INFORMATIE
BEVEILIGINGS
DIENST

TACTISCHE BASELINE INFORMATIEBEVEILIGING NEDERLANDSE GEMEENTEN

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN
VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Meer informatie

Heeft u vragen over onderhavig document? De Informatiebeveiligingsdienst voor gemeenten beantwoordt deze graag via IBD@kinggemeenten.nl of via 070 373 8011.

Wijzigingshistorie:

Versie	Datum	Opmerkingen
1	6 mei 2013	Eerste versie van de BIG
1.01	Mei 2015	Opmerkingen verwerkt welke uit de gemeenten zijn ontvangen in de voorgaande periode. Zie apart wijzigingenblad
1.02	Juni 2016	copyright aangepast in verband met ISO tekst gebruik, link naar de NEN

De Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) is geheel gestructureerd volgens NEN/ISO 27001, bijlage A en NEN/ISO 27002. Met klem vermeldt zij dat de Tactische BIG deze normen niet vervangt. De overheid is conform de voorschriften van het College Standaardisatie, verplicht om aan ISO 27001 en ISO 27002 te voldoen middels pas toe of leg uit. De Basisrichtlijn Informatiebeveiliging Rijksdienst (BIR) is een toepassingshandleiding voor NEN/ISO 27001 en 27002 voor de Rijksoverheid. De BIR beschrijft de aanvullingen op NEN/ISO27001 en 27002 voor de overheid. In de Tactische Baseline zijn die aanvullingen gemerkt met een [A].
NEN/ISO 27001 en 27002 beschrijven details voor implementatie, zogenaamde implementatierichtlijnen, en eisen voor wat betreft de procesinrichting (o.a. het ISMS uit NEN/ISO 27001). Die documenten geven dus de details voor toepassing en kunnen naast de tactische BIG gebruikt worden.

Gerelateerde documenten

Titel	Auteur	Jaartal	Omschrijving
NEN-ISO/IEC-27001/27002	NEN	2005 / 2007	De code voor informatiebeveiliging, www.nen.nl
Wbp			Wet bescherming persoonsgegevens
SUWI			SUWI-wet en -aansluitvoorwaarden
Normenkader GeVS	BKWI	2011	Gezamenlijke elektronische Voorzieningen SUWI
BIR familie			Baseline Informatiebeveiliging Rijksdienst
BRP[1]			Basisregistratie Personen.
BIA	ISF	2007	Business Impact Analyse
GEMMA	KING		GEMeentelijk Model Architectuur (GEMMA)
NORA		2007	De Nederlandse Overheid Referentie Architectuur
ITIL security management	Spruit, M. (HEC)	2003	www.marcelspruit.nl/papers/itilsecman.pdf
RASCI			www.kwaliteitshandvesten.nl
Best Practice Normen Informatiebeveiliging ICT-Voorzieningen	Jaap van der Veen	2009	Versie 1.0
Diverse NCSC documenten			www.ncsc.nl

[1] De Basisregistratie Personen (BRP) heeft de Gemeentelijke Basisadministratie Personen (GBA) vervangen. In de BRP staan persoonsgegevens van inwoners in Nederland (de ingezetenen) en van personen in het buitenland die een relatie hebben met de Nederlandse overheid (de niet-ingezetenen).

Basiskennis informatiebeveiliging volgens NEN-ISO 2700x	J. Hintzbergen en anderen	2011	van Haren Publishing
Provinciale Baseline Informatiebeveiliging	Diverse auteurs	2010	
Diverse informatie beveiligingsplannen gemeenten	Diverse auteurs		
Het inrichten van een beveiligingsorganisatie. Welke factoren zijn van invloed	PvIB	2006	http://www.pvib.nl/download/?id=6259853

Management samenvatting

De Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten is het normenkader dat de beschikbaarheid, integriteit en exclusiviteit van gemeentelijke informatie(systemen) bevordert. Deze Tactische Baseline is een normenkader die een totaalpakket aan informatiebeveiligingsmaatregelen omvat die voor iedere gemeente geldt. Deze Tactische Baseline is opgezet rondom bestaande normen; de NEN/ISO 27002:2007 en NEN/ISO 27001:2005. Deze standaarden zijn voor de Nederlandse overheid gekozen en algemeen aanvaard als de norm voor informatiebeveiliging. Voor specifieke maatregelen is in onderhavige Tactische Baseline ook gebruik gemaakt van de Wbp, de SUWI-wet, BRP[2], BAG en PUN. In de update van de BIG versie 1.01 van 2015 is nog niet de nieuwe NEN/ISO 27001:2013 en NEN/ISO27002:2013 meegenomen, Omdat de BIG en aanverwante baselines zoals de BIWA, de BIR volgt zal de update naar de nieuwe ISO normen niet eerder plaatsvinden nadat de BIR is aangepast. Bovendien is het zo dat gemeenten die de huidige BIG invoeren er niet bij gebaad zijn om midden in dit proces te confronteren met een nieuwe BIG.

Achtergrond

Door de toenemende digitalisering is het zorgvuldig omgaan met de informatie en gegevens van burgers, bedrijven en ketenpartners voor gemeenten van groot belang. Uitval van computers of telecommunicatiesystemen, het in ongerede raken van gegevensbestanden of het door onbevoegden kennisnemen dan wel manipuleren van bepaalde gegevens kan ernstige gevolgen hebben voor de continuïteit van de bedrijfsvoering en het primaire proces. Een betrouwbare, beschikbare en correcte informatiehuishouding is essentieel voor de dienstverlening van gemeenten. Het is niet ondenkbaar dat hieraan ook politieke consequenties verbonden zijn of dat het imago van de gemeente en daarmee van de overheid in het algemeen wordt geschaad.

De DigiNotar-crisis en Lektober in 2011 hebben aangetoond dat de ICT-infrastructuur van gemeenten kwetsbaar is. Uit de acties rondom Lektober is gebleken dat de gemeentelijke beveiliging van de ICT-infrastructuur en de opgeslagen informatie niet bij alle gemeenten even goed op orde is.

In 2012 hebben gemeenten aanzienlijke investeringen gedaan om incidenten op te lossen als gevolg van het zogenaamde Dorifel virus[3]. Onderzoek van TNO geeft aan dat cybercriminaliteit de Nederlandse economie jaarlijks ongeveer €10 miljard kost. Deze

[2] De Basisregistratie Personen (BRP) heeft de Gemeentelijke Basisadministratie Personen (GBA) vervangen. In de BRP staan persoonsgegevens van inwoners in Nederland (de ingezetenen) en van personen in het buitenland die een relatie hebben met de Nederlandse overheid (de niet-ingezetenen).

[3] http://webwereld.nl/nieuws/111490/dorifel-kost-gemeenten-tienduizenden-euro-s.html

raming zou kunnen betekenen dat de schade door cybercriminaliteit voor gemeenten jaarlijks ongeveer €300 miljoen bedraagt.[4]

Maar de beveiligingsincidenten gaan over meer dan geld alleen. De overheid beheert veel persoonsgegevens. Als de overheid de beveiliging hiervan niet voldoende kan waarborgen, is het vertrouwen in de overheid in het geding. Een incident met de rioleringspompen in een gemeente liet zien dat het mogelijk is om op afstand via internet pompen, en vergelijkbare systemen als sluizen en gemalen, te hacken. In dergelijke gevallen is ook de fysieke veiligheid van burgers in het geding.

De belangrijkste les uit de incidenten is dan ook dat er behoefte is aan een fundamentele oplossing van het informatieveiligheidsprobleem bij gemeenten. De Rijksoverheid gaat eveneens nadere eisen stellen aan de beveiliging van de gemeentelijke informatiehuishouding, bijvoorbeeld als voorwaarde om aangesloten te zijn en te blijven op DigiD. Ook in het onderzoek van de Onderzoeksraad voor Veiligheid naar het DigiNotar-incident is een dergelijk aanbeveling opgenomen. Naast het ontwikkelen van een Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten is de volgende stap op dit pad het ontwikkelen van een Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten. Deze ligt nu voor u.

Opdracht

Doel

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft opdracht gegeven voor het ontwikkelen van een Baseline Informatiebeveiliging Nederlandse Gemeenten. De Baseline Informatiebeveiliging Nederlandse Gemeenten is bedoeld om:

1. Gemeenten op een vergelijkbare manier efficiënt te laten werken met informatiebeveiliging.
2. Gemeenten een hulpmiddel te geven om aan alle eisen op het gebied van Informatiebeveiliging te kunnen voldoen.
3. De auditlast bij gemeenten te verminderen.
4. Gemeenten een aantoonbaar betrouwbare partner te laten zijn.

Een betrouwbare informatievoorziening is essentieel voor het goed functioneren van de processen bij gemeenten. Informatiebeveiliging is het proces dat deze betrouwbare informatievoorziening borgt. Het opnemen van informatiebeveiliging als kwaliteitscriterium voor een gezonde bedrijfsvoering is tegenwoordig niet langer een keuze, het is bittere noodzaak geworden.

De integrale Baseline Informatiebeveiliging Nederlandse Gemeenten bestaat uit drie delen:

[4] http://www.nu.nl/internet/2783983/cybercrime-kost-nederland-10-miljard-per-jaar--.html

1. BIG – Strategische Baseline

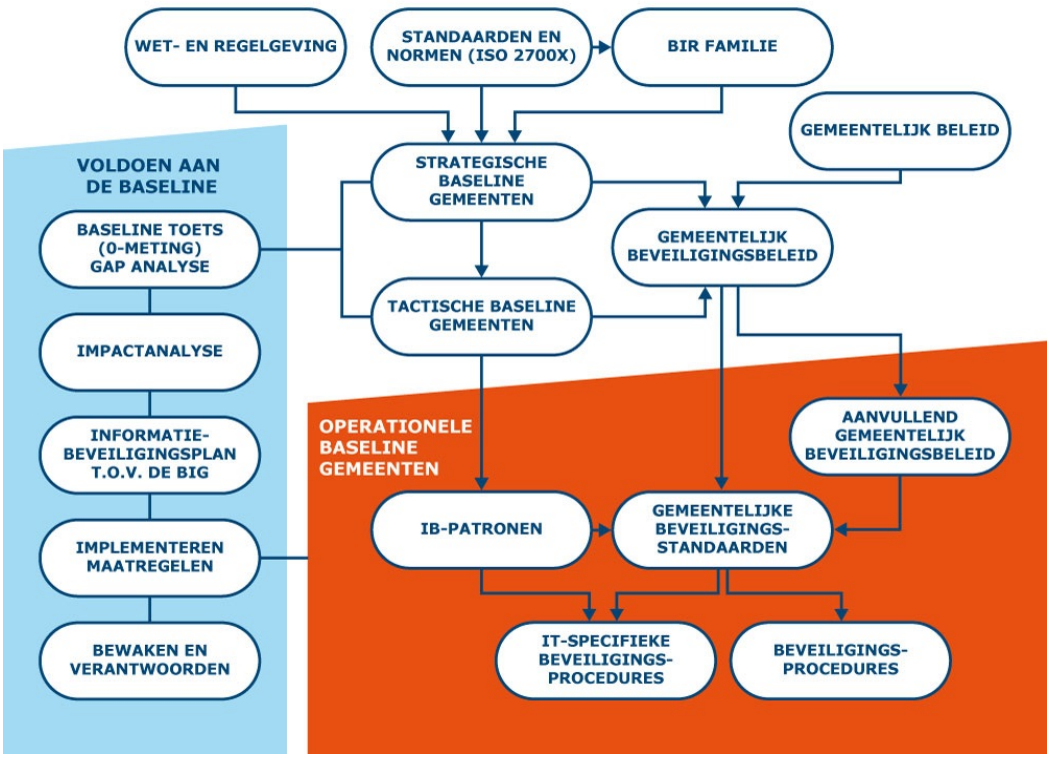
   De Strategisch Baseline kan gezien worden als de 'kapstok' waaraan de elementen van informatiebeveiliging opgehangen kunnen worden. Centraal staan de organisatie en de verantwoording over informatiebeveiliging binnen de gemeente. De Strategische Baseline is een separaat document.

2. BIG – Tactische Baseline

   De Tactische Baseline beschrijft de normen en maatregelen ten behoeve van controle en risicomanagement. De Tactische Baseline beschrijft aan de hand van dezelfde indeling als de internationale beveiligingsnorm ISO/IEC 27002:2007, de controls/maatregelen die als Tactische Baseline gelden voor de gemeenten. De Tactische Baseline omvat onderhavig document.

3. BIG – Operationele baseline

   Om de invoering van de Strategische en Tactische Baseline te ondersteunen, zijn door de IBD producten ontwikkeld op operationeel niveau. Deze producten zijn samen met een groot aantal betrokken gemeenten vervaardigd, vertegenwoordigers van deze gemeenten hebben de producten gereviewd.



Figuur 1: Structuur van de BIG documenten

Leeswijzer

Structuur

De indeling van dit document is als volgt:

1. Het algemene deel over deze Tactische Baseline, uitleg, relaties met architectuur frameworks, hoe met onderhavige Tactische Baseline kan worden omgegaan etc.

    Hoofdstuk 1 tot en met 4

2. Een Tactisch Baseline met de basisset aan maatregelen die voor alle gemeenten geldt.

    Hoofdstuk 5 tot en met 15

3. Een drietal bijlagen

Doelgroepen

Deze Tactische Baseline bevat aandachtsgebieden voor verschillende functionarissen binnen de doelgroep gemeenten. Hieronder worden per functionaris de hoofdstukken genoemd die relevant zijn.

IB functionarissen (Dat wil zeggen, Informatiebeveiligingsfunctionarissen van alle niveaus[5])

Alle hoofdstukken

Informatiebeveiligingsadviseurs en ICT-auditors

Alle hoofdstukken

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

Beleidsmakers

Hoofdstukken 4, 5, 6, 10 en 12

[5] Afhankelijk van de grootte van de gemeente zijn er meer of minder beveiligingsfunctionarissen. Voor dit document speelt dat geen rol. Samenhang van maatregelen (organisatorisch, procedureel, technisch of fysiek) is essentieel en om die reden dienen op alle niveaus alle beveiligingsfunctionarissen kennis te nemen van deze Tactische Baseline.

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

Lijnmanagers in hun personeelsverantwoordelijkheid

Hoofdstukken 6 en 8

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

Lijnmanagers in hun verantwoordelijkheid voor de uitvoering van de processen

Hoofdstukken 6, 10, 12, 13 en 14

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

Personeelszaken

Hoofdstuk 8

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

Fysieke beveiliging

Hoofdstuk 9

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

ICT-diensten en -infrastructuren

Hoofdstukken 6, 7, 9, 10, 11 en 12

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

Applicatie- en systeemeigenaren

Hoofdstukken 7, 10, 11 en 12

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

Een belangrijk onderdeel van informatiebeveiliging vormen de eindgebruikers. Zij dienen kennis te hebben van de gevolgen van hun gedrag op beveiliging.

Externe leveranciers

Alle hoofdstukken

De externe leveranciers zijn een bijzondere doelgroep. De opdrachtgever/ proceseigenaar is altijd verantwoordelijk voor de kwaliteit en veiligheid van de uitbestede diensten. De opdrachtgever eist van de externe leveranciers dat zij voldoen aan alle aspecten van deze Tactische Baseline die voor de dienst of het betreffende systeem **van belang zijn** en betrekking hebben op de geleverde dienst. Denk hier zeker ook aan de Wbp (Wet bescherming persoonsgegevens) en het afsluiten van een bewerkersovereenkomst en de jaarlijkse audit hierop.

INHOUDSOPGAVE

1 Waarom deze Tactische Baseline

1.1 Inleiding

Door de toenemende digitalisering is het zorgvuldig omgaan met de informatie en gegevens van burgers, bedrijven en ketenpartners voor gemeenten van groot belang. Uitval van computer- of telecommunicatiesystemen, het in ongerede raken van gegevensbestanden of het door onbevoegden kennisnemen dan wel manipuleren van bepaalde gegevens kan ernstige gevolgen hebben voor de continuïteit van de bedrijfsvoering en het primaire proces. Een betrouwbare, beschikbare en correcte informatiehuishouding is essentieel voor de dienstverlening van gemeenten. Het is niet ondenkbaar dat hieraan ook politieke consequenties verbonden zijn of dat het imago van de gemeenten en daarmee van de overheid in het algemeen wordt geschaad.

Maar het is niet alleen de automatisering. De samenwerking met andere overheden (in ketens) en de contacten met burgers en bedrijven wordt steeds vaker digitaal van aard. Dit legt (deels nieuwe) eisen op aan de kwaliteit van de informatievoorziening van de gemeente. Al was het maar dat van digitale dienstverlening vaak verwacht wordt dat deze 24 uur per dag en 7 dagen per week beschikbaar is, en dat bij een calamiteit de dienstverlening weer snel op gang komt.

Daarnaast spelen wet- en regelgeving een belangrijke rol. De Wet bescherming persoonsgegevens (Wbp) en de Archiefwet zijn voorbeelden van wetten die eisen stellen aan de verwerking en opslag van informatie.

Tot slot is er de maatschappelijke verantwoordelijkheid die een overheidsinstantie zoals de gemeente tegenover de burgers en bedrijven heeft. Van gemeenten mag verwacht worden dat zij zorgvuldig omgaan met de gegevens die zij beheren, en dat de gegevens die zij leveren juist, accuraat en tijdig zijn.

Kortom, de structurele aandacht voor de betrouwbaarheid van de informatievoorziening, het domein van informatiebeveiliging, helpt de gemeente bij een goede invulling van haar maatschappelijke taken. Een goede borging van informatiebeveiliging zorgt voor een betere betrouwbaarheid van de informatievoorziening en een grotere continuïteit van de gemeentelijke bedrijfsvoering.

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft opdracht voor deze Tactische Baseline gegeven. De totale Baseline Informatiebeveiliging Nederlandse Gemeenten is bedoeld om alle gemeenten op een vergelijkbare manier te laten werken met informatiebeveiliging.

Deze totale Baseline moet naast eenduidigheid ook bewerkstelligen dat de audit- en verantwoordingslast op gemeenten afneemt, dat ligt in lijn met de SiSa systematiek van

BZK[6]. Deze systematiek zorgt ervoor dat de auditlast afneemt omdat er nog maar één (1) keer per jaar verantwoording hoeft te worden afgelegd over het gevolgde financiële beleid. Hiervoor loopt het project ENSIA bij BZK[7]. ENSIA moet ervoor gaan zorgen dat nog maar eenmalig verantwoording afgelegd gaat worden over de BIG, doormiddel van een in control statement, en dat er over de overeenkomstige maatregelen die vanuit (basisregistratie) wetgeving is opgelegd niets meer gerapporteerd hoeft te worden.

Deze Tactische Baseline wordt later aangevuld met meerdere sets van voorbeelden voor beleid en operationele procedures.

Deze Tactische Baseline is tot stand gekomen door samenwerking met een expertgroep Informatiebeveiliging waarin deelnemers vanuit diverse gemeenten zitting hebben gehad. Daarnaast is er afgestemd met BZK en mensen uit andere decentrale overheden/projecten zoals de waterschappen en provincies, maar ook met SUWINET, BAG, RvIG, NORA en GEMMA.

Deze Tactische Baseline kan niet gedeeltelijk worden geïmplementeerd, er bestaat geen stukje informatiebeveiliging. Deze Tactische Baseline is het afgewogen minimale beveiligingsniveau waaraan een gemeente moet willen voldoen. De maatregelen hebben een samenhang. Dus indien gekozen wordt voor het invoeren van deze Tactische Baseline, dan kan dat alleen zoals deze is, tenzij er goede redenen zijn om hiervan af te wijken. Hiervoor geldt 'comply or explain' of 'pas toe of leg uit' ten aanzien van de maatregelen in deze Tactische Baseline.

1.2 Scope

De scope van deze Tactische Baseline omvat de bedrijfsvoeringprocessen, onderliggende informatiesystemen en informatie van de gemeente in de meest brede zin van het woord. Deze Tactische Baseline is van toepassing op alle ruimten van een gemeentehuis en aanverwante gebouwen, alsmede op apparaten die door gemeenteambtenaren gebruikt worden bij de uitoefening van hun taak op diverse locaties. Deze Tactische Baseline heeft betrekking op de informatie die daarbinnen verwerkt wordt. Ook als systemen niet binnen de gemeente draaien is deze Tactische Baseline van toepassing.[8]

Binnen de scope van deze Tactische Baseline vallen alle op dit moment geldende normen en regels op het gebied van informatiebeveiliging die door derden aan de gemeente zijn opgelegd. Deze Tactische Baseline bevat minimaal al deze maatregelen en brengt ze met elkaar in verband.

6 Zie ook: http://www.rijksoverheid.nl/onderwerpen/financien-gemeenten-en-provincies/uitwisseling-financiele-gegevens-met-sisa-en-iv3/single-information-single-audit-sisa
7 Eenduidige Normatiek Single Information Audit
8 Denk aan een SaaS-oplossing, uitbesteding van taken etc.

Binnen de scope is ook rekening gehouden met de verregaande digitalisering van de overheid en met de in de toekomst nog volgende basisregistraties of aanvullingen op bestaande basisregistraties.

1.3 Randvoorwaarden

De randvoorwaarden voor deze Tactische Baseline zijn:

1. Informatiebeveiliging is en blijft een verantwoordelijkheid van het lijnmanagement.
2. Het primaire uitgangspunt voor informatiebeveiliging is en blijft risicomanagement[9].
3. De klassieke informatiebeveiligingsaanpak waarbij inperking van mogelijkheden de boventoon voert maakt plaats voor veilig faciliteren.
4. Methoden voor rubricering en continue evaluatie ervan zijn hanteerbaar om onder- en over-rubricering te voorkomen (deze Tactische Baseline geeft geen aanpak voor rubriceren van informatie).
5. De focus van informatiebeveiliging verschuift van netwerkbeveiliging naar gegevensbeveiliging.
6. Bewust en verantwoord gedrag van mensen is essentieel voor een goede informatiebeveiliging.
7. Deze Tactische Baseline wordt gemeentebreed afgesproken en overheidsbrede kaders en maatregelen worden overheidsbreed afgesproken, waarbij de gemeentebrede kaders en maatregelen geënt worden op de overheidsbrede kaders. In uitzonderingsgevallen wordt – in overleg – afgeweken.
8. Kennis en expertise zijn essentieel voor een toekomst vaste informatiebeveiliging en moeten geborgd worden.
9. Informatiebeveiliging vereist een integrale aanpak, zowel binnen de gemeenten als voor (overheidsbrede) gemeenschappelijke voorzieningen.
10. Deze Tactische Baseline is gebaseerd op de ISO 27001:2005 en ISO 27002:2007.[10]
11. Deze Tactische Baseline kan gefaseerd worden ingevoerd.

1.4 Normenkaders en aansluitvoorwaarden

Gemeenten hebben in toenemende mate te maken met normenkaders zoals aansluitvoorwaarden op basisregistraties. Deze normenkaders verschillen in opbouw, overlappen elkaar deels en zijn daardoor moeilijk te beheren en te implementeren. Het

[9] Hiermee wordt niet bedoeld dat deze Tactische Baseline niet van toepassing is. De Tactische Baseline bevat het basisbeveiligingsniveau. Er dient voor informatiesystemen te worden vastgesteld of deze Tactische Baseline wel voldoende afdekt.

[10] Voor specifieke maatregelen is in onderhavige Tactische Baseline ook gebruik gemaakt van de Wbp, de SUWI-wet, BRP , BAG en PUN.

bestaan van zoveel verschillende normenkaders is verwarrend en belemmert een beheerste beveiliging en het implementeren en het beheren van de normenkaders[11].

In deze Tactische Baseline zijn de laatste uitgangspunten van de gemeenten, voor zover dat mogelijk is gegeven de huidige stand van de techniek, verwerkt.

1.4.1 Open standaarden

Er is gekozen voor een optimale aansluiting bij de wereld van geaccepteerde standaarden, ISO 27001:2005 en ISO 27002:2007 en de daarvan afgeleide overheidsstandaarden zoals de VIR[12]/BIR. 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 deze gemeente slechts te controleren op de aanvullende bepalingen voor bijvoorbeeld aansluitvoorwaarden voor een specifiek register.

1.5 Wetten en regels

De juridische grondslag voor informatiebeveiliging is terug te vinden in wet- en regelgeving, zoals onder meer de Wet bescherming persoonsgegevens (Wbp). Informatiebeveiliging en bescherming van persoonsgegevens zijn onlosmakelijk met elkaar verbonden. De Wbp regelt in artikel 13 welke maatregelen organisaties moeten treffen in het kader van informatiebeveiliging om op een adequate manier persoonsgegevens te beschermen. Voor wat betreft de gemeente is daarnaast uitgegaan van de verwerking van persoonsgegevens, zoals bedoeld in artikel 16 van de Wbp. Deze maatregelen dienen deel uit van het informatiebeveiligingsbeleid van een gemeente. Er zijn veel wetten en regelgeving van toepassing op de gemeente. De gemeente dient zich aan al deze wetten en regelgeving te houden, waaruit maatregelen ontstaan op het gebied van informatiebeveiliging. Wetten en regelingen die van toepassing zijn (niet limitatief):

- Wet Bescherming Persoonsregistratie en Vrijstellingsbesluit Wet bescherming persoonsregistratie (Wbp)
- Wet Openbaarheid van Bestuur (WOB)
- Wet Computercriminaliteit II
- Comptabiliteitswet
- Archiefwet
- Wet Particuliere Beveiligingsorganisaties en Recherchebureaus (WBPR)
- Wet Veiligheidsonderzoeken (WVO)
- Wet Politiegegevens (WPG)
- Ambtenarenwet
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)

[11] Het niet voldoen aan de aansluitvoorwaarden kan leiden tot afsluiting van de basisregistratie zoals de BRP, waardoor het primaire bedrijfsvoering in gevaar komt.

[12] Voorschrift Informatiebeveiliging Rijksdienst (http://wetten.overheid.nl/BWBR0022141/)

- Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIRBI 2013)[13]
- Beveiligingsvoorschrift Rijksdienst 2013 (BVR 2013)
- CAR-UWO
- PUN
- Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT2014)
- Kader Rijkstoegangsbeleid
- Uitgangspunten online communicatie rijksambtenaren
- Programma van Eisen PKI Overheid
- Code voor Informatiebeveiliging (ISO 27001:2005 en ISO 27002:2007)
- Telecommunication Infrastructure Standard for Data Centers (TIA-942)
- Wet SUWI
- Wet op de identificatieplicht
- Wet Elektronisch Bestuurlijk Verkeer (WEBV)
- Wet GBA en wet BRP
- Wet Werk en Bijstand
- Registratiewet
- Wet Openbaar Bestuur
- Algemene wet bestuursrecht
- Richtlijnen van het Nationaal Cyber Security Centrum (NCSC)

De volgende normen bestaan binnen de Rijksoverheid, deze zijn niet van toepassing op gemeenten. Echter de Strategische en Tactische Baseline zijn nauw verwant aan deze normen:

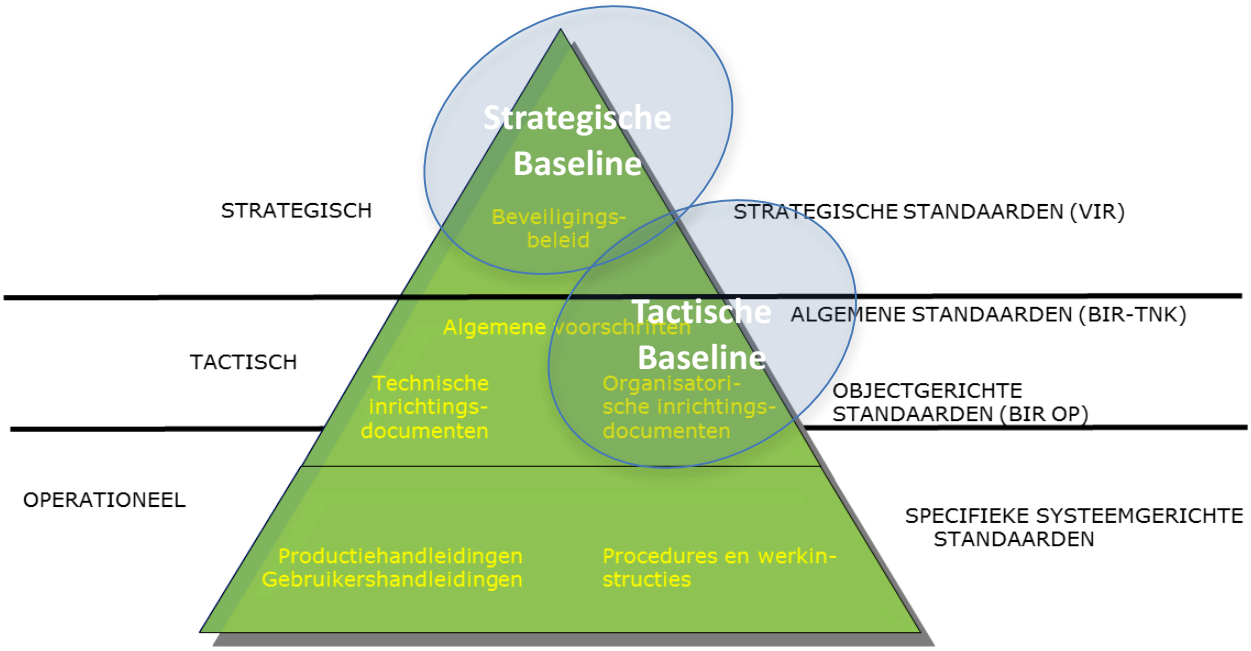
- het VIR, Besluit Voorschrift Informatiebeveiliging Rijksdienst.
- het Besluit Voorschrift Informatiebeveiliging - Bijzondere Informatie (VIRBI). Het VIRBI benadrukt de zorgplicht van ieder departement en van diens lijnmanagement voor de beveiliging van bijzondere informatie bij de rijksdienst. Het VIRBI is te beschouwen als een aanvulling op het VIR. Het VIRBI, hoewel geschreven voor de rijksdienst bevat prima aanvullingen die ook voor gemeenten te gebruiken zijn bij de bescherming van bijzondere informatie. Met de toenemende vervlechting van processen en informatie dient er op termijn een soortgelijk voorschrift, bijvoorbeeld een classificatie voorschrift en maatregelen voor gemeenten te komen.
- De BIR, Baseline Informatiebeveiliging Rijksdienst, bestaande uit BIR-TNK (tactisch normenkader) en BIR OP (BIR Operationele handreiking).
- De Interprovinciale Baseline Informatiebeveiliging.
- Het VIR heeft ook een relatie met het Algemeen Rijksambtenarenreglement (ARAR). Het ARAR is niet op gemeenten van toepassing, daarvoor heeft men de CAR-UWO en de Ambtenarenwet.

  De CAR-UWO bepaalt de rechten en plichten van gemeenteambtenaren. Aan de plichtenkant bevinden zich enkele bepalingen waarin de rol van de ambtenaar in

[13] http://wetten.overheid.nl/BWBR0033507/

de beveiliging wordt toegelicht. Het gaat daarbij onder andere om de geheimhoudingsplicht.

Overzicht verhouding Strategische Baseline en Tactische Baseline ten opzichte van VIR en BIR:



Inrichting

Voor gemeenten bestaat geen vergelijkbaar document zoals het 'beveiligingsvoorschrift Rijksdienst' waarin geregeld is dat er een beveiligingsambtenaar is voor de beveiliging van een departement. De gemeente heeft al wel de wettelijke taak om de rol van beveiligingsbeheerder GBA te hebben. Deze beveiligingsbeheerder kijkt alleen naar de GBA. Gemeenten doen er goed aan om een vergelijkbare brede rol in te voeren analoog aan wat geregeld is voor de rijksdienst, in de vorm van een CISO, de Chief Information Security Officer. Ook voor wat betreft de Wbp kan de gemeente een eigen functionaris gegevensbescherming (FG) hebben.

We praten voor de CISO nadrukkelijk over een rol. Bij kleine gemeenten kan deze rol ook in deeltijd uitgevoerd worden, waarbij het ook mogelijk is om dit te combineren over verschillende gemeenten in een regionale opzet. Zoals dat soms al vaker gebeurt voor andere gemeentelijke processen.

1.6 Basis beveiligingsniveau

Binnen het vakgebied informatiebeveiliging wordt onderscheid gemaakt tussen beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid. Deze Tactische Baseline sluit aan bij dit onderscheid.

Beschikbaarheid

Deze Tactische Baseline definieert een basisset aan eisen voor beschikbaarheid voor de informatie-infrastructuur van de gemeentelijke overheid. Deze dient als basis voor het maken van afspraken over de beschikbaarheid tussen de eigenaar van het informatiesysteem en de (SaaS) leverancier. Dit houdt in dat voor de beschikbaarheid van de informatievoorziening een minimale set van normen wordt opgesteld waarbij per dienst en/of applicatie nadere afspraken gemaakt kunnen worden.

Integriteit

Het onderwerp integriteit op Uitvlak 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 of fysiek (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 een minimale set van normen opgesteld waarbij er per dienst en/of applicatie nadere afspraken gemaakt kunnen worden.

Vertrouwelijkheid

Deze Tactische Baseline beschrijft de maatregelen die nodig zijn voor het basis vertrouwelijkheidsniveau (gemeentelijk) Vertrouwelijk[14] en persoonsvertrouwelijke informatie zoals bedoeld in Artikel 16 van de Wbp.

Het algemene dreigingsprofiel voor (gemeentelijk) Vertrouwelijk is voor deze Tactische Baseline vastgesteld op de volgende bedreigende factoren:

- de onbetrouwbare medewerker
- de wraakzuchtige medewerker
- de wraakzuchtige burger
- de verontruste burger
- de actiegroep
- de crimineel opportunist
- de ingehuurde medewerker
- de vreemde overheden

[14] Departementaal Vertrouwelijk volgens de VIR-BI (Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie, http://wetten.overheid.nl/BWBR0033507/)

Hierbij zijn de volgende bedreigingen specifiek gedefinieerd voor (gemeentelijk) Vertrouwelijk:

- infiltratie light
- social engineering
- 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
- inpluggen op fysiek netwerk
- verlies/diefstal van media
- publieke balies
- achterblijven van patches
- beproeving van fysieke, technische en elektronische weerstand

Naast de bovenstaande specifieke bedreigingen gaat deze Tactische Baseline 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[15]

- terreurgroep
- inlichtingendienst
- georganiseerde criminaliteit

Specifieke bedreigingen komende van deze laatst genoemde bedreigers worden niet meegenomen in het definiëren van de normen in deze Tactische Baseline.

Opzettelijke menselijke bedreigingen

Er kunnen diverse redenen zijn waarom mensen opzettelijk schade toebrengen aan informatiesystemen. Dat kunnen oorzaken van buitenaf zijn, zoals een hacker of

[15] Deze bedreigers zijn uitgesloten, aangezien daarmee de Tactische Baseline 'te zwaar' wordt. Het is dus niet zo dat deze niet kunnen optreden. De bedreigers kunnen middelen inzetten die sterker zijn dan de Tactische Baseline en uitgaan boven het niveau van risicomitigatie van de Tactische Baseline.

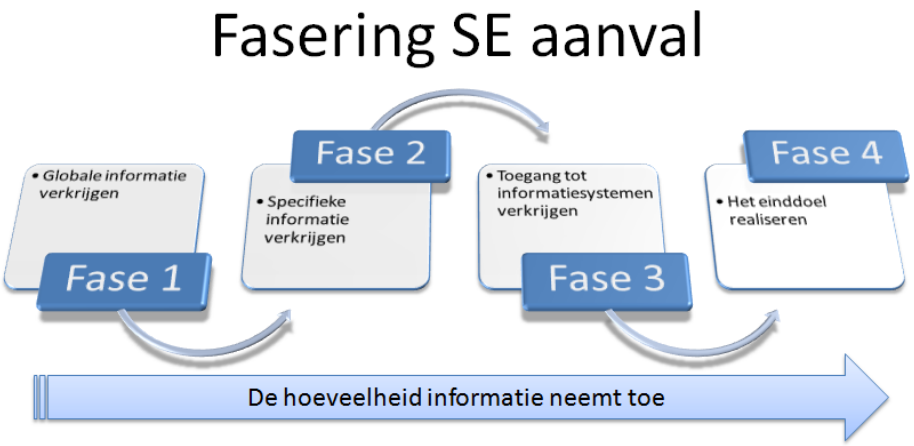
hackergroep die iets heeft tegen de gemeente en daarom binnendringt of door een denial of service aanval de toegang voor burgers tot gemeentelijke systemen ontzegt.

Het kan ook een medewerker zijn die ontevreden is over de gang van zaken binnen de gemeente en die uit boosheid data vernietigt. Het kan ook een frauderende medewerker zijn die uit persoonlijk gewin gegevens manipuleert in systemen of gegevens verkoopt.

Social engineering

Bij social engineering wordt gebruik gemaakt van kwaadwillende personen om van medewerkers informatie te ontfutselen. Dit kan gaan om bedrijfsgeheimen of informatie die niet voor iedereen bestemd is uit gemeentelijke systemen. Denk hier aan bijvoorbeeld wachtwoorden, ontwikkelingsplannen, verblijfplaatsen van mensen. De social engineer maakt gebruik van zwakheden in de mens om zijn doel te bereiken. Meestal is men zich hier niet goed van bewust. Het is heel normaal om een onbekende op de gang aan te spreken en te vragen of ze hulp nodig hebben. Toch hebben veel mensen hier moeite mee en gebeurt het niet. Het is ook goed om je af te vragen met wie je spreekt aan de telefoon en jezelf de vraag te stellen 'waarom wordt me deze vraag gesteld'.

Fasering social engineer aanval:



Figuur 2: fasering SE aanval

Bedenk dat een social engineer van buiten en van binnen kan komen.

Onopzettelijke menselijke bedreigingen

Mensen kunnen onopzettelijk schade toebrengen. Iemand drukt op de delete-toets en let niet goed op de vraag of hij het wel zeker weet. Iemand steekt een USB-stick besmet met een virus in de pc en brengt op die manier het virus over op een heel

netwerk. Iemand gebruikt in paniek een poederblusser om een beginnend brandje te blussen en vernietigt daarmee een server.

Niet menselijke bedreigingen

Invloeden van buitenaf zoals blikseminslag, brand, overstroming en stormschade zijn voorbeelden van niet-menselijke dreigingen. Deze bedreigingen zijn mede afhankelijk van de locatie van de gemeente, maar ook van de locatie van de belangrijkste informatiesystemen en apparatuur van de gemeente. Er kunnen zelfs verschillen zijn tussen gemeenten onderling, bijvoorbeeld de ene gemeente ligt grotendeels onder NAP en de andere er boven.

1.7 De Tactische Baseline onder architectuur

Informatiebeveiliging wordt bereikt door een geschikte verzameling beheersmaatregelen in te zetten, waaronder beleid, werkwijzen, procedures, organisatiestructuren en programmatuur- en apparatuurfuncties.

Deze beheersmaatregelen moeten worden vastgesteld, gecontroleerd, beoordeeld en waar nodig verbeterd om te waarborgen dat de specifieke beveiligings- en bedrijfsdoelstellingen van de organisatie worden bereikt. Dit behoort te worden gedaan in samenhang met andere bedrijfsbeheerprocessen.

Informatiebeveiligingsbeleid

Het treffen en onderhouden van een samenhangend pakket van maatregelen ter waarborging van de betrouwbaarheid van het informatievoorzieningsproces.

Risicomanagement

Risicomanagement is het systematisch opzetten, uitvoeren en bewaken van acties om risico’s te identificeren, te prioriteren, te analyseren en voor deze risico’s oplossingen te bepalen, te selecteren en uit te voeren.

Incidentmanagement

Een incident, in het kader van incidentmanagement, is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden. Incidentmanagement is het geheel van organisatorische en procedurele maatregelen dat ervoor moet zorgen dat een incident adequaat gedetecteerd, gemeld en behandeld wordt om daarmee de kans op uitval van bedrijfsvoeringsprocessen of schade ontstaan als gevolg van het incident te minimaliseren, dan wel te voorkomen.

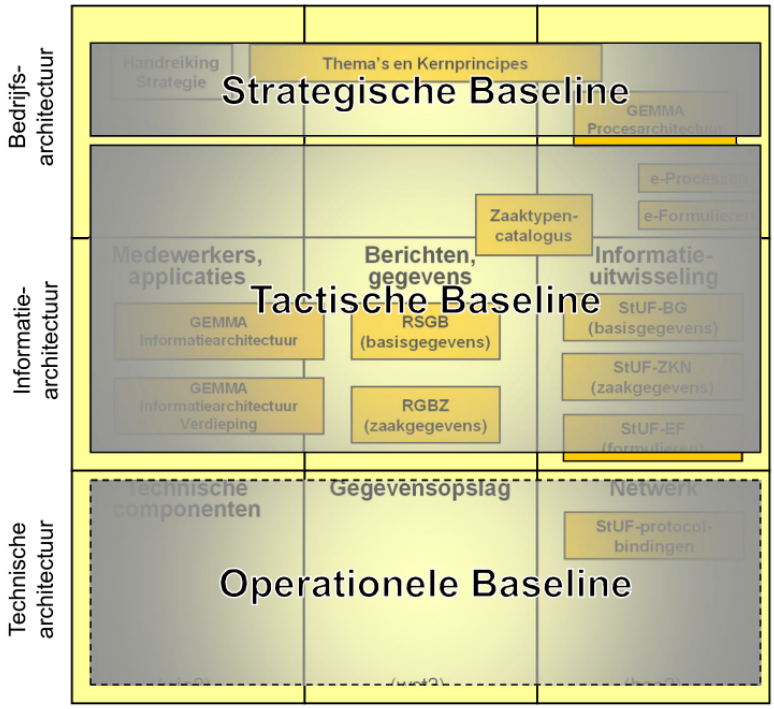
Bedrijfscontinuïteitsmanagement

Bedrijfscontinuïteitsmanagement is een proces waarbij de organisatie de nodige maatregelen treft om ongeacht de omstandigheden de continuïteit van de meest kritische processen te garanderen. In geval van een onderbreking van een of meerdere van deze processen moet de organisatie in staat zijn snel en kordaat op te treden, zodat deze activiteiten binnen de kortst mogelijke termijn kunnen worden hersteld.

Een product van bedrijfscontinuïteitsmanagement is een BCP – Bedrijfscontinuïteitsplan. Dit is het product van bedrijfscontinuïteitsmanagement, waarin de maatregelen en belangrijke gegevens van de bedrijfsprocessen van de organisatie worden beschreven, die tot doel hebben de onderbrekingstijd tot een minimum te beperken.

De bovenstaande processen zullen onderdeel worden van de volgende GEMMA-versie om daarmee de basis voor informatiebeveiliging te verankeren als integraal onderdeel van de bedrijfsvoering.

In het huidige overzicht van de GEMMA op het 9-vlaks model kan deze Tactische Baseline als volgt gepositioneerd worden.



Figuur 3 - GEMMA model en positionering BIG delen

1.8 Opzet, beheer en onderhoud van de Tactische Baseline

VNG/KING is eigenaar van dit document en daarmee verantwoordelijk voor het beheer en onderhoud van deze Tactische Baseline. Deze Tactische Baseline is gemaakt door de Informatiebeveiligingsdienst voor gemeenten (IBD) en bevat de basisset aan beveiligingsmaatregelen die nodig zijn als stabiele veilige basis binnen de gemeente.

Dit document en de daarin opgenomen maatregelen worden periodiek op inhoud, uitvoerbaarheid, invoering en werking beoordeeld en, indien nodig, aangepast om te voorkomen dat deze Tactische Baseline veroudert.

De inhoudelijke toetsing en bijstelling van deze Tactische Baseline vinden plaats door de IBD vanuit het nog te starten IB-overleg.

Herziening is mede afhankelijk van wijzigingen in de wetgeving, de onderliggende normen, het beleid en de beheerorganisatie. Beveiligingsincidenten vormen aanwijzingen waar voor de gemeentelijke overheid specifieke kwetsbaarheden liggen. Voor de aanpassing van het minimumniveau wordt dan ook gebruik gemaakt van een analyse van incidenten uit de periode voorafgaand aan het vaststellen van het minimumniveau.

Daarom wordt van de bij de **gemeente verantwoordelijke functionarissen verwacht** dat zij zorg dragen voor een juiste en volledige registratie van security incidenten en het melden **daarvan aan de Informatiebeveiligingsdienst voor gemeenten,** als onderdeel van de minimum set van maatregelen.

2 De structuur van de norm

Hoofdstuk 3 gaat over de implementatie van deze Tactische Baseline en geeft aan welke stappen gezet dienen te worden.

Hoofdstuk 4 laat zien hoe bepaald kan worden welke ICT-voorzieningen binnen deze Tactische Baseline vallen en voor welke ICT-voorzieningen er aanvullende maatregelen genomen dienen te worden.

Hoofdstukken 5 t/m 15 bevatten hoofdbeveiligingscategorieën en subcategorieën.

Bij elke subcategorie is de doelstelling (uit ISO 27002:2007) vermeld. Elke subcategorie kent een aantal beheersmaatregelen, waarvan de nummering exact overeenkomt met ISO 27002:2007. De tekst van de beheersmaatregelen uit de ISO 27002:2007 is cursief weergegeven.

Bijlage 1 bevat een woordenlijst.

Bijlage 2 bevat een mapping naar de belangrijkste wet- en regelgeving.

Bijlage 3 bevat een opsomming van de belangrijkste wijzigingen van versie 1.01.

3 Implementatie van de Tactische Baseline

De volgende logische stappen zijn belangrijk bij de implementatie van deze Tactische Baseline:

- benoem verantwoordelijken.
- Voer een GAP-analyse uit.
- benoem quick wins en voer deze uit, bijvoorbeeld het beschrijven en implementeren van procedures.
- maak een integraal implementatieplan (Information Security Management System - ISMS) en begin met periodiek rapporteren over de voortgang.

3.1 Benoem verantwoordelijken

Vastgestelde maatregelen dienen te worden geïmplementeerd. Vaak vallen deze binnen een verantwoordelijkheidsgebied van een specifieke manager. Bijvoorbeeld:

- toegangsbeveiligingsmaatregelen behoren door de facilitair manager te worden ingevoerd en gewaarborgd.
- personele maatregelen behoren meestal bij de afdeling HRM. Denk hierbij aan aannamebeleid, ontslagbeleid, benoemen vertrouwensfuncties.

In de onderstaande tabel is dit verder uitgewerkt:

	Omschrijving
Communicatie	Communicatiefunctie, heeft raakvlakken met vrijgave informatie (publiek)
Organisatie	Maatregelen die samenhangen met de organisatie zoals functies, functiescheiding en competenties.
Personeel	Beveiligingsmaatregelen betreffende arbeidsvoorwaarden, aanname procedures, ontslagprocedures, functiewisseling procedures etc.
Administratieve organisatie	Maatregelen die samenhangen met administratieve systemen, ‘harde’ procedures, randvoorwaarden/ beperkingen en controle.
Financiën	Maatregelen die samenhangen met de financiële functie, verantwoording.

Informatievoorziening	Maatregelen betreffende systeemeisen t.a.v. ontwikkeling, beheer en informatiehuishouding binnen de gemeente over relevante systemen & documentenstromen en website.
Juridische zaken	Maatregelen die samenhangen met inkoopvoorwaarden en beveiligingseisen, (raam-) contracten, rechtspositie en bewerkersovereenkomsten
Technologie	Maatregelen t.a.v. automatisering, internet(web), systemen en contractpartijen
Huisvesting	Maatregelen betreffende fysieke beveiliging, brandbeveiliging, infrastructuur, werkplekken en faciliteiten.

Benoem een informatiebeveiligingsfunctionaris zoals een CISO (Chief Information Security Officer) of wijs iemand de CISO rol toe. De CISO is de rol die uitgevoerd wordt om beveiliging te coördineren binnen een organisatie, waarbij de CISO bij voorkeur niet binnen de ICT-organisatie gepositioneerd wordt. Afhankelijk van de grootte van de gemeente kunnen er meer informatiebeveiligingsfunctionarissen zijn.

3.2 Voer een GAP-analyse uit

De GAP-analyse geeft als instrument antwoord op vragen als: 'Waar zijn we nu' en 'Waar willen we heen'. Met het gebruiken van deze Tactische Baseline weet de gemeente nog niet wat er gedaan moet worden om deze Tactische Baseline ingevoerd te krijgen. Door middel van de GAP-analyse kan de gemeente met het stellen van vragen vaststellen welke Tactische Baseline-maatregelen al ingevoerd zijn, en belangrijker, welke maatregelen uit deze Tactische Baseline nog niet ingevoerd zijn.

Met het gevonden resultaat kan vervolgens planmatig worden omgegaan en kunnen de actiehouders beginnen met het invoeren van maatregelen en hierover ook periodiek in de managementrapportages over rapporteren.

Onderzoek welke maatregelen al genomen zijn en geef per maatregel aan:

- of er iets over beschreven is, en zo ja, waar dat opgelegd is (opzet)
    - (rood: niets beschreven, oranje beschreven)
- of de verantwoordelijken bekend zijn met de maatregel (bestaan)
    - (groen: verantwoordelijken zijn bekend, geel: niet bekend)

3.3 'Benoem quick wins

Na het uitvoeren van de GAP-analyse kan het beste worden begonnen met quick wins de maatregelen die over het algemeen ook het minste geld kosten. Relatief gezien

wordt hier vaak ook het meeste resultaat behaald tegen de laagste kosten. Voorbeelden van procedures zijn:

- Wachtwoordprocedures over wachtwoordlengte, de termijn dat wachtwoorden moeten worden veranderd, de soort tekens die gebruikt moeten worden en hoe lang wordt bijgehouden welke wachtwoorden reeds gebruikt zijn.
- Procedures betreffende toegang tot het pand of de locatie.

3.4 Maak een integraal implementatieplan en rapporteer

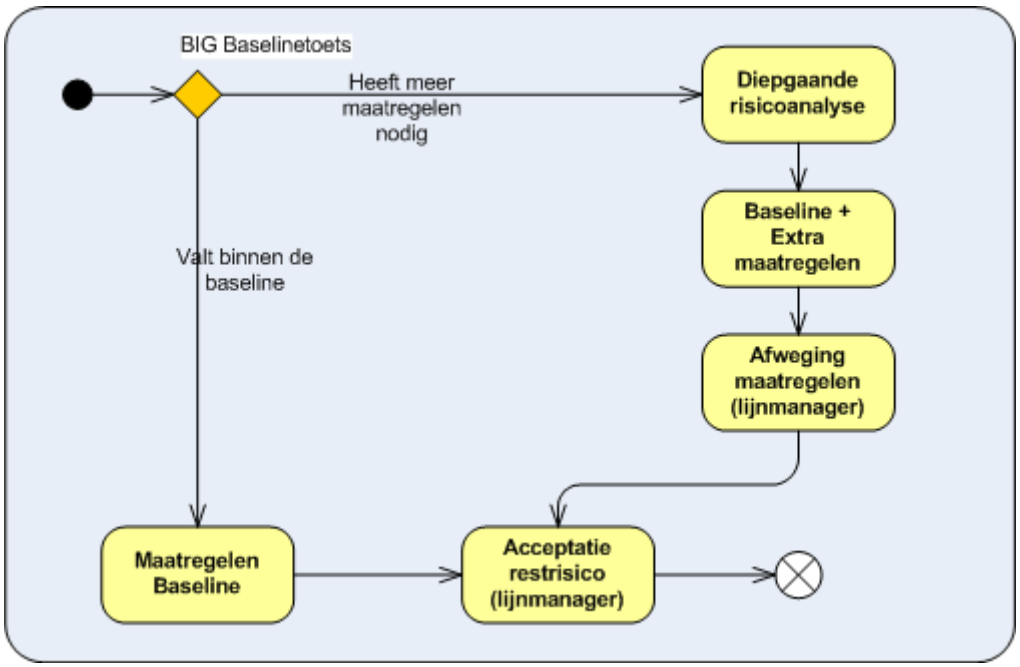
Het is noodzakelijk dat ontbrekende beveiligingsmaatregelen die veel tijd kosten of kostbaar zijn planmatig worden ingevoerd. Maak een plan om te komen tot implementatie van deze Tactische Baseline en stuur op de voortgang. Daarbij horen goede rapportages van de verantwoordelijken die benoemd zijn om specifieke maatregelen in te voeren. Dit proces kan ondersteund worden door een Information Security Management System (ISMS) dat onder andere als doel heeft het continue beoordelen welke beveiligingsmaatregelen passend zijn en indien nodig bij te stellen.

Door de beheersing van deze planning op te nemen in de planning- en controlcyclus en hierover door de organisatieonderdelen verantwoording af te laten leggen door reguliere voortgangsrapportages, wordt beveiliging zowel bestuurlijk als ambtelijk in de organisatie te geborgd. Gemeenten dienen hierin transparant te zijn. Dit kunnen gemeenten verwezenlijken door hierover zowel horizontaal als verticaal verantwoording af te leggen. Aansluiting bij een dergelijke cyclus hierbij voorkomt dat informatiebeveiliging als een eigenstandig onderwerp wordt behandeld en daardoor laag geprioriteerd wordt. Over het functioneren van de informatiebeveiliging, de kwaliteitscirkel, wordt conform de planning- en controlcyclus binnen de gemeente en richting B&W verantwoording afgelegd door het management.

4 Risicobeoordeling en risicoafweging

Volgens de Strategische Baseline moet er een risicoafweging plaatsvinden. De mogelijke methodes hiervoor zijn het uitvoeren van een baselinetoets BIG gevolgd door een diepgaande risicoanalyse of certificering of Privacy Impact Assessment (PIA).

Het beveiligingsniveau van deze Tactische Baseline is zo gekozen dat dit voor de meeste processen en ondersteunende ICT-voorzieningen bij gemeenten voldoende is. Hiermee wordt voorkomen dat er voor ieder systeem een diepgaande risicoanalyse uitgevoerd moet worden. Om vast te stellen dat het niveau van deze Tactische Baseline voldoende is, moet een baselinetoets BIG uitgevoerd worden. Dit is schematisch weergegeven in het onderstaande figuur:



Figuur 4: baselinetoets BIG

In de baselinetoets BIG wordt onder meer bekeken of er geheime of bijzondere persoonsgegevens of geclassificeerde informatie verwerkt wordt, er sprake is van persoonsvertrouwelijke informatie zoals bedoeld in artikel 16 van de Wbp, er hogere beschikbaarheidseisen vereist zijn of er dreigingen relevant zijn die niet in het dreigingsprofiel van deze Tactische Baseline meegenomen zijn.

Voor wat betreft integriteit en vertrouwelijkheid is er sprake van hogere betrouwbaarheidseisen als het om geheimen gaat (rubricering hoger dan 'Vertrouwelijk'). Of als bij de verwerking van persoonsgegevens zowel de kans op ongewenste gevolgen groter is alsook de schade die dit kan veroorzaken voor de

betrokkene groter is. Hogere betrouwbaarheidseisen kunnen ook voorkomen als er een dreiging relevant is die niet in het dreigingsprofiel van deze Tactische Baseline is meegenomen. 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. Bij het verwerken van (nieuwe) persoonsgegevens wordt door de uitslag van de Baselinetoets BIG ook aangeraden een Privacy Impact Assessment (PIA) uit te voeren.

Acceptatie door de manager:

Er kan op verschillende manieren met (rest) risico's worden omgegaan. De meest gebruikelijke strategieën zijn:

1. risicodragend
2. risiconeutraal
3. risicomijdend

Risicodragend wil zeggen dat risico's geaccepteerd worden. Dat kan zijn omdat de kosten van de beveiligingsmaatregelen de mogelijke schade overstijgen. Maar het management kan ook besluiten om niets te doen, ondanks dat de kosten niet hoger zijn dan de schade die kan optreden.

- De maatregelen die een risicodragende organisatie neemt op het gebied van informatiebeveiliging zijn veelal van repressieve aard.

Onder **risiconeutraal** wordt verstaan dat er dusdanige beveiligingsmaatregelen worden genomen dat dreigingen óf niet meer manifest worden óf, wanneer de dreiging wel manifest wordt, de schade als gevolg hiervan geminimaliseerd is. De meeste maatregelen die een risiconeutrale organisatie neemt op het gebied van informatiebeveiliging zijn een combinatie van preventieve, detectieve en repressieve maatregelen.

Onder **risicomijdend** verstaan we dat er zodanige maatregelen worden genomen dat de dreigingen zo veel mogelijk worden geneutraliseerd, zodat de dreiging niet meer tot een incident leidt.

Denk hierbij aan het invoeren van nieuwe software waardoor de fouten in de oude software geen dreiging meer vormen. In simpele bewoordingen: een ijzeren emmer kan roesten. Neem een kunststof emmer en de dreiging, roest, valt weg. Veel van de maatregelen binnen deze strategie hebben een preventief karakter.

Welke strategie een organisatie ook kiest, de keuze dient bewust door het management te worden gemaakt en de gevolgen ervan dienen te worden gedragen.

5 Beveiligingsbeleid

5.1 Informatiebeveiligingsbeleid

Doelstelling

Borgen van betrouwbare dienstverlening en een aantoonbaar niveau van informatiebeveiliging dat voldoet aan de relevante wetgeving, algemeen wordt geaccepteerd door haar (keten-)partners en er mede voor zorgt dat de kritische bedrijfsprocessen bij een calamiteit en incident voortgezet kunnen worden.

5.1.1 Beleidsdocumenten voor informatiebeveiliging

Informatiebeveiligingsbeleid behoort door het hoogste management te worden goedgekeurd en gepubliceerd. Het document dient tevens kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen.

1. Er is een beleid voor informatiebeveiliging door het College van Burgemeester en Wethouders vastgesteld, gepubliceerd en beoordeeld op basis van inzicht in risico's, kritische bedrijfsprocessen en toewijzing van verantwoordelijkheden en prioriteiten.

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. [A]Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld. Zie ook 6.1.8.1.

6 Organisatie van de informatiebeveiliging

6.1 Interne organisatie

Doelstelling

Beheren van de informatiebeveiliging binnen de organisatie.

6.1.1 Betrokkenheid van het College van B&W bij beveiliging

Het hoogste management behoort actief informatiebeveiliging 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. [A]Het College van B&W 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 de opzet, het bestaan en de werking van de informatiebeveiligingsmaatregelen te bespreken in het overleg van B&W en hiervan verslag te doen.

6.1.2 Coördineren van beveiliging

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

1. [A] De rollen van de CISO (Chief Information Security Officer), en het lijnmanagement zijn beschreven.
    a. De CISO rapporteert rechtstreeks aan de gemeentesecretaris.
    b. De CISO bevordert en adviseert gevraagd en ongevraagd over de beveiliging van de gemeente, verzorgt rapportages over de status, controleert of m.b.t. de beveiliging van de gemeente de maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de informatiebeveiliging van de gemeente.

6.1.3 Verantwoordelijkheden

Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd.

1. [A]Elke lijnmanager is verantwoordelijk voor de integrale informatiebeveiliging van zijn of haar organisatieonderdeel.

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 ICT-voorzieningen en wijzigingen in ICT-voorzieningen (in ITIL termen: wijzigingsbeheer).

6.1.5 Geheimhoudingsovereenkomst

Eisen voor vertrouwelijkheid of voor een 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. [A]De algemene geheimhoudingsplicht voor ambtenaren is geregeld in de Ambtenarenwet art. 125a, lid 3.
   Daarnaast dienen personen die te maken hebben met Bijzondere Informatie[16] een geheimhoudingsverklaring te ondertekenen. Daaronder valt ook vertrouwelijke informatie. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding.

6.1.6 Contact met overheidsinstanties

Er behoren geschikte contacten met relevante overheidsinstanties te worden onderhouden.

1. [A]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. Informatiebeveiligingsspecifieke informatie van relevante expertisegroepen, leveranciers van hardware, software en diensten wordt gebruikt om de informatiebeveiliging te verbeteren.
2. De CISO onderhoudt contact met de Informatiebeveiligingsdienst voor gemeenten.

6.1.8 Beoordeling van het informatiebeveiligingsbeleid

De benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan (d.w.z. beheerdoelstellingen, beheersmaatregelen, beleid, processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met

[16] Bijzondere Informatie is informatie die vergelijkbaar met het VIR-BI geclassificeerd/gerubriceerd is.

geplande tussenpozen te worden beoordeeld, of zodra zich wijzigingen voordoen in de implementatie van de beveiliging.

1. [A]Het informatiebeveiligingsbeleid wordt minimaal één keer in de drie jaar geëvalueerd (door een onafhankelijke deskundige) en desgewenst bijgesteld. Zie ook 5.1.2.

2. [A]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

Het 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. Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke waarde en gevoeligheid de informatie 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. [A]Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een bewerkersovereenkomst (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.

7. Over het naleven van de afspraken van de externe partij wordt jaarlijks gerapporteerd.

6.2.2 Beveiliging beoordelen in de omgang met klanten

Alle geïdentificeerde beveiligingseisen behoren te worden beoordeeld 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, 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 om 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 en de geheimhoudingsverklaring.

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

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. [A]Er zijn regels voor acceptabel gebruik van bedrijfsmiddelen (met name internet, e-mail en mobiele apparatuur). De CAR-UWO verplicht ambtenaren zich hieraan te houden. Voor extern personeel is dit in het contract vastgelegd.

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. [A]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.

Informatie behoort te worden geclassificeerd om bij het verwerken van de informatie de noodzaak, prioriteiten en verwachte graad van bescherming te kunnen aangeven.

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. [A]De organisatie heeft rubriceringrichtlijnen opgesteld.

2. In overeenstemming met hetgeen in het Wbp is vastgesteld, dient er een helder onderscheid te zijn in de herleidbare (artikel 16 Wbp) en de niet herleidbare persoonsgegevens.

7.2.2 Labeling en verwerking van informatie

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

1. [A]De lijnmanager heeft maatregelen getroffen om te voorkomen dat niet-geautoriseerden kennis kunnen nemen van gerubriceerde informatie.

2. [A]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 Voorafgaand aan het dienstverband

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 en worden onderhouden. In de functiebeschrijving wordt minimaal aandacht besteed aan:
    - uitvoering van het informatiebeveiligingsbeleid
    - bescherming van bedrijfsmiddelen
    - rapportage van beveiligingsincidenten
    - expliciete vermelding van de verantwoordelijkheden voor het beveiligen van persoonsgegevens

2. [A]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 functie 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. [A]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 informatiebeveiliging. Het is aantoonbaar dat medewerkers bekend zijn met hun verantwoordelijkheden op het gebied van informatiebeveiliging.

8.1.2 Screening

Verificatie van de achtergrond van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers behoort 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. [A]Voor alle medewerkers (ambtenaren en externe medewerkers) is minimaal een recente 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.

3. [A]Het is noodzakelijk om de VOG of screening periodiek te herhalen volgens de voorschriften.

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 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

Het lijnmanagement 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 gemeenteambtenaren en ingehuurd personeel (onder andere die kritische bedrijfsactiviteiten op het gebied van IB uitoefenen) te kunnen beschikken.

2. Het lijnmanagement bevordert dat gemeenteambtenaren, 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 Bewustwording, opleiding en training ten aanzien van informatiebeveiliging

Alle werknemers van de organisatie en, voor zover 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.[17]
2. [A]Bespreek het onderwerp informatiebeveiliging in functionerings- en beoordelingsgesprekken van medewerkers die risicovolle functies bekleden.

8.2.3 Disciplinaire maatregelen

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

1. [A]Er is een disciplinair proces vastgelegd voor medewerkers die inbreuk maken op het informatiebeveiligingsbeleid (zie ook: CAR/UWO art 16, disciplinaire straffen).

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 of 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

[17] Bewustwordingstrainingen zijn een van de meest effectiefste maatregelen om de menselijke fouten tegen te gaan.

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, of behoort na wijziging te worden aangepast.

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. De gemeente en haar omgeving worden ingedeeld in verschillende zones. Deze zones bestaan uit:
    a. Zone 0: de omgeving en het gebouw
    b. Zone 1: de wachtruimten en de spreekkamers
    c. Zone 2: de werkruimten
    d. Zone 3: de ICT-ruimte/beveiligde ruimte voor bijvoorbeeld paspoort opslag.

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 ICT-gericht vandalisme.

4. [A]Er zijn op verschillende plekken zogenaamde overval alarmknoppen geplaatst, dit is met name van belang voor de wachtruimten en de spreekkamers en die ruimtes waar bezoekers in contact komen met gemeente ambtenaren.

5. Er is 24 uur, 7 dagen per week bewaking; een inbraakalarm gekoppeld aan alarmcentrale is het minimum.

6. [A]Van ingehuurde 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.

7. In gebouwen met serverruimtes houdt beveiligingspersoneel toezicht op de toegang. Hiervan wordt een registratie bijhouden.

8. [A]Voor toegang tot speciale ruimten is een doelbinding vereist, dat wil zeggen dat personen op grond van hun werkzaamheden toegang kan worden verleend. (bijvoorbeeld Beheer, BhV et cetera).

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. [A]De beveiligingszones en toegangsbeveiliging daarvan zijn ingericht conform het gemeentelijk toegangsbeleid.

3. In gebouwen met beveiligde zones 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. toegangsbeveiliging zoals die worden gesteld aan computerruimtes.

8. [A]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, tenzij de vertrouwelijke informatie op de mobiele gegevensdrager voldoende versleuteld is.

2. [A]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. [A]Serverruimtes, 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) of de NEN-norm NPR 5313 of de Europese norm NEN-EN 50600 serie

9.1.4 Bescherming tegen bedreigingen van buitenaf

Er behoort fysieke bescherming tegen schade door brand, overstroming, aardschokken, 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. [A]Beveiligde ruimten waarin zich bedrijfskritische apparatuur bevindt zijn voldoende beveiligd tegen wateroverlast.

4. [A]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. [A]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 ICT-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 ICT-voorzieningen, om onbevoegde toegang te voorkomen.

1. [A]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 compromitteren 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 overspanningsbeveiliging.

2. Standaard accounts in apparatuur worden gewijzigd en de bijbehorende standaard leveranciers wachtwoorden worden gewijzigd bij ingebruikname van apparatuur.

3. Gebouwen zijn beveiligd tegen blikseminslag.

4. Eten en drinken zijn verboden in computerruimtes.

5. [A]Apparatuur 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.[18]

9.2.2 Nutsvoorzieningen

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

9.2.3 Beveiliging van kabels

Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, behoren tegen interceptie of beschadiging te worden beschermd conform de norm NEN 1010.[19]

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. [A]Reparatie en onderhoud van apparatuur (hardware) vindt op locatie plaats door bevoegd personeel, tenzij er geen data op het apparaat aanwezig of

[18] Gemeenten die server virtualisatie toepassen dienen zelf de risicoafweging te maken of en hoe zij systemen willen scheiden.
[19] Zie ook het handboek ICT-huisvesting en bekabeling van de Rijksgebouwendienst: http://www.rgd.nl/actueel/publicaties/handboek-ict-huisvesting-en-bekabeling-hib-versie-10/

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 fysieke beveiligingsmaatregelen zoals sloten en camera toezicht 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. [A]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.[20]

2. [A]Hergebruik van apparatuur buiten de organisatie is slechts toegestaan indien de informatie is verwijderd met een voldoende veilige methode. Een veilige methode is Secure Erase[21] 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.

[20] Er zijn gemeenten die BYOD toestaan, in dat geval dient een policy ingesteld te worden, die regelt dat data wordt verwijderd als de apparatuur niet meer gebruikt wordt door de medewerker.
[21] 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, zie ook NIST 800-88 - Guidelines for Media Sanitization

10 Beheer van Communicatie- en Bedieningsprocessen

10.1 Bedieningsprocedures en -verantwoordelijkheden

Doelstelling

Waarborgen van een correcte en veilige bediening van ICT-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-up- 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 ICT-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. [A]Instellingen van informatiebeveiligingsfuncties (bijvoorbeeld 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. [A]Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerwerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder,

normale gebruikstaken alleen wanneer ingelogd als gebruiker.

3. [A]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. [A]Verantwoordelijkheden voor beheer, 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. [A]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 middels audits of rapportages en gebeurt minimaal eens per jaar (voor ieder systeem).

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. [A]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 beschikbaarheid eis 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. [A]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. [A]In koppelpunten met externe of onvertrouwde zones worden maatregelen getroffen om DDOS (Denial of Service) 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.[22]

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. [A]Van acceptatietesten wordt een log bijgehouden.

2. Er zijn acceptatiecriteria vastgesteld voor het testen van de beveiliging. Dit betreft minimaal OWASP[23] 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.

1. [A]Bij het openen van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, automatisch plaats.

2. [A]Inkomende en uitgaande e-mails worden gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities 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 antivirusprogrammatuur van verschillende leveranciers toegepast.

[22] Zie bijvoorbeeld de NCSC aanbevelingen: https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/factsheets/factsheet-continuiteit-van-online-diensten/1/Factsheet%2BFS%2B2013%2B01%2BDDoS%2Bv1.6.pdf
[23] Open Web Application Security Project (http://www.owasp.org)

4. [A]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.

6. Op mobile devices wordt antivirus software toegepast, waarbij bij BYOD de eindgebruiker verplicht is deze zelf toe te passen.

10.4.2 Maatregelen tegen 'mobile code'

Als gebruik van 'mobile code'[24] 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 wordt aangetast.

2. Een gebruiker moet geen extra rechten kunnen toekennen aan programma's (bijv. internet browsers)die mobile code uitvoeren.

10.5 Back-up

Doelstelling

Handhaven van de integriteit en beschikbaarheid van informatie en ICT-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 foutherstel van verwerkingen.

2. Back-upstrategieën zijn vastgesteld op basis van de 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.

[24] Mobile code is software die tussen systemen wordt overgedragen en welke vervolgens wordt uitgevoerd op het locale system, denk hier bijvoorbeeld aan javascript of flash animaties. Meestal gebeurt dit in een browser maar het kan ook een e-mail bijlage, een office document, een afbeelding of een PDF zijn.

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. [A]Gegevensuitwisseling tussen vertrouwde en onvertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.

3. [A]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 beheereisen 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. [A]Er zijn procedures opgesteld en geïmplementeerd voor opslag van vertrouwelijke informatie voor verwijderbare media.

2. [A]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. [A]Er zijn procedures vastgesteld en in werking gesteld voor het verwijderen van vertrouwelijke data en de vernietiging van verwijderbare media. Verwijderen van data wordt gedaan met een Secure Erase[25] 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

Systeemdocumentatie behoort te worden beschermd tegen onbevoegde toegang.

1. Systeemdocumentatie die vertrouwelijke informatie bevat is niet vrij toegankelijk.

2. [A]Wanneer de eigenaar er expliciet voor kiest om gerubriceerde systeemdocumentatie buiten de gemeente 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.

[25] 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.

10.8.1 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. [A]Het meenemen van Departementaal Vertrouwelijke[26] of vergelijkbaar geclassificeerde informatie, of hogere, buiten de gemeente 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, ingesproken berichten op antwoordapparaten en het gebruik van de diverse digitale berichtendiensten 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 ten minste 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.

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. [A]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.

[26] Hier wordt verwezen naar een rijks classificatie zodat dit aansluit bij andere baselines en beveiligingsvoorschriften.

10.8.3 Fysieke media die worden getransporteerd

Media die informatie bevatten behoren te worden beschermd tegen onbevoegde toegang, misbruik of corrumperen 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. [A]Fysieke verzending van bijzondere informatie dient te geschieden met 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 berichtuitwisseling behoort op geschikte wijze te worden beschermd.

1. [A]Digitale documenten binnen de gemeente waar eindgebruikers rechten aan kunnen ontlenen maken gebruik van PKI Overheid certificaten voor tekenen en/of encryptie.

2. 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 gemeentelijk informatie in kantoorapplicaties met zich meebrengen en richtlijnen voor de bepaling van de beveiliging van deze informatie binnen deze kantoorapplicaties. Hierin is minimaal aandacht besteed aan de toegang tot de interne informatievoorziening, toegankelijkheid van agenda's, afscherming van documenten, privacy, beschikbaarheid, back-up en in voorkomend geval cloud diensten.

10.9 Diensten voor e-commerce

Doelstelling

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

10.9.1 E-commerce

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

1. [A]Conform verplichting worden authentieke basisregistraties van de overheid gebruikt (bijvoorbeeld. GBA) (eenmalige vastlegging, meervoudig gebruik).

10.9.2 Online-transacties

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 (geautoriseerd) door een (gekwalificeerde) 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 worden beoordeeld. Deze periode dient te worden gerelateerd aan de mogelijkheid van misbruik en de schade die kan optreden. De GBA logging kan bijvoorbeeld dagelijks nagelopen worden, evenals financiële systemen, controle van het Internet gebruik kan bijvoorbeeld per maand of kwartaal.

2. Een log-regel 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. [A]In een log-regel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, enz.).

4. [A]Logberichten worden overzichtelijk samengevat. Daartoe zijn systemen die logberichten genereren bij voorkeur[27]aangesloten op een Security Information and Event Management systeem (SIEM[28]) 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 vol lopen 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 ICT-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, wachtwoord reset, uitgifte en intrekken van cryptosleutels.
    - beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities of kwetsbaarheden, 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, zoals goede en foute inlogpogingen, systeemtoegang, gebruik van online transacties en toegang tot bestanden

[27] Voor kleinere gemeenten zal dit bijna ondoenlijk zijn, echter het is aan te bevelen om gebruik te maken van SIEM.
[28] 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.

door systeembeheerders.

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. [A]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 instellingenaangepast moeten worden zal daarbij altijd het vier ogen principe toegepast worden.

5. [A]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.

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 organisatie-eisen 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. [A]Authenticatiegegevens worden bijgehouden in één bronbestand zodat consistentie is gegarandeerd.

3. [A]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.

4. Er is aandacht voor het wijzigen van bevoegdheden bij verandering van functie/ afdeling.

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 gecombineerd met een salt 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 of hardware worden meegegeven worden bij eerste gebruik vervangen door een persoonlijk wachtwoord.
    - Gebruikers bevestigen de ontvangst van een wachtwoord.
    - Wachtwoorden zijn alleen bij de gebruiker bekend.
    - Wachtwoorden bestaan uit minimaal 8 karakters, waarvan tenminste 1 hoofdletter, 1 cijfer en 1 vreemd teken.
    - Wachtwoorden zijn maximaal 60 dagen geldig en mogen niet binnen 6 keer herhaald worden.

11.2.4 Beoordeling van toegangsrechten van gebruikers

Het management 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.
- Wachtwoorden mogen niet opeenvolgend zijn.
- 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. Zie ook: 11.5.5.

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. [A]Schermbeveiligingsprogrammatuur (een screensaver) maakt na een periode van inactiviteit van maximaal 15 minuten alle informatie op het beeldscherm onleesbaar en ontoegankelijk.

4. [A]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. [A]Alleen geïdentificeerde en geauthenticeerde apparatuur kan worden aangesloten op een vertrouwde zone. Eigen, geauthenticeerde, 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. [A]Werkstations worden zo ingericht dat routeren van verkeer tussen verschillende zones of netwerken niet mogelijk is.

2. [A]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. [A]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 het beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie.

4. [A]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 bedrijfstoepassingen (zie 11.1).

11.4.7 Beheersmaatregelen voor netwerkroutering

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

1. Netwerken zijn voorzien van beheersmaatregelen voor routering 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. [A]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. [A]Nadat voor een gebruikersnaam 3 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 ICT-voorzieningen worden gebruikers minimaal geauthenticeerd op basis van wachtwoorden.

3. [A]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 wachtwoorden[29], regelmatige wijziging, directe wijziging van initieel wachtwoord).

2. [A]Wachtwoorden hebben een geldigheidsduur zoals beschreven bij 11.2.3. Daarbinnen dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd.

3. [A]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 typefouten 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. [A]De periode van inactiviteit van een werkstation is vastgesteld op maximaal 15 minuten. Daarna wordt de PC vergrendeld. Bij remote desktop sessies geldt dat

[29] 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', en Gartner research note G00124970 (http://www.indevis.de/dokumente/gartner_passwords_breakpoint.pdf).

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. [A]De toegang voor onderhoud op afstand door een leverancier wordt alleen opengesteld op basis een wijzigingsverzoek of storingsmelding. Met 2-factor authenticatie en tunneling.

11.6 Toegangsbeheersing voor toepassingen en informatie

Doelstelling

Voorkomen van onbevoegde toegang tot informatie in toepassingssystemen.

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 ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.

2. [A]Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten.

3. [A]Bij extern gebruik vanuit een onvertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.

4. [A]Een beheerder gebruikt two-factor authenticatie voor het beheer van kritische apparaten, bijvoorbeeld 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. [A]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. [A]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. [A]Er zijn, waar mogelijk, voorzieningen om de actualiteit van anti-malware programmatuur op mobiele apparaten te garanderen.

3. [A]Bij melding van verlies of diefstal wordt de communicatiemogelijkheid met de centrale applicaties afgesloten.

11.7.2 Telewerken

Er behoort 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. Er wordt beleid vastgesteld met daarin de uitwerking welke systemen niet en welke systemen wel vanuit de thuiswerkplek of andere telewerkvoorzieningen mogen worden geraadpleegd. Dit beleid wordt bij voorkeur ondersteund door een MDM-oplossing (Mobile Device Management).

3. [A]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 vooraf een risicoafweging plaats door de verantwoordelijk manager.

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 guidelines[30]).

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 NBV[31] goedkeuring of certificering volgens ISO/IEC 15408 (common criteria).

6. Er is expliciet aandacht voor leveranciers accounts, hardcoded wachtwoorden en mogelijke 'achterdeurtjes'.

12.2 Correcte verwerking in toepassingen

Doelstelling

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

[30] Voor voorbeelden van secure coding guidelines, zie http://www.cert.org/secure-coding/ of bijvoorbeeld ook OWASP
[31] NBV: Nationaal Bureau voor Verbindingsbeveiliging, onderdeel van het ministerie van BZK.

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, toevoegen van parameters (SQL-injection) 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.

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. 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. [A]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 dient te zijn 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. [A]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 leverancier[32] 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.

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

2. Broncode staat op aparte (logische) systemen.

12.5 Beveiliging bij ontwikkelings- 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 ITIL[33] en voor applicaties ASL.

[32] Dit kan ook een interne leverancier zijn.
[33] Information Technology Infrastructure Library, zie http://www.itil-officialsite.com

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.[34]
2. Er dient een proces te zijn om te melden dat (persoons) informatie is uitgelekt (zie 13.1.1).

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).

[34] Het gaat hier dan om informatie die zich daar voor leent. Encrypted informatie is niet zondermeer te scannen.

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 bloot staat 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 het melden van incidenten aan de Informatiebeveiligingsdienst voor gemeenten, 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. [A]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.

5. Indien nog geen patch beschikbaar is dient gehandeld te worden volgens het advies van de Informatiebeveiligingsdienst voor gemeenten of een andere Computer Emergency Response Team (CERT) zoals het NCSC.

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. Er is een procedure voor communicatie met de Informatiebeveiligingsdienst voor gemeenten.

3. [A]Er is een contactpersoon (Deelnemer Security Contact (DSC))[35] aangewezen voor het rapporteren van beveiligingsincidenten. Voor integriteitsschendingen is ook een vertrouwenspersoon aangewezen die meldingen in ontvangst neemt.

4. Alle beveiligingsincidenten worden vastgelegd in een systeem en geëscaleerd aan de Informatiebeveiligingsdienst voor gemeenten.

5. Vermissing of diefstal van apparatuur of media die gegevens van de gemeente kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident.

6. Informatie over de beveiligingsrelevante handelingen, bijvoorbeeld loggegevens, foutieve inlogpogingen, van de gebruiker wordt regelmatig nagekeken. De CISO bekijkt periodiek – bij voorkeur maandelijks - een samenvatting van de informatie.

[35] Lees ook als: Vertrouwde Contactpersoon Informatiebeveiliging (VCIB) of Algemeen Contactpersoon Informatiebeveiliging (ACIB) of CISO of gelijkwaardig

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 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 worden gekwantificeerd en gecontroleerd.

1. De informatie verkregen uit het beoordelen van beveiligingsmeldingen wordt geëvalueerd met als doel beheersmaatregelen te verbeteren (Plan–Do–Check–Act (PDCA) Cyclus).

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. [A]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 vooraf afgesproken niveau en binnen 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
    - wie mag het continuïteitsplan wanneer activeren
    - wanneer wordt er gecontroleerd teruggaan naar de standaard situatie
    - 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. [A]Er worden minimaal jaarlijks oefeningen en/of 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.
   Deze lijst is in conceptvorm te vinden op:
   https://www.ibdgemeenten.nl/wp-content/uploads/2014/04/20101126_Conceptlijst-aanvullende-inhoud-Informatiebeveiliging-v040.pdf

15.1.2 Intellectuele eigendomsrechten (Intellectual Property Rights (IPR))

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 bepalingen.[36]

[36] Zie artikel 12 WBP

15.1.5 Voorkomen van misbruik van ICT-voorzieningen

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

1. Er is een beleid met betrekking tot het gebruik van ICT-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.

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 de uitvoering en de beveiligingsprocedures en de toetsing daarop (o.a. jaarlijkse in control statement). Conform de Strategische Baseline zorgt de CISO, namens de gemeentesecretaris, voor het toezicht op de uitvoering van het beveiligingsbeleid. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door of vanwege de CISO dan wel door interne of externe auditteams.

2. [A]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 compromitteren te voorkomen.

Bijlage A: Begrippen

Audit trail	Vastlegging van de complete keten van opeenvolgende wijzigingen op een object in een bepaalde periode.
A&K analyse	Een analyse methode om de afhankelijkheden en kwetsbaarheden in kaart te brengen.
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, bedrijfscontinuïteitsbeheer en artikel 16 van de Wbp 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, bedrijfscontinuïteitsbeheer, 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.
DSC	Deelnemer Security Contact, de contactpersoon binnen het incident management proces.
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.
ENSIA	Eenduidige Normatiek Single Information Audit, is een systematiek om verschillende audits die nu apart plaatsvinden te gaan samenvoegen. Het is nog een project en op termijn moet hier verlaging van de auditlast en verantwoording van gemeenten uit voortkomen. Zie SiSa
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	Binnen de gebruikelijke Planning en Control cyclus moet door B&W een in control statement worden afgegeven over het BIG. De in control statement moet inzicht geven aan welke BIG normen wordt voldaan en voor welke BIG normen een explain is gedefinieerd.
Informatie-beveiliging	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 gemeenten: het lijnmanagement is integraal verantwoordelijk en dus ook voor de beveiliging van de TBB.
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 integriteitseis 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 in 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.
SiSa	Single information, single audit betekent eenmalige informatieverstrekking, eenmalige accountantscontrole. SiSa is de manier waarop medeoverheden (provincies, gemeenten en gemeenschappelijke regelingen) aan het Rijk ieder jaar verantwoorden of en hoe ze de specifieke uitkeringen hebben besteed. Zie ENSIA.
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 (bijvoorbeeld password, PIN); • Iets dat de gebruiker heeft (bijvoorbeeld toegangspas, sleutel); en • Iets dat de gebruiker is (bijvoorbeeld 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 BIG worden maatregelen beschreven die voldoen voor de behandeling van gerubriceerde informatie tot en met vertrouwelijke en persoonsvertrouwelijke informatie, zoals bedoeld in artikel 16 van de Wbp
Verwijderbare media	Opslagmiddelen die los van apparatuur kunnen worden verwijderd en meegenomen. Zoals CD-ROM, USB stick, verwijderbare schijven, tapes of gedrukte media.
Zone	De logische verzameling van ICT-voorzieningen met hetzelfde beveiligingsniveau, die via beveiligde koppelvlakken gegevens kunnen uitwisselen

Bijlage B Mapping BIG

In dit hoofdstuk is de mapping opgenomen naar de belangrijkste wetgeving. In de BRP en de BAG zijn specifieke maatregelen opgenomen over bestandscontrole, deze hebben niet specifiek betrekking op de ISO 27002 en zijn hier dus ook niet verwerkt.

Sectie	SubSectie	Gebied	Omschrijving	BRP	SUWI	BAG	Wbp	PUN
5	1	1	Beleidsdocument voor informatiebeveiliging	X	X		X	X
5	1	2	Beoordeling van het informatiebeveiligingsbeleid	X	X		X	X
6	1	1	Betrokkenheid van het College bij informatiebeveiliging	X	X		X	X
6	1	2	Coördinatie van informatiebeveiliging	X	X		X	X
6	1	3	Toewijzing van verantwoordelijkheden voor informatiebeveiliging	X	X		X	X
6	1	4	Goedkeuringsproces voor ICT-voorzieningen	X	X		X	X
6	1	5	Geheimhoudingsovereenkomst	X	X		X	X
6	1	6	Contact met overheidsinstanties					
6	1	7	Contact met speciale belangengroepen					
6	1	8	Onafhankelijke beoordeling van informatiebeveiliging	X	X		X	X
6	2	1	Identificatie van risico's die betrekking hebben op externe partijen	X	X		X	X
6	2	2	Beveiliging behandelen in de omgang met klanten		X			X
6	2	3	Beveiliging behandelen in overeenkomsten met een derde partij	X	X		X	X
7	1	1	Inventarisatie van bedrijfsmiddelen	X	X		X	X
7	1	2	Eigendom van bedrijfsmiddelen	X	X		X	X
7	1	3	Aanvaardbaar gebruik van bedrijfsmiddelen	X	X		X	X
7	2	1	Richtlijnen voor het classificeren		X		X	
7	2	2	Labeling en verwerking van informatie		X		X	
8	1	1	Rollen en verantwoordelijkheden	X	X		X	X
8	1	2	Screening	X	X		X	X
8	1	3	Arbeidsvoorwaarden	X	X		X	X
8	2	1	Directieverantwoordelijkheid	X	X		X	X
8	2	2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	X	X		X	X
8	2	3	Disciplinaire maatregelen	X	X		X	X
8	3	1	Beëindiging van verantwoordelijkheden	X	X		X	X
8	3	2	Retournering van bedrijfsmiddelen	X	X		X	X
8	3	3	Blokkering van toegangsrechten	X	X		X	X
9	1	1	Fysieke beveiliging van de omgeving	X	X		X	X
9	1	2	Fysieke toegangsbeveiliging	X	X		X	X
9	1	3	Beveiliging van kantoren, ruimten en faciliteiten	X	X		X	X
9	1	4	Bescherming tegen bedreigingen van buitenaf	X	X		X	X
9	1	5	Werken in beveiligde ruimten	X	X		X	X
9	1	6	Openbare toegang en gebieden voor laden en lossen		X			X
9	2	1	Plaatsing en bescherming van apparatuur	X	X		X	X
9	2	2	Nutsvoorzieningen	X	X		X	X
9	2	3	Beveiliging van kabels		X			
9	2	4	Onderhoud van apparatuur	X	X		X	X
9	2	5	Beveiliging van apparatuur buiten het terrein	X	X		X	X

Sectie	SubSectie	Gebied	Omschrijving	BRP	SUWI	BAG	Wbp	PUN
9	2	6	Veilig verwijderen en hergebruiken van apparatuur	X	X		X	X
9	2	7	Verwijdering van bedrijfseigendommen	X	X		X	X
10	1	1	Gedocumenteerde bedieningsprocedures	X	X		X	X
10	1	2	Wijzigingsbeheer	X	X		X	X
10	1	3	Functiescheiding	X	X		X	X
10	1	4	Scheiding van faciliteiten voor ontwikkeling, testen en productie		X			X
10	2	1	Dienstverlening	X	X		X	X
10	2	2	Controle en beoordeling van dienstverlening door een derde partij	X	X		X	X
10	2	3	Beheer van wijzigingen in dienstverlening door een derde partij	X	X		X	X
10	3	1	Capaciteitsbeheer	X	X		X	
10	3	2	Systeemacceptatie	X	X		X	
10	4	1	Maatregelen tegen virussen	X	X		X	X
10	4	2	Maatregelen tegen ‘mobile code’	X	X		X	X
10	5	1	Reservekopieën maken (back-ups)	X	X		X	X
10	6	1	Maatregelen voor netwerken	X	X		X	X
10	6	2	Beveiliging van netwerkdiensten	X	X		X	X
10	7	1	Beheer van verwijderbare media	X	X		X	X
10	7	2	Verwijdering van media	X	X		X	X
10	7	3	Procedures voor de behandeling van informatie	X	X		X	X
10	7	4	Beveiliging van systeemdocumentatie	X	X		X	X
10	8	1	Beleid en procedures voor informatie-uitwisseling	X	X		X	X
10	8	2	Uitwisselingsovereenkomsten	X	X		X	X
10	8	3	Fysieke media die worden getransporteerd	X	X		X	X
10	8	4	Elektronische berichtuitwisseling	X	X		X	X
10	8	5	Systemen voor bedrijfsinformatie	X	X		X	X
10	9	1	E-commerce					
10	9	2	Online transacties	X	X		X	X
10	9	3	Openbaar beschikbare informatie	X	X		X	
10	10	1	Aanmaken auditlogbestanden	X	X		X	X
10	10	2	Controle van systeemgebruik	X	X		X	X
10	10	3	Bescherming van informatie in logbestanden	X	X		X	X
10	10	4	Logbestanden van administrators en operators	X	X		X	X
10	10	5	Registratie van storingen	X	X		X	X
10	10	6	Synchronisatie van systeemklokken					
11	1	1	Toegangsbeleid	X	X		X	X
11	2	1	Registratie van gebruikers	X	X		X	X
11	2	2	Beheer van speciale bevoegdheden	X	X		X	X
11	2	3	Beheer van gebruikerswachtwoorden	X	X		X	X
11	2	4	Beoordeling van toegangsrechten van gebruikers	X	X		X	X
11	3	1	Gebruik van wachtwoorden	X	X		X	X
11	3	2	Onbeheerde gebruikersapparatuur	X	X		X	X
11	3	3	‘Clear desk’- en ‘clear screen’-beleid	X	X		X	X
11	4	1	Beleid ten aanzien van het gebruik van netwerkdiensten	X	X		X	X
11	4	2	Authenticatie van gebruikers bij externe verbindingen.	X	X		X	X
11	4	3	Identificatie van (netwerk)apparatuur	X	X		X	X

Sectie	SubSectie	Gebied	Omschrijving	BRP	SUWI	BAG	Wbp	PUN
11	4	4	Bescherming op afstand van poorten voor diagnose en configuratie	X	X		X	X
11	4	5	Scheiding van netwerken	X	X		X	X
11	4	6	Beheersmaatregelen voor netwerkverbindingen	X	X		X	X
11	4	7	Beheersmaatregelen voor netwerkroutering	X	X		X	X
11	5	1	Beveiligde inlogprocedures	X	X		X	X
11	5	2	Gebruikersidentificatie en -authenticatie	X	X		X	X
11	5	3	Systemen voor wachtwoordbeheer	X	X		X	X
11	5	4	Gebruik van systeemhulpmiddelen	X	X		X	X
11	5	5	Time-out van sessies	X	X		X	X
11	5	6	Beperking van verbindingstijd	X	X		X	X
11	6	1	Beperking van toegang tot informatie	X	X		X	X
11	6	2	Isolatie van gevoelige systemen	X	X		X	X
11	7	1	Draagbare computers en communicatievoorzieningen	X	X		X	
11	7	2	Telewerken	X	X		X	
12	1	1	Analyse en specificatie van beveiligingseisen	X	X		X	X
12	2	1	Validatie van invoergegevens	X	X		X	X
12	2	2	Beheersing van interne gegevensverwerking	X	X	X	X	X
12	2	3	Integriteit van berichten	X	X	X	X	X
12	2	4	Validatie van uitvoergegevens	X	X		X	X
12	3	1	Beleid voor het gebruik van cryptografische beheersmaatregelen	X	X		X	X
12	3	2	Sleutelbeheer	X	X		X	X
12	4	1	Beheersing van operationele software	X	X		X	X
12	4	2	Bescherming van test data					
12	4	3	Toegangsbeheersing voor broncode van programmatuur					
12	5	1	Procedures voor wijzigingsbeheer				X	X
12	5	2	Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem				X	X
12	5	3	Restricties op wijzigingen in programmatuurpakketten					
12	5	4	Uitlekken van informatie	X	X		X	X
12	5	5	Uitbestede ontwikkeling van programmatuur					
12	6	1	Beheersing van technische kwetsbaarheden	X			X	X
13	1	1	Rapportage van informatiebeveiligingsgebeurtenissen	X	X		X	X
13	1	2	Rapportage van zwakke plekken in de beveiliging	X	X		X	X
13	2	1	Verantwoordelijkheden en procedures	X	X		X	X
13	2	2	Leren van informatiebeveiligingsincidenten	X	X		X	X
13	2	3	Verzamelen van bewijsmateriaal	X	X		X	X
14	1	1	Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer	X	X	X	X	
14	1	2	Bedrijfscontinuïteit en risicobeoordeling	X	X	X	X	
14	1	3	Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging	X	X	X	X	
14	1	4	Kader voor de bedrijfscontinuïteitsplanning	X	X	X	X	
14	1	5	Testen, onderhoud en herbeoordelen van continuïteitsplannen	X	X	X	X	
15	1	1	Identificatie van toepasselijke wetgeving	X	X		X	X
15	1	2	Intellectuele eigendomsrechten (Intellectual Property Rights, IPR)					

Sectie	SubSectie	Gebied	Omschrijving	BRP	SUWI	BAG	Wbp	PUN
15	1	3	Bescherming van bedrijfsdocumenten	X	X		X	X
15	1	4	Bescherming van gegevens en geheimhouding van persoonsgegevens	X	X		X	X
15	1	5	Voorkoming van misbruik van ICT-voorzieningen	X	X		X	
15	1	6	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	X	X		X	
15	2	1	Naleving van beveiligingsbeleid en -normen	X	X		X	X
15	2	2	Controle op technische naleving	X	X		X	
15	3	1	Beheersmaatregelen voor audits van informatiesystemen	X	X		X	X
15	3	2	Bescherming van hulpmiddelen voor audits van informatiesystemen	X	X		X	X

Wijzigingenblad BIG TNK 1.01

Waar in document	Wijziging
Gehele document	Diverse correcties in grammatica en schrijfwijzen, zoals: • WBP wijzigen in Wbp • GBA wijzigen in BRP • IT wijzigen in ICT • BhV wijzigen in BHV. • Vir-bi aangepast naar VIRBI • Daar waar BPR staat, dit aangepast naar RvIG (Rijksdienst voor Identiteitsgegevens) • De BIG-OP producten hebben ook gezorgd voor enkele aanpassingen, zoals het toevoegen van de Baselinetoets BIG, Diepgaande Risicoanalyse en Privacy Impact Assessment (PIA). ➢ Diverse bronvermeldingen aangepast en toegevoegd ➢ Diverse Engelse woorden vertaald naar het Nederlands
Management samenvatting	Relatie BIG, BIR en update naar nieuwe ISO nader uitgelegd en herschreven
Opdracht : Doel	BIG-OP toegevoegd en verwijzing naar toekomstige BIG-OP verwijderd
Leeswijzer: doelgroepen	Geherstructureerd
Inleiding	ENSIA toegevoegd bij de inleiding, verantwoordingsdruk vervangen voor verantwoordingslast
2	moeten vervangen voor dienen, zinsbouw aangepast
3	zinsbouw aangepast
3.4	Informatiebeveiligingsplan en koppeling naar P&C cyclus aangescherpt.
4	A&K-analyse verwijderd
6.1.2.1	lidwoord toegevoegd voor CISO
6.2.1.5	WBP aangepast in Wbp
7.2.1.2	WBP aangepast in Wbp en de risicoklassen persoonsgegevens verwijderd in verband met de richtsnoeren persoonsgegevens
8.1.3	‘behoren te zijn’ veranderd in ‘zijn’.
8.3.1.1	‘(zowel in dienst van een derde bedrijf als individueel)’ aangepast in ‘(zowel in dienst van een derde bedrijf of als individueel)’.

9.1.1.3	IT gewijzigd in ICT
9.1.1.8	BhV gewijzigd in BHV
9.1.3.1	toegevoegd: 'tenzij de vertrouwelijke informatie op de mobiele gegevens drager voldoende versleuteld is'
9.1.3.3	toegevoegd: 'of de NEN-norm NPR 5313 of de Europese norm NEN-EN 50600 serie'
9.2.1.5	[A]: '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' is onjuist, norm gaat over apparatuur, voorbeeldmaatregel aangepast naar: '[A]Apparatuur 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'.
10.1.3.4	komma ingevoegd na 'informatiesysteemfuncties'.
10.4.2	Uitleg toegevoegd in de voetnoot over mobile code.
10.7.2.1	toegevoegd 'gesteld' na 'en in werking'
10.8.1.2	komma toegevoegd na 'faxen'
11.5.3.4	interpunctie aangepast
11.6.1.4	'bijvoorbeeld' uitgeschreven
11.7.2.3	'Voor printen in onvertrouwde omgevingen vindt een risicoafweging plaats.' vervangen door 'Voor printen in onvertrouwde omgevingen vindt vooraf een risicoafweging plaats door de verantwoordelijk manager.'
14.1.3.1	Interpunctie aangepast
15.1.1.1	Link aangepast
Bijlage A	Begrippen, ENSIA toegevoegd

KWALITEITSINSTITUUT
NEDERLANDSE GEMEENTEN

NASSAULAAN 12
2514 JS DEN HAAG

POSTBUS 30435
2500 GK DEN HAAG

T 070 373 80 08
F 070 363 56 82

INFO@IBDGEMEENTEN.NL
WWW.IBDGEMEENTEN.NL