



Baseline Informatiebeveiliging Rijksdienst

Tactisch Normenkader (TNK)

De BIR is geheel gestructureerd volgens NEN/ISO 27001, bijlage A en NEN/ISO 27002. De overheid is verplicht om aan ISO 27001 en ISO 27002 te voldoen. Het college standaardisatie heeft deze voorschriften opgenomen in de lijst met verplichte standaarden voor de publieke sector, volgens het comply or explain principe.

De BIR beschrijft de invulling van NEN/ISO27001 en 27002 voor de rijksoverheid. In de BIR zijn deze specifieke rijksnormen gemerkt met een [R].

NEN/ISO 27001 en 27002 beschrijven details voor implementatie (implementatierichtlijnen) en eisen voor de procesinrichting (o.a. het ISMS uit NEN/ISO 27001). Die documenten geven dus de details voor de toepassing, die niet in de BIR zijn beschreven en die nodig blijven voor een goede implementatie van de BIR.

Het gebruik van de NEN/ISO normen 27001 en 27002 voor de BIR geschiedt met toestemming van het NNI.



Inhoudsopgave

1. Inleiding	4
1.1. Aanleiding	4
1.2. Aansluiting bij open standaarden	4
2. Uitgangspunten en werkingsgebied	6
2.1. Uitgangspunten	6
2.2. Basis beveiligingsniveau	9
2.3. Controleerbaarheid en auditeerbaarheid	10
2.4. Werkingsgebied	10
2.5. Brondocumenten	10
2.6. Evaluatie en bijstelling	11
2.7. Doelgroepen	11
3. Structuur van de norm	13
4. Risicobeoordeling en risicobehandeling	14
5. Beveiligingsbeleid	15
5.1. Informatiebeveiligingsbeleid	15
6. Organisatie van de Informatiebeveiliging	16
6.1. Interne organisatie	16
6.2. Externe Partijen	17
7. Beheer van bedrijfsmiddelen	19
7.1. Verantwoordelijkheid voor bedrijfsmiddelen	19
7.2. Classificatie van informatie	19
8. Personele beveiliging	21
8.1. Beveiligen van personeel	21
8.2. Tijdens het dienstverband	22
8.3. Beëindiging of wijziging van het dienstverband	22
9. Fysieke beveiliging en beveiliging van de omgeving	24
9.1. Beveiligde ruimten	24
9.2. Beveiliging van apparatuur	26
10. Beheer van Communicatie- en Bedieningsprocessen	28
10.1. Bedieningsprocedures en verantwoordelijkheden	28
10.2. Exploitatie door een derde partij	29
10.3. Systeemplanning en –acceptatie	29
10.4. Bescherming tegen virussen en “mobile code”	30
10.5. Back-up	31
10.6. Beheer van netwerkbeveiliging	32
10.7. Behandeling van media	32
10.8. Uitwisseling van informatie	33
10.9. Diensten voor e-commerce	34
10.10. Controle	35
11. Toegangsbeveiliging	38
11.1. Toegangsbeleid	38
11.2. Beheer van toegangsrechten van gebruikers	38
11.3. Verantwoordelijkheden van gebruikers	39
11.4. Toegangsbeheersing voor netwerken	40
11.5. Toegangsbeveiliging voor besturingssystemen	41
11.6. Toegangsbeheersing voor toepassingen en informatie	42
11.7. Draagbare computers en telewerken	43
12. Verwerving, ontwikkeling en onderhoud van Informatiesystemen	45



12.1. Beveiligingseisen voor informatiesystemen	45
12.2. Correcte verwerking in toepassingen	45
12.3. Cryptografische beheersmaatregelen	46
12.4. Beveiliging van systeembestanden	47
12.5. Beveiliging bij ontwikkelings- en ondersteuningsprocessen	48
12.6. Beheer van technische kwetsbaarheden	49
13. Beheer van Informatiebeveiligingsincidenten	50
13.1. Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken	50
13.2. Beheer van informatiebeveiligingsincidenten en –verbeteringen	50
14. Bedrijfscontinuïteitsbeheer	52
14.1. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	52
15. Naleving	54
15.1. Naleving van wettelijke voorschriften	54
15.2. Naleving van beveiligingsbeleid en -normen en technische naleving	55
15.3. Overwegingen bij audits van informatiesystemen	55
16. Bijlage A: Begrippen	56



1. Inleiding

1.1. Aanleiding

De inspanningen in de laatste jaren om tot gemeenschappelijke normenkaders voor informatiebeveiliging te komen hebben geleid tot een groeiend stelsel normenkaders, zoals de Haagse Ring, Rijksweb, mobiele data dragers, Departementaal Vertrouwelijke webapplicaties en DWR¹. Deze vijf normenkaders verschillen in opbouw, overlappen elkaar deels en zijn daardoor moeilijk te beheren en te implementeren. Bovendien hebben de departementen en uitvoeringsorganisaties ieder afzonderlijk een eigen baseline informatiebeveiliging. Zoveel verschillende normenkaders is verwarrend en belemmert een beheerste beveiliging en het implementeren en beheren van de normen.

Met het van kracht worden van de BIR:2012 vervallen deze vijf rijksnormenkaders.

In de Baseline Informatiebeveiliging Rijksdienst (BIR:2012) zijn de uitgangspunten van de visie op beveiliging van de rijksdienst, zover mogelijk als de stand der techniek toelaat, verwerkt.

Die visie is:

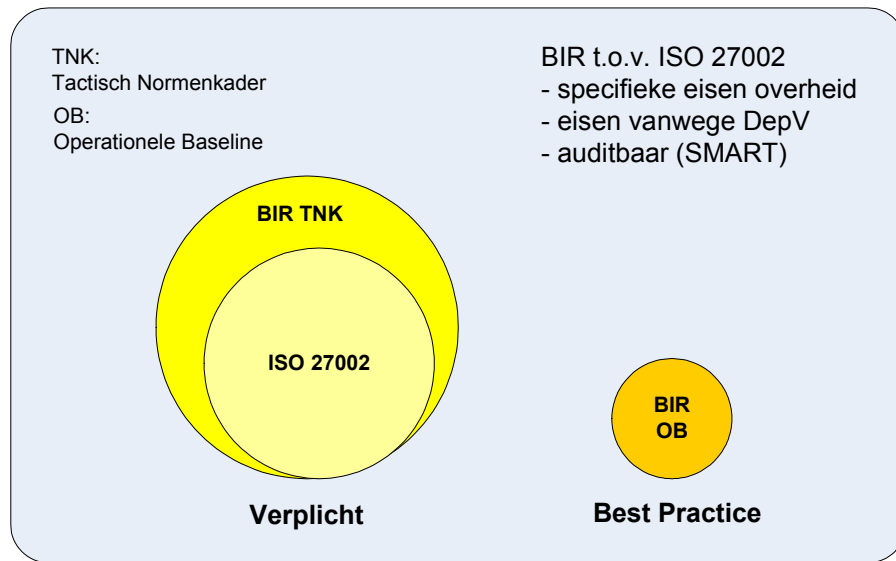
- Informatiebeveiliging is en blijft een verantwoordelijkheid van het lijnmanagement
- Het primaire uitgangspunt voor informatiebeveiliging is en blijft risicomanagement
- De klassieke informatiebeveiligingsaanpak waarbij inperking van mogelijkheden de boventoon voert maakt plaats voor veilig faciliteren
- Methoden voor rubricering en continue evaluatie ervan zijn hanteerbaar om onder- en overrubricering te voorkomen
- De focus verschuift van netwerkbeveiliging naar gegevensbeveiliging
- Verantwoord en bewust gedrag van mensen is essentieel voor een goede informatiebeveiliging
- Kaders en maatregelen worden overheidsbreed afgesproken en ingezet. In uitzonderingsgevallen wordt – in overleg – afgeweken
- Kennis en expertise zijn essentieel voor een toekomstvaste informatiebeveiliging en moeten (centraal) geborgd worden
- Informatiebeveiliging vereist een integrale aanpak

1.2. Aansluiting bij open standaarden

Er is gekozen voor een optimale aansluiting bij de wereld van de open en geaccepteerde standaarden, ISO 27001:2005 en ISO 27002:2007. Indien een organisatieonderdeel of een toeleverancier haar zaken op orde heeft volgens ISO 27001:2005, rekening houdend met de implementatiemaatregelen uit ISO 27002:2007, dan hoeft die organisatie slechts te controleren op de aanvullende bepalingen voor de rijksdienst. Die aanvullende bepalingen voor de Rijksdienst zijn in de BIR:2012 gemarkeerd met **(R)** zodat ze herkenbaar en apart toetsbaar zijn.

De BIR:2012 bestaat uit een tactisch normenkader (TNK) en een operationele baseline (OB). Het tactische normenkader is verplicht (comply or explain). De operationele baseline is niet verplicht, het is een best practice. De patronen uit de OB voldoen aan het TNK maar het toepassen van een patroon uit de operationele baseline ontslaat de organisatie niet van de verplichting om aan te tonen dat zij voldoet aan het gehele TNK.

¹ DWR: Digitale Werkomgeving Rijksdienst.



Figuur 1: Samenhang BIR:2012 TNK, BIR OB en ISO 27001:2005



2. Uitgangspunten en werkingsgebied

2.1. Uitgangspunten

Kwaliteit en betrouwbaarheid

In de samenleving is een roep tot grotere openheid en transparantie van het Rijk. Tegelijkertijd wordt het Rijk in de media en in de samenleving harder afgerekend op fouten of vermeende fouten. Dit zorgt voor een groeiende druk op de betrouwbaarheid van de informatievoorziening van het Rijk en de ondersteunende rol van ICT daarbij.

Samenwerking, altijd en overal

De vernieuwing van de Rijksdienst vraagt om een medewerker die altijd en overal toegang heeft tot de informatie die voor hem op dat moment noodzakelijk is. Het mag er, gegeven de juiste authenticatie en autorisatiemechanismen, daarbij niet toe doen bij welk ministerie die informatie of die medewerker zich bevindt. De nauwere samenwerking tussen de departementen op het gebied van bedrijfsvoering leidt tot harmonisering en uniformering. De ambtenaar van de toekomst krijgt één uniforme toegang tot de informatie en één rijkspas.

De BIR:2012 biedt één normenkader voor de beveiliging van de informatiehuishouding van het Rijk. Dit maakt het mogelijk om veilig samen te werken en onderling gegevens uit te wisselen. De BIR:2012 zorgt voor één heldere set afspraken zodat een bedrijfsonderdeel weet dat de gegevens die verstuurd worden naar een ander onderdeel van de rijksdienst op het juiste beveiligingsniveau (vertrouwelijkheid, integriteit en beschikbaarheid) worden behandeld.

Bij de rijksdienst wordt veel samengewerkt in ketens. Voorlopig bestrijkt de BIR:2012 alleen de direct onder de ministeries ressorterende diensten. Door optimale aansluiting bij de open en geaccepteerde industriestandaarden (ISO 27001:2005 en ISO 27002:2007) wordt maximale aansluiting bij ketenpartners bereikt. De ketenpartners worden uitgenodigd de toevoegingen van de BIR:2012 op ISO 27002:2007 te implementeren.

Departementaal Vertrouwelijk niveau

Het basisvertrouwelijkheidsniveau is vastgesteld als "Departementaal Vertrouwelijk", zoals gedefinieerd in het Besluit Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIRBI²), en met betrekking tot de bescherming van privacygevoelige informatie op risicoklasse 2, gedefinieerd in het document 'Beveiliging van persoonsgegevens' van de registratiekamer, ook bekend onder de afkorting A&V nr. 23³. Informatie met vertrouwelijkheidsniveau WBP-*risicoklasse 2* (WBP2) en Departementaal Vertrouwelijk (DepV) komt veelvuldig voor bij de Rijksdienst. Het gaat dan bijvoorbeeld om persoonsvertrouwelijke informatie, commercieel vertrouwelijke informatie of gevoelige informatie in het kader van beleidsvorming ("beleidsintimiteit").

Tot persoonsinformatie die volgens de WBP vertrouwelijk is behoren: (*risicoklasse 1*) informatie betreffende lidmaatschappen, arbeidsrelaties, klantrelaties en overeenkomstige relaties tussen een betrokkene en een organisatie en (*risicoklasse 2*) godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens.

Dit betekent dat het standaard berichtenverkeer binnen de Rijksdienst behandeld wordt met middelen en processen die berekend zijn op de vertrouwelijkheidsniveaus WBP2 en departementaal vertrouwelijk. Een medewerker hoeft zich dan niet per geval af te vragen of het medium waarover hij het bericht (t/m WBP2 / DepV) verstuurt voldoende veilig is en of de ontvangende organisatie het bericht wel

² Het VIRBI:2004 is momenteel in bewerking. Er is een concept voor een nieuw VIRBI. In de BIR:2012 is uitgegaan van het concept voor het nieuwe VIRBI. Het nieuwe VIRBI verschilt niet van de VIRBI:2004 voor wat betreft de definitie van departementaal vertrouwelijk en voor wat betreft de risicobenadering. Het normenkader in de nieuwe VIRBI verschilt wel van de VIRBI:2004.

Mocht bij definitieve vaststelling van de nieuwe VIRBI blijken dat er verschillen zijn met het concept dan zal de BIR hiermee worden gelijkgetrokken.

³ http://www.cbpweb.nl/Pages/av_23_Beveiliging.aspx



voldoende veilig behandelt. De verzender kan er van uit gaan dat een ontvangende partij bij de Rijksdienst de informatie op een voldoende vertrouwelijke manier behandelt. De BIR:2012 beschrijft de beveiligingsmaatregelen daarvoor. Niet alleen voor werken op kantoor maar ook voor plaats en tijd onafhankelijk werken met vaste of mobiele apparatuur.

Op het moment dat een organisatie er bewust voor kiest bepaalde informatie openbaar te maken (overheidswebsites, correspondentie naar externe partijen e.d.) kiest de verantwoordelijke medewerker of die bepaalde informatie naar de beoogde ontvangers kan en of de kanalen daarvoor geschikt zijn. Dat is de verantwoording van de betreffende medewerker voor de specifieke, per geval door hem beoordeelde informatie. Hetzelfde geldt voor het doorsturen van informatie naar privé-mail. De medewerker bepaalt dan per geval of de betreffende informatie doorgestuurd kan worden. Automatisch doorzending van alle mail naar een privé-adres of andere onveilige omgeving wordt dan ook niet toegestaan omdat dan niet per bericht door de medewerker beoordeeld kan worden of de informatie naar een onvoldoende veilige omgeving kan worden gestuurd.

Vertrouwen in toetsing

Als ministeries hun informatievoorziening en IT inrichten volgens de BIR:2012 (in opzet, bestaan en werking) dan moet dat voldoende garantie bieden dat ministeries hun eigen informatie en die van andere ministeries veilig (beschikbaar, integer en vertrouwelijk) behandelen. Ministeries moeten elkaar hierop kunnen aanspreken. Bij de implementatie geldt voor de tactische normen en eisen een comply or explain regime. Het toetsen vindt plaats aan de hand van de in control verklaring. De in control verklaring moet dus inzicht geven aan welke BIR:2012 normen wordt voldaan en voor welke BIR:2012 normen een explain is gedefinieerd. Er wordt, buiten het kader van BIR, bij de Rijksdienst een accreditatieproces ontwikkeld waarin departementen elkaar kunnen aanspreken op explains die de vertrouwelijkheid van berichtenverkeer over meerdere ministeries heen nadelig beïnvloeden.

VIR:2007 – toelichting:

In feite wordt aan het management een managementverantwoording (in control statement) wat betreft de informatiebeveiliging gevraagd.

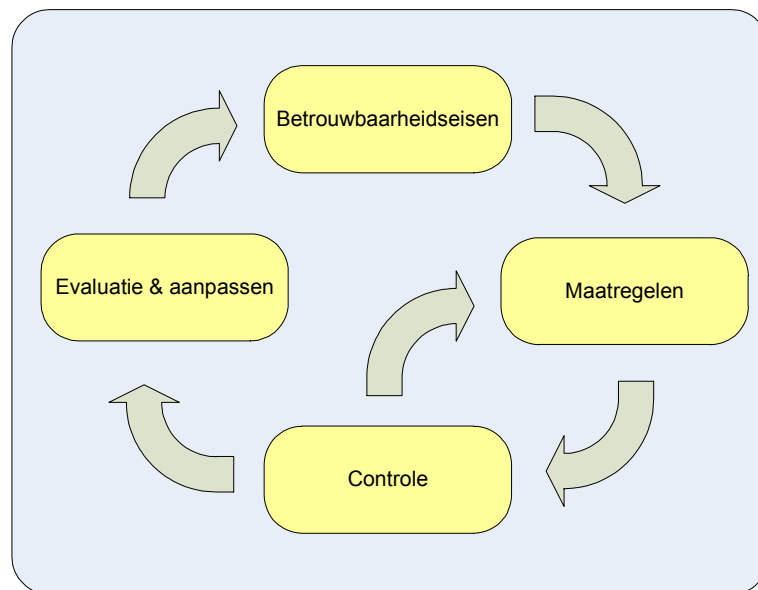
Doordat het VIR:2007 integraal onderdeel is van de bedrijfsvoering sluit het aan bij de Planning en Control cyclus. Om het VIR:2007 te effectueren wordt gebruik gemaakt van de kwaliteitscirkel van Deming (Plan Do Check Act cyclus).

Als nadere toelichting wordt daar gegeven (in de toelichting per artikel – artikel 2):

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.

(in VIR:2007 toelichting per artikel – artikel 4)

Voor het effectueren van informatiebeveiliging wordt gewerkt via de Plan Do Check Act cyclus (zie figuur 2). Na het vaststellen wat nodig is 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 2: PDCA cyclus voor informatiebeveiliging

Schaalbaarheid

In het VIR:2007 en VIRBI wordt risicoanalyse gepresenteerd als de methode om de noodzakelijke maatregelen aan specifieke risico's te kunnen koppelen. Als dit toegepast wordt op rijksbrede applicaties dan worden door het grote aantal (potentiële) gebruikers en het grote aantal verschillende toepassingen snel zware beveiligingsmaatregelen gedicteerd. Beveiligingsoplossingen die voldoende zijn bij een kleine groep gebruikers zijn niet voldoende bij een grotere groep gebruikers aangezien het aantal potentieel kwaadwillende personen dan ook toeneemt. Het BIR:2012 onderkent dit gevolg van Rijksbrede ketensamenwerking en heeft hiermee in de eisen rekening gehouden. Eén van de mogelijke maatregelen is compartimentering, met sterkere maatregelen gericht op "externe" gebruikers dan op "lokale" gebruikers.

Voor de BIR:2012 zijn de volgende keuzes gemaakt:

- De BIR:2012 is opgesteld op basis van de huidige situatie ("wat er nu is"): gelaagde beveiliging⁴, zoals ook in het tactische normenkader van DWR is gebruikt.
- Het Schengen principe wordt gehanteerd. Dit houdt in, dat de onderdelen van de Rijksdienst elkaar beschouwen als vertrouwde partner en niet als onvertrouwde buitenwereld. Het gevolg hiervan is dat iedereen afzonderlijk zijn omgeving beveiligt en "schoon" houdt en dat de andere omgevingen hierop kunnen vertrouwen. Hierbij vormt controle de basis van het vertrouwen (governance).
- Het beveiligingsniveau is in lagen uitbreidbaar. Bij de opbouw van de BIR:2012 wordt het principe van gelaagde opbouw gehanteerd. Er is een basisbeveiligingsniveau (overeenkomend met "Departementaal Vertrouwelijk"). Daar waar bepaalde toepassingen, werkomgevingen of specifieke dreigingen een hogere beveiligingsgraad of specialistische maatregelen vereisen, kunnen extra maatregelen getroffen worden bovenop het basisbeveiligingsniveau. De baseline is zo opgebouwd dat er, zonder de voor het basisniveau getroffen maatregelen aan te tasten, een verdieping bovenop gebouwd kan worden om te voldoen aan de hogere of specialistische eisen.
- Specialistische maatregelen voor afwijkende situaties of hogere beveiligingsniveaus dan het basisniveau, zijn niet in de BIR:2012 opgenomen. Voor dit soort bijzondere omstandigheden zal teruggegrepen moeten worden naar een gerichte risicoafweging.

⁴ Naarmate het meer mogelijk wordt de gegevens zelf te beveiligen zal dit in toekomstige versies van de BIR verwerkt worden.



- Het gekozen baseline niveau is zodanig, dat er in een overgrote meerderheid van de gevallen geen aanleiding bestaat om tot extra maatregelen over te gaan.

2.2. Basis beveiligingsniveau

Binnen het vakgebied informatiebeveiliging wordt onderscheid gemaakt tussen beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid. De BIR:2012 sluit hierbij aan.

Beschikbaarheid

De BIR:2012 definieert een basisset aan eisen voor beschikbaarheid voor de departementale en interdepartementale infrastructuur. Deze dient als basis voor het maken van afspraken over de beschikbaarheid tussen de eigenaar van het informatiesysteem en de dienstenleverancier. Dit houdt in dat voor de beschikbaarheid van de informatievoorziening er een minimale set van normen wordt opgesteld waarbij per dienst en/of applicatie nadere afspraken gemaakt kunnen worden.

Integriteit

De integriteit op het IT vlak valt normaliter in twee delen uiteen: de integriteit van datacommunicatie en opslag enerzijds (d.w.z. niet gerelateerd aan het proces zelf), en de integriteit van de informatie in de applicaties (d.w.z. gerelateerd aan het proces zelf). Integriteit gekoppeld aan de applicatie is altijd situatieafhankelijk en afhankelijk van de eisen van een specifiek proces. Voor de functionele integriteit van de informatievoorziening wordt er een minimale set van normen opgesteld waarbij er per dienst en/of applicatie nadere afspraken gemaakt kunnen worden.

Vertrouwelijkheid

De BIR:2012 beschrijft de maatregelen die nodig zijn voor het basisvertrouwelijkheidsniveau Departementaal Vertrouwelijk en WBP risicoklasse 2.

Het algemene dreigingprofiel voor Departementaal Vertrouwelijk is voor de BIR:2012 vastgesteld op de volgende bedreigers:

- De onbetrouwbare medewerker
- Wraakzuchtige medewerker
- De verontruste burger
- Actiegroep
- Crimineel opportunist
- Contractor
- Georganiseerde internet crimineel

Hierbij zijn de volgende bedreigingen specifiek gedefinieerd voor Departementaal Vertrouwelijk.:

- Infiltratie light
- Publiek benaderbare sociale netwerken
- Verhoor (fysiek geweld tegen personen)
- Hacking op afstand
- Malware (met en zonder remote control)
- Crypto kraken
- Draadloze netwerken interceptie
- Draadloze netwerken actief benaderen
- Beproeving van fysieke, technische en elektronische weerstand

Naast de bovenstaande specifieke bedreigingen gaat de BIR:2012 ook uit van een set algemene dreigingen waarvan de hoofdgroepen zijn:



- Onopzettelijk menselijk handelen
- Opzettelijk menselijk handelen
- Onbeïnvloedbare externe factoren
- Technisch falen

Uitgesloten zijn de volgende bedreigers:

- Terreurgroep
- Inlichtingendienst
- Georganiseerde criminaliteit

Specifieke bedreigingen komende van deze bedreigers worden niet meegenomen in het definiëren van de normen in de BIR:2012.

2.3. Controleerbaarheid en auditeerbaarheid

In hoofdstuk 2.1 is de VIR:2007 aangehaald met betrekking tot de controleerbaarheid. Het in control statement vervult daarin een essentiële rol. Het in control statement wordt door de ministeries zelf opgesteld en vermeld in de bedrijfsvoeringparagraaf van het jaarrapport dat aan de tweede kamer wordt gezonden. Om te komen tot het in control statement zullen de bedrijfsonderdelen van een ministerie aan de hand van de normen van BIR:2012 TNK zelf na moeten gaan in welke mate (comply/explain) zij daaraan voldoen (interne audit).

Die interne toetsing vindt plaats op basis van een toets aan ISO 27001:2005 (bijlage 1) + de BIR:2012 rijksspecifieke aanvullingen. Die rijksspecifieke invullingen zijn in de BIR:2012 met een (R) aangeduid.

2.4. Werkingsgebied

De BIR:2012 geldt voor de Rijksdienst (hiertoe worden gerekend de ministeries met de daaronder ressorterende diensten, bedrijven en instellingen). Dat wil zeggen dat de BIR:2012 geldt voor de bestuursdepartementen, taakorganisaties en agentschappen. Zelfstandige BestuursOrganen (ZBO's) nemen een bijzondere positie in. Zij zijn niet verplicht om de BIR:2012 toe te passen, maar via de subsidievoorwaarden kunnen ministeries hen wel deze verplichting opleggen. De BIR:2012 heeft daarmee hetzelfde bereik als het VIR:2007.

In de BIR:2012 staan de minimale eisen die gesteld worden aan de informatiebeveiliging van de IT-infrastructuur van de Rijksdienst. Het document geldt daarmee ook als aansluitvoorwaarde voor de basis IT-infrastructuur van departementen die aangesloten zijn op de generieke basis IT-infrastructuur van de Rijksdienst.

Deze baseline geeft invulling aan artikel 3 lid d van het Besluit voorschrijft informatiebeveiliging rijksdienst 2007 (VIR:2007).

2.5. Brondocumenten

Voor de BIR:2012 zijn de volgende brondocumenten van toepassing:

- Wet Bescherming Persoonsgegevens (WBP)
- Wet Particuliere Beveiligingsorganisaties en Recherchebureaus (WBPR)
- Wet Veiligheidsonderzoeken (WVO)
- Wet Politiegegevens (WPG)
- Ambtenarenwet
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIRBI2012)



- Beveiligingsvoorschrift 2005 (BVR)
- Algemeen Rijksambtenarenreglement (ARAR)
- Ambtseed/belofte
- Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT2010)
- Kader Rijkstoegangsbeleid⁵
- Uitgangspunten online communicatie rijksambtenaren⁶
- Programma van Eisen PKI Overheid
- Code voor Informatiebeveiliging (ISO 27001:2005 en ISO 27002:2007)
- Telecommunication Infrastructure Standard for Data Centers (TIA-942)

Waar dat van toepassing is wordt in de BIR:2012 verwezen naar bestaande normenkaders op aan informatiebeveiliging aanpalende gebieden zoals fysieke beveiliging (Kader Rijkstoegangsbeleid), persoonlijke integriteit (ARAR), enz.

2.6. Evaluatie en bijstelling

Dit document wordt jaarlijks geëvalueerd en indien nodig bijgesteld onder de verantwoordelijkheid van het Interdepartementale Commissie Chief Information Officers (ICCIO). De evaluatie en eventuele bijstelling vinden plaats in overleg met het Coördinerend Beraad Integrale Beveiliging, namens het SG-beraad.

2.7. Doelgroepen

Dit normenkader bevat aandachtsgebieden voor verschillende doelgroepen. Hieronder worden per doelgroep de hoofdstukken genoemd die relevant zijn.

IB functionarissen

Informatiebeveiligingsfunctionarissen van alle niveaus.

Alle hoofdstukken

Lijnmanager in zijn personeelsverantwoordelijkheid

De lijnmanager is verantwoordelijk voor het handhaven van de personele beveiliging met eventuele ondersteuning door Personeelszaken.

Zie hoofdstukken 6 en 8

Lijnmanager in zijn verantwoordelijkheid voor de uitvoering van de processen

De lijnmanager is verantwoordelijk voor het uitvoeren van activiteiten in processen (algemene procesverantwoordelijkheid) op basis van beschreven inrichting ervan. De verantwoordelijkheid voor de naleving van specifieke beveiligingsaspecten hangt af van het soort proces, zoals dat in de BIR:2012 is uitgewerkt.

Zie hoofdstukken 6, 10, 12, 13 en 14

5

http://portal.rp.rijksweb.nl/irj/portal/?NavigationTarget=HLPFS://cisrijksportaal/ciskerntaken/cisrijksbreed/cisorganisatieenbedrijfsvoering/ci-sonderdelenbedrijfsvoering/cisbeveiligingsbeleid_1/cisvisieenstrategie_7/cisbeleidskaders_beveiliging/ciskader_rijkstoegangsbeleid_2

⁶ <http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2010/06/30/uitgangspunten-online-communicatie-rijksambtenaren.html>



Beleidsmakers

De beleidsmakers zijn verantwoordelijk voor het ontwikkelen van een veilig en werkbaar beleid. Het beleid moet goed uitvoerbaar en controleerbaar zijn.

Zie hoofdstukken 4, 5, 6, 10 en 12

Personeelszaken

Personeelszaken is verantwoordelijk voor werving, selectie en algemene zaken rond het functioneren van personeel, inclusief bewustwording en gedrag.

Zie hoofdstukken 8 en 13

Fysieke beveiliging

Fysieke beveiliging is vaak belegd bij Facility Management of bewakingsdiensten. Zij zijn verantwoordelijk voor de beveiliging van percelen, panden en ruimtes.

Zie hoofdstukken 4 en 9

IT-diensten en IT-infrastructuren

De IT diensten en infrastructuren zijn ondersteunend aan bijna alle processen. De eisen die aan IT voorzieningen gesteld worden zijn hierdoor zeer ingrijpend en bepalen voor een significant deel de inrichting van het IT landschap.

Zie hoofdstukken 4, 6, 10, 11 en 12

Applicatie eigenaren en systeemeigenaren

Applicatie eigenaren en systeemeigenaren zijn verantwoordelijk voor de veilige en correcte verwerking van de relevante data binnen de applicatie.

Zie hoofdstukken 7, 10 en 12

Eindgebruikers

Een belangrijk onderdeel van informatiebeveiliging is het gedrag van de eindgebruiker in de omgang met informatie.

Alle hoofdstukken

Informatiebeveiligingsadviseurs en IT auditors

Bij het helpen bepalen welke maatregelen relevant zijn en het controleren of de maatregelen daadwerkelijk genomen zijn is het hele document relevant.

Alle hoofdstukken

Externe leveranciers

De externe leveranciers zijn een bijzondere doelgroep. De opdrachtgever / systeemeigenaar altijd verantwoordelijk voor de kwaliteit en veiligheid van uitbestede diensten. De opdrachtgever eist van de externe leveranciers dat zij voldoen aan alle aspecten van BIR:2012 die voor de dienst of het betreffende systeem van belang zijn en betrekking hebben op de geleverde dienst.



3. Structuur van de norm

Hoofdstuk 4 laat zien hoe bepaald kan worden welke ICT-voorzieningen binnen de BIR:2012 vallen en voor welke ICT-voorzieningen er aanvullende maatregelen genomen moeten worden.

Hoofdstukken 5 t/m 15 bevatten hoofdveiligingscategorieën en subcategorieën.

Bij elke subcategorie is de doelstelling (uit ISO 27001:2005) vermeld. Elke subcategorie kent een aantal beheersmaatregelen, waarvan de nummering exact overeenkomt met ISO 27001:2005. De ISO 27001:2005 tekst van de beheersmaatregelen is cursief weergegeven.

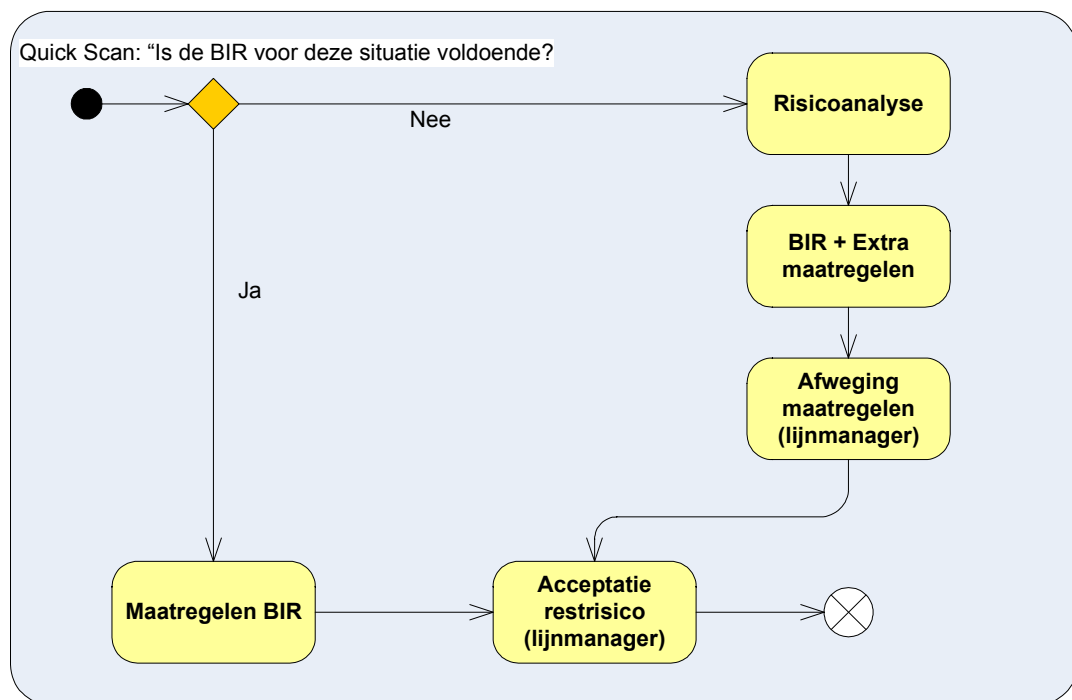
4. Risicobeoordeling en risicobehandeling

Volgens het VIR:2007 moet er een risicoafweging plaatsvinden. De mogelijke methodes hiervoor zijn risicoanalyse, baselinetoets, afhankelijkheid en kwetsbaarheid analyse of certificering.

Het beveiligingsniveau van de BIR:2012 is zo gekozen dat dit voor de meeste processen en ondersteunende IT voorzieningen bij de rijksdienst voldoende is. Hiermee wordt voorkomen dat er voor ieder systeem een uitgebreide risicoanalyse of A&K analyse uitgevoerd moet worden. Om vast te stellen dat het niveau van de BIR:2012 voldoende is, moet een baselinetoets uitgevoerd worden. Dit is schematisch weergegeven in figuur 3.

In de baselinetoets wordt onder meer bekeken of er staatsgeheime informatie verwerkt wordt, er sprake is van een WBP risicoklasse hoger dan 2, er hogere beschikbaarheidseisen vereist zijn of er dreigingen relevant zijn die niet in het dreigingprofiel van de BIR:2012 meegenomen zijn.

Voor wat betreft integriteit en vertrouwelijkheid is er sprake van hogere betrouwbaarheidseisen als het om staatsgeheimen (rubricering hoger dan Departementaal Vertrouwelijk) of Wet Bescherming Persoonsgegevens risicoklasse III gaat. Hogere betrouwbaarheidseisen kunnen ook voorkomen als er een dreiging relevant is die niet in het dreigingprofiel van de BIR:2012 is meegenomen (zie 2.2). Tot slot kan het mogelijk zijn dat een hogere beschikbaarheid noodzakelijk is. In deze gevallen zal een volledige risicoanalyse uitgevoerd moeten worden die kan leiden tot extra maatregelen.



Figuur 3: Gebruik van de maatregelen in de BIR:2012

Het lijnmanagement zal moeten afwegen of de kosten van de aanvullende maatregelen opwegen tegen de mogelijke schade van de risico's. Bij het niet nemen van een maatregel moet het restrisico (bewust) geaccepteerd worden.



5. Beveiligingsbeleid

5.1. Informatiebeveiligingsbeleid

Doelstelling

Directie richting en ondersteuning bieden voor Informatiebeveiliging overeenkomstig de bedrijfsmatige eisen en relevante wetten en voorschriften.

5.1.1. Beleidsdocumenten voor informatiebeveiliging

Een document met informatiebeveiligingsbeleid behoort door de directie te worden goedgekeurd en gepubliceerd en kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen.

1. Er is beleid voor informatiebeveiliging door het lijnmanagement vastgesteld, gepubliceerd en beoordeeld op basis van inzicht in risico's, kritische bedrijfsprocessen en toewijzing van verantwoordelijkheden en prioriteiten⁷

5.1.2. Beoordeling van het informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid behoort met geplande tussenpozen, of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.

1. **(R)** Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zonodig bijgesteld. Zie ook 6.1.8.1.

⁷ Het VIR:2007, VIRBI en BIR zijn vastgesteld rijksbreed beleid, het lijnmanagement is verantwoordelijk voor de invulling en uitvoering hiervan.



6. Organisatie van de Informatiebeveiliging

6.1. Interne organisatie

Doelstelling

Beheren van de informatiebeveiliging binnen de organisatie.

6.1.1. Betrokkenheid van de directie bij beveiliging

De directie behoort actief beveiliging binnen de organisatie te ondersteunen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen.

1. **(R)** Het lijnmanagement⁸ waarborgt dat de informatiebeveiligingsdoelstellingen worden vastgesteld, voldoen aan de kaders zoals gesteld in dit document en zijn geïntegreerd in de relevante processen. Dit gebeurt door één keer per jaar opzet, bestaan en werking van de IB-maatregelen te bespreken in het overleg van de departementsleiding en hiervan verslag te doen. Zie ook het in control statement zoals beschreven in het VIR:2007.

6.1.2. Coördineren van beveiliging

Activiteiten voor informatiebeveiliging behoren te worden gecoördineerd door vertegenwoordigers uit verschillende delen van de organisatie met relevante rollen en functies.

1. **(R)** De rollen van BVA, BVC en het lijnmanagement zijn beschreven in het Beveiligingsvoorschrift Rijksdienst 2005⁹.

6.1.3. Verantwoordelijkheden

Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd.

1. **(R)** Elke lijnmanager is verantwoordelijk voor de integrale beveiliging van zijn of haar dienstonderdeel.

6.1.4. Goedkeuringsproces voor ICT-voorzieningen

Er behoort een goedkeuringsproces voor nieuwe ICT-voorzieningen te worden vastgesteld en geïmplementeerd.

1. Er is een goedkeuringsproces voor nieuwe IT voorzieningen en wijzigingen in IT voorzieningen.

6.1.5. Geheimhoudingsovereenkomst

Eisen voor vertrouwelijkheid of geheimhoudingsovereenkomst die een weerslag vormen van de behoefte van de organisatie aan bescherming van informatie behoren te worden vastgesteld en regelmatig te worden beoordeeld.

1. **(R)** De algemene geheimhoudingsplicht voor ambtenaren is geregeld in de Ambtenarenwet art. 125a, lid 3. Daarnaast dienen personen die te maken hebben met Bijzondere Informatie een geheimhoudingsverklaring te ondertekenen (zie VIRBI); daaronder valt ook de departementaal vertrouwelijke informatie. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding.

⁸ In het VIR:2007 wordt de term “het lijnmanagement” gebruikt. In ISO 27002:2005 wordt van “de directie” gesproken.

⁹ Indien een functionaris gegevensbescherming is aangesteld, coördineert deze de informatiebeveiligings-aspecten van de Wet Bescherming Persoonsgegevens.



6.1.6. Contact met overheidsinstanties

Er behoren geschikte contacten met relevante overheidsinstanties te worden onderhouden.

1. **(R)** Het lijnmanagement stelt vast in welke gevallen en door wie er contacten met autoriteiten (brandweer, toezichthouders, enz.) wordt onderhouden.

6.1.7. Contact met speciale belangengroepen

Er behoren geschikte contacten met speciale belangengroepen of andere specialistische platforms voor beveiliging en professionele organisaties te worden onderhouden.

1. IB-specifieke informatie van relevante expertisegroepen, leveranciers van hardware, software en diensten wordt gebruikt om de informatiebeveiliging te verbeteren.

6.1.8. Beoordeling van het informatiebeveiligingsbeleid

De benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan (d.w.z. beheersdoelstellingen, beheersmaatregelen, beleid, processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met geplande tussenpozen te worden beoordeeld, of zodra zich significante wijzigingen voordoen in de implementatie van de beveiliging.

1. **(R)** Het informatiebeveiligingsbeleid wordt minimaal één keer in de drie jaar geëvalueerd (door een onafhankelijke deskundige) en desgewenst bijgesteld. Zie ook 5.1.2.
2. **(R)** Periodieke beveiligingsaudits worden uitgevoerd in opdracht van het lijnmanagement.
3. Over het functioneren van de informatiebeveiliging wordt, conform de P&C cyclus, jaarlijks gerapporteerd aan het lijnmanagement.

6.2. Externe Partijen

Doelstelling

Beveiligen van de informatie en ICT-voorzieningen van de organisatie handhaven waartoe externe partijen toegang hebben of die door externe partijen worden verwerkt of beheerd, of die naar externe partijen wordt gecommuniceerd.

6.2.1. Identificatie van risico's die betrekking hebben op externe partijen

De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend.

1. Informatiebeveiliging is aantoonbaar (op basis van een risicoafweging) meegewogen bij het besluit een externe partij wel of niet in te schakelen.
2. Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke toegang (fysiek, netwerk of tot gegevens) de externe partij(en) moet(en) hebben om de in het contract overeen te komen opdracht uit te voeren en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn.
3. **(R)** Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke waarde en gevoeligheid de informatie (bijv. risicoklasse van WBP of vertrouwelijkheidsklasse volgens VIRBI) heeft waarmee de derde partij in aanraking kan komen en of hierbij eventueel aanvullende beveiligingsmaatregelen nodig zijn.



4. Voorafgaand aan het afsluiten van een contract voor uitbesteding en externe inhuur is bepaald hoe geauthenticeerde en geautoriseerde toegang vastgesteld wordt.
5. **(R)** Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een bewerkrovereenkomst (conform WBP artikel 14) afgesloten.
6. Er is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd. (zie ook 6.2.3.3). Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits en penetratietests) en hoe het toezicht is geregeld.

6.2.2. Beveiliging behandelen in de omgang met klanten

Alle geïdentificeerde beveiligingseisen behoren te worden behandeld voordat klanten toegang wordt verleend tot de informatie of bedrijfsmiddelen van de organisatie.

1. Alle noodzakelijke beveiligingseisen worden op basis van een risicoafweging vastgesteld en geïmplementeerd voordat aan gebruikers toegang tot informatie op bedrijfsmiddelen wordt verleend.

6.2.3. Beveiliging behandelen in overeenkomsten met een derde partij

In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of ICT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan ICT-voorzieningen waarbij sprake is van toegang, behoren alle relevante beveiligingseisen te zijn opgenomen.

1. De maatregelen behorend bij 6.2.1 zijn voorafgaand aan het afsluiten van het contract gedefinieerd en geïmplementeerd.
2. Uitbesteding (ontwikkelen en aanpassen) van software is geregeld volgens formele contracten waarin o.a. intellectueel eigendom, kwaliteitsaspecten, beveiligingsaspecten, aansprakelijkheid, escrow en reviews geregeld worden.
3. In contracten met externe partijen is vastgelegd hoe men dient te gaan met wijzigingen en hoe ervoor gezorgd wordt dat de beveiliging niet wordt aangetast door de wijzigingen.
4. In contracten met externe partijen is vastgelegd hoe wordt omgegaan met geheimhouding.
5. Er is een plan voor beëindiging van de ingehuurde diensten waarin aandacht wordt besteed aan beschikbaarheid, vertrouwelijkheid en integriteit.
6. In contracten met externe partijen is vastgelegd hoe escalaties en aansprakelijkheid geregeld zijn.
7. Als er gebruikt gemaakt wordt van onderaannemers dan gelden daar dezelfde beveiligingseisen voor als voor de contractant. De hoofdaannemer is verantwoordelijk voor de borging bij de onderaannemer van de gemaakte afspraken.
8. De producten, diensten en daarbij geldende randvoorwaarden, rapporten en registraties die door een derde partij worden geleverd, worden beoordeeld op het nakomen van de afspraken in de overeenkomst. Verbeteracties worden geïnitieerd wanneer onder het afgesproken niveau wordt gepresteerd.



7. Beheer van bedrijfsmiddelen

7.1. Verantwoordelijkheid voor bedrijfsmiddelen

Doelstelling

Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.

7.1.1. Inventarisatie van bedrijfsmiddelen

Alle bedrijfsmiddelen behoren duidelijk te zijn geïdentificeerd en er behoort een inventaris van alle belangrijke bedrijfsmiddelen te worden opgesteld en bijgehouden.

1. Er is een actuele registratie van bedrijfsmiddelen die voor de organisatie een belang vertegenwoordigen zoals informatie(verzamelingen), software, hardware, diensten, mensen en hun kennis/vaardigheden. Van elk middel is de waarde voor de organisatie, het vereiste beschermingsniveau en de verantwoordelijke lijnmanager bekend.

7.1.2. Eigendom van bedrijfsmiddelen

Alle informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen behoren een eigenaar te hebben in de vorm van een aangewezen deel van de organisatie.

1. Voor elk bedrijfsproces, applicatie, gegevensverzameling en ICT-faciliteit is een verantwoordelijke lijnmanager benoemd.

7.1.3. Aanvaardbaar gebruik van bedrijfsmiddelen

Er behoren regels te worden vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen.

1. **(R)** Er zijn regels voor acceptabel gebruik van bedrijfsmiddelen (met name internet, e-mail en mobiele apparatuur). Het ARAR verplicht ambtenaren zich hieraan te houden. Voor extern personeel is dit in het contract vastgelegd. Zie ook "Uitgangspunten online communicatie rijksambtenaren" (Ministerie van Algemene Zaken, 2010)¹⁰.
2. Gebruikers hebben kennis van de regels.
3. Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen. De toestemming kan generiek geregeld worden in het kader van de functieafspraken tussen manager en medewerker.
4. **(R)** Informatiedragers worden dusdanig gebruikt dat vertrouwelijke informatie niet beschikbaar kan komen voor onbevoegde personen.

7.2. Classificatie van informatie

Doelstelling

Bewerkstelligen dat informatie een geschikt niveau van bescherming krijgt.

¹⁰ <http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2010/06/30/uitgangspunten-online-communicatie-rijksambtenaren.html>



Het VIRBI noemt classificatie "Rubricering" en beschrijft hoe de rubricering van informatie moet geschieden

7.2.1. Richtlijnen voor classificatie van informatie

Informatie behoort te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.

1. **(R)** De organisatie heeft rubriceringrichtlijnen opgesteld (ter invulling van het VIRBI).

7.2.2. Labeling en verwerking van informatie

Er behoren geschikte, samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de labeling en verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd.

1. **(R)** De lijnmanager heeft maatregelen (conform VIRBI) getroffen om te voorkomen dat niet geautoriseerde personen kennis kunnen nemen van gerubriceerde informatie.
2. **(R)** De opsteller van de informatie doet een voorstel tot rubricering en brengt deze aan op de informatie. De vaststeller van de inhoud van de informatie stelt tevens de rubricering vast.



8. Personele beveiliging

8.1. Beveiligen van personeel

Doelstelling

Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen..

8.1.1. Rollen en verantwoordelijkheden

De rollen en verantwoordelijkheden van werknemers, ingehuurd personeel en externe gebruikers ten aanzien van beveiliging behoren te worden vastgesteld en gedocumenteerd overeenkomstig het beleid voor informatiebeveiliging van de organisatie.

1. De taken en verantwoordelijkheden van een medewerker zijn opgenomen in de functiebeschrijving (zie ook de Ambtenarenwet) en worden onderhouden. In de functiebeschrijving wordt minimaal aandacht besteed aan:
 - uitvoering van het informatiebeveiligingsbeleid
 - bescherming van bedrijfsmiddelen
 - rapportage van beveiligingsincidenten
2. **(R)** Alle ambtenaren en ingehuurde medewerkers krijgen bij hun aanstelling hun verantwoordelijkheden ten aanzien van informatiebeveiliging ter inzage. De schriftelijk vastgestelde en voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging, welke zij bij de vervulling van hun dienst hebben na te leven, worden op een gemakkelijk toegankelijke plaats ter inzage gelegd. Overeenkomstige voorschriften maken deel uit van de contracten met externe partijen. Ook voor hen geldt de toegankelijkheid van geldende regelingen en instructies.
3. **(R)** Indien een medewerker speciale verantwoordelijkheden heeft t.a.v. informatiebeveiliging dan is hem dat voor indiensttreding (of bij functiewijziging), bij voorkeur in de aanstellingsbrief of bij het afsluiten van het contract, aantoonbaar duidelijk gemaakt.
4. De algemene voorwaarden van het arbeidscontract van medewerkers bevatten de wederzijdse verantwoordelijkheden ten aanzien van beveiliging. Het is aantoonbaar dat medewerkers bekend zijn met hun verantwoordelijkheden op het gebied van beveiliging.

8.1.2. Screening

Verificatie van de achtergrond van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers behoren te worden uitgevoerd overeenkomstig relevante wetten, voorschriften en ethische overwegingen, en behoren evenredig te zijn aan de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de waargenomen risico's.

1. **(R)** Voor alle medewerkers (ambtenaren en externe medewerkers) is minimaal een relevante Verklaring Omtrent het Gedrag (VOG) vereist. Indien het een vertrouwensfunctie betreft wordt ook een veiligheidsonderzoek (Verklaring van Geen Bezwaar) uitgevoerd.
2. Bij de aanstelling worden de gegevens die de medewerker heeft verstrekt over zijn arbeidsverleden en scholing geverifieerd (voor ambtenaren zie: ARAR art. 9, lid 3).



8.1.3. Arbeidsvoorwaarden

Als onderdeel van hun contractuele verplichting behoren werknemers, ingehuurd personeel en externe gebruikers de algemene voorwaarden te aanvaarden en te ondertekenen van hun arbeidscontract, waarin hun verantwoordelijkheden en die van de organisatie ten aanzien van informatiebeveiliging behoren te zijn vastgelegd.

8.2. Tijdens het dienstverband

Doelstelling

Bewerkstelligen dat alle werknemers, ingehuurd personeel en externe gebruikers zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheid en aansprakelijkheid, en dat ze zijn toegerust om het beveiligingsbeleid van de organisatie in hun dagelijkse werkzaamheden te ondersteunen, en het risico van een menselijke fout te verminderen.

8.2.1. Directieverantwoordelijkheid

De directie behoort van werknemers, ingehuurd personeel en externe gebruikers te eisen dat ze beveiliging toepassen overeenkomstig vastgesteld beleid en vastgestelde procedures van de organisatie.

1. Het lijnmanagement heeft een strategie ontwikkeld en geïmplementeerd om blijvend over specialistische kennis en vaardigheden van rijksambtenaren en ingehuurd personeel (die kritische bedrijfsactiviteiten op het gebied van IB uitoefenen) te kunnen beschikken.
2. Het lijnmanagement bevordert dat rijksambtenaren, ingehuurd personeel en (waar van toepassing) externe gebruikers van interne systemen algemene beveiligingsaspecten toepassen in hun gedrag en handelingen overeenkomstig vastgesteld beleid.

8.2.2. Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Alle werknemers van de organisatie en, voorzover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie.

1. Alle medewerkers van de organisatie worden regelmatig attent gemaakt op het beveiligingsbeleid en de beveiligingsprocedures van de organisatie, voor zover relevant voor hun functie.

8.2.3. Disciplinaire maatregelen

Er behoort een formeel disciplinair proces te zijn vastgesteld voor werknemers die inbreuk op de beveiliging hebben gepleegd.

1. **(R)** Er is een disciplinair proces vastgelegd voor medewerkers die inbreuk maken op het beveiligingsbeleid (zie ook: ARAR hoofdstuk VIII voor ambtenaren).

8.3. Beëindiging of wijziging van het dienstverband

Doelstelling

Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers ordelijk de organisatie verlaten of hun dienstverband wijzigen.

8.3.1. Beëindiging van verantwoordelijkheden

De verantwoordelijkheden voor beëindiging of wijziging van het dienstverband behoren duidelijk te zijn vastgesteld en toegewezen.



1. Voor ambtenaren is in de ambtseed of belofte vastgelegd welke verplichtingen ook na beëindiging van het dienstverband of bij functiewijziging nog van kracht blijven en voor hoe lang. Voor ingehuurd personeel (zowel in dienst van een derde bedrijf als individueel) is dit contractueel vastgelegd. Indien nodig wordt een geheimhoudingsverklaring ondertekend.
2. Het lijnmanagement heeft een procedure vastgesteld voor beëindiging van dienstverband, contract of overeenkomst waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten, innemen van bedrijfsmiddelen en welke verplichtingen ook na beëindiging van het dienstverband blijven gelden.
3. Het lijnmanagement heeft een procedure vastgesteld voor verandering van functie binnen de organisatie, waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten en innemen van bedrijfsmiddelen die niet meer nodig zijn na het beëindigen van de oude functie.

8.3.2. Retournering van bedrijfsmiddelen

Alle werknemers, ingehuurd personeel en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben te retourneren bij beëindiging van hun dienstverband, contract of overeenkomst.

1. Zie 8.3.1.3

8.3.3. Blokkering van toegangsrechten

De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en ICT-voorzieningen behoren te worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of behoort na wijziging te worden aangepast.

1. Zie 8.3.1.3



9. Fysieke beveiliging en beveiliging van de omgeving

9.1. Beveiligde ruimten

Doelstelling

Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie.

9.1.1. Fysieke beveiliging van de omgeving

Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en ICT-voorzieningen bevinden.

1. Voor iedere locatie is een beveiligingsplan opgesteld op basis van een risicoafweging.
2. Voor voorzieningen (binnen of buiten het gebouw) zijn duidelijke beveiligingsgrenzen bepaald.
3. Gebouwen bieden voldoende weerstand (bepaald op basis van een risicoafweging) bij gewelddadige aanvallen zoals inbraak en IT gericht vandalisme.
4. Er is 24-uur, 7 dagen per week bewaking; een inbraakalarm gekoppeld aan alarmcentrale is het minimum.
5. **(R)** Van ingehuurd bewakingsdiensten is vooraf geverifieerd dat zij voldoen aan de wettelijke eisen gesteld in de Wet Particuliere Beveiligingsorganisaties en Recherchebureaus. Deze verificatie wordt minimaal jaarlijks herhaald.
6. In gebouwen met serverruimtes houdt beveiligingspersoneel toezicht op de toegang. Hiervan wordt een registratie bijhouden.

9.1.2. Fysieke toegangsbeveiliging

Beveiligde zones behoren te worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.

1. Toegang tot gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.
2. **(R)** De beveiligingszones en toegangsbeveiliging daarvan zijn ingericht conform het Kader Rijkstoegangsbeleid.
3. In gebouwen met serverruimtes houdt beveiligingspersoneel toezicht op de toegang. Hiervan wordt een registratie bijhouden.
4. De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afgestemd op de zonering.
5. De uitgifte van toegangsmiddelen wordt geregistreerd.
6. Niet uitgegeven toegangsmiddelen worden opgeborgen in een beveiligd opbergmiddel.
7. Apparatuur en bekabeling in kabelverdeelruimtes en patchruimtes voldoen aan dezelfde eisen t.a.v. toegangbeveiliging zoals die worden gesteld aan computerruimtes.
8. **(R)** Er vindt minimaal één keer per half jaar een periodieke controle/evaluatie plaats op de autorisaties voor fysieke toegang.

9.1.3. Beveiliging van kantoren, ruimten en faciliteiten

Er behoort fysieke beveiliging van kantoren, ruimten en faciliteiten te worden ontworpen en toegepast.



1. Papieren documenten en mobiele gegevensdragers die vertrouwelijke informatie bevatten worden beveiligd opgeslagen.
2. **(R)** Er is actief beheer van sloten en kluizen met procedures voor wijziging van combinaties door middel van een sleutelplan. Ten behoeve van opslag van gerubriceerde informatie.
3. **(R)** Serruimtes, datacenters en daar aan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende best practices. Een goed voorbeeld van zo'n best practice is Telecommunication Infrastructure Standard for Data Centers (TIA-942).

9.1.4. Bescherming tegen bedreigingen van buitenaf

Er behoort fysieke bescherming tegen schade door brand, overstroming, aardshokken, explosies, oproer en andere vormen van natuurlijke of menselijke calamiteiten te worden ontworpen en toegepast.

1. Bij maatregelen is rekening gehouden met specifieke bedreigingen van aangrenzende panden of terreinen.
2. Reserve apparatuur en back-ups zijn op een zodanige afstand ondergebracht dat één en dezelfde calamiteit er niet voor kan zorgen dat zowel de hoofdlocatie als de back-up/reserve locatie niet meer toegankelijk zijn.
3. **(R)** Beveiligde ruimten waarin zich bedrijfskritische apparatuur bevindt zijn voldoende beveiligd tegen wateroverlast.
4. **(R)** Bij het betrekken van nieuwe gebouwen wordt een locatie gekozen waarbij rekening wordt gehouden met de kans op en de gevolgen van natuurrampen en door mensen veroorzaakte rampen.
5. Gevaarlijke of brandbare materialen zijn op een zodanige afstand van een beveiligde ruimte opgeslagen dat een calamiteit met deze materialen geen invloed heeft op de beveiligde ruimte.
6. **(R)** Er is door de brandweer goedgekeurde en voor de situatie geschikte brandblusapparatuur geplaatst en aangesloten. Dit wordt jaarlijks gecontroleerd.

9.1.5. Werken in beveiligde ruimten

Er behoren een fysieke bescherming en richtlijnen voor werken in beveiligde ruimten te worden ontworpen en toegepast.

1. Medewerkers die zelf niet geautoriseerd zijn mogen alleen onder begeleiding van bevoegd personeel en als er een duidelijke noodzaak voor is toegang krijgen tot fysiek beveiligde ruimten waarin IT voorzieningen zijn geplaatst of waarin met vertrouwelijke informatie wordt gewerkt.
2. Beveiligde ruimten (zoals een serverruimte of kluis) waarin zich geen personen bevinden zijn afgesloten en worden regelmatig gecontroleerd.
3. Zonder expliciete toestemming mogen binnen beveiligde ruimten geen opnames (foto, video of geluid) worden gemaakt.

9.1.6. Openbare toegang en gebieden voor laden en lossen

Toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, behoren te worden beheerst en indien mogelijk worden afgeschermd van IT voorzieningen, om onbevoegde toegang te voorkomen.

1. **(R)** Er bestaat een procedure voor het omgaan met verdachte pakketten en brieven in postkamers en laad- en losruimten.



9.2. Beveiliging van apparatuur

Doelstelling

Het voorkomen van verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.
Plaatsing en bescherming van apparatuur

9.2.1. Plaatsing en bescherming van apparatuur

Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang wordt verminderd.

1. Apparatuur wordt opgesteld en aangesloten conform de voorschriften van de leverancier. Dit geldt minimaal voor temperatuur en luchtvochtigheid, aarding, spanningsstabiliteit en overspanningbeveiliging.
2. Gebouwen zijn beveiligd tegen blikseminslag.
3. Eten en drinken is verboden in computerruimtes.
4. Een informatiesysteem voldoet altijd aan de hoogste beveiligingseisen die voor kunnen komen bij het verwerken van informatie. Indien dit niet mogelijk is wordt een gescheiden systeem gebruikt voor de informatieverwerking waaraan hogere eisen gesteld worden.

9.2.2. Nutsvoorzieningen

Apparatuur behoort te worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.

9.2.3. Beveiliging van kabels

Voedingskabels en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, behoren tegen interceptie of beschadiging te worden beschermd.

9.2.4. Onderhoud van apparatuur

Apparatuur behoort op correcte wijze te worden onderhouden, om te waarborgen dat deze voortdurend beschikbaar is en in goede staat verkeert.

1. **(R)** Reparatie en onderhoud van apparatuur (hardware) vindt op locatie plaats door bevoegd personeel, tenzij er geen data op het apparaat aanwezig of toegankelijk is.

9.2.5. Beveiliging van apparatuur buiten het terrein

Apparatuur buiten de terreinen behoort te worden beveiligd waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie.

1. Alle apparatuur buiten de terreinen wordt beveiligd met maatregelen die zijn vastgesteld op basis van een risicoafweging.

9.2.6. Veilig verwijderen of hergebruiken van apparatuur

Alle apparatuur die opslagmedia bevat, behoort te worden gecontroleerd om te bewerkstelligen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn overschreven voordat de apparatuur wordt verwijderd.

1. **(R)** Bij beëindiging van het gebruik of bij een defect worden apparaten en informatiedragers bij de beheersorganisatie ingeleverd. De beheerorganisatie zorgt voor een verantwoorde afvoer zodat er geen data op het apparaat aanwezig of



toegankelijk is. Als dit niet kan wordt het apparaat of de informatiedrager fysiek vernietigd. Het afvoeren of vernietigen wordt per bedrijfseenheid geregistreerd.

2. **(R)** Hergebruik van apparatuur buiten de organisatie is slechts toegestaan indien de informatie is verwijderd met een voldoende veilige methode. Een veilige methode is Secure Erase¹¹ voor apparaten die dit ondersteunen. In overige gevallen wordt de data twee keer overschreven met vaste data, één keer met random data en vervolgens wordt geverifieerd of het overschrijven is gelukt.

9.2.7. Verwijdering van bedrijfseigendommen

Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.

¹¹ G.F. Hughes, D.M. Commins, and T. Coughlin, Disposal of disk and tape data by secure sanitization, IEEE Security and Privacy, Vol. 7, No. 4, (July/August 2009), pp. 29-34.



10. Beheer van Communicatie- en Bedieningsprocessen

10.1. Bedieningsprocedures en verantwoordelijkheden

Doelstelling

Waarborgen van een correcte en veilige bediening van IT voorzieningen

10.1.1. Gedocumenteerde bedieningsprocedures

Bedieningsprocedures behoren te worden gedocumenteerd, te worden bijgehouden en beschikbaar te worden gesteld aan alle gebruikers die deze nodig hebben.

1. Bedieningsprocedures bevatten informatie over opstarten, afsluiten, back-uppen en herstelacties, afhandelen van fouten, beheer van logs, contactpersonen, noodprocedures en speciale maatregelen voor beveiliging.
2. Er zijn procedures voor de behandeling van digitale media die ingaan op ontvangst, opslag, rubricering, toegangsbeperkingen, verzending, hergebruik en vernietiging.

10.1.2. Wijzigingsbeheer

Wijzigingen in IT voorzieningen en informatiesystemen behoren te worden beheerst.

1. In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan:
 - het administreren van significante wijzigingen
 - impactanalyse van mogelijke gevolgen van de wijzigingen
 - goedkeuringsprocedure voor wijzigingen
2. **(R)** Instellingen van informatiebeveiligingsfuncties (b.v. security software) op het koppelvlak tussen vertrouwde en onvertrouwde netwerken, worden automatisch op wijzigingen gecontroleerd.

10.1.3. Functiescheiding

Taken en verantwoordelijkheidsgebieden behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.

1. Niemand in een organisatie of proces mag op uitvoerend niveau rechten hebben om een gehele cyclus van handelingen in een kritisch informatiesysteem te beheersen. Dit in verband met het risico dat hij of zij zichzelf of anderen onrechtmatig bevoordeelt of de organisatie schade toe brengt. Dit geldt voor zowel informatieverwerking als beheeracties.
2. **(R)** Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerswerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.
3. **(R)** Vóór de verwerking van gegevens die de integriteit van kritieke informatie of kritieke informatie systemen kunnen aantasten worden deze gegevens door een tweede persoon geïnspecteerd en geaccepteerd. Van de acceptatie wordt een log bijgehouden.
4. **(R)** Verantwoordelijkheden voor beheer en wijziging van gegevens en bijbehorende informatiesysteemfuncties moeten eenduidig toegewezen zijn aan één specifieke (beheerders)rol.



10.1.4. Scheiding van faciliteiten voor ontwikkeling, testen en productie

Faciliteiten voor ontwikkeling, testen en productie behoren te zijn gescheiden om het risico van onbevoegde toegang tot of wijzigingen in het productiesysteem te verminderen.

1. Er zijn minimaal logisch gescheiden systemen voor Ontwikkeling, Test en/of Acceptatie en Productie (OTAP). De systemen en applicaties in deze zones beïnvloeden systemen en applicaties in andere zones niet.
2. Gebruikers hebben gescheiden gebruiksprofielen voor Ontwikkeling, Test en/of Acceptatie en Productiesystemen om het risico van fouten te verminderen. Het moet duidelijk zichtbaar zijn in welk systeem gewerkt wordt.
3. **(R)** Indien er een experimenteer of laboratorium omgeving is, is deze fysiek gescheiden van de productieomgeving.

10.2. Exploitatie door een derde partij

Doelstelling

Een geschikt niveau van informatiebeveiliging en dienstverlening implementeren en bijhouden in overeenstemming met de overeenkomsten voor dienstverlening door een derde partij.

10.2.1. Dienstverlening

Er behoort te worden bewerkstelligd dat de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd en worden bijgehouden door die derde partij.

1. De uitbestedende partij blijft verantwoordelijk voor de betrouwbaarheid van uitbestede diensten.
2. Uitbesteding is goedgekeurd door de voor het informatiesysteem verantwoordelijke lijnmanager.

10.2.2. Controle en beoordeling van dienstverlening door een derde partij

De diensten, rapporten en registraties die door de derde partij worden geleverd, behoren regelmatig te worden gecontroleerd en beoordeeld en er behoren regelmatig audits te worden uitgevoerd.

1. Er worden afspraken gemaakt over de inhoud van rapportages, zoals over het melden van incidenten en autorisatiebeheer.
2. De in dienstverleningscontracten vastgelegde betrouwbaarheidseisen worden gemonitord. Dit kan bijvoorbeeld met audits of rapportages en gebeurt minimaal eens per drie maanden.
3. Er zijn voor beide partijen eenduidige aanspreekpunten.

10.2.3. Beheer van wijzigingen in dienstverlening door een derde partij

Wijzigingen in de dienstverlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, behoren te worden beheerd, waarbij rekening wordt gehouden met de onmisbaarheid van de betrokken bedrijfssystemen en -processen en met heroverweging van risico's.

1. Zie 10.1.2

10.3. Systeemplanning en –acceptatie

Doelstelling



Het risico van systeemstoringen tot een minimum beperken.

10.3.1. Capaciteitsbeheer

Het gebruik van middelen behoort te worden gecontroleerd en afgestemd en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen, om de vereiste systeemprestaties te bewerkstelligen.

1. **(R)** De ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. Er worden voorzieningen geïmplementeerd om de beschikbaarheid van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen).
Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen.
Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheidsis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen, waaronder verbindingen op te vangen.
2. **(R)** Er worden beperkingen opgelegd aan gebruikers en systemen ten aanzien van het gebruik van gemeenschappelijke middelen, zodat een enkele gebruiker (of systeem) niet meer van deze middelen kan opeisen dan nodig is voor de uitvoering van zijn of haar taak en daarmee de beschikbaarheid van systemen voor andere gebruikers (of systemen) in gevaar kan brengen.
3. **(R)** In koppelpunten met externe of onvertrouwde zones worden maatregelen getroffen om DDOS (Denial of Service attacks) aanvallen te signaleren en hierop te reageren. Het gaat hier om aanvallen die erop gericht zijn de verwerkingscapaciteit zodanig te laten vollopen, dat onbereikbaarheid of uitval van computers het gevolg is.¹²

10.3.2. Systeem acceptatie

Er behoren aanvaardingscriteria te worden vastgesteld voor nieuwe informatiesystemen, upgrades en nieuwe versies en er behoort een geschikte test van het systeem of de systemen te worden uitgevoerd tijdens ontwikkeling en voorafgaand aan de acceptatie.

1. **(R)** Van acceptatietesten wordt een log bijgehouden.
2. Er zijn acceptatiecriteria vastgesteld voor het testen van de beveiliging. Dit betreft minimaal OWASP¹³ of gelijkwaardig.

10.4. Bescherming tegen virussen en “mobile code”

Doelstelling

Beschermen van de integriteit van programmatuur en informatie.

10.4.1. Maatregelen tegen virussen

Er behoren maatregelen te worden getroffen voor detectie, preventie en herstellen om te beschermen tegen virussen en er behoren geschikte procedures te worden ingevoerd om het bewustzijn van de gebruikers te vergroten.

¹² Zie bijvoorbeeld de GovCert aanbevelingen: <http://www.govcert.nl/binaries/live/govcert/hst%3Acontent/dienstverlening/kennis-en-publicaties/whitepapers/bescherming-tegen-ddos-aanvallen/bescherming-tegen-ddos-aanvallen/govcert%3AdocumentResource/govcert%3Aresource>

¹³ Open Web Application Security Project (<http://www.owasp.org>)



1. **(R)** Bij het openen van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectie definities vindt frequent, minimaal één keer per dag, automatisch plaats.
2. **(R)** Inkomende en uitgaande e-mails worden gecontroleerd op virussen, trojans en andere malware. De update voor de detectie definities vindt frequent, minimaal één keer per dag, (automatisch) plaats.
3. In verschillende schakels van een keten binnen de infrastructuur van een organisatie wordt bij voorkeur antivirus programmatuur van verschillende leveranciers toegepast.
4. **(R)** Er zijn maatregelen om verspreiding van virussen tegen te gaan en daarmee schade te beperken (bijv. quarantaine en compartimentering).
5. Er zijn continuïteitsplannen voor herstel na aanvallen met virussen waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven.

10.4.2. Maatregelen tegen “mobile code”

Als gebruik van “mobile code” is toegelaten, behoort de configuratie te bewerkstelligen dat de geautoriseerde “mobile code” functioneert volgens een duidelijk vastgesteld beveiligingsbeleid, en behoort te worden voorkomen dat onbevoegde ‘mobile code’ wordt uitgevoerd.

1. Mobile code wordt uitgevoerd in een logisch geïsoleerde omgeving (sandbox) om de kans op aantasting van de integriteit van het systeem te verkleinen. De mobile code wordt altijd uitgevoerd met minimale rechten zodat de integriteit van het host systeem niet aangetast wordt.
2. Een gebruiker moet geen extra rechten kunnen toekennen aan programma's (bijv. internet browsers) die mobiele code uitvoeren.

10.5. Back-up

Doelstelling

Handhaven van de integriteit en beschikbaarheid van informatie en IT voorzieningen.

10.5.1. Reservekopieën maken (back-ups)

Er behoren back-upkopieën van informatie en programmatuur te worden gemaakt en regelmatig te worden getest overeenkomstig het vastgestelde back-upbeleid.

1. Er zijn (geteste) procedures voor back-up en recovery van informatie voor herinrichting en further herstel van verwerkingen.
2. Back-upstrategieën zijn vastgesteld op basis van het soort gegevens (bestanden, databases, enz.), de maximaal toegestane periode waarover gegevens verloren mogen raken, en de maximaal toelaatbare back-up- en hersteltijd.
3. Van back-upactiviteiten en de verblijfplaats van de media wordt een registratie bijgehouden, met een kopie op een andere locatie. De andere locatie is zodanig gekozen dat een incident/calamiteit op de oorspronkelijke locatie niet leidt tot schade aan of toegang tot de kopie van die registratie.
4. Back-ups worden bewaard op een locatie die zodanig is gekozen dat een incident op de oorspronkelijke locatie niet leidt tot schade aan de back-up.



5. De fysieke en logische toegang tot de back-ups, zowel van systeemschijven als van data, is zodanig geregeld dat alleen geautoriseerde personen zich toegang kunnen verschaffen tot deze back-ups.

10.6. Beheer van netwerkbeveiliging

Doelstelling

Bewerkstelligen van de bescherming van informatie in netwerken en bescherming van de ondersteunende infrastructuur.

10.6.1. Maatregelen voor netwerken

Netwerken behoren adequaat te worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd.

1. Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimum niveau komt.
2. **(R)** Gegevensuitwisseling tussen vertrouwde en onvertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.
3. **(R)** Bij transport van vertrouwelijke informatie over onvertrouwde netwerken, zoals het internet, dient altijd geschikte encryptie te worden toegepast. Zie hiertoe 12.3.1.3.
4. Er zijn procedures voor beheer van apparatuur op afstand.

10.6.2. Beveiliging van netwerkdiensten

Beveiligingskenmerken, niveaus van dienstverlening en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten.

10.7. Behandeling van media

Doelstelling

Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten.

10.7.1. Beheer van verwijderbare media

Er behoren procedures te zijn vastgesteld voor het beheer van verwijderbare media.

1. **(R)** Er zijn procedures opgesteld en geïmplementeerd voor opslag van vertrouwelijke informatie voor verwijderbare media.
2. **(R)** Verwijderbare media met vertrouwelijke informatie mogen niet onbeheerd worden achtergelaten op plaatsen die toegankelijk zijn zonder toegangscontrole.
3. In het geval dat media een kortere verwachte levensduur hebben dan de gegevens die ze bevatten, worden de gegevens gekopieerd wanneer 75% van de levensduur van het medium is verstreken.
4. Gegevensdragers worden behandeld volgens de voorschriften van de fabrikant.

10.7.2. Verwijdering van media

Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn,



overeenkomstig formele procedures.

1. **(R)** Er zijn procedures vastgesteld en in werking voor verwijderen van vertrouwelijke data en de vernietiging van verwijderbare media. Verwijderen van data wordt gedaan met een Secure Erase¹⁴ voor apparaten waar dit mogelijk is. In overige gevallen wordt de data twee keer overschreven met vaste data, één keer met random data en vervolgens wordt geverifieerd of het overschrijven is gelukt. Zie ook 9.2.6.

10.7.3. Procedures voor de behandeling van informatie

Er behoren procedures te worden vastgesteld voor de behandeling en opslag van informatie om deze te beschermen tegen onbevoegde openbaarmaking of misbruik.

10.7.4. Beveiliging van systeemdocumentatie

Systeemdokumentatie behoort te worden beschermd tegen onbevoegde toegang.

1. Systeemdokumentatie die vertrouwelijke informatie bevat is niet vrij toegankelijk.
2. **(R)** Wanneer de eigenaar er expliciet voor kiest om gerubriceerde systeemdokumentatie buiten de rijksdienst te brengen, doet hij dat niet zonder risicoafweging.

10.8. Uitwisseling van informatie

Doelstelling

Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld binnen een organisatie en met enige externe entiteit.

10.8.1. Beleid en procedures voor informatie-uitwisseling

Er behoren formeel beleid, formele procedures en formele beheersmaatregelen te zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.

1. **(R)** Het meenemen van Departementaal Vertrouwelijke informatie buiten gecontroleerd gebied vindt uitsluitend plaats indien dit voor de uitoefening van de functie noodzakelijk is.
2. Medewerkers zijn geïnstrueerd om zodanig om te gaan met (telefoon)gesprekken, e-mail, faxen en ingesproken berichten op antwoordapparaten dat de kans op uitlekken van vertrouwelijke informatie geminimaliseerd wordt.
3. Medewerkers zijn geïnstrueerd om zodanig om te gaan met mobiele apparatuur en verwijderbare media dat de kans op uitlekken van vertrouwelijke informatie geminimaliseerd wordt. Hierbij wordt minimaal aandacht besteed aan het risico van adreslijsten en opgeslagen boodschappen in mobiele telefoons.
4. Medewerkers zijn geïnstrueerd om geen vertrouwelijke documenten bij de printer te laten liggen.
5. Er zijn maatregelen getroffen om het automatisch doorsturen van interne e-mail berichten naar externe e-mail adressen te voorkomen.

10.8.2. Uitwisselingsovereenkomsten

Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.

¹⁴ G.F. Hughes, D.M. Commins, and T. Coughlin, Disposal of disk and tape data by secure sanitization, IEEE Security and Privacy, Vol. 7, No. 4, (July/August 2009), pp. 29-34.



1. Er zijn afspraken gemaakt over de beveiliging van de uitwisseling van gegevens en software tussen organisaties waarin de maatregelen om betrouwbaarheid, waaronder traceerbaarheid en onweerlegbaarheid, van gegevens te waarborgen zijn beschreven en getoetst.
2. Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, alsmede procedures over melding van incidenten.
3. Het eigenaarschap van gegevens en programmatuur en de verantwoordelijkheid voor de gegevensbescherming, auteursrechten, licenties van programmatuur zijn vastgelegd.
4. **(R)** Indien mogelijk wordt binnenkomende programmatuur (zowel op fysieke media als gedownload) gecontroleerd op ongeautoriseerde wijzigingen aan de hand van een door de leverancier via een gescheiden kanaal geleverde checksum of certificaat.

10.8.3. Fysieke media die worden getransporteerd

Media die informatie bevatten behoren te worden beschermd tegen onbevoegde toegang, misbruik of corrupteren tijdens transport buiten de fysieke begrenzing van de organisatie.

1. Om vertrouwelijke informatie te beschermen worden maatregelen genomen, zoals:
 - versleuteling
 - bescherming door fysieke maatregelen, zoals afgesloten containers
 - gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen
 - persoonlijke aflevering
 - opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes
2. **(R)** Fysieke verzending van bijzondere informatie dient te geschieden met ministerieel goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.

10.8.4. Elektronisch berichtenuitwisseling

Informatie die een rol speelt bij elektronische berichtenuitwisseling behoort op geschikte wijze te worden beschermd.

1. **(R)** Digitale documenten binnen de rijksdienst waar eindgebruikers rechten aan kunnen ontleen maken gebruik van PKI Overheid.
2. **(R)** Er is een (spam) filter geactiveerd voor e-mail berichten.

10.8.5. Systemen voor bedrijfsinformatie

Beleid en procedures behoren te worden ontwikkeld en geïmplementeerd om informatie te beschermen die een rol speelt bij de onderlinge koppeling van systemen voor bedrijfsinformatie.

1. Er zijn richtlijnen met betrekking tot het bepalen van de risico's die het gebruik van kantoorapplicaties met zich meebrengen en richtlijnen voor de bepaling van de beveiliging van kantoorapplicaties. Hierin is minimaal aandacht besteed aan de toegang tot de interne informatievoorziening, toegankelijkheid van agenda's, afscherming van documenten, beschikbaarheid en backup.

10.9. Diensten voor e-commerce

Doelstelling



Bewerkstelligen van de beveiliging van diensten voor e-commerce en het veilig gebruik van de diensten.

10.9.1. E-commerce

Informatie die een rol speelt bij e-commerce en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en modificatie.

1. **(R)** Waar mogelijk worden authentieke basisregistraties van de overheid gebruikt (b.v. GBA).

10.9.2. Onlinetransacties

Informatie die een rol speelt bij online transacties behoort te worden beschermd om onvolledige overdracht, onjuiste routing, onbevoegde wijziging van berichten, onbevoegde openbaarmaking, onbevoegde duplicatie of weergave van berichten te voorkomen.

1. Een transactie wordt bevestigd door een (gekwalficeerde) elektronische handtekening of een andere wilsuiting (bijv. een TAN code) van de gebruiker.
2. Een transactie is versleuteld, de partijen zijn geauthenticeerd en de privacy van betrokken partijen is gewaarborgd.

10.9.3. Openbaar beschikbare informatie

De betrouwbaarheid van de informatie die beschikbaar wordt gesteld op een openbaar toegankelijk systeem behoort te worden beschermd om onbevoegde modificatie te voorkomen.

1. Er zijn procedures die waarborgen dat gepubliceerde informatie is aangeleverd door daartoe geautoriseerde medewerkers.

10.10. Controle

Doelstelling

Ontdekken van onbevoegde informatieverwerkingsactiviteiten.

10.10.1. Aanmaken audit-logbestanden

Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.

1. Van logbestanden worden rapportages gemaakt die periodiek, minimaal maandelijks, worden beoordeeld.
2. **(R)** Een logregel bevat minimaal:
 - een tot een natuurlijk persoon herleidbare gebruikersnaam of ID
 - de gebeurtenis (zie 10.10.2.1)
 - waar mogelijk de identiteit van het werkstation of de locatie
 - het object waarop de handeling werd uitgevoerd
 - het resultaat van de handeling
 - de datum en het tijdstip van de gebeurtenis
3. **(R)** In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit Betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, enz.).



4. **(R)** Logberichten worden overzichtelijk samengevat. Daartoe zijn systemen die logberichten genereren aangesloten op een Security Information and Event Management systeem (SIEM¹⁵) waarmee meldingen en alarmoproepen aan de beheerorganisatie gegeven worden. Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen gegenereerd worden.
5. Controle op opslag van logging: het vollopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijv. een logserver die niet bereikbaar is).

10.10.2. Controle van systeemgebruik

Er behoren procedures te worden vastgesteld om het gebruik van IT voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld.

1. De volgende gebeurtenissen worden in ieder geval opgenomen in de logging:
 - gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling; uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore
 - gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases)
 - handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoordreset, uitgifte en intrekken van cryptosleutels
 - beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services)
 - verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen)
 - handelingen van gebruikers en systeembeheerders, zoals systeemtoegang, gebruik van online transacties en toegang tot bestanden.

10.10.3. Bescherming van informatie in logbestanden

Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.

1. Het (automatisch) overschrijven of verwijderen van logbestanden wordt gelogd in de nieuw aangelegde log.
2. **(R)** Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.
3. Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.
4. De instellingen van logmechanismen worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingen aangepast moeten te worden zal daarbij altijd het vier ogen principe toegepast worden.
5. **(R)** De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de systeemeigenaar. Bij een (vermoed) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.

¹⁵ Een SIEM systeem kan, afhankelijk van de context, meer of minder uitgebreid zijn. Essentieel is dat de loggegevens van beveiligingscomponenten en authenticatiemiddelen dusdanig overzichtelijk worden gepresenteerd dat belangrijke meldingen niet gemist worden.



6. Controle op opslag van logging: het vollopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijv. een logserver die niet bereikbaar is).

10.10.4. Logbestanden van administrators en operators

Activiteiten van systeemadministrators en systeemoperators behoren in logbestanden te worden vastgelegd.

1. Zie 10.10.1

10.10.5. Registratie van storingen

Storingen behoren in logbestanden te worden vastgelegd en te worden geanalyseerd en er behoren geschikte maatregelen te worden genomen.

1. Zie 10.10.1

10.10.6. Synchronisatie van systeemklokken

De klokken van alle relevante informatiesystemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.

1. Systeemklokken worden zodanig gesynchroniseerd dat altijd een betrouwbare analyse van logbestanden mogelijk is.



11. Toegangsbeveiliging

11.1. Toegangsbeleid

Doelstelling

Beheersen van de toegang tot informatie.

11.1.1. Toegangsbeleid

Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang.

11.2. Beheer van toegangsrechten van gebruikers

Doelstelling

Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot informatiesystemen voorkomen.

11.2.1. Registratie van gebruikers

Er behoren formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.

1. Gebruikers worden vooraf geïdentificeerd en geautoriseerd. Van de registratie wordt een administratie bijgehouden.
2. **(R)** Authenticatiegegevens worden bijgehouden in één bronbestand) zodat consistentie is gegarandeerd.
3. **(R)** Op basis van een risicoafweging wordt bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.

11.2.2. Beheer van (speciale) bevoegdheden

De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst.

1. Gebruikers hebben toegang tot speciale bevoegdheden voor zover dat voor de uitoefening van hun taak noodzakelijk is (need to know, need to use).
2. Systeemprocessen draaien onder een eigen gebruikersnaam (een functioneel account), voor zover deze processen handelingen verrichten voor andere systemen of gebruikers.
3. Gebruikers krijgen slechts toegang tot een noodzakelijk geachte set van applicaties en commando's.

11.2.3. Beheer van gebruikerswachtwoorden

De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst.

1. Wachtwoorden worden nooit in originele vorm (plaintext) opgeslagen of verstuurd, maar in plaats daarvan wordt bijvoorbeeld de hashwaarde van het wachtwoord opgeslagen.
2. Ten aanzien van wachtwoorden geldt:



- Wachtwoorden worden op een veilige manier uitgegeven (controle identiteit van de gebruiker).
- Tijdelijke wachtwoorden of wachtwoorden die standaard in software worden meegegeven worden bij eerste gebruik vervangen door een persoonlijk wachtwoord.
- Gebruikers bevestigen de ontvangst van een wachtwoord.

11.2.4. Beoordeling van toegangsrechten van gebruikers

De directie behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces.

1. Toegangsrechten van gebruikers worden periodiek, minimaal jaarlijks, geëvalueerd. Het interval is beschreven in het toegangsbeleid en is bepaald op basis van het risiconiveau.

11.3. Verantwoordelijkheden van gebruikers

Doelstelling

Voorkomen van onbevoegde toegang door gebruikers, en van beschadiging of diefstal van informatie en ICT-voorzieningen.

11.3.1. Gebruik van wachtwoorden

Gebruikers behoren goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden.

1. Aan de gebruikers is een set gedragsregels aangereikt met daarin minimaal het volgende:
 - Wachtwoorden worden niet opgeschreven.
 - Gebruikers delen hun wachtwoord nooit met anderen.
 - Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde.
 - Wachtwoorden worden niet gebruikt in automatische inlogprocedures (bijv. opgeslagen onder een functietoets of in een macro).

11.3.2. Onbeheerde gebruikersapparatuur

Gebruikers behoren te bewerkstelligen dat onbeheerde apparatuur passend is beschermd.

1. De gebruiker vergrendelt de werkplek tijdens afwezigheid.

11.3.3. Clear desk en clear screen

Er behoort een 'clear desk'-beleid voor papier en verwijderbare opslagmedia en een 'clear screen'-beleid voor ICT-voorzieningen te worden ingesteld.

1. In het clear desk beleid staat minimaal dat de gebruiker geen vertrouwelijke informatie op het bureau mag laten liggen. Deze informatie moet altijd worden opgeborgen in een afsluitbare opbergmogelijkheid (kast, locker, bureau of kamer).
2. Bij afdrukken van gevoelige informatie wordt, wanneer mogelijk, gebruik gemaakt van de functie "beveiligd afdrukken" (pincode verificatie).
3. **(R)** Schermbeveiligingsprogrammatuur (een screensaver) maakt na een periode van inactiviteit van maximaal 15 minuten alle informatie op het beeldscherm onleesbaar en ontoegankelijk.
4. **(R)** Toegangsbeveiliging lock wordt automatisch geactiveerd bij het verwijderen van een token (indien aanwezig).



11.4. Toegangsbeheersing voor netwerken

Doelstelling

Het voorkomen van onbevoegde toegang tot netwerkdiensten.

11.4.1. Beleid ten aanzien van het gebruik van netwerkdiensten

Gebruikers behoort alleen toegang te worden verleend tot diensten waarvoor ze specifiek bevoegd zijn.

1. Er is een gedocumenteerd beleid met betrekking tot het gebruik van netwerken en netwerkdiensten. Gebruikers krijgen slechts toegang tot de netwerkdiensten die voor het werk noodzakelijk zijn. Zie ook 11.2.2.3.

11.4.2. Authenticatie van gebruikers bij externe verbindingen

Er behoren geschikte authenticatiemethoden te worden gebruikt om toegang van gebruikers op afstand te beheersen.

1. Zie ook 11.6.1.3.

11.4.3. Identificatie van (netwerk)apparatuur

Automatische identificatie van apparatuur behoort te worden overwogen als methode om verbindingen vanaf specifieke locaties en apparatuur te authenticeren.

1. **(R)** Alleen geïdentificeerde en geauthenteerde apparatuur kan worden aangesloten op een vertrouwde zone. Eigen, ongeauthenteerde, apparatuur (Bring Your Own Device) wordt alleen aangesloten op een onvertrouwde zone.

11.4.4. Bescherming op afstand van poorten voor diagnose en configuraties

De fysieke en logische toegang tot poorten voor diagnose en configuratie behoort te worden beheerst.

1. Poorten, diensten en soortgelijke voorzieningen op een netwerk of computer die niet vereist zijn voor de dienst dienen te worden afgesloten.

11.4.5. Scheiding van netwerken

Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.

1. **(R)** Werkstations worden zo ingericht dat routeren van verkeer tussen verschillende zones of netwerken niet mogelijk is.
2. **(R)** De indeling van zones binnen de technische infrastructuur vindt plaats volgens een operationeel beleidsdocument waarin is vastgelegd welke uitgangspunten voor zonering worden gehanteerd. Van systemen wordt bijgehouden in welke zone ze staan. Er wordt periodiek, minimaal één keer per jaar, geëvalueerd of het systeem nog steeds in de optimale zone zit of verplaatst moet worden.
3. **(R)** Elke zone heeft een gedefinieerd beveiligingsniveau. Zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie.
4. **(R)** Beheer en audit van zones vindt plaats vanuit een minimaal logisch gescheiden, separate zone.
5. Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).



11.4.6. Beheersmaatregelen voor netwerkverbindingen

Voor gemeenschappelijke netwerken, vooral waar deze de grenzen van de organisatie overschrijden, behoren de toegangsmogelijkheden voor gebruikers te worden beperkt, overeenkomstig het toegangsbeleid en de eisen van bedrijfstoeepassingen (zie 11.1).

11.4.7. Beheersmaatregelen voor netwerkrouting

Netwerken behoren te zijn voorzien van beheersmaatregelen voor netwerkrouting, om te bewerkstelligen dat computerverbindingen en informatiestromen niet in strijd zijn met het toegangsbeleid voor de bedrijfstoeepassingen.

1. Netwerken zijn voorzien van beheersmaatregelen voor routing gebaseerd op mechanismen ter verificatie van bron en bestemmingsadressen.

11.5. Toegangsbeveiliging voor besturingssystemen

Doelstelling

Voorkomen van onbevoegde toegang tot besturingssystemen.

11.5.1. Beveiligde inlogprocedures

Toegang tot besturingssystemen behoort te worden beheerst met een beveiligde inlogprocedure.

1. **(R)** Toegang tot kritische toepassingen of toepassingen met een hoog belang wordt verleend op basis van twee-factor authenticatie.
2. Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.
3. Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.
4. Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.
5. **(R)** Nadat voor een gebruikersnaam 5 keer een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lockout periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lockout op te heffen of het wachtwoord te resetten.

11.5.2. Gebruikersidentificatie en –authenticatie

Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen.

1. Bij uitgifte van authenticatiemiddelen wordt minimaal de identiteit vastgesteld evenals het feit dat de gebruiker recht heeft op het authenticatiemiddel.
2. Bij het intern gebruik van IT voorzieningen worden gebruikers minimaal geauthenticeerd op basis van wachtwoorden.
3. **(R)** Applicaties mogen niet onnodig en niet langer dan noodzakelijk onder een systeemaccount (een privileged user zoals administrator of root) draaien. Direct na het uitvoeren van handelingen waar hogere rechten voor nodig zijn, wordt weer teruggeschakeld naar het niveau van een gewone gebruiker (een unprivileged user).



11.5.3. Systemen voor wachtwoordenbeheer

Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.

1. Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (o.a. voldoende sterke wachtwoorden¹⁶, regelmatige wijziging, directe wijziging van initieel wachtwoord).
2. **(R)** Wachtwoorden hebben een geldigheidsduur van maximaal 3 maanden. Daarbinnen dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd.
3. **(R)** Wachtwoorden die gereset zijn en initiële wachtwoorden hebben een zeer beperkte geldigheidsduur en moeten bij het eerste gebruik worden gewijzigd.
4. De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Hierbij geldt het volgende:
 - Voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geauthenticeerd.
 - Ter voorkoming van typfouten in het nieuw gekozen wachtwoord is er een bevestigingsprocedure.

11.5.4. Gebruik van systeemhulpmiddelen

Het gebruik van hulpprogrammatuur waarmee systeem- en toepassingsbeheersmaatregelen zouden kunnen worden gepasseerd behoort te worden beperkt en behoort strikt te worden beheerst.

11.5.5. Time-out van sessies

Inactieve sessies behoren na een vastgestelde periode van inactiviteit te worden uitgeschakeld.

1. **(R)** De periode van inactiviteit van een werkstation is vastgesteld op maximaal 15 minuten. Daarna wordt de PC vergrendeld. Bij remote desktop sessies geldt dat na maximaal 15 minuten inactiviteit de sessie verbroken wordt.

11.5.6. Beperking van verbindingstijd

De verbindingstijd behoort te worden beperkt als aanvullende beveiliging voor toepassingen met een verhoogd risico.

1. **(R)** De toegang voor onderhoud op afstand door een leverancier wordt alleen opengesteld op basis een wijzigingsverzoek of storingsmelding.

11.6. Toegangsbeheersing voor toepassingen en informatie

Doelstelling

Voorkomen van onbevoegde toegang tot informatie in toepassingssystemen.

¹⁶ Een voldoende sterk wachtwoord is een wachtwoord waarvan de entropie hoog is, deze is afhankelijk van de lengte en het aantal mogelijke tekens. Zie ook "The true costs of unusable password policies", (<http://www.cl.cam.ac.uk/~rja14/shb10/angela2.pdf>) en Gartner research note G00124970 (http://www.indevis.de/dokumente/gartner_passwords_breakpoint.pdf).



11.6.1. Beperken van toegang tot informatie

Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel behoort te worden beperkt overeenkomstig het vastgestelde toegangsbeleid.

1. In de soort toegangsregels wordt tenminste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.
2. **(R)** Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten.
3. **(R)** Bij extern gebruik vanuit een onvertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.
4. **(R)** Een beheerder gebruikt two-factor authenticatie voor het beheer van kritische apparaten. B.v. een sleutel tot beveiligde ruimte en een password of een token en een password.

11.6.2. Isoleren van gevoelige systemen

Gevoelige systemen behoren een eigen, vast toegewezen (geïsoleerde) computeromgeving te hebben.

1. **(R)** Gevoelige systemen (met hoge beschikbaarheid of grote vertrouwelijkheid) behoren een eigen vast toegewezen (geïsoleerde) computeromgeving te hebben. Isoleren kan worden bereikt door fysieke of logische methoden.

11.7. Draagbare computers en telewerken

Doelstelling

Waarborgen van informatiebeveiliging bij het gebruik van draagbare computers en faciliteiten voor telewerken.

11.7.1. Draagbare computers en communicatievoorzieningen

Er behoort formeel beleid te zijn vastgesteld en er behoren geschikte beveiligingsmaatregelen te zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.

1. **(R)** Het mobiele apparaat is waar mogelijk zo ingericht dat geen bedrijfsinformatie wordt opgeslagen ("zero footprint"). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, geldt: een mobiel apparaat (zoals een handheld computer, tablet, smartphone, PDA) biedt de mogelijkheid om de toegang te beschermen d.m.v. een wachtwoord en versleuteling van die gegevens.
Voor printen in onvertrouwde omgevingen vindt een risicoafweging plaats
2. **(R)** Er zijn, waar mogelijk, voorzieningen om de actualiteit van anti-malware programmatuur op mobiele apparaten te garanderen.
3. **(R)** Bij melding van verlies of diefstal wordt de communicatiemogelijkheid met de centrale applicaties afgesloten.

11.7.2. Telewerken

Er behoren beleid, operationele plannen en procedures voor telewerken te worden ontwikkeld en geïmplementeerd.

1. Er wordt een beleid met gedragsregels en een geschikte implementatie van de techniek opgesteld t.a.v. telewerken.
2. **(R)** De telewerkvoorzieningen zijn waar mogelijk zo ingericht dat op de werkplek (thuis of op een andere locatie) geen bedrijfsinformatie wordt opgeslagen ("zero footprint") en mogelijke malware vanaf de werkplek niet in het vertrouwde deel



terecht kan komen.

Voor printen in onvertrouwde omgevingen vindt een risicoafweging plaats.



12. Verwerving, ontwikkeling en onderhoud van Informatiesystemen

12.1. Beveiligingseisen voor informatiesystemen

Doelstelling

Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.

12.1.1. Analyse en specificatie van beveiligingseisen

In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen behoren ook eisen voor beveiligingsmaatregelen te worden opgenomen.

1. In projecten worden een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen.
2. In standaarden voor analyse, ontwikkeling en testen van informatiesystemen wordt structureel aandacht besteed aan beveiligingsaspecten. Waar mogelijk wordt gebruikt gemaakt van bestaande richtlijnen (bijv. secure coding guidelines¹⁷).
3. Bij aanschaf van producten wordt een proces gevolgd waarbij beveiliging een onderdeel is van de specificatie.
4. Waar het gaat om beveiligingsrelevante producten wordt de keuze voor een bepaald product verantwoord onderbouwd.
5. Voor beveiliging worden componenten gebruikt die aantoonbaar voldoen aan geaccepteerde beveiligingscriteria zoals NBV¹⁸ goedkeuring of certificering volgens ISO/IEC 15408 (common criteria)¹⁹.

12.2. Correcte verwerking in toepassingen

Doelstelling

Voorkomen van fouten, verlies, onbevoegde modificatie of misbruik van informatie in toepassingen.

12.2.1. Validatie van invoergegevens

Gegevens die worden ingevoerd in toepassingen behoren te worden gevalideerd om te bewerkstelligen dat deze gegevens juist en geschikt zijn.

1. Er moeten controles worden uitgevoerd op de invoer van gegevens. Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen en inconsistentie van gegevens.

12.2.2. Beheersing van interne gegevensverwerking

Er behoren validatiecontroles te worden opgenomen in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken.

¹⁷ Voor voorbeelden van secure coding guidelines, zie <http://www.cert.org/secure-coding/>

¹⁸ NBV: Nationaal Bureau voor Verbindingsbeveiliging, onderdeel van het ministerie van BZK.

¹⁹ Voor een common criteria beoordeling moet een bewuste keuze worden gedaan voor een EAL niveau en een protection profiële dat voldoende is voor de toepassing.



1. Er bestaan voldoende mogelijkheden om reeds ingevoerde gegevens te kunnen corrigeren door er gegevens aan te kunnen toevoegen.
2. Het informatiesysteem moet functies bevatten waarmee vastgesteld kan worden of gegevens correct verwerkt zijn. Hiermee wordt een geautomatiseerde controle bedoeld waarmee (duidelijke) transactie- en verwerkingsfouten kunnen worden gedetecteerd.
3. Stapelen van fouten wordt voorkomen door toepassing van “noodstop” mechanismen.
4. Verwerkingen zijn bij voorkeur herstelbaar zodat bij het optreden van fouten en/of wegraken van informatie dit hersteld kan worden door het opnieuw verwerken van de informatie.

12.2.3. Integriteit van berichten

Er behoren eisen te worden vastgesteld, en geschikte beheersmaatregelen te worden vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.

12.2.4. Validatie van uitvoergegevens

Gegevensuitvoer uit een toepassing behoort te worden gevalideerd, om te bewerkstelligen dat de verwerking van opgeslagen gegevens op de juiste manier plaatsvindt en geschikt is gezien de omstandigheden.

1. De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijv. door checksums).
2. Bij uitvoer van gegevens wordt gegarandeerd dat deze met het juiste niveau van vertrouwelijkheid beschikbaar gesteld worden (bijv. beveiligd printen).
3. **(R)** Alleen gegevens die noodzakelijk zijn voor de doeleinden van de gebruiker worden uitgevoerd (need to know).

12.3. Cryptografische beheersmaatregelen

Doelstelling

Beschermen van de vertrouwelijkheid, authenticiteit of integriteit van informatie met behulp van cryptografische middelen.

12.3.1. Beleid voor het gebruik van cryptografische beheersmaatregelen

Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.

1. De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst.
2. Bij de inzet van cryptografische producten volgt een afweging van de risico's aangaande locaties, processen en behandelende partijen.
3. **(R)** De cryptografische beveiligingsvoorzieningen en componenten voldoen aan algemeen gangbare beveiligingscriteria (zoals FIPS 140-2 en waar mogelijk NBV).



12.3.2. Sleutelbeheer

Er behoort sleutelbeheer te zijn vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie.

1. In het sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden.
2. De geldigheidsduur van cryptografische sleutels wordt bepaald aan de hand van de beoogde toepassing en is vastgelegd in het cryptografisch beleid.
3. De vertrouwelijkheid van cryptografische sleutels moet worden gewaarborgd tijdens generatie, gebruik, transport en opslag van de sleutels.
4. Er is een procedure vastgesteld waarin is bepaald hoe wordt omgegaan met gecompromitteerde sleutels.
5. **(R)** Bij voorkeur is sleutelmanagement ingericht volgens PKI Overheid

12.4. Beveiliging van systeembestanden

Doelstelling

Beveiliging van systeembestanden bewerkstelligen.

12.4.1. Beheersing van operationele programmatuur

Er behoren procedures te zijn vastgesteld om de installatie van programmatuur op productiesystemen te beheersen.

1. Alleen geautoriseerd personeel kan functies en software installeren of activeren.
2. Programmatuur behoort pas te worden geïnstalleerd op een productieomgeving na een succesvolle test en acceptatie.
3. Geïnstalleerde programmatuur, configuraties en documentatie worden bijgehouden in een configuratiedatabase.
4. Er worden alleen door de leverancier²⁰ onderhouden (versies van) software gebruikt.
5. Van updates wordt een log bijgehouden.
6. Er is een rollbackstrategie.

12.4.2. Bescherming van testdata

Testgegevens behoren zorgvuldig te worden gekozen, beschermd en beheerst.

1. Het gebruik van kopieën van operationele databases voor testgegevens wordt vermeden. Indien toch noodzakelijk, worden de gegevens zoveel mogelijk geanonimiseerd en na de test zorgvuldig verwijderd.

12.4.3. Toegangsbeheersing voor broncode van programmatuur

De toegang tot broncode van programmatuur behoort te worden beperkt.

²⁰ Dit kan ook een interne leverancier zijn.



1. De toegang tot broncode wordt zoveel mogelijk beperkt om de code tegen onbedoelde wijzigingen te beschermen. Alleen geautoriseerde personen hebben toegang.

12.5. Beveiliging bij ontwikkelingsprocessen en ondersteuningsprocessen

Doelstelling

Beveiliging van toepassingsprogrammatuur en -informatie handhaven.

12.5.1. Procedures voor wijzigingsbeheer

De implementatie van wijzigingen behoort te worden beheerst door middel van formele procedures voor wijzigingsbeheer.

1. Er is aantoonbaar wijzigingsmanagement ingericht volgens gangbare best practices zoals ITIL²¹.

12.5.2. Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem

Bij wijzigingen in besturingssystemen behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de activiteiten of beveiliging van de organisatie.

1. Van aanpassingen (zoals updates) aan softwarematige componenten van de technische infrastructuur wordt vastgesteld dat deze de juiste werking van de technische componenten niet in gevaar brengen.

12.5.3. Restricties op wijzigingen in programmatuurpakketten

Wijzigingen in programmatuurpakketten behoren te worden ontmoedigd, te worden beperkt tot noodzakelijke wijzigingen, en alle wijzigingen behoren strikt te worden beheerst.

1. Bij het instellen van besturingsprogrammatuur en programmapakketten wordt uitgegaan van de aanwijzingen van de leverancier.

12.5.4. Uitlekken van informatie

Er behoort te worden voorkomen dat zich gelegenheden voordoen om informatie te laten uitlekken.

1. Op het grensvlak van een vertrouwde en een onvertrouwde omgeving vindt content-scanning plaats.

12.5.5. Uitbestede ontwikkeling van programmatuur

Uitbestede ontwikkeling van programmatuur behoort onder supervisie te staan van en te worden gecontroleerd door de organisatie.

1. Uitbestede ontwikkeling van programmatuur komt tot stand onder supervisie en verantwoordelijkheid van de uitbestedende organisatie. Er worden maatregelen getroffen om de kwaliteit en vertrouwelijkheid te borgen (bijv. stellen van veiligheidseisen, regelen van beschikbaarheid en eigendomsrecht van de code, certificatie, kwaliteitsaudits, testen en aansprakelijkheidsregelingen).

²¹ Information Technology Infrastructure Library, zie <http://www.itil-officialsite.com>



12.6. Beheer van technische kwetsbaarheden

Doelstelling

Risico's verminderen als gevolg van benutting van gepubliceerde technische kwetsbaarheden.

12.6.1. Beheersing van technische kwetsbaarheden

Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's.

1. Er is een proces ingericht voor het beheer van technische kwetsbaarheden; dit omvat minimaal periodieke penetratietests, risicoanalyses van kwetsbaarheden en patching.
2. Van softwarematige voorzieningen van de technische infrastructuur kan (bij voorkeur geautomatiseerd) gecontroleerd worden of de laatste updates (patches) in zijn doorgevoerd. Het doorvoeren van een update vindt niet geautomatiseerd plaats, tenzij hier speciale afspraken over zijn met de leverancier.
3. Indien een patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch te worden geëvalueerd (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch).
4. **(R)** Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde



13. Beheer van Informatiebeveiligingsincidenten

13.1. Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken

Doelstelling

Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.

13.1.1. Rapportage van informatiebeveiligingsgebeurtenissen

Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.

1. Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident.
2. **(R)** Er is een contactpersoon aangewezen voor het rapporteren van beveiligingsincidenten. Voor integriteitsschendingen is ook een vertrouwenspersoon aangewezen die meldingen in ontvangst neemt.
3. Vermissing of diefstal van apparatuur of media die gegevens van de Rijksdienst kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident.
4. **(R)** Informatie over de beveiligingsrelevante handelingen van de gebruiker wordt regelmatig nagekeken. De BVA bekijkt maandelijks een samenvatting van de informatie.

13.1.2. Rapportage van zwakke plekken in de beveiliging

Van alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen en –diensten behoort te worden geëist dat zij alle waargenomen of verdachte zwakke plekken in systemen of diensten registreren en rapporteren.

1. Er is een proces om eenvoudig en snel beveiligingsincidenten en zwakke plekken in de beveiliging te melden.

13.2. Beheer van informatiebeveiligingsincidenten en –verbeteringen

Doelstelling

Bewerkstelligen dat een consistente en doeltreffende benadering wordt toegepast voor het beheer van informatiebeveiligingsincidenten.

13.2.1. Verantwoordelijkheden en procedures

Er behoren leidinggevende verantwoordelijkheden en procedures te worden vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen.

1. Er zijn procedures voor rapportage van gebeurtenissen en escalatie. Alle medewerkers behoren op de hoogte te zijn van deze procedures.

13.2.2. Leren van informatiebeveiligingsincidenten

Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen gekwantificeerd en gecontroleerd.



1. De informatie verkregen uit het beoordelen van beveiligingsmeldingen wordt geëvalueerd met als doel beheersmaatregelen te verbeteren.

13.2.3. Verzamelen van bewijsmateriaal

Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

1. Voor een vervolgprocedure naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.



14. Bedrijfscontinuïteitsbeheer

14.1. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Doelstelling

Tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.

14.1.1. Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer

Er behoort een beheerd proces voor bedrijfscontinuïteit in de gehele organisatie te worden ontwikkeld en bijgehouden, voor de naleving van eisen voor informatiebeveiliging die nodig zijn voor de continuïteit van de bedrijfsvoering.

1. (R) Calamiteitenplannen worden gebruikt in de jaarlijkse bewustwording-, training- en testactiviteiten.

14.1.2. Bedrijfscontinuïteit en risicobeoordeling

Gebeurtenissen die tot onderbreking van bedrijfsprocessen kunnen leiden, behoren te worden geïdentificeerd, tezamen met de waarschijnlijkheid en de gevolgen van dergelijke onderbrekingen en hun gevolgen voor informatiebeveiliging.

1. Er is een Business Impact Analyse (BIA) waarin de gebeurtenissen worden geïdentificeerd die kunnen leiden tot discontinuïteit in het bedrijfsproces. Aan de hand van een risicoanalyse zijn de waarschijnlijkheid en de gevolgen van de discontinuïteit in kaart gebracht in termen van tijd, schade en herstelperiode.

14.1.3. Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging

Er behoren plannen te worden ontwikkeld en geïmplementeerd om de bedrijfsactiviteiten te handhaven of te herstellen en om de beschikbaarheid van informatie op het vereiste niveau en in de vereiste tijdspanne te bewerkstelligen na onderbreking of uitval van kritische bedrijfsprocessen.

1. In de continuïteitsplannen wordt minimaal aandacht besteed aan:
 - Identificatie van essentiële procedures voor bedrijfscontinuïteit.
 - Veilig te stellen informatie (aanvaardbaarheid van verlies van informatie).
 - Prioriteiten en volgorde van herstel en reconstructie.
 - Documentatie van systemen en processen.
 - Kennis en kundigheid van personeel om de processen weer op te starten.

14.1.4. Kader voor de bedrijfscontinuïteitsplanning

Er behoort een enkelvoudig kader voor bedrijfscontinuïteitsplannen te worden gehandhaafd om te bewerkstelligen dat alle plannen consistent zijn, om eisen voor informatiebeveiliging op consistente wijze te behandelen en om prioriteiten vast te stellen voor testen en onderhoud.

14.1.5. Testen, onderhoud en herbeoordelen van bedrijfscontinuïteitsplannen

Bedrijfscontinuïteitsplannen behoren regelmatig te worden getest en geüpdate, om te bewerkstelligen dat ze actueel en doeltreffend blijven.



1. **(R)** Er worden minimaal jaarlijks oefeningen en testen gehouden om de bedrijfscontinuïteitsplannen en mate van readiness van de organisatie te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold.



15. Naleving

15.1. Naleving van wettelijke voorschriften

Doelstelling

Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van enige beveiligingseisen.

15.1.1. Identificatie van toepasselijke wetgeving

Alle relevante wettelijke en regelgevende eisen en contractuele verplichtingen en de benadering van de organisatie in de naleving van deze eisen, behoren expliciet te worden vastgesteld, gedocumenteerd en actueel te worden gehouden voor elk informatiesysteem en voor de organisatie.

1. Er is vastgesteld welke wetten en wettelijke maatregelen van toepassing zijn op de organisatie of organisatieonderdelen.

15.1.2. Intellectuele eigendomsrechten (Intellectual Property Rights)

Er behoren geschikte procedures te worden geïmplementeerd om te bewerkstelligen dat wordt voldaan aan de wettelijke en regelgevende eisen en contractuele verplichtingen voor het gebruik van materiaal waarop intellectuele eigendomsrechten kunnen berusten en het gebruik van programmatuur waarop intellectuele eigendomsrechten berusten.

1. Er is toezicht op het naleven van wettelijke verplichtingen m.b.t. intellectueel eigendom, auteursrechten en gebruiksrechten.

15.1.3. Bescherming van bedrijfsdocumenten

Belangrijke registraties behoren te worden beschermd tegen verlies, vernietiging en vervalsing, overeenkomstig wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.

15.1.4. Bescherming van gegevens en geheimhouding van persoonsgegevens

De bescherming van gegevens en privacy behoort te worden bewerkstelligd overeenkomstig relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen²².

15.1.5. Voorkomen van misbruik van IT voorzieningen

Gebruikers behoren ervan te worden weerhouden IT voorzieningen te gebruiken voor onbevoegde doeleinden.

1. Er is een beleid met betrekking tot het gebruik van IT voorzieningen door gebruikers. Dit beleid is bekendgemaakt en op de goede werking ervan wordt toegezien

15.1.6. Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Cryptografische beheersmaatregelen behoren overeenkomstig alle relevante overeenkomsten, wetten en voorschriften te worden gebruikt.

1. Er is vastgesteld aan welke overeenkomsten, wetten en voorschriften de toepassing van cryptografische technieken moet voldoen. Zie ook 12.3.

²² Zie artikel 12 Wet Bescherming persoonsgegevens



15.2. Naleving van beveiligingsbeleid en -normen en technische naleving

Doelstelling

Bewerkstelligen dat systemen voldoen aan het beveiligingsbeleid en de beveiligingsnormen van de organisatie.

15.2.1. Naleving van beveiligingsbeleid en -normen

Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen.

1. Het lijnmanagement is verantwoordelijk voor uitvoering en beveiligingsprocedures en toetsing daarop (o.a. jaarlijkse in control verklaring). Conform het BVR zorgt de Beveiligingsambtenaar, namens de Secretaris Generaal, voor het toezicht op de uitvoering van het beveiligingsbeleid. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door of vanwege de BVA dan wel door interne of externe auditteams.
2. **(R)** In de P&C cyclus wordt gerapporteerd over informatiebeveiliging aan de hand van het in control statement.

15.2.2. Controle op technische naleving

Informatiesystemen behoren regelmatig te worden gecontroleerd op naleving van implementatie van beveiligingsnormen.

1. Informatiesystemen worden regelmatig gecontroleerd op naleving van beveiligingsnormen. Dit kan door bijv. kwetsbaarheidsanalyses en penetratietesten. Zie ook 12.6.1.1.

15.3. Overwegingen bij audits van informatiesystemen

Doelstelling

Doeltreffendheid van audits van het informatiesysteem maximaliseren en verstoring als gevolg van systeemaudits minimaliseren.

15.3.1. Beheersmaatregelen voor audits van informatiesystemen

Eisen voor audits en andere activiteiten waarbij controles worden uitgevoerd op productiesystemen, behoren zorgvuldig te worden gepland en goedgekeurd om het risico van verstoring van bedrijfsprocessen tot een minimum te beperken.

15.3.2. Bescherming van hulpmiddelen voor audits van informatiesystemen

Toegang tot hulpmiddelen voor audits van informatiesystemen behoort te worden beschermd om mogelijk misbruik of compromittering te voorkomen.



16. Bijlage A: Begrippen

Audittrail	Vastlegging van de complete keten van opeenvolgende wijzigingen op een object in een bepaalde periode.
Basis beveiligingsniveau	Het geheel van maatregelen van beveiliging dat wordt bereikt door het implementeren en toepassen van de normen zoals geformuleerd in de Code voor Informatiebeveiliging, Business Continuity Management en WBP risicoklasse 2 en waaraan de NORA een nadere uitwerking geeft, onder meer door normen voor ICT-voorzieningen.
Bedrijfsmiddel	Elk middel waarin of waarmee bedrijfsgegevens kunnen worden opgeslagen en/of verwerkt en waarmee toegang tot gebouwen, ruimten en ICT-voorzieningen kan worden verkregen: een bedrijfsproces, een gedefinieerde groep activiteiten, een gebouw, een apparaat, een ICT-voorziening of een gedefinieerde groep gegevens.
Beschikbaarheid	De waarborg dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen).
Beveiliging	Het brede begrip van informatiebeveiliging, d.w.z. inclusief fysieke beveiliging, Business Continuity Management (BCM), ofwel beschikbaarheid van bedrijfsprocessen en persoonlijke veiligheid en integriteit.
Beveiligingsincident	Het manifest worden van een beveiligingsrisico (dreiging, oorzaak) als gevolg van een overtreding van beveiligingsregel, bijv. onbevoegde toegang tot ICT-voorzieningen.
Beveiligingsinstellingen	In ICT-voorzieningen kunnen in veel gevallen functionaliteiten die invloed hebben op beveiliging geactiveerd, gewijzigd of uitgeschakeld worden door het opgeven van parameterwaarden.
Clear Desk	Anders dan Clean Desk, waarbij het bureau helemaal leeg is, betekent Clear Desk dat er geen vertrouwelijke informatie op het bureau ligt.
Controleerbaarheid	De mate waarin de werkelijkheid of representaties daarvan toetsbaar zijn, dat wil zeggen te vergelijken met andere "werkelijkheden of representaties daarvan" zodat objectieve oordeelsvorming mogelijk wordt.
Elektronische handtekening	Een elektronische handtekening is een methode voor het bevestigen van de juistheid van digitale informatie door middel van technieken van de asymmetrische cryptografie. De elektronische handtekening bestaat uit twee algoritmen: een om te bevestigen dat de informatie niet door derden veranderd is, de ander om de identiteit te bevestigen van degene die de informatie "ondertekent". De technieken worden toegepast met behulp van een PKI.
Filtering	Het gecontroleerd doorlaten van gegevens op het grensvlak tussen zones in een netwerk.
Firewall	Het geheel van software- en eventueel ook hardwarevoorzieningen dat voorkomt dat ongewenst verkeer van de ene netwerkzone terecht komt in de andere, teneinde de veiligheid in de laatstgenoemde te verhogen.
Hardening	Overbodige functies in besturingssystemen uitschakelen en/of van het systeem verwijderen en zodanige waarden toekennen aan beveiligingsinstellingen dat een maximale beveiliging ontstaat.
IB-functie	Een geheel van automatische informatiebeveiligingsverwerkingen die logisch met elkaar samenhangen.



ICT-voorzieningen	Applicaties en technische infrastructuur, of wel het geheel van ICT-voorzieningen.
In control statement	In de toelichting van VIR:2007 wordt een managementverantwoording – een in control statement – gevraagd voor wat betreft de informatiebeveiliging. Daarbij moet worden aangesloten bij de Planning en Control cyclus. BIR voegt hier aan toe: De in control verklaring moet inzicht geven aan welke BIR:2012 normen wordt voldaan en voor welke BIR:2012 normen een explain is gedefinieerd.
Informatiebeveiliging	Het proces van vaststellen van de vereiste betrouwbaarheid van informatieverwerking in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
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.
Integrale beveiliging	Integrale beveiliging is de beveiliging van vastgestelde te beschermen belangen (TBB) door op basis van risicomanagement en een kosten/batenanalyse een samenhangend stelsel van beveiligingsmaatregelen te selecteren en te implementeren. Het besturingsmodel voor integrale beveiliging sluit aan bij de besturingsuitgangspunten binnen de departementen: het lijnmanagement is integraal verantwoordelijk en dus ook voor de beveiliging van de TBB. (bron: eindproduct werkgroep integrale beveiliging, Geaccepteerd in de ICBR d.d. 10 juli 2012).
Integriteit	Het waarborgen van de juistheid en volledigheid en tijdigheid van informatie en de verwerking ervan. Als de tijdigheid van gegevens bepaald wordt door omstandigheden buiten het systeem, kan deze vanzelfsprekend niet als integriteits voor het systeem gesteld worden.
Logging	Vastlegging van systeemhandelingen.
Malware	Software met ongewenste functies, zoals virussen en trojans.
Mobile code	Code afkomstig van een ander systeem die lokaal uitgevoerd wordt, bijv. Javascript, Flash of Silverlight.
Onvertrouwd	Geen zekerheid over het beveiligingsniveau of zekerheid over het lager dan vereiste beveiligingsniveau
Onweerlegbaarheid	Het niet kunnen ontkennen iets te hebben gedaan (bijvoorbeeld een bericht te hebben ontvangen dan wel te hebben verstuurd).
Patch	Klein onderdeel van software dat de leverancier van software uitgeeft om fouten aan door hem vervaardigde software te repareren
Query	Bevraging in een vraagtaal, die op basis van gebruikersvriendelijke en krachtige commando's selecties en berekeningen op bestanden kan uitvoeren, in eerste instantie alleen voor raadpleegdoeleinden.
Technische infrastructuur	Het geheel van ICT-voorzieningen voor generiek gebruik, zoals servers, firewalls, netwerkapparatuur, besturingssystemen voor netwerken en servers, database management systemen en beheer- en beveiligingstools, inclusief bijbehorende systeembestanden.
Two-factor authenticatie	Two-factor authenticatie vereist het gebruik van twee van de drie volgende authenticatiemethoden: • iets dat de gebruiker weet (b.v. password, PIN); • iets dat de gebruiker heeft (b.v. toegangspas, sleutel); en • iets dat de gebruiker is (b.v. biometrische eigenschap zoals een vingerafdruk).



Vertrouwd	In overeenstemming met een door een bevoegde autoriteit vastgesteld beveiligingsniveau. Bijvoorbeeld vertrouwde zones of vertrouwde netwerken zoals in 10.6.1.2 en 10.6.1.3.
Vertrouwelijkheid	Het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.
Vertrouwelijke informatie	Informatie die niet algemeen bekend mag worden (bron: van Dale) In het kader van de BIR:2012 worden maatregelen beschreven die voldoen voor de behandeling van gerubriceerde informatie tot en met departementaal vertrouwelijk (volgens definitie uit VIRBI) en persoonsvertrouwelijke informatie van risicoklassen 1 en 2 zoals gedefinieerd de toelichting op de WBP: AV23 ²³ .
Verwijderbare media	Opslagmiddelen die los van apparatuur kunnen worden verwijderd en meegenomen. Zoals CRDROMs, USB sticks, verwijderbare schijven, tapes of gedrukte media.
Zone	De logische verzameling van ICT-voorzieningen met hetzelfde beveiligingsniveau, die via beveiligde koppelvlakken gegevens kunnen uitwisselen

²³ Beveiliging van persoonsgegevens.

Registratiekamer: Achtergrondstudies en Verkenningen 23

http://www.cbpweb.nl/Pages/av_23_Beveiliging.aspx