen	55
14.1 Beveiligingseisen voor informatiesystemen	55
14.2 Beveiliging in ontwikkelings- en ondersteunende processen	56
14.3 Testgegevens	57
15. Leveranciersrelaties	59
15.1 Informatiebeveiliging in leveranciersrelaties	59
15.2 Beheer van dienstverlening van leveranciers	61
16. Beheer van informatie-beveiligingsincidenten	63
16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen	63
17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	65
17.1 Informatiebeveiligingscontinuïteit	65
17.2 Redundante componenten	66
18. Naleving </	

DEEL 3 Addendum BIO		73
Inleiding Addendum		74
5.	Informatiebeveiligingsbeleid	75
5.1	Aansturing door de directie van de informatiebeveiliging	75
6.	Organiseren van informatiebeveiliging	75
6.1	Interne organisatie	75
7.	Veilig personeel	76
7.1	Voorafgaand aan het dienstverband	76
7.2	Tijdens het dienstverband	76
8.	Beheer van bedrijfsmiddelen	76
8.1	Verantwoordelijkheid voor bedrijfsmiddelen	76
8.3	Behandelen van media	76
11.	Fysieke beveiliging en beveiliging van de omgeving	77
11.1	Beveiligde gebieden	77
14.	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	77
14.1	Beveiligingseisen voor informatiesystemen	77
15.	Leveranciersrelaties	78
15.1	Informatiebeveiliging in leveranciersrelaties	78
16.	Beheer van informatiebeveiligingsincidenten	78
16.1	Beheer van informatiebeveiligings-incidenten en -verbeteringen	78

Deel 1

Achtergrond BIO

1

Informatiebeveiliging bij de overheid

1.1 Inleiding

Informatiebeveiliging is het proces van vaststellen van de vereiste beveiliging van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen¹⁾.

De BIO beoogt de beveiliging van informatie(systemen) bij alle bedrijfsonderdelen van de overheid te bevorderen, zodat deze bedrijfsonderdelen erop kunnen vertrouwen dat gegevens die worden verstuurd naar of worden ontvangen van andere onderdelen van de overheid, in lijn met wet- en regelgeving, passend beveiligd zijn.

De BIO beoogt zo de beveiliging van informatie(systemen) bij alle bestuurslagen en bestuursorganen van de overheid te bevorderen, zodat alle onderdelen erop kunnen vertrouwen dat onderling uitgewisselde gegevens, in lijn met wet- en regelgeving, passend beveiligd zijn. Het doel is continuïteit in de bedrijfsprocessen door waarborgen van juiste en tijdige informatie. Daarmee is de BIO ook van toepassing op besturings- en meetprocessen voor zover deze binnen een bestuursorgaan gebruikt worden.

De BIO is van toepassing op de overheid. In verband hiermee is de BIO van toepassing op de volgende bestuursorganen:

- Rijksdienst
- Provincies
- Waterschappen
- Gemeentes

Daarnaast wordt aanbevolen de BIO te verankeren in de taakomschrijving van de overige overheidsorganisaties en organisaties waarmee de overheid publiek privaat samenwerkt en private samenwerkingen waarbij de overheid de enige aandeelhouder is.

1.2 Informatiebeveiligingskaders en uitgangspunten overheid

De overheid past risicomanagement toe om tot de juiste beveiliging van informatie en informatiesystemen te komen binnen de context van de bedrijfsdoelstellingen. Risicomanagement is het inzichtelijk en systematisch inventariseren, beoordelen en – door het treffen van maatregelen – beheersbaar maken van risico's en kansen, die het bereiken van de doelstellingen van de organisatie bedreigen dan wel bevorderen, op een zodanige wijze dat verantwoording kan worden afgelegd over de gemaakte keuzes²⁾.

1) Artikel 1 sub a Voorschrift Informatiebeveiliging Rijksdienst 2007, *Stcrt.* 2007, 122/11.

2) Artikel 5 lid 2 BVR en Artikel 1 sub d BVR.

Deel 2

Kader BIO

9

Toegangsbeveiliging

Algemene handreiking: **Beleid logisch toegangsbeveiliging**

9.1 Bedrijfseisen voor toegangsbeveiliging

Doelstelling: Toegang tot informatie en informatie verwerkende faciliteiten beperken.

9.1.1	1	Beleid voor toegangsbeveiliging Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Secretaris	
9.1.2	1	Toegang tot netwerken en netwerkdiensten Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	Dienstenleverancier	
Handreiking: MDM				
9.1.2.1	1	Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone.		
9.1.2.2	1	Gebruikers met eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.		

9.2 Beheer van toegangsrechten van gebruikers

Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.

9.2.1	1	Registratie en afmelden van gebruikers Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Proceseigenaar Dienstenleverancier
9.2.1.1	1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	
9.2.1.2	1	Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	

