gemeente Tholen

GEMEENTEBLAD

Officiële uitgave van de gemeente Tholen

Nr. 81445

18 april

2018

Beleidsregel van het college van burgemeester en wethouders van de gemeente Tholen houdende regels omtrent het Informatie Beveiligingsbeleid 2017-2020

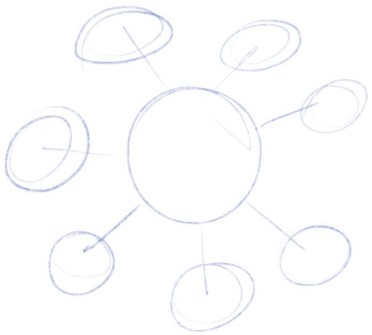
1 Inleiding

1.1 Context

Een gemeente kan steeds meer worden beschouwd als een informatie-verwerkende organisatie: informatie als productiefactor. En hoewel gemeenten een publiekrechtelijke taak vervullen met een grote mate van openbaarheid, heeft het beschermen van de 'kroonjuwelen' – onder meer persoonsgebonden en strategische informatie – een topprioriteit. We kunnen uitsluitend adequaat functioneren wanneer we de beveiliging van onze kroonjuwelen op orde hebben. Dat wil zeggen: wanneer wij ervoor zorgen dat de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie gewaarborgd is en blijft.

Dit Informatiebeveiligingsbeleid (voortaan: 'IB Beleid') is gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG), opgesteld door de Informatie Beveiligings Dienst (IBD, ingesteld door VNG en KING). Tijdens de Buitengewone Algemene Ledenvergadering op 29 november 2013 is de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' vastgesteld. Daarin is opgenomen dat alle gemeenten hun informatiebeveiliging inrichten conform BIG waarbij geldt: pas-toe-of-leg-uit (compy or explain). De BIG is gebaseerd op de internationale standaarden en normen voor informatiebeveiliging, de zogenaamde Code voor Informatiebeveiliging (NEN-ISO/IEC 27002:2007) alsmede op de wettelijke bepalingen waaraan de aangesloten organisaties onderhevig zijn.

1.2 Wat maakt dit IB Beleid zo bijzonder?



De deelnemende gemeenten hebben samen de beheerorganistie "GR ICT Samenwerking West-Brabant West" (ICTWBW) opgericht. ICTWBW is verantwoordelijk voor het beheer, de veiligheid en continuïteit van de infrastructuur.

De BIG gaat steeds uit van een 'enkelvoudige organisatie': één gemeentelijke organisatie met alle basisfuncties – waaronder 'informatisering en automatisering' – in eigen huis.

Deze 'governance' wordt in hoofdstuk 4 en het document "IB Beleid – deel 2" verder uitgewerkt.

Scope van het IB Beleid

Dit IB Beleid heeft betrekking op de volgende aangesloten organisaties:

De gemeenten:
- Bergen op Zoom
- Etten-Leur
- Roosendaal
- Moerdijk
- Tholen

De Gemeenschappelijke Regeling:
- ICT Samenwerking West-Brabant West ('ICTWBW')

Individueel aangehaald als 'aangesloten organisatie', samen aangehaald als 'de samenwerking'.

Als een nieuwe 'aangesloten organisatie' zich bij ICTWBW aanmeldt, geldt als aansluitvoorwaarde het accepteren van het onderhavige IB Beleid.

Subjecten van het IB Beleid
Cruciaal voor een goede informatiebeveiliging is de deelname van alle medewerkers binnen de aangesloten organisaties.
Alle personeelsleden in loondienst van de aangesloten organisaties en alle externe krachten die tijdelijk of voor onbepaalde duur bij de aangesloten organisaties tewerkgesteld zijn of voor de aangesloten organisaties werkzaamheden verrichten (bijv. onderaannemers, consultants, leveranciers, ...) dienen overeenkomstig het IB Beleid te handelen en zijn dus verantwoordelijk voor het toepassen van het IB Beleid binnen hun verantwoordelijkheidsgebied.

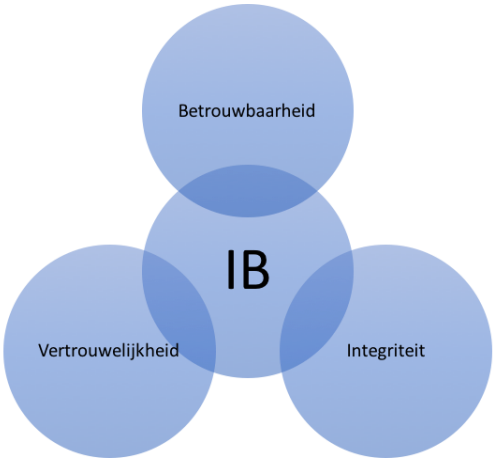
Objecten van het IB Beleid
Het IB Beleid geldt voor alle informatie, hetzij geschreven, geprint of elektronisch opgeslagen, die eigendom is van, in bewaring is bij of gebruikt wordt door welk gedeelte van de aangesloten organisaties dan ook. Het IB Beleid geldt ook voor alle (hulp)middelen gebruikt in het creëren, verwerken, versturen, sorteren, gebruiken of controleren van gegevens en informatie.

2 De duiding van informatiebeveiliging

2.1 Defintie informatiebeveiliging
Informatiebeveiliging is het geheel van preventieve, detectieve, repressieve en correctieve maatregelen alsmede procedures en processen die de beschikbaarheid, integriteit en vertrouwelijkheid van alle vormen van informatie binnen een organisatie of een maatschappij garanderen, met als doel de continuïteit van de informatie en de informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken.

2.2 Belang van informatiebeveiliging
De kwaliteit van de informatievoorziening wordt voornamelijk gedefinieerd in termen van beschikbaarheid, integriteit en vertrouwelijkheid. Het IB Beleid geeft aan hoe de aangesloten organisaties haar gegevens en informatiesystemen op de hiervoor genoemde gebieden gaan beschermen.
Deze kernbegrippen worden als volgt gedefinieerd:

- **Beschikbaarheid** betekent dat informatie(systemen) beschikbaar zijn op de juiste momenten. Hierdoor hebben medewerkers toegang tot relevante bedrijfsinformatie om hun werk en hun dienstverlening richting de burgers ongestoord voort te zetten.
- **Integriteit** betekent het waarborgen van de correctheid en de volledigheid van de informatieverwerking. Voor een efficiënte en effectieve dienstverlening is het voor de aangesloten organisaties van belang dat de correcte informatie aanwezig is in de systemen.
- **Vertrouwelijkheid** betekent dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn. Voor de aangesloten organisaties is het van belang dat vertrouwelijke informatie zoals de persoonsgegevens, medische gegevens, financiële gegevens en/of informatie met strategische waarde niet toegankelijk is voor onbevoegden.



Dit IB Beleid richt zich niet alleen op de geautomatiseerde gegevensverwerking met behulp van ICT-voorzieningen, maar uitdrukkelijk ook op de bescherming van niet-geautomatiseerde gegevens (zoals papieren documenten) en van bedrijfseigendommen (door middel van fysieke beveiliging).

2.3 Betrouwbare informatievoorziening

We beheren de informatie van en over onze burgers en bedrijven zodat deze niet verloren gaat, ongewenst aangepast wordt, onnodig bekend wordt en bovendien slechts gebruikt wordt voor het doel waarvoor die informatie verzameld is. Informatie is dan ook een van de voornaamste bedrijfsmiddelen van een gemeente. Verlies van informatie, onbevoegde kennisname, manipulatie of het niet beschikbaar zijn van informatie door uitval van of fouten in informatievoorziening kan ernstige gevolgen hebben. Dergelijk incidenten hebben mogelijk negatieve gevolgen voor onze klanten; burgers, bedrijven, partners maar ook de eigen organisatie. Grote incidenten hebben waarschijnlijk ook politieke consequenties. Een betrouwbare informatievoorziening is daarom essentieel voor de aangesloten organisaties. Informatiebeveiliging is ook het proces dat deze betrouwbare informatievoorziening borgt.

Het opnemen van informatiebeveiliging als normaal kwaliteitscriterium voor een gezonde bedrijfsvoering is tegenwoordig niet langer een keuze maar een noodzaak. Een noodzaak die ook door alle gemeenten in Nederland is bekrachtigd in de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente'. Een noodzaak die ook voortkomt uit de toenemende digitalisering van de gemeentelijke dienstverlening. Hierdoor groeit immers de afhankelijkheid van de geautomatiseerde informatieverwerking. En omdat die digitalisering ook naar voren komt in de samenwerking met steeds meer ketenpartners legt ook dat eisen op aan de kwaliteit van de informatievoorziening van de gemeente. Het vraagt tevens van de gemeente dat zij afspraken met ketenpartners maakt over de betrouwbaarheid van de door hen geleverde dienstverlening. Wet en regelgeving is een derde grond. De Wbp (Wet Bescherming Persoonsgegevens), Wet BRP (Wet Basisregistratie Personen) zijn twee van de tientallen wetten die eisen stellen aan de kwaliteit van de informatie. Als laatste noemen we hier de maatschappelijke verantwoordelijkheid die gemeenten aan haar burgers hebben. Een verantwoordelijkheid die onder meer naar voren komt bij de invoering van een landelijk stelsel van basisregistraties waarvan gemeenten onder meer de BRP en de BAG (Basisregistratie Adressen en Gebouwen) voeren.
Uiteindelijk zorgt een goede borging van informatiebeveiliging dus voor een betere betrouwbaarheid van de informatievoorziening en daardoor voor een grotere continuïteit van de gemeentelijke bedrijfsvoering

De risicobronnen waar de informatie en informatievoorziening van de aangesloten organisaties aan zijn blootgesteld komen onder andere voort uit:
- de door de organisatie gewenste functionaliteit;
- de gebruikers van de informatiesystemen;
- de kwetsbaarheden van de ICT-infrastructuur;
- externe oorzaken (bijvoorbeeld inbraak, ongeoorloofd gebruik, vernieling, natuurgeweld, maar ook technische calamiteiten zoals brand en lekkage).

2.4 Uitgangspunten van informatiebeveiliging

Om de beheersbare en betrouwbare informatievoorziening te realiseren is het van belang een aantal gemeenschappelijke uitgangspunten te hanteren en deze uit te dragen.
De aangesloten organisaties gebruiken de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) als kader en uitgangspunt voor informatiebeveiliging. Deze gezamenlijke basis betekent dat het informatiebeveiligingsbeleid, de risicoanalyse en het informatiebeveiligingsplan dezelfde structuren en methodieken kunnen blijven gebruiken.

2.5 Speerpunten

Binnen het brede gebied van informatiebeveiliging in de samenwerking gelden de volgende speerpunten:
- **Bewustwording**; vanuit de redenering dat elke technische maatregel nutteloos is wanneer de medewerkers die met informatie omgaan het belang van een betrouwbare informatievoorziening niet inzien en er naar handelen, is bewustwording een belangrijke pijler van informatiebeveiliging.
- **Continuïteit van de dienstverlening en de bedrijfsvoering** door het waarborgen van de betrouwbaarheid van de informatiehuishouding van de aangesloten organisatie.
- **Risicomanagement** wordt hierbij gebruikt om de juiste (beveiligings-)maatregelen te bepalen en te implementeren.
- **Samenwerken** is een effectieve manier om de specialistische kennis die voor informatiebeveiliging nodig is te verkrijgen en vasthouden. Dat betekent samenwerken met de aangesloten organisaties en samenwerken met de Informatiebeveiligingsdienst (IBD)
- **Controle**, vanuit het streven naar kwaliteitsverbetering is controle van de maatregelen die in het kader van informatiebeveiliging worden genomen een instrument. De controle analyseert of en in welke mate maatregelen ook het gewenste effect sorteren.

2.6 IB in drie lagen

Ook informatiebeveiliging is op te delen in het strategische, tactische en operationele niveau.

Op het **strategischeniveau** spreken we van **beleid**. De uitgangspunten in dit beleid zijn gebaseerd op (inter-)nationale standaarden en normen voor informatiebeveiliging en op de wettelijke bepalingen waaraan de aangesloten organisaties onderhevig zijn. Het beleid richt zich op het 'waarom' van IB. Dat is het onderwerp van de Strategische BIG en het daarvan afgeleide onderhavige IB Beleidsdocument.

Op het **tactischeniveau** worden de **beveiligingsmaatregelen** beschreven als uitwerking van de **doelstellingen** in het IB Beleid. Het gaat hierbij om zowel procedurele, organisatorische als om technische beveiligingsmaatregelen. Deze kunnen gedefinieerd zijn voor de informatiebeveiliging in het algemeen of voor specifieke domeinen. Dit niveau gaat in op het 'wat' van IB. In de Tactische BIG worden de 11 aspecten uitgewerkt (zie de bijlagen 5 t/m 15). Het is van essentieel belang zich te realiseren dat het IB Beleid in algemene termen uitspraken doet over beveiligingsaspecten. Het geeft middels richtlijnen dwingend richting aan de implementatie van een adequaat beveiligingsniveau voor alle (geautomatiseerde) informatie. Maatregelen op specifieke toepassingen op hardware/software niveau komen in het beleid niet aan de orde.

Op het **operationeleniveau** zijn de **beveiligingsmaatregelen** gedefinieerd die bestaan uit **dagelijkse beheersactiviteiten** met betrekking tot de informatiebeveiliging. De Operationele BIG-producten vullen dit in: 'hoe' en 'waarmee'.

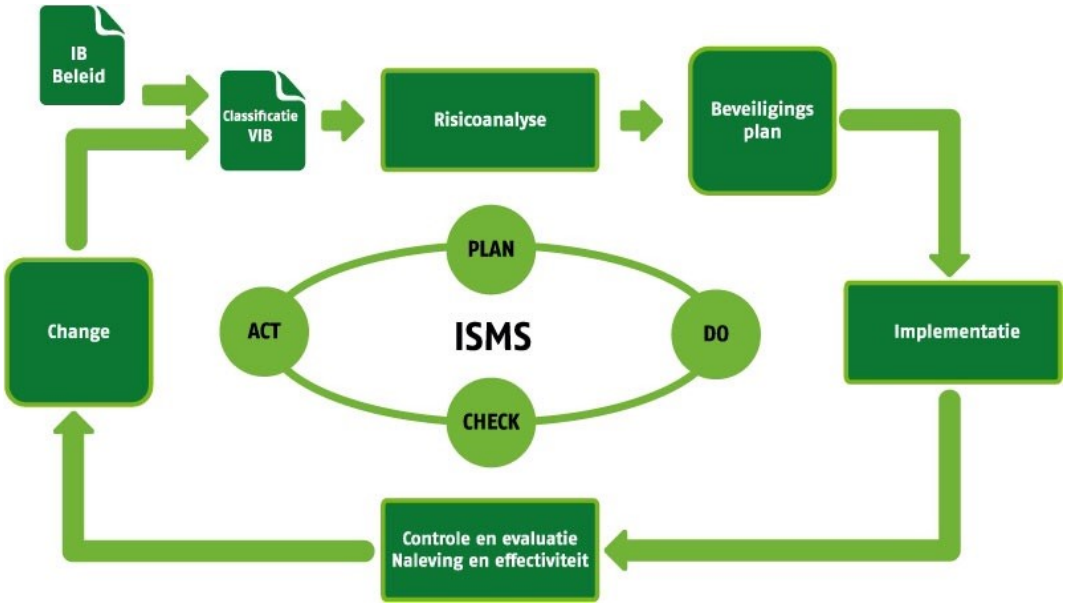
Voor elk niveau – maar zeker op het operationele – geldt dat de BIG een leidraad, een handreiking is. De aangesloten organisaties mogen daar van af wijken: comply-or-explain. Daar waar de samenwerking geen eigen varianten van de operationele maatregelen heeft ontwikkeld, zijn de Operationele BIG-producten van toepassing.

3 Het proces van informatiebeveiliging

3.1 IB als proces: ISMS

IB gaat over inhoud: de 11 aspecten, hun doelstellingen, beheersmaatregelen en beveiligingsmaatregelen. IB gaat ook over het proces van het continu omgaan met interne en externe ontwikkelingen en het nastreven van de ambities. Dit continue verbeterproces wordt in ISO27001 en BIG beschreven als het Information Security Management System, ofwel ISMS.

Het ISMS is een cyclisch proces wat in principe op jaarbasis wordt uitgevoerd. Het is een implementatie van de bekende Deming Circle (Plan-Do-Check-Act) en loopt parallel aan de gemeentelijke Planning & Control Cyclus. Informatiebeveiliging is namelijk één van de kwaliteitscriteria die in de P&C cyclus worden bijgehouden. Dat impliceert dat eisen uit de omgeving, zoals die in het informatiebeleid, eisen uit het programma e-overheid, en opmerkingen van de accountant (in de management letter) afgestemd worden en een plaats krijgen in de bedrijfsvoering van de aangesloten organisatie.
In onderstaand figuur zijn de stappen in het ISMS – en PDCA – aangegeven.



De IBF / CISO is de kennisbron op het gebied van informatiebeveiliging voor de organisatie. Hij is de coördinator van het ISMS proces, wat wordt uitgevoerd door de organisatie.

3.2 IB Beleid en IB Plan

Uit het ISMS blijkt duidelijk dat het IB Beleid het kader vormt op strategisch niveau waarin de ambitie van de gemeente betreffende de betrouwbaarheid van de informatievoorziening is vastgelegd.

In elke cyclus wordt een risico-analyse uitgevoerd. Hierin is opgenomen welke BIG-beveiligingsmaatregelen zijn geïmplementeerd en welke (nog) niet. Bovendien wordt vastgesteld wat de grootste risico's zijn en met welke beveiligingsmaatregelen (procedures, werkinstructies, technische maatregelen) die moeten worden afgedekt. Deze stap leidt tot het IB Plan. Dit is het projectplan voor de komende periode. De analyse levert daarnaast een 'Verklaring van Toepasselijkheid' op, waarmee de ambtelijke organisatie verantwoording naar het bestuur kan afleggen middels de ENSIA methodiek[1] (vanaf 2017).
In onderstaand schema is de samenhang tussen beleid, plan, VVT en de maatregelen aangegeven.

3.3 Risicobeoordeling en risico-afweging

Ten aanzien van risico's die voortkomen uit de risicoanalyse zullen de aangesloten organisaties per risico steeds één van de volgende strategieën kiezen om deze te verkleinen:

- Reduceren (treat the risk): verkleinen van het risico door middel van het nemen van preventieve informatiebeveiligingsmaatregelen.
- Accepteren (take the risk): het risico is zo klein dat de gevolgen acceptabel zijn.
- Vermijden (terminate the risk): wanneer een er een groot risico bestaat voor een bedrijfsactiviteit die weinig tot niets oplevert dan wordt deze bedrijfsactiviteit gestaakt.
- Overdragen (transfer the risk): overhevelen van het risico naar een derde partij door middel van uitbesteding of het afsluiten van verzekeringen.

De correcte uitvoering van informatiebeveiliging wordt jaarlijks via de ENSIA methodiek beoordeeld.

De samenwerking staat een neutrale risico-strategie voor, waarbij de basismaatregelen (BIG) het uitgangspunt vormen. Op deze basismaatregelen kunnen – op basis van periodieke risico-evaluatie – aanvullende maatregelen komen.

3.4 Evaluatie en bijstelling

Het IB Beleid van de samenwerking wordt elke drie jaar herzien. De directie is verantwoordelijk voor deze revisie. Indien omstandigheden daar aanleiding toe geven zijn ook tussentijdse aanpassingen mogelijk.
Het IB Plan wordt jaarlijks herzien. Het bevat immers een planningshorizon van een jaar. De risicoanalyse die nodig is om het IB Plan te kunnen maken wordt elk jaar uitgevoerd.

1) 1 ENSIA: Eénduidige Normatiek Single Information Audit: IB-verantwoordingsmechanisme door College aan de Raad

4 De organisatie van informatiebeveiliging

4.1 Lokale verantwoordelijkheid

IB is en blijft een lokale verantwoordelijkheid, zowel politiek-bestuurlijk als ambtelijk. Om deze verantwoordelijkheid goed vorm te geven, worden taken, verantwoordelijkheden en bevoegdheden tussen diverse rollen verdeeld.

Het College van B&W van elke gemeente is eindverantwoordelijk voor alle informatiebeveiligingsaangelegenheden. In het college is één portefeuillehouder aansprakelijk. De directie ondersteunt informatiebeveiliging door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen. De directie stelt middelen beschikbaar om invulling te geven (de coördinatie) van informatiebeveiliging.

Voor wat betreft ICTWBW geldt dat het Algemeen Bestuur deze eindverantwoordelijkheid draagt en dat ook hier de directie informatiebeveiliging steunt.

De organisatiebrede coördinatie van activiteiten binnen een aangesloten organisatie is belegd bij een 'informatie-beveiligings-functionaris' of IBF. In de Angelsaksische literatuur beter bekend als *ChiefInformation Security Officer*, of CISO. Beide benamingen kunnen worden gebruikt, afhankelijk van de *couleur locale*.

Het lijnmanagement van elke organisatorische eenheid (afdeling, team) van de aangesloten organisaties is en blijft onverkort verantwoordelijk voor de beveiliging en voor de kwaliteit van de informatie en informatiesystemen voor eigen gebruik en de aan anderen geleverde informatie en informatiediensten. De uitvoering van deze beveiligingsactiviteiten van een afdeling kan door het management (deels) worden gedelegeerd aan de afdelingscoördinator Informatiebeveiliging.

Verder is er voor de inhoudelijke afstemming met de meest betrokken lijnmanagers een klankbordgroep ingesteld waarvoor de IBF/CISO het initiatief neemt.

Daarnaast hebben medewerkers, oftewel gebruikers van informatie en informatiesystemen van de aangesloten organisaties een eigen verantwoordelijkheid. Men is verplicht zich te houden aan de verstrekte richtlijnen aangaande de omgang met informatie, informatieverwerking en desbetreffende bedrijfsmiddelen. Bij (het vermoeden van) een security incident is een medewerker verplicht dit te melden.

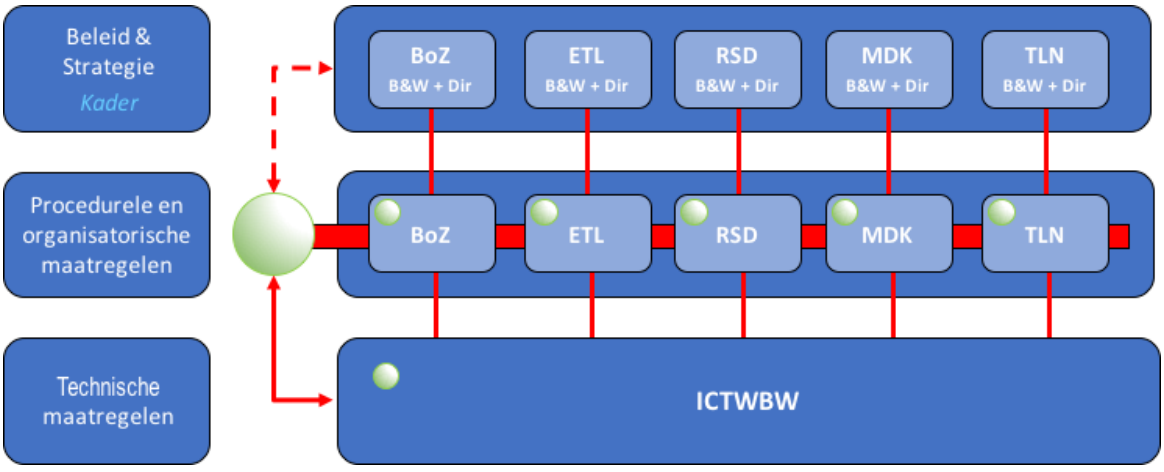
4.2 Regionale samenwerking

Doordat de aangesloten organisaties gebruik maken van (virtueel) één infrastructuur die door ICTWBW beheerd wordt, is het evident dat zij een centrale rol in informatiebeveiliging speelt, met name dus op het gebied van het implementeren en in stand houden van technische maatregelen en incidentmanagement (inclusief eventueel opschalen van lokaal naar regionaal niveau).

In de Product Diensten Catalogus (PDC) tussen de aangesloten organisaties en ICTWBW is dit nader uitgewerkt.

4.3 Regionale governance

De regionale samenwerking kan als volgt worden weergegeven.



We hanteren de onderstaande uitgangspunten bij de regionale samenwerking:

1. **Lijnverantwoordelijkheid**
   - IB is een lokale lijnverantwoordelijkheid
   - Iedere aangesloten organisatie kent zijn eigen risico-profiel en stemt daar zelf de organisatorische, procedurele en technische maatregelen op af (prioriteit, IB Plan)

2. **Kennis delen, schaal vergroten**
   - Er is één Strategisch IB Beleid (BIG) voor de aangesloten organisaties
   - Vaststellen en implementeren is een verantwoordelijk van de individuele aangesloten organisaties
   - Organisatorische en procedurele aspecten: eigen verantwoordelijkheid van de aangesloten organisaties
   - Technische aspecten: verplicht samen optrekken naar ICTWBW, escalatie naar DBO (gremium Directeuren Bedrijfsvoering)
   - Samenwerken, tenzij lokaal verschil / inzicht anders nodig maakt, ofwel comply-or-explain

3. **Regionale afstemming**
   - Ontwikkelingen op strategisch en tactisch niveau worden regionaal besproken in het 'Tactische Afstemming IB West-Brabant West' (vaak: *regionaal IB overleg*)
   - Hierin participeren de IBF/CISO's van de aangesloten organisaties met de coördinatie van de regie-CISO.
   - De regie-CISO heeft hierin de positie van 'primus inter pares': geen hiërarchische positie, maar een coördinerende. Hij is regionaal eerste aanspreekpunt voor beleidsvraagstukken en vraagstukken die organisatie-overstijgend zijn en is 'adviseur van de adviseurs'

5 Doelgroepen

Informatiebeveiliging - en daarmee ook dit IB Beleid - geldt voor alle medewerkers (ook uitzend- en inhuurkrachten), ketenpartners en zakelijke relaties van de aangesloten organisaties die te maken hebben met het verwerken van informatie in opdracht van de gemeente. Hieronder worden voor de verschillende doelgroepen / functionarissen de relevante aspecten (als bijlage bij het IB Beleid opgenomen) opgesomd.

IB functionarissen (van alle niveaus)
Alle aspecten

Informatiebeveiligingsadviseurs en ICT-auditors
Alle aspecten
Bij het helpen bepalen welke maatregelen relevant zijn en het controleren of de maatregelen daadwerkelijk genomen zijn, is het doornemen van alle bijlagen relevant.

Beleidsadviseurs alle domein en
Aspecten 4, 5, 6, 10 en 12
De beleidsadviseur is verantwoordelijk voor het ontwikkelen van een werkbaar beleid. Het beleid moet goed uitvoerbaar en controleerbaar zijn.

Lijnmanagers in hun personeelsverantwoordelijkheid
Aspecten 6 en 8
De lijnmanager is verantwoordelijk voor het handhaven van de personele beveiliging met eventuele ondersteuning door Personeelszaken (of organisatorische eenheid belast met het uitvoeren van HRM-taken).

Lijnmanagers in hun verantwoordelijkheid voor de uit voering van de processen
Aspecten 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
Aspect 8

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

Facilit aire zaken
Aspect 9
Fysieke beveiliging is vaak belegd bij Facilitaire zaken of vergelijkbare organisatorische eenheid. Zij zijn verantwoordelijk voor de beveiliging van percelen, panden en ruimtes.

Beheerders van technische infrastructuren
Aspecten 6, 7, 9, 10, 11 en 12
Informatievoorziening en de technische infrastructuren zijn ondersteunend aan bijna alle processen. De eisen die vanuit de business hier aan gesteld worden, zijn hierdoor zeer ingrijpend en bepalen voor een significant deel de inrichting van het ICT-landschap.

Applicatie-eigenaren en gebruikers
Aspecten 7, 10, 11 en 12
Applicatie-eigenaren 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 aspecten
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 dit IB Beleid 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.

6 Leeswijzer voor de bijlagen

De bijlagen maken een integraal onderdeel uit van het IB Beleid.

Bijlage 1 lokale governance voor de eigen organisatie
Bijlage 2-4 ontbreken om de nummer van de volgende bijlagen synchroon te houden aan de nummering van de BIG-maatregelen
Bijlagen 5-15 beheersmaatregelen uit de BIG -> zie document ‘Tactische Baseline Informatiebeveiliging’ van de IBD
Bijlage 16 BIG-beheersmaatregelen opgenomen in de PDC van ICTWB
De bijlagen zijn opgenomen in het document “IB Beleid – deel 2”

Bijlage 1 Lokale governance Informatiebeveiliging gemeente Tholen

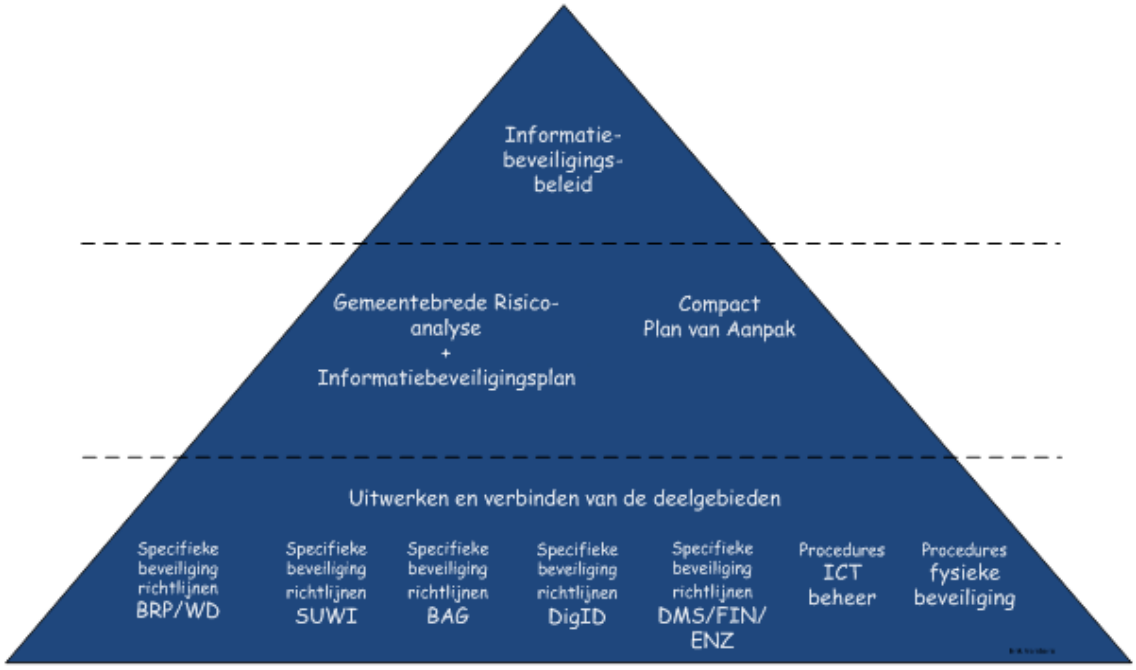
1.0 Verantwoordelijkheid en bevoegdheid informatieveiligheidsbeleid

De gemeenteraad draagt een specifieke bevoegdheid voor de controle en de toetsing op de werking van beleid binnen de gemeente, zo ook voor informatiebeveiliging. De verantwoordelijkheid voor informatiebeveiliging ligt op bestuurlijk niveau bij het college van burgemeester en wethouders en op ambtelijk niveau bij de gemeentesecretaris.

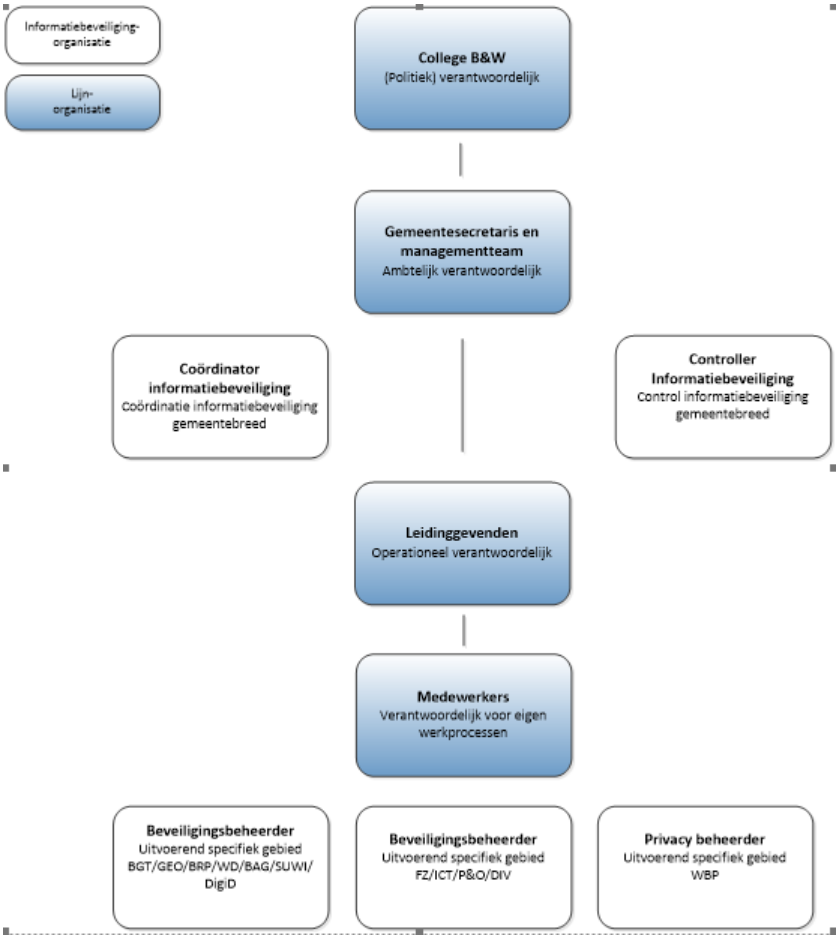
De vaststelling en implementatie van de informatiebeveiligingsstructuur en de gemeentebrede beleidsnormen vormen de verantwoordelijkheid van het college van burgemeester en wethouders van de gemeente Tholen. Voor het nemen van operationele maatregelen is de gemeentesecretaris gemandateerd. Dit geldt ook in geval van ketenafhankelijkheid en bij afdeling-overstijgende (informatie)systemen.

De leidinggevenden zijn verantwoordelijk voor de informatiesystemen waarvan zij eigenaar zijn. Zijdienen deze systemen te classificeren en in te richten zodat er adequate maatregelen kunnen worden getroffen om de veiligheidsrisico's te beheersen. Een belangrijk aspect van deze verantwoordelijkheid is om de medewerkers mee te nemen in hun verantwoordelijkheid ten aanzien van de veiligheid van informatie in hun dagelijkse werkprocessen.

1.1 Informatiebeveiligingspiramide



1.2 Informatieveiligheidsorganisatie



2.0 Beschrijving van rollen, taken en verantwoordelijkheden

College Burgemeester & Wethouders
Het College van B&W van de gemeente Tholen draagt als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen de politieke verantwoordelijkheid voor een passend niveau van informatiebeveiliging. Het college stelt de kaders ten aanzien van informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders. Het college is verantwoordelijk voor een duidelijk te volgen informatieveiligheidsbeleid en stimuleert het management van de organisatieonderdelen om beveiligingsmaatregelen te nemen. Als eigenaar van informatie en (informatie)systemen heeft het college zijn verantwoordelijkheden (macht tot handelen) op het gebied van beveiliging gemandateerd aan de gemeentesecretaris.

Gemeentesecretaris
De gemandateerde verantwoordelijkheid voor informatiebeveiliging ligt bij de gemeentesecretaris. Deze stelt met het managementteam het gewenste niveau van informatiebeveiliging vast voor de gemeente. De beveiligingseisen worden per bedrijfsproces vastgesteld. De gemeentesecretaris is verantwoordelijk voor de juiste implementatie van de beveiliging in de bedrijfsprocessen en in de in- en externe (informatie)systemen en wijst voor ieder (informatie)systeem een procesverantwoordelijke of systeemeigenaar aan. De operationele verantwoordelijkheid voor deze systemen en informatieprocessen is belegd bij leidinggevenden op organisatieniveau. De gemeentesecretaris en *het* MT hebben in ieder geval de volgende verantwoordelijkheden:

- Het stellen van kaders en het geven van sturing ten aanzien van de veiligheid van informatie;
- Het sturen op concern risico's;
- Periodiek evalueren van beleidskaders en deze bijstellen waar nodig;
- Het (laten) controleren of de getroffen veiligheidsmaatregelen overeenstemmen met de betrouwbaarheidseisen en of deze veiligheidsmaatregelen voldoende bescherming bieden;
- Het beleggen van de verantwoordelijkheid voor informatiebeveiligingscomponenten en systemen;
- Het inrichten van functiescheiding tussen uitvoerende, controlerende en beleidsbepalende taken met betrekking tot informatiebeveiliging;

- Het aanwijzen van een coördinator informatiebeveiliging en een controller informatiebeveiliging.

Functionaris Gegevensbescherming
De Functionaris gegevensbescherming (FG) is intern toezichthouder op de verwerking van persoonsgegevens. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de AVG de Wet bescherming persoonsgegevens (Wbp). De FG implementeert essentiële elementen van de AVG, zoals de beginselen van gegevensverwerking, de rechten van de betrokkenen, "privacy by design en privacy by default", de administratie van gegevensverwerkingen, beveiliging van het verwerkingsproces, en melding van en communicatie over datalekken. De rol van FG heeft een strategisch karakter. De FG:

- Draagt zorg voor inventarisaties van gegevensverwerkingen;
- Houdt meldingen van gegevensverwerkingen bij;
- Behandelt vragen en klachten van mensen binnen en buiten de organisatie;
- Ontwikkelt Interne regelingen;
- Adviseert over technologie en beveiliging (privacy by design);
- Levert input bij het opstellen of aanpassen van gedragscodes.

Coördinator Informatieveiligheid (CISO)
Deze rol is op organisatieniveau verantwoordelijk voor het actueel houden van het beleid, het adviseren bij projecten en het managen van risico's evenals het opstellen van rapportages. De coördinator informatiebeveiliging ziet organisatiebreed toe op de naleving van het informatieveiligheidsbeleid en daaruit voortvloeiende maatregelen, zorgt voor onderzoek en adviseert in complexe beveiligingsvraagstukken, initieert security audits (indien van toepassing ook risico analyses), organiseert organisatiebrede security awareness programma's en opleidingen en vervult een adviserende rol naar managementteam en gemeentebestuur. Tevens zorgt de coördinator informatiebeveiliging voor heldere communicatie bij incidenten op het vlak van informatiebeveiliging. De rol van CISO heeft een strategisch karakter. De CISO:

- Coördineert het formuleren van informatieveiligheidsbeleid en houdt dit actueel;
- Stelt het informatieveiligheidsplan op en zorgt voor de actualisatie van dat plan;
- Coördineert de uitvoering van informatieveiligheidsmaatregelen uit het informatieveiligheidsplan;
- Stelt een afstemmingsmechanisme op voor overleg en rapportage met betrekking tot informatieveiligheid;
- Ondersteunt de directie en de leidinggevenden met kennis over informatieveiligheid, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen en initieert organisatiebrede security awareness programma's;
- Is aanspreekpunt voor medewerkers van de gemeente over het onderwerp informatieveiligheid;
- Volgt de externe invloeden die van invloed zijn op het informatieveiligheidsbeleid en het informatieveiligheidsplan;
- Zorgt voor registratie van informatieveiligheidsincidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Toetst of informatieveiligheid een onderdeel uitmaakt van het informatieplannings-, systeemontwikkelings- en onderhoudsproces;
- Initieert security audits (indien van toepassing ook risico analyses);
- Rapporteert over de informatieveiligheid van de gemeente in de P&C managementrapportages;
- Ziet toe op naleving van het informatieveiligheidsbeleid en daaruit vloeiende maatregelen.

Verantwoordelijkheden en taken op afdelingsniveau en teamniveau
De leidinggevenden (afdelingshoofden respectievelijk de teamleiders) zijn verantwoordelijk voor de (informatie) veiligheid en de betrouwbaarheid van de informatieprocessen en systemen binnen hun afdeling c.q. team. De leidinggevenden hebben in ieder geval de volgende verantwoordelijkheden:

- Het uit (laten) voeren van maatregelen uit het informatieveiligheidsplan die op de afdeling van toepassing zijn;
- Op basis van een expliciete risicoafweging opstellen van betrouwbaarheidseisen voor de afdelingsinformatiesystemen;
- De keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- Het sturen op beveiligingsbewustzijn, op bedrijfscontinuïteit en op naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- Het rapporteren, via de coördinator informatiebeveiliging, over compliance aan wet- en regelgeving en algemeen beleid van de gemeente in de P&C managementrapportages.

Controller Informatieveiligheid
Deze rol is op organisatieniveau verantwoordelijk voor de verbijzonderde interne controle op de naleving van het informatieveiligheidsbeleid, de realisatie van voorgenomen veiligheidsmaatregelen en de escalatie van beveiligingsincidenten. De Controller informatiebeveiliging:

- Toetst periodieke op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van informatieveiligheid;
- Controleert de voortgang van het uitvoeren van de maatregelen uit het informatieveiligheidsplan;
- Houdt toezicht op de periodieke actualisatie van informatieveiligheidsbeleid en het Informatiebeveiligingsplan;
- Toets en bewaakt het niveau van informatieveiligheid;
- Toetst het evaluatieproces van beveiligingsincidenten.

Regiefunctionaris ICT
De regiefunctionaris ICT is in de organisatie direct aanspreekpunt voor het ICT samenwerkingsverband ICTWBW. ICTWBW beheert de werkplekken, serverplatformen, lokale netwerken en de toegang tot straalverbindingen, externe netwerkverbindingen (zoals Gemnet en SUWInet) en verzorgt het technische (wijzigings)beheer van databases, bedrijfsapplicaties en kantoorautomatiseringshulpmiddelen. Verder zijn zij verantwoordelijk voor het (laten) realiseren van alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen. Daarnaast is zij verantwoordelijk voor de implementatie van ICT-technische beveiligingsmaatregelen. Verantwoording over het gevoerde beheer van de getroffen beveiligingsmaatregelen wordt aan de procesverantwoordelijken voor (informatie)systemen afgelegd.

Privacy beheerder
Deze rol is gericht op de uitvoering en de naleving van de Wet Bescherming van Persoonsgegevens (WBP). De privacy beheerder is aanspreekpunt op het vlak van bescherming van persoonsgegevens en privacy binnen de organisatie en informeert en adviseert het management, bestuur en de collega's van de organisatie over de wijze waarop optimaal gebruik van informatie kan worden gemaakt. De Privacy beheerder draagt tevens bij aan de bewustwording en doorontwikkeling van Informatiebeveiliging en Privacy in de organisatie. De Privacy beheerder:

- Houdt toezicht op de naleving van specifieke regelgeving, waaronder de AVG, de Wet Bescherming van Persoonsgegevens (WBP) en de Wet Basisregistratie Personen (BRP);
- Adviseert organisatiebreed over privacybescherming en over activiteiten ter bescherming van persoonsgegevens;
- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Geeft aanwijzingen aan gebruikers van systemen met betrekking tot persoonsregistraties;
- Geeft (ongevraagd) advies over alle procedures en producten die betrekking hebben op de registratie van personen;
- Is contactpersoon van de gemeente voor het College Bescherming Persoonsgegevens (CBP);
- Beheert het register met daarin alle persoonsregistraties die onder verantwoordelijkheid van de organisatie vallen.
- Levert een bijdrage aan de ontwikkeling van beleid, protocollen, normen, regelingen en gedragscodes.

Ensia Coördinator
De Ensia Coördinator werkt aan het begeleiden, bewaken en bijsturen van het ENSIA- verantwoordingsproces. De kerntaken zijn het creëren van bewustzijn over informatieveiligheid voor de hele gemeente en het organiseren van samenwerking.

Beveiligingsbeheerder
Deze rol is verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid van specifieke gegevensverzamelingen. In wetgeving worden verschillende benamingen aan rollen gegeven voor veelal dezelfde taken en verantwoordelijkheden ten aanzien van specifieke gegevensverzamelingen. Om eenduidigheid in naamgeving te verkrijgen wordt in dit beleidsdocument de veiligheidsverantwoordelijkheid ten aanzien van een specifieke gegevensverzameling toegewezen aan, en gedefinieerd als Beveiligingsbeheerder. Hierna volgen de deelgebieden waarbij een beveiligingsbeheerder is aangewezen met vermelding van eventuele officiële rolbenaming: BRP, Reisdocumenten (officieel autorisatiebevoegde Reisdocumenten/Aanvraagstations), Rijbewijzen (Autorisatiebevoegde Rijbewijzen), BAG, SUWI (officieel Security Officer SUWI volgens het BKWI) en DigiD. Daarnaast worden er beveiligingsbeheerders aangewezen op verschillende aspecten van de gemeentelijke be-

drijfsvoering: Facilitaire Zaken, ICT, DIV, P&O en BGT/GEO. De beveiligingsbeheerder is -voor het toegewezen deelgebied- verantwoordelijk voor:

- Het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid en de onderliggende informatieveiligheidsplannen. Hieronder vallen de preventie van beveiligingsincidenten, de detectie van dergelijke incidenten en het geven van een adequate respons;
- De medewerker voert interne controles uit en let op de naleving van specifieke wet- en regelgeving. De beveiligingsbeheerder rapporteert aan de coördinator informatiebeveiliging en de controller informatiebeveiliging.

Beveiligingsbeheerder BRP

De Beveiligingsbeheerder BRP is verantwoordelijk voor het toezicht op het beheer en de ontwikkeling van beveiligingsprocessen Basisregistratie Personen, het toetsen op de uitvoering van regelgeving en procedures ten aanzien van de Basisregistratie Personen, de evaluatie van de beveiligingsprocessen en het verzorgen van een managementrapportage aan de opdrachtgever Basisregistratie Personen (College B&W).
De Beveiligingsbeheerder BRP:

- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Coördineert de toepassing van specifieke wet- en regelgeving;
- Rapporteert aan de coördinator informatieveiligheid (CISO) en de Controller informatieveiligheid.

Beveiligingsbeheerder waardedocumenten (PNIK)

De Beveiligingsbeheerder waardedocumenten is verantwoordelijk voor het toezicht op het beheer en de ontwikkeling van beveiligingsprocessen Waardedocumenten (PNIK), het toetsen op de uitvoering van regelgeving en procedures ten aanzien van het waardedocumentenproces, de evaluatie van de beveiligingsprocessen en het verzorgen van een managementrapportage aan de opdrachtgever Waardedocumenten (College B&W). De Beveiligingsbeheerder waardedocumenten (PNIK):

- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Coördineert de toepassing van specifieke wet- en regelgeving;
- Rapporteert aan de coördinator informatieveiligheid (CISO) en de Controller informatieveiligheid.

Beveiligingsbeheerder BAG

De Beveiligingsbeheerder BAG is verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de normenkaders voor audit en (zelf)evaluatie en het informatieveiligheidsplan. Hieronder vallen de preventie van beveiligingsincidenten, de detectie van dergelijke incidenten en het geven van een adequate respons. De medewerker coördineert de toepassing van specifieke wet- en regelgeving. De beveiligingsbeheerder rapporteert aan de coördinator informatieveiligheid / CISO en de controller informatieveiligheid.

Beveiligingsbeheerder SUWI

De beveiligingsbeheerder SUWI beheert beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd.
De beveiligingsbeheerder SUWI:

- Bevordert en adviseert over de beveiliging van Suwinet;
- Ziet er op toe dat de maatregelen worden nageleefd;
- Adviseert medewerkers en management en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet;
- Evalueert de uitkomsten van verbetermaatregelen;
- Verzorgt rapportages met betrekking tot de beveiligingsstatus van Suwinet aan het hoogste management en/of college;
- Vraagt meerdere keren per jaar rapportages op bij het BKWI over het gebruik van SUWInet door de gemeente;
- Rapporteert aan de coördinator informatieveiligheid (CISO) en de controller informatieveiligheid.

Beveiligingsbeheerder DigiD

De Beveiligingsbeheerder DigiD is verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de normenkaders voor audit en (zelf)evaluatie en het informatieveiligheidsplan. Hieronder vallen de preventie van beveiligingsincidenten, de detectie van dergelijke incidenten en het geven van een adequate respons. De medewerker coördineert de toepassing van specifieke wet- en regelgeving. De beveiligingsbeheerder rapporteert aan de coördinator informatieveiligheid (CISO) en de Controller informatieveiligheid.

Beveiligingsbeheerder Facilitaire Zaken
De Beveiligingsbeheerder Facilitaire Zaken is de directe contactpersoon voor de organisatie ten aanzien van alle activiteiten informatieveiligheid die betrekking hebben op facilitaire zaken en Huisvesting en Services en is verantwoordelijk voor de fysieke toegangsbeveiliging en kantoorinrichting (archiefkasten, kluizen enzovoort).
De Beveiligingsbeheerder Facilitaire Zaken:
- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Coördineert de toepassing van specifieke wet- en regelgeving;
- Rapporteert aan de coördinator informatieveiligheid (CISO) en de Controller informatieveiligheid

Beveiligingsbeheerder ICT
De Beveiligingsbeheerder ICT is de directe contactpersoon voor de organisatie ten aanzien van alle activiteiten informatieveiligheid die betrekking hebben op ICT. De Beveiligingsbeheerder ICT is verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de normenkaders voor audit en (zelf)evaluatie en het Informatieveiligheidsplan. De Beveiligingsbeheerder ICT:
- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Coördineert de toepassing van specifieke wet- en regelgeving;
- Rapporteert aan de coördinator informatieveiligheid (CISO) en de Controller informatieveiligheid.

Beveiligingsbeheerder DIV
De Beveiligingsbeheerder DIV is de directe contactpersoon voor de organisatie ten aanzien van alle activiteiten informatieveiligheid die betrekking hebben op DIV en is verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de normenkaders voor audit en (zelf)evaluatie, het informatieveiligheidsplan en wet en regelgeving specifiek ten aanzien van DIV, waaronder de Archiefwet in relatie tot de wet Revitalisering Generiek Toezicht (RGT). De Beveiligingsbeheer DIV:
- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Coördineert de toepassing van specifieke wet- en regelgeving;
- Rapporteert aan de coördinator informatieveiligheid (CISO) en de Controller informatieveiligheid.

Beveiligingsbeheerder P&O
De Beveiligingsbeheerder P&O is de directe contactpersoon voor de organisatie ten aanzien van alle activiteiten informatieveiligheid die betrekking hebben op P&O en heeft een belangrijke adviesrol op het gebied van organisatie en informatieprocessen. De Beveiligingsbeheerder P&O is verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de normenkaders voor audit en (zelf)evaluatie en het informatieveiligheidsplan. De Beveiligingsbeheer P&O
- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Coördineert de toepassing van specifieke wet- en regelgeving;
- Rapporteert aan de coördinator informatieveiligheid (CISO) en de Controller informatieveiligheid.

Functioneel applicatiebeheerder

De Functioneel applicatiebeheer is verantwoordelijk voor het geheel van activiteiten gericht op het ondersteunen van de informatiesystemen en de waarborging van continuïteit aan de gebruikerszijde van de informatievoorziening.
Certificaatbeheerder De certificaatbeheerder beheert de elektronische sleutels van PKI/Overheid conform de voorschriften. Public key infrastructure (PKI) is het systeem waarmee uitgiften en beheer van digitale certificaten wordt gerealiseerd. Aan het gebruik zijn voorschriften verbonden ten aanzien van installatie, beveiliging, update, geldigheid en toepassing. De certificaatbeheerder is hiervoor verantwoordelijk.
Gegevensbeheerder De Gegevensbeheerder is verantwoordelijk voor het geheel van activiteiten gericht op de inhoudelijke kwaliteitszorg betreffende het gegevens verzamelen, de gegevensverwerking en de informatievoorziening.
Informatiebeheerder De Informatiebeheerder is verantwoordelijk voor het geheel van activiteiten gericht op beleidsvoorbereiding ter zake de specifieke gegevensverzameling, de ontwikkeling van kwaliteitsprocedures, beveiligingsprocedures, verstrekking- en privacyprocedures, evenals de coördinatie bij de uitvoering van deze procedures.
Autorisatiebevoegde Reisdocumenten/Aanvraagstations De Autorisatiebevoegde Reisdocumenten is verantwoordelijk voor het beheer van de autorisaties voor de reisdocumentenmodules (RAAS en aanvraagstations).
Autorisatiebevoegde Rijbewijzen De Autorisatiebevoegde Rijbewijzen is verantwoordelijk voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW.
Vertrouwde Contactpersoon Informatiebeveiliging (VCIB) De VCIB krijgt waarschuwingen en informatie van de IBD met een vertrouwelijk karakter over mogelijke bedreigingen en incidenten waarvan de inhoud een vertrouwelijk karakter heeft en die niet met anderen gedeeld mogen worden.
Algemene Contactpersoon Informatiebeveiliging (ACIB) – kunnen meerdere personen zijn De ACIB krijgt algemene waarschuwingen en informatie van de IBD met een niet vertrouwelijk karakter over algemene bedreigingen en incidenten.

NB in een aparte bijlage staan de namen vermeld van de toegewezen rollen in de beveiligingsorganisatie. De toewijzing van de rollen wordt door het MT vastgesteld.

3.0 Overleg en afstemmingsorganen
De coördinator informatieveiligheid is voorzitter van het overleg informatiebeveiliging dat 4 maal per jaar bij elkaar komt. Bij dit overleg zijn aanwezig:

- De coördinator informatieveiligheid (CISO);
- De controller informatiebeveiliging;
- Agendaleden: Beveiligingsbeheerders t.a.v: BRP en WD, BAG, SUWI, DigiD, GEO/BGT;
- Agendaleden: Beveiligingsbeheerders t.a.v: FZ, ICT, DIV en P&O;
- Agendalid: Privacy beheerder;
- Agendaleden: Managementteam (MT)lid of specialist, Regiefunctionaris ICT.

3.1 Onderwerpen:

- Voortgang uitvoering maatregelen Beveiligingsplan c.q. Plan van Aanpak;
- Behandeling veiligheidsincidenten;
- Planning en voorbereiding van audits, inspecties en evaluaties;
- Evaluatie en actualisatie informatiebeveiliging en informatieveiligheidsplan.

4.0 ICT crisisbeheersing
Voor interne crisisbeheersing is een kernteam informatiebeveiliging geïnstalleerd. Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten. Dit team bestaat uit:

• De coördinator informatieveiligheid (CISO);
• Regiofunctionaris;
• De beveiligingsbeheerder ICT;
• Betrokken MT lid (verantwoordelijk voor ICT/Informatievoorziening);
• Relevante experts;
• Een lid van het team Communicatie;

5.0 Rapporteren beveiligingsincidenten
De coördinator Informatieveiligheid (CISO) wordt door de procesverantwoordelijken geïnformeerd over beveiligingsincidenten en legt deze vast ten behoeve van rapportages. Hieronder vallen o.a. inbreuken op en (ver)storingen in de informatietechnologie, datacommunicatie of andere infrastructurele voorzieningen die gevolgen kunnen hebben voor de continuïteit en integriteit van de bedrijfsprocessen evenals signaleringen dat het informatieveiligheidsbeleid niet wordt nageleefd. Afspraken (geïnitieerd door de coördinator informatiebeveiliging) worden gemaakt over:
• doel van de registratie;
• inhoud van de registratie;
• mate van detaillering;
• wijze van handelen;
• wijze van rapporteren.

Er wordt minimaal eenmaal per jaar gerapporteerd aan het MT door de coördinator Informatieveiligheid (CISO).

6.0 Verantwoordelijkheden afdeling overstijgende (informatie)systemen
Afdeling overstijgende (informatie)systemen binnen de gemeente Tholen worden onder de verantwoordelijkheid door ICTWBW gefaciliteerd en onderhouden. Deze systemen, die door meer dan één gemeentelijk organisatieonderdeel worden gebruikt, bevatten gegevens die door meerdere organisatieonderdelen worden vastgelegd. Voor ieder afdeling overstijgend (informatie)systeem heeft de directie het primaat dit te mandateren aan een organisatieonderdeel dat daarmee verantwoordelijk wordt voor de gehele gegevensverzameling of het (informatie)systeem.
De gemandateerd eigenaar van een afdeling overstijgend (informatie)systeem draagt er zorg voor dat bij het gebruik ervan de wettelijke eisen en de gemeentelijke voorschriften (het gemeentelijk informatieveiligheidsbeleid) worden nageleefd en dat de verantwoordelijkheden voor (informatie)beveiliging voor alle betrokken partijen duidelijk omschreven zijn.

De procesverantwoordelijke maakt schriftelijk afspraken met het gemeentelijke organisatieonderdeel of de externe organisatie dat van het afdeling overstijgend (informatie)systeem gebruik maakt (de gebruikende partij).

Minimaal worden in deze afspraken vastgelegd:
- Voorwaarden voor het toegestane gebruik van het afdeling overstijgend (informatie)systeem;
- De verantwoordelijkheden van de gebruikende partij voor de gegevens uit het afdeling overstijgend (informatie)systeem;
- Voorwaarden met betrekking tot de bescherming van het verwerken van persoonsgegevens;
- Voorwaarden die de gebruikende partij verplichten voorzieningen te treffen voor een passend niveau van informatiebeveiliging;
- Procedure(s) betreffende autorisatie van medewerkers;
- Procedure(s) betreffende toezicht op de naleving van de afspraken en oplossing van eventuele geschillen;
- Het recht op inzage in de resultaten van de externe audit bij de gebruikende partij waaruit blijkt in welke mate deze aan het gemeentelijk informatieveiligheidsbeleid voldoet.

7.0 Contracten met derden

7.1 Service level agreement (niveau van dienstverlening)
Bij structurele / langdurige ondersteuning (externe inhuur) en/of uitbesteding van beheer van (een deel van) de (informatie)systemen, netwerken, en/of werkstations of hosting van websites wordt tussen de gemeente / een afdeling en de externe partij een Service Level Agreement (SLA) afgesloten. Hierin staan afspraken over het niveau van informatiebeveiliging en een duidelijke definitie van de verantwoordelijkheden op het gebied van informatiebeveiliging. In het ondersteunings- of uitbestedingscontract wordt verwezen naar de SLA.

7.2 Inhuur derden

Bij incidentele inhuur, bijvoorbeeld in het geval van verstoringen en calamiteiten, werkt een externe onder verantwoordelijkheid van het verantwoordelijke afdelingshoofd. Deze manager dient te waarborgen dat activiteiten binnen het kader van het informatieveiligheidsbeleid worden uitgevoerd.

7.3 Toegang

Bij toegang van derden tot de gemeentelijke ICT voorzieningen gelden de onderstaande uitgangspunten:

- Informatiebeveiliging is aantoonbaar (op basis van een risicoafweging) meegewogen bij het besluit een externe partij wel of niet in te schakelen;
- 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;
- 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;
- Voorafgaand aan het afsluiten van een contract voor uitbesteding en externe inhuur is bepaald hoe geauthenticeerde en geautoriseerde toegang vastgesteld wordt;
- Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een bewerkersovereenkomst (conform WBP artikel 14) afgesloten;
- 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;
- Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits en penetratietests) en hoe het toezicht is geregeld;
- Over het naleven van de afspraken van de externe partij wordt jaarlijks gerapporteerd.

7.4 Grote projecten

Voor grote ICT-projecten gelden specifieke, op centraal niveau vastgestelde, richtlijnen, met name ten aanzien van Europese aanbesteding, screening van bedrijven en juridische aspecten.

Bijlage 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

IB Beleid 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 IB Beleid

Het IB Beleid behoort met geplande tussenpozen, of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.
1. Het IB Beleid wordt minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld. Zie ook 6.1.8.1.

Bijlage 6 Organisatie van de informatiebeveiliging
6.1 Interne organisatie

Doelstelling
Beheren van de informatiebeveiliging binnen de orgsnisatie.

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. 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. 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. 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. De algemene geheimhoudingsplicht voor ambtenaren is geregeld in de Ambtenarenwet art. 125a, lid 3. Daarnaast dienen personen die te maken hebben met Bijzondere Informatie [1] 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. Het lijnmanagement stelt vast in welke gevallen en door wie er contacten met autoriteiten (brandweer, toezichthouders, enz.) wordt onderhouden.

1) Bijzondere Informatie is informatie die vergelijkbaar met het VIR-BI geclassificeerd/gerubriceerd is.

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 IB Beleid

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

1. Het IB Beleid wordt minimaal één keer in de drie jaar geëvalueerd (door een onafhankelijke deskundige) en desgewenst bijgesteld. Zie ook 5.1.2.
2. 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. 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.

Bijlage 7 Beheer van bedrijfsmiddelen

7.1 Verantwoordelijkheid voor bedrijfsmiddelen

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

7.1.1 Inventarisatie van bedrijfsmiddelen

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

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

7.1.2 Eigendom van bedrijfsmiddelen

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

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

7.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen

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

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

2. 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.

Bijlage 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:
   a. uitvoering van het IB Beleid
   b. bescherming van bedrijfsmiddelen
   c. rapportage van beveiligingsincidenten
   d. expliciete vermelding van de verantwoordelijkheden voor het beveiligen van persoonsgegevens

2. 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. 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.

8.2 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. 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. 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 IB Beleid 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 IB Beleid en de beveiligingsprocedures van de organisatie, voor zover relevant voor hun functie.[2]
2. 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. Er is een disciplinair proces vastgelegd voor medewerkers die inbreuk maken op het IB Beleid (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.

2) Bewustwordingstrainingen zijn een van de meest effectiefste maatregelen om de menselijke fouten tegen te gaan.

3. Het lijnmanagement heeft een procedure vastgesteld voor verandering van functie binnen de organisatie, waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten en innemen van bedrijfsmiddelen die niet meer nodig zijn na het beëindigen van de oude functie.

8.3.2 Retournering van bedrijfsmiddelen

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

Bijlage 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. 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. 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. 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. 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. 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. 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. 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.

- Bij maatregelen is rekening gehouden met specifieke bedreigingen van aangrenzende panden of terreinen.

- 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.

- Beveiligde ruimten waarin zich bedrijfskritische apparatuur bevindt zijn voldoende beveiligd tegen wateroverlast.

- 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.

- 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.

- 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.

- 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.

- Beveiligde ruimten (zoals een serverruimte of kluis) waarin zich geen personen bevinden zijn afgesloten en worden regelmatig gecontroleerd.

- 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. 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. 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.[3]

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. [4]

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

9.2.5 Beveiliging van apparatuur buiten het terrein

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

3) Gemeenten die server virtualisatie toepassen dienen zelf de risicoafweging te maken of en hoe zij systemen willen scheiden.

4) 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/

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. 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. [5]
2. 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 [6] 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.

5) 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.

6) 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

Bijlage 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:
   a. het administreren van significante wijzigingen
   b. impactanalyse van mogelijke gevolgen van de wijzigingen
   c. goedkeuringsprocedure voor wijzigingen

2. 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. 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. 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. 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. 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.

- Er worden afspraken gemaakt over de inhoud van rapportages, zoals over het melden van incidenten en autorisatiebeheer.
- De in dienstverleningscontracten vastgelegde betrouwbaarheidseisen worden gemonitord. Dit kan bijvoorbeeld middels audits of rapportages en gebeurt minimaal eens per jaar (voor ieder systeem).
- 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. 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. 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. 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.[7]

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. Van acceptatietesten wordt een log bijgehouden.

2. Er zijn acceptatiecriteria vastgesteld voor het testen van de beveiliging. Dit betreft minimaal OWASP[8] 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. 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. 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.

4. 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'[9] is toegelaten, behoort de configuratie te bewerkstelligen dat de geautoriseerde 'mobile code' functioneert volgens een duidelijk vastgesteld IB Beleid, 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.

7) 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

8) Open Web Application Security Project (http://www.owasp.org)

9) 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.

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 fout-herstel 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.

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

3. 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. Er zijn procedures opgesteld en geïmplementeerd voor opslag van vertrouwelijke informatie voor verwijderbare media.

2. 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. 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 [10] 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. 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.

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. Het meenemen van Departementaal Vertrouwelijke [11] of vergelijkbaar geclassificeerde informatie, of hogere, buiten de gemeente vindt uitsluitend plaats indien dit voor de uitoefening van de functie noodzakelijk is.

10)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.

11)Hier wordt verwezen naar een rijks classificatie zodat dit aansluit bij andere baselines en beveiligingsvoorschriften.

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. Indien mogelijk wordt binnenkomende programmatuur (zowel op fysieke media als gedownload) gecontroleerd op ongeautoriseerde wijzigingen aan de hand van een door de leverancier via een gescheiden kanaal geleverde checksum of certificaat.

10.8.3 Fysieke media die worden getransporteerd

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

1. Om vertrouwelijke informatie te beschermen worden maatregelen genomen, zoals:
   a. versleuteling
   b. bescherming door fysieke maatregelen, zoals afgesloten containers
   c. gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen
   d. persoonlijke aflevering
   e. opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes

2. 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. 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. 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.

- 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:
   a. een tot een natuurlijk persoon herleidbare gebruikersnaam of ID
   b. de gebeurtenis (zie 10.10.2.1)
   c. waar mogelijk de identiteit van het werkstation of de locatie
   d. het object waarop de handeling werd uitgevoerd
   e. het resultaat van de handeling
   f. de datum en het tijdstip van de gebeurtenis

3. 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. Logberichten worden overzichtelijk samengevat. Daartoe zijn systemen die logberichten genereren bij voorkeur [12] aangesloten op een Security Information and Event Management systeem (SIEM [13]) 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:
   a. 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.
   b. gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases).
   c. handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels.
   d. 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).
   e. verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen).
   f. handelingen van gebruikers, zoals goede en foute inlogpogingen, systeemtoegang, gebruik van online transacties en toegang tot bestanden door systeembeheerders.

10.10.3 Bescherming van informatie in logbestanden

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

- Het (automatisch) overschrijven of verwijderen van logbestanden wordt gelogd in de nieuw aangelegde log.

- Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.

- Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.

- 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.

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

13 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.

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

Bijlage 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.

- Gebruikers worden vooraf geïdentificeerd en geautoriseerd. Van de registratie wordt een administratie bijgehouden.
- Authenticatiegegevens worden bijgehouden in één bronbestand zodat consistentie is gegarandeerd.
- 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:
   a. Wachtwoorden worden op een veilige manier uitgegeven (controle identiteit van de gebruiker).
   b. Tijdelijke wachtwoorden of wachtwoorden die standaard in software of hardware worden meegegeven worden bij eerste gebruik vervangen door een persoonlijk wachtwoord.
   c. Gebruikers bevestigen de ontvangst van een wachtwoord.
   d. Wachtwoorden zijn alleen bij de gebruiker bekend.
   e. Wachtwoorden bestaan uit minimaal 8 karakters, waarvan tenminste 1 hoofdletter, 1 cijfer en 1 vreemd teken.
   f. 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:
   a. Wachtwoorden worden niet opgeschreven.
   b. Gebruikers delen hun wachtwoord nooit met anderen.
   c. Wachtwoorden mogen niet opeenvolgend zijn.
   d. Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde.
   e. 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.

- De gebruiker vergrendelt de werkplek tijdens afwezigheid. Zie ook: 1.23.5.

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.

- 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).

- Bij afdrukken van gevoelige informatie wordt, wanneer mogelijk, gebruik gemaakt van de functie ‘beveiligd afdrukken’ (pincode verificatie).

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

- 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. 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. Werkstations worden zo ingericht dat routeren van verkeer tussen verschillende zones of netwerken niet mogelijk is.

2. 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. 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. 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 netwerkverbindinge n

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 netwerkrouting

Netwerken behoren te zijn voorzien van beheersmaatregelen voor netwerkrouting, om te bewerkstelligen dat computerverbindingen en informatiestromen niet in strijd zijn met het toegangsbeleid voor de 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. 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. 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. 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 [14], regelmatige wijziging, directe wijziging van initieel wachtwoord).

2. Wachtwoorden hebben een geldigheidsduur zoals beschreven bij 1.20.3. Daarbinnen dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd.

3. 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:
   a. voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geauthenticeerd;
   b. ter voorkoming van typefouten in het nieuw gekozen wachtwoord is er een bevestigingsprocedure.

14 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).

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

11.5.6 Beperking van verbindingstijd

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

1. 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.

- In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.
- Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten.
- Bij extern gebruik vanuit een onvertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.
- 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. 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 Mobiele (werkplek) devices

Doelstelling
Waarborgen van informatiebeveiliging bij het gebruik van mobiele (werkplek) devices en faciliteiten voor het werken buiten het vaste stadskantoor

11.7.1. Mobiele (werkplek) devices 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 mobiele (werkplek) devivces.

1. Het mobiele (werkplek) device 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 (werkplek) device (smarthone, tablet, laptop etc) 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. Er zijn, waar mogelijk, voorzieningen om de actualiteit van het besturingssysteem en anti-malware programmatuur op mobiele (werkplek) devices te garanderen.

3. Dit beleid wordt bij voorkeur ondersteund door oplossingen voor Mobile Device & Data Management.

4. Bij melding van verlies of diefstal wordt de communicatiemogelijkheid met de centrale applicaties afgesloten.

5. Beveiligingsmaatregelen hebben betrekking op zowel door de gemeente verstrekte middelen als privé-apparatuur ('bring your own device' (BYOD)). Op privé-apparatuur waarmee verbinding wordt gemaakt met het gemeentelijke netwerk is de gemeente bevoegd om beveiligingsinstellingen af te dwingen. Dit betreft onder meer: controle op wachtwoord, encryptie, aanwezigheid van malware, etc. Het gebruik van privé-apparatuur waarop beveiligingsinstellingen zijn verwijderd ('jail break', 'rooted device') is niet toegestaan.

6. Op verzoek van de gemeente dienen medewerkers de installatie van software om bovenstaande beleidsregel te handhaven toe te staan (denk bijvoorbeeld aan ‘mobile device management software’). De beveiligingsinstellingen, zoals bedoeld in bovenstaande regel, zijn uitsluitend bedoeld ter bescherming van gemeentelijke informatie en integriteit van het gemeentelijke netwerk.

7. In geval van dringende redenen kunnen noodmaatregelen worden getroffen, zoals selectief wissen van gemeentelijke gegevens op afstand.

11.7.2 Werken buiten het vaste stadskantoor

Er behoort beleid, operationele plannen en procedures voor het werken buiten het vaste stadskantoor te worden ontwikkeld en geïmplementeerd.

1. Er wordt een beleid met gedragsregels en een geschikte implementatie van de techniek opgesteld t.a.v. werken buiten het vaste stadskantoor.
2. Er wordt beleid vastgesteld met daarin de uitwerking welke systemen niet en welke systemen wel buiten het vaste stadskantoor mogen worden geraadpleegd.

Bijlage 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 [15]).
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 [16] 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.

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.

15)Voor voorbeelden van secure coding guidelines, zie http://www.cert.org/secure-coding/ of bijvoorbeeld ook OWASP

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

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 be hoort 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. 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. 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 [17] 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 [18] en voor applicaties ASL.

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.

17 Dit kan ook een interne leverancier zijn.

18 Information Technology Infrastructure Library, zie http://www.itil-officialsite.com

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. [19]
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).

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. 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.

19)Het gaat hier dan om informatie die zich daar voor leent. Encrypted informatie is niet zondermeer te scannen.

Bijlage 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. Er is een contactpersoon (Deelnemer Security Contact (DSC))[20] 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.

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

20 Lees ook als: Vertrouwde Contactpersoon Informatiebeveiliging (VCIB) of Algemeen Contactpersoon Informatiebeveiliging (ACIB) of CISO of gelijkwaardig

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.

Bijlage 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. Calamiteitenplannen worden gebruikt in de jaarlijkse bewustwording-, training- en testactiviteiten.

Bedrijfscontinuïteitsbeheer

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:
   a. identificatie van essentiële procedures voor bedrijfscontinuïteit
   b. wie mag het continuïteitsplan wanneer activeren
   c. wanneer wordt er gecontroleerd teruggaan naar de standaard situatie
   d. veilig te stellen informatie (aanvaardbaarheid van verlies van informatie)
   e. prioriteiten en volgorde van herstel en reconstructie
   f. documentatie van systemen en processen
   g. 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. 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.

Bijlage 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.

- 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. [21]

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 IB Beleid en -normen en technische naleving

Doelstelling
Bewerkstelligen dat systemen voldoen aan het IB Beleid en de beveiligingsnormen van de organisatie.

21 Zie artikel 12 WBP

15.2.1 Naleving van IB Beleid en -normen
Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van IB Beleid 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 IB Beleid. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door of vanwege de CISO dan wel door interne of externe auditteams.

2. 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 16 Beheersmaatregelen in PDC

In deze bijlage zijn de BIG-beheersmaatregelen opgenomen, waarvan de verantwoordelijkheid voor implementatie en borging door de aangesloten organisaties is overgedragen aan ICTWBW.

Nr	Doel	Beheersmaatregel
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
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
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
9.1.4	Berscherming 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.
9.1.5	Werken in beveiligde ruimten	Er behoren een fysieke bescherming en richtlijnen voor werken in beveiligde ruimten te worden ontworpen en toegepast
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.
9.2.2	Nutsvoorzieningen	Apparatuur behoort te worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen
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.
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.
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
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.
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
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 voo r uitbestede diensten.
10.7.4	Beveiliging van systeemdocumentatie	Systeemdocumentatie behoort te worden beschermd tegen onbevoegde toegang
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.

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
10.10.3	Bescherming van informatie in logbestanden	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.
10.10.4	Logbestanden van administrators en operators	Activiteiten van systeemadministrators en systeemoperators behoren in logbestanden te worden vastgelegd
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
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
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.
11.2.3	Beheer van gebruikerswachtwoorden	De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst
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.
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
11.4.5	Scheiding van netwerken	Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden
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
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.
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.
12.5.1	Procedures voor wijzigingsbeheer	De implementatie van wijzigingen behoort te worden beheerst door middel van formele procedures voor wijzigingsbeheer.
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
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
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.