Agendapunt 6 algemeen bestuur

Onderwerp : Informatiebeveiligingsbeleid

Datum : 26 januari 2018

Opsteller : Erwin van Leiden

Behandeling DSO : 8 februari 2018

Bijlage(n) : Informatie beveiligingsbeleid Syntrophos versie 2.1

Samenvatting :

Het dagelijks bestuur heeft kennisgenomen van het informatie beveiligingsbeleid(IBB) Syntrophos versie 2.1. en besloten deze voor te leggen aan het algemeen bestuur voor definitieve vaststelling.

Advies DSO: akkoord.

Besluit :

Akkoord te gaan met het informatie beveiligingsbeleid(IBB) Syntrophos versie 2.1.

Aldus besloten in de vergadering van het algemeen bestuur van 23 februari 2018.

De secretaris, De voorzitter,

M.C. Schadé D. van der Schaaf

2018

Informatiebeveiligingsbeleid Syntrophos

Organisatie: Syntrophos
Auteur: A. Snijders\ E. van Leiden
Datum: 30-1-2018
Versie: 2.1

Syntrophos
Shared Service Center

Configuratie historie

Versienummer	Datum	Aangebrachte wijzigingen	Auteur
0.1	20-06-2013	Eerste concept versie	Raymond v.d. Meijs
0.2	07-10-2013	Toevoeging classificatiemodel IBD	Raymond v.d. Meijs
0.3	04-11-2013	Afronding eerste definitieve versie	Raymond v.d. Meijs
1.0	24-01-2014	Splitsing Governance-/technische normen + aanvulling	Raymond v.d. Meijs
1.1	03-03-2014	Diverse toevoegingen n.a.v. opmerkingen DM's	Raymond v.d. Meijs
1.2	18-08-2014	Beperkte tekstuele aanpassingen	Raymond v.d. Meijs
2.0	11-05-2017	Herziening algemene gedeelte. Omzetting naar BIG normen	Ad Snijders
2.1	30-1-2018	Bespreekpunten normen verwerkt	Erwin van Leiden

Distributie

Versienummer	Datum	Naar contactgroep(en)
0.2	15-10-2013	Syntrophos staf-groep
0.3	08-11-2013	Syntrophos staf-groep, Demand Managers
1.0	24-01-2014	Syntrophos MT
1.1	03-03-2014	Demand Managers
2.0	16-08-2017	Syntrophos MT, tkn Staf groep
2.1	05-02-2018	Syntrophos MT, tkn Staf groep
2.1	08-02-2018	DSO, Ciso's

Inhoud

1 Inleiding

Sinds 1 maart 2013 is de gemeenschappelijke regeling Shared Service Center van toepassing. De nieuwe gevestigde organisatie genaamd Syntrophos geeft invulling aan deze regeling en bestaat uit ICT, GEO, Financiën en Advies diensten. Syntrophos heeft het volledige beheer van de informatievoorziening en de coördinatie van gegevensuitwisseling op zich genomen.
Het in beheer nemen van de informatievoorziening brengt belangrijke verantwoordelijkheden met zich mee; verantwoordelijkheden waarbij elke handeling een risico op de informatievoorziening met zich mee kan brengen. De veiligheid welke met technische middelen kan worden bereikt is begrensd en dient te worden ondersteund door passend beheer en procedures. In dit Informatiebeveiligingsbeleid (IBB) wordt op strategisch/tactisch niveau beschreven welke uitgangspunten gelden ten aanzien van de Informatiebeveiliging van Syntrophos. Dit document zal samen met de technische beveiligingsmaatregelen en de procedures een adequaat niveau van beveiliging voor de organisatie moeten opleveren waardoor de beschikbaarheid, de integriteit en de vertrouwelijkheid van de gegevens binnen de organisatie is gewaarborgd.

1.1 Aanleiding

De afhankelijkheid van informatiesystemen en archieven voor de uitvoering van de gemeentelijke taken is zeer groot. Een gemiddelde ambtenaar kan zijn werk niet uitvoeren als hij/zij niet over de juiste gegevens, informatie en systemen beschikt. Informatiebeveiliging wordt ook al lange tijd gezien als een ICT aangelegenheid. Hoewel technologie nieuwe beveiligingsrisico's heeft geïntroduceerd, blijkt bij beveiligingsincidenten dikwijls de mens de zwakste schakel. Zelfs de beste beveiligingstechniek kan niet voorkomen dat medewerkers wachtwoorden delen of gevoelige data kwijtraken. Binnen het vakgebied verschuift daarom de aandacht van de *techniek* van beveiliging naar de *organisatie* van beveiliging. In dit kader is informatiebeveiliging al lang niet meer een ICT aangelegenheid. De komende jaren zal Syntrophos in combinatie met haar klanten invulling geven aan het creëren, naleven en evalueren van het informatiebeveiligingsbeleid.

1.2 Wat is informatiebeveiliging?

Informatiebeveiliging heeft een directe relatie met de bedrijfsvoering van een organisatie en haar directe en indirecte werkomgeving. Het is een samenhangend geheel van maatregelen van procedurele, organisatorische, fysieke, technische, personele en juridische aard. Onder informatiebeveiliging wordt verstaan: het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te garanderen en te beschermen tegen interne en externe bedreigingen.

1.3 Doel van informatiebeveiliging

Informatiebeveiliging maakt het mogelijk dat de juiste informatie op het juiste moment voor de juiste personen beschikbaar is. Over het algemeen hanteert men de volgende definitie voor informatiebeveiliging: 'het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening te waarborgen'.

De term 'betrouwbaarheid' bestaat uit de drie kwaliteitsaspecten beschikbaarheid, vertrouwelijkheid en integriteit die als volgt worden gedefinieerd:

- Beschikbaarheid gaat over de mate waarin informatie op de juiste momenten beschikbaar is;
- Vertrouwelijkheid gaat over de mate waarin toegang tot informatie beperkt is tot diegenen die daartoe bevoegd zijn;
- Integriteit gaat over de mate waarin informatie correct geregistreerd en zonder fouten is.

1.4 Belang van informatiebeveiliging

Een betrouwbare informatievoorziening is van essentieel belang voor een kwalitatief hoogwaardige en efficiënte dienstverlening. Digitale dienstverlening is alleen mogelijk wanneer de basisgegevens op orde zijn en wanneer kan worden gerekend op de betrouwbaarheid van de informatievoorziening.
Burgers en bedrijven verwachten daarnaast dat er zorgvuldig wordt omgegaan met privacygevoelige informatie. De gemeente heeft op dit gebied een belangrijke wettelijke en maatschappelijke verantwoordelijkheid en hecht belang aan het beschermen van de privacy van haar klanten.

1.5 Scope

Informatiebeveiliging is een breed gebied en reikt normaliter verder dan alleen de geautomatiseerde informatiesystemen en ICT-infrastructuur. Gelet op het taakgebied van Syntrophos, de steeds snellere ontwikkelingen op automatiseringsgebied, het voldoen aan de Baseline Informatiebeveiliging Gemeenten (BIG), de WBP (tot mei 2018) en de AVG (vanaf mei 2018), is ervoor gekozen om dit beleidsdocument te baseren op de BIG normen.

Governancenormen worden separaat binnen de informatiebeveiligingsdocumentatie van de klanten van Syntrophos beschreven.

1.6 Het Informatiebeveiligingsproces

Het informatiebeveiligingsproces wordt doorgaans geborgd door het doorlopen van 3 beveiligingsniveaus, te weten het strategisch, tactisch en operationeel niveau.

Strategisch niveau

Dit betreft het Informatiebeveiligingsbeleid van Syntrophos. Op strategisch niveau worden de bedrijfsbelangen met de relevante uitgangspunten, zoals beschikbaarheid, integriteit en vertrouwelijkheid vastgesteld. Het beleid is bedoeld als richtinggevend document en gaat derhalve niet in op specifieke technische of organisatorische maatregelen. Het stuk is wel dusdanig opgezet zodat praktijksituaties eenvoudig opgezet en/of getoetst kunnen worden.

Tactisch niveau

Het tactisch niveau is gericht op het implementatietraject. De implementatie begint met het uitvoeren van een risico inventarisatie en evaluatie (RI&E) en/of GAP analyse. Hierbij worden de techniek, de regels én de procedures onderzocht, op basis van de BIG.

De RI&E/GAP geeft weer welke onderwerpen kritisch zijn en waar nog aanvullende maatregelen nodig zijn. De uitkomst van de analyse wordt vervolgens gebruikt als input voor het informatiebeveiligingsplan (IBP). Dit document kan gezien worden als een plan van aanpak voor de verdere implementatie.

Operationeel niveau

Op operationeel niveau wordt een complete set aan maatregelen (BIG normen) opgeleverd die gericht zijn op de specifieke eisen van een onderdeel. Zo een onderdeel kan een applicatie of server betreffen, maar kan ook gericht zijn op de ICT beheerprocessen.

1.7 Verantwoordelijkheid en bevoegdheid

De complete beheercyclus (zowel vaststelling als implementatie) van het informatiebeveiligingsproces valt onder de verantwoordelijkheid van het MT van Syntrophos. Onderdeel van het informatiebeveiligingsproces zijn beleidsvorming, implementatie, verantwoording, controle en bijstelling.

2 Uitgangspunten

2.1 Informatiebeveiligingsbeleid

De directie behoort het Informatiebeveiligingsbeleid (IBB) goed te keuren, uit te geven en kenbaar te maken aan alle medewerkers en alsmede hiernaar te handelen.

Het beleidsdocument heeft in principe een looptijd van drie jaar, maar moet in de jaarlijkse evaluatie meegenomen worden en zo nodig tussentijds worden geactualiseerd.

2.2 Informatiebeveiligingsplan

Op basis van het Informatiebeveiligingsbeleid (IBB) wordt door de directie een Informatiebeveiligingsplan (IBP) vastgesteld waarin wordt aangegeven op welke wijze het beleid uitgevoerd zal worden. De kernelementen in het Informatiebeveiligingsplan zijn:

- Een beschrijving van het huidige niveau van informatiebeveiliging en de mate waarin aan de beveiligingseisen en -prioriteiten (normen) uit het Informatiebeveiligingsbeleid wordt voldaan. Recente ontwikkelingen worden ook beschreven, zoals het in productie nemen van een nieuw informatiesysteem of technische infrastructuur die gevolgen kunnen hebben voor het beveiligingsniveau.

- Een planning van de nog te realiseren normen.

Het Informatiebeveiligingsplan kan maximaal dezelfde doorlooptijd hebben als het Informatiebeveiligingsbeleid maar is over het algemeen korter. Het plan wordt jaarlijks geëvalueerd en zo nodig tussentijds geactualiseerd.

2.3 Aanvullende maatregelen

- Als normenkader en uitgangspunt hanteert Syntrophos de Baseline Informatiebeveiliging voor Gemeenten (BIG) waarmee indirect aan de ISO 27001 en ISO 27002 wordt geconformeerd. De BIG is de algemeen aanvaarde basis voor informatiebeveiliging die door het College Standaardisatie en de Informatie Beveiligings Dienst (IBD) is vastgesteld als standaard voor de Nederlandse overheid. Hiermee wordt tevens de relatie gelegd met de op dit gebied relevante punten uit de WBP, respectievelijk AVG.

- Om het risico van onbedoelde wijzigingen of onbevoegde toegang tot productiesystemen en programmatuur en bedrijfsgegevens te beperken, moeten test- en productieomgeving gescheiden worden. De overgang van de test- naar de productieomgeving worden volgens een vastgestelde procedure uitgevoerd en zijn gedocumenteerd.

- Syntrophos ondersteunt een belangrijk onderdeel van het gemeentelijk proces, namelijk de technische informatievoorziening. Syntrophos is dan ook verantwoordelijk voor het beveiligen van de technische informatievoorziening en afkaderen van de rechten.

- Het toenemende gebruik van één grootschalige informatievoorziening voor meerdere gemeenten zal er toe leiden dat er steeds vaker, en op diverse manieren, informatie kan worden uitgewisseld. Dit kan kwetsbaarheden met zich mee brengen. Syntrophos maakt heldere afspraken met haar klanten over de beschikbaarheid, de integriteit en de vertrouwelijkheid van de technische informatievoorziening. Het is belangrijk dat Syntrophos de controle heeft over de betrouwbaarheid van de technische informatievoorziening.

- De betrouwbaarheid van overheidsinformatie moet worden gegarandeerd. Daarom zijn er een aantal wettelijke verplichtingen waar elke overheidinstantie aan moet voldoen. In wetten op dit gebied, zoals de Wet Bescherming Persoonsgegevens (WBP), de Structuur Uitvoering Werk en Inkomen (SUWI) en het DigiD beveiligingsassessment zijn beveiligingsverplichtingen opgenomen. De klanten van Syntrophos dienen individueel aan deze wettelijke verplichtingen te voldoen. Syntrophos kan hierin adviseren en ondersteunen.

  Nb: medio 2017/2018 worden de diverse audits/assessements vervangen door de ENSIA.

- Hoewel Syntrophos de technische voorziening beheert, is het bestuur van de deelnemende gemeenten aan de GR zelf verantwoordelijk indien in strijd met wet- en regelgeving wordt gehandeld.

- Syntrophos verwacht van haar klanten dat aansluiting wordt gezocht bij de Informatiebeveiligingsdienst (IBD). Deze landelijke dienst monitort de meest recente digitale bedreigingen en benaderd proactief overheidsinstanties welke met deze bedreigingen kunnen worden geconfronteerd. De IBD heeft nauwe relaties met het Nationaal Cyber Security Center (NCSC), hetgeen zich bezighoudt met informatiebeveiliging op nationaal niveau.

- Dit informatiebeveiligingsbeleid focust zich vooralsnog niet op het gebruik van smartphones en/of tablets. Hiervoor moeten nog concrete afspraken worden gemaakt tussen Syntrophos en haar klanten.

3 Organisatie van de informatiebeveiliging

3.1 Verantwoordelijken beveiligingsproces Syntrophos

Binnen Syntrophos zijn de volgende partijen bij het Informatiebeveiligingsproces betrokken:

Dagelijks bestuur

Het dagelijks bestuur van de Syntrophos draagt als eigenaar van de gemeentelijke informatiesystemen de verantwoordelijkheid voor een passend niveau van informatiebeveiliging. De informatie zelf blijft eigendom van de gemeenten. Het DB is verantwoordelijk voor een duidelijk te volgen Informatiebeveiligingsbeleid en stimuleert om treffende beveiligingsmaatregelen te nemen. Als eigenaar van gegevensinformatie en informatiesystemen heeft het DB haar verantwoordelijkheden (macht tot handelen) op het gebied van beveiliging gemandateerd aan het MT van Syntrophos.

MT

Het MT stelt het gewenste niveau van informatiebeveiliging vast voor Syntrophos. De beveiligingseisen worden per bedrijfsproces vastgesteld. De directeur geeft sturing aan het proces en is verantwoordelijk voor de juiste implementatie van de beveiliging in de bedrijfsprocessen en de in- en externe informatiesystemen.

Beveiligingsfunctionaris

De uitvoering van het informatiebeveiligingsproces is belegd binnen het team ICT. **De Adviseur Informatiebeveiliging is aangewezen als beveiligingsfunctionaris**, welke de verantwoordelijkheid draagt over het ontwikkelen van informatiebeveiligingsbeleid & -plan, de uitvoering van de risicoanalyse, de implementatie van het beveiligingsplan, het evalueren van de documentatie en de naleving van het beleid.
De eindverantwoordelijkheid ligt bij de Teamcoördinator ICT, respectievelijk bij het MT.

3.2 Strategisch niveau

Wie	Plan: Bepalen beveiligingsbeleid	Do: Opstellen beveiligingsbeleid	Check: Beveiligingsrisico's afgedekt?	Act: Evalueren beleid
DB	-	-	Controleert het informatieveiligheids-beleid en stelt deze vast.	-
MT	Vaststellen van de beveiligingseisen en de scope.	-	Controleert het voorgestelde beleid	-
Bev. Func.	Formuleren van beveiligingseisen, uitgangspunten en bepalen scope van het beleid.	Ontwikkelen van kaders en reglementen.	Adviseert over het voorgestelde beleid aan het MT	Ziet toe op naleving beleid. Geeft opdracht tot uitvoeren audits / risicoanalyse. Adviseert MT over eventuele aanpassingen van het beleid.

3.3 Tactisch niveau

Wie	Plan: Vastgesteld beveiligingsbeleid	Do: Opstellen beveiligingsplan	Check: Gekozen oplossing afdoende?	Act: Evalueren plannen
DB	-	-	Controleert de risicoanalyse en het informatiebeveiligings-plan en stelt deze vast.	-
MT	Wordt geïnformeerd over mogelijke beveiligings-risico's	-	Bepaalt welke maatregelen worden geïmplementeerd op operationeel niveau.	-
Bev. Func.	Zet de uitgangspunten uit het informatiebeveiligings-beleid af tegenover de resultaten uit de audits / risicoanalyse.	Stelt het IB-plan op bestaande uit maatregelen hoe te komen tot de uitgangspunten uit het informatie-beveiligingsbeleid.	Controleert of de voorgestelde maatregelen uit het plan de risico's uit de risicoanalyse voldoende afdekken en adviseert het MT.	-

3.4 Operationeel niveau

Wie	Plan: Vastgesteld beveiligingsplan	Do: Implementatie maatregelen	Check: Incident afhandeling	Act: Evalueren maatregelen
DB	-	-	Wordt geïnformeerd over de geïmplementeerde maatregelen.	-
MT	Bepaalt welke maatregelen worden geïmplementeerd op operationeel niveau	-	Neemt kennis van de geïmplementeerde maatregelen en de effectiviteit hiervan.	-
Bev. Func.			Controleert of de risico's zijn afgedekt door de maatregelen en tegemoet treden aan het vastgestelde beveiligingsbeleid. De beveiligingsfunctionaris rapporteert hierover aan MT en DB.	Bewaakt de resultaten van de geïmplementeerde maatregelen en onderneemt actie waar nodig.
TC ICT	Plant de maatregelen uit het beveiligingsplan in de tijd en koppelt hier investeringsbedragen aan.	Implementeert de door het MT geselecteerde maatregelen op operationeel niveau		

4 Begrippen

Audit trail
Vastlegging van de complete keten van opeenvolgende wijzigingen op een object in een bepaalde periode.

A&K analyse
Een analyse methode om de afhankelijkheden en kwetsbaarheden in kaart te brengen.

Basis beveiligingsniveau
Het geheel van maatregelen van beveiliging dat wordt bereikt door het implementeren en toepassen van de normen zoals geformuleerd in de Code voor Informatiebeveiliging, bedrijfscontinuïteitsbeheer en artikel 16 van de WBP en waaraan de NORA een nadere uitwerking geeft, onder meer door normen voor ICT-voorzieningen.

Bedrijfsmiddel
Elk middel waarin of waarmee bedrijfsgegevens kunnen worden opgeslagen en/of verwerkt en waarmee toegang tot gebouwen, ruimten en ICT-voorzieningen kan worden verkregen.

Beschikbaarheid
De waarborg dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen
(informatiesystemen).

Beveiliging
Het brede begrip van informatiebeveiliging, d.w.z. inclusief fysieke beveiliging, bedrijfscontinuïteitsbeheer, ofwel beschikbaarheid van bedrijfsprocessen en persoonlijke veiligheid en integriteit.

Beveiligingsincident
Het manifest worden van een beveiligingsrisico (dreiging,
oorzaak) als gevolg van een overtreding van beveiligingsregel, bijv. onbevoegde toegang tot ICTvoorzieningen.

Beveiligingsinstellingen
In ICT-voorzieningen kunnen in veel gevallen functionaliteiten die invloed hebben op beveiliging geactiveerd, gewijzigd of uitgeschakeld worden door het opgeven van parameterwaarden.

Clear Desk
Anders dan Clean Desk, waarbij het bureau helemaal leeg is,
betekent Clear Desk dat er geen vertrouwelijke informatie op het bureau ligt.

Controleerbaarheid
De mate waarin de werkelijkheid of representaties daarvan toetsbaar zijn, dat wil zeggen te vergelijken met andere ‘werkelijkheden of representaties daarvan’ zodat objectieve oordeelsvorming mogelijk wordt.

DSC
Deelnemer Security Contact, de contactpersoon binnen het incident management proces.

Elektronische handtekening
Een elektronische handtekening is een methode voor het bevestigen van de juistheid van digitale informatie door middel van technieken van de asymmetrische cryptografie.
De elektronische handtekening bestaat uit twee algoritmen: een om te bevestigen dat de informatie niet door derden veranderd is, de ander om de identiteit te bevestigen van degene die de informatie ‘ondertekent’. De technieken
worden toegepast met behulp van een PKI.

ENSIA
Eenduidige Normatiek Single Information Audit, is een systematiek om verschillende audits die nu apart plaatsvinden te gaan samenvoegen. Het is nog een project en op termijn moet hier verlaging van de auditlast en verantwoording van gemeenten uit voortkomen. Zie ook SiSa.

Filtering
Het gecontroleerd doorlaten van gegevens op het grensvlak tussen zones in een netwerk.

Firewall
Het geheel van software- en eventueel ook hardwarevoorzieningen dat voorkomt dat ongewenst verkeer van de ene netwerkzone terecht komt in de andere, teneinde de veiligheid in de laatstgenoemde te verhogen.

Hardening
Overbodige functies in besturingssystemen uitschakelen en/of van het systeem verwijderen en zodanige waarden toekennen aan beveiligingsinstellingen dat een maximale beveiliging ontstaat.

ICT-voorzieningen
Applicaties en technische infrastructuur, of wel het geheel van ICT-voorzieningen.

In control statement
Binnen de gebruikelijke Planning en Control cyclus moet door B&W een in control statement worden afgegeven over het BIG.
De in control statement moet inzicht geven aan welke BIG normen wordt voldaan en voor welke BIG normen een explain is gedefinieerd.

Informatiebeveiliging
Het proces van vaststellen van de vereiste betrouwbaarheid van informatieverwerking in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen,
onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.

Informatiesysteem
Een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.

Integrale beveiliging
Integrale beveiliging is de beveiliging van vastgestelde te beschermen belangen (TBB) door op basis van risicomanagement en een kosten/batenanalyse een samenhangend stelsel van beveiligingsmaatregelen te selecteren en te implementeren. Het besturingsmodel voor integrale beveiliging sluit aan bij de besturingsuitgangspunten binnen de gemeenten: het lijnmanagement is integraal verantwoordelijk en dus ook voor
de beveiliging van de TBB.

Integriteit
Het waarborgen van de juistheid en volledigheid en tijdigheid van informatie en de verwerking ervan. Als de tijdigheid van gegevens bepaald wordt door omstandigheden buiten het systeem, kan deze vanzelfsprekend niet als integriteitseis voor het systeem gesteld worden.

Logging
Vastlegging van systeemhandelingen.

Malware
Software met ongewenste functies, zoals virussen en trojans.

Mobile code
Code afkomstig van een ander systeem die lokaal uitgevoerd wordt, bijv. Javascript, Flash of Silverlight.

Onvertrouwd
Geen zekerheid over het beveiligingsniveau of zekerheid over het lager dan vereiste beveiligingsniveau.

Onweerlegbaarheid
Het niet kunnen ontkennen iets te hebben gedaan (bijvoorbeeld een bericht te hebben ontvangen dan wel te hebben verstuurd).

Patch
Klein onderdeel van software dat de leverancier van software uitgeeft om fouten in door hem vervaardigde software te repareren.

Query
Bevraging in een vraagtaal, die op basis van gebruikersvriendelijke en krachtige commando's selecties en berekeningen op bestanden kan uitvoeren, in eerste instantie
alleen voor raadpleegdoeleinden.

SiSa
Single information, single audit betekent eenmalige informatieverstrekking, eenmalige accountantscontrole. SiSa is de manier waarop medeoverheden (provincies, gemeenten en gemeenschappelijke regelingen) aan het Rijk ieder jaar verantwoorden of en hoe ze de specifieke uitkeringen hebben besteed. Zie ENSIA.

Technische infrastructuur
Het geheel van ICT-voorzieningen voor generiek gebruik, zoals servers, firewalls, netwerkapparatuur, besturingssystemen voor netwerken en servers, database management systemen en beheer- en beveiligingstools, inclusief bijbehorende systeembestanden.

Two-factor authenticatie
Two-factor authenticatie vereist het gebruik van twee van de drie volgende authenticatiemethoden:
• Iets dat de gebruiker weet (bijvoorbeeld password, PIN);
• Iets dat de gebruiker heeft (bijvoorbeeld toegangspas, sleutel); en
• Iets dat de gebruiker is (bijvoorbeeld biometrische eigenschap zoals een vingerafdruk).

Vertrouwd
In overeenstemming met een door een bevoegde autoriteit vastgesteld beveiligingsniveau. Bijvoorbeeld vertrouwde zones of vertrouwde netwerken zoals in 10.6.1.2 en 10.6.1.3.

Vertrouwelijkheid
Het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.

Vertrouwelijke informatie
Informatie die niet algemeen bekend mag worden (bron: van Dale).
In het kader van de BIG worden maatregelen beschreven die voldoen voor de behandeling van gerubriceerde informatie tot en met vertrouwelijke en ersoonsvertrouwelijke informatie, zoals bedoeld in artikel 16 van de Wbp

Verwijderbare media
Opslagmiddelen die los van apparatuur kunnen worden verwijderd en meegenomen. Zoals CD-ROM, USB stick, verwijderbare schijven, tapes of gedrukte media.

Zone
De logische verzameling van ICT-voorzieningen met hetzelfde beveiligingsniveau, die via beveiligde koppelvlakken gegevens kunnen uitwisselen

5 Beveiligingsbeleid

5.1 Informatiebeveiligingsbeleid

Doelstelling

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

5.1.1 Beleidsdocumenten voor informatiebeveiliging

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

5.1.1.1 Er is een beleid voor informatiebeveiliging door het Dagelijks bestuur vastgesteld, gepubliceerd en beoordeeld op basis van inzicht in risico's, kritische bedrijfsprocessen en toewijzing van verantwoordelijkheden en prioriteiten.

5.1.2 Beoordeling van het informatiebeveiligingsbeleid

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

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

6 Organisatie van de informatiebeveiliging

6.1 Interne organisatie

Doelstelling

Beheren van de informatiebeveiliging binnen de organisatie.

6.1.1 Betrokkenheid van Dagelijks bestuurbij 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.

6.1.1.1 Het Dagelijks bestuur 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.

6.1.2.1 De rollen van de beveiligingsfunctionaris (Syntrophos: Adviseur Informatiebeveiliging) en het lijnmanagement zijn beschreven.
a. De beveiligingsfunctionaris rapporteert rechtstreeks aan het MT van Syntrophos.
b. De beveiligingsfunctionaris bevordert en adviseert gevraagd en ongevraagd over de beveiliging van Syntrophos, verzorgt rapportages over de status, controleert of m.b.t. de beveiliging van Syntropohos de maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de informatiebeveiliging van Syntrophos.

6.1.3 Verantwoordelijkheden

Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd.

6.1.3.1 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.

6.1.4.1 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.

6.1.5.1 De algemene geheimhoudingsplicht voor ambtenaren is geregeld in de Ambtenarenwet art. 125a, lid 3.
Daarnaast dienen personen die te maken hebben met Bijzondere Informatie (dit is informatie die vergelijkbaar met het VIR-BI geclassificeerd/gerubriceerd is) 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.

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

6.1.7 Contact met speciale belangengroepen

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

6.1.7.1 Informatiebeveiligingsspecifieke informatie van relevante expertisegroepen, leveranciers van hardware, software en diensten wordt gebruikt om de informatiebeveiliging te verbeteren.

6.1.7.2 De Beveiligingsfunctionaris onderhoudt contact met de Informatiebeveiligingsdienst voor gemeenten (IBD).

6.1.8 Beoordeling van het informatiebeveiligingsbeleid

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

6.1.8.1 Het informatiebeveiligingsbeleid wordt minimaal één keer in de drie jaar geëvalueerd (door een onafhankelijke deskundige) en desgewenst bijgesteld. Zie ook 5.1.2. Dit wordt in samenspraak met de gemeenten uitgevoerd.

6.1.8.2 Periodieke beveiligingsaudits worden uitgevoerd in opdracht van het lijnmanagement.

6.1.8.3 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.

6.2.1.1 Informatiebeveiliging is aantoonbaar (op basis van een risicoafweging) meegewogen bij het besluit een externe partij wel of niet in te schakelen.

6.2.1.2 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.

6.2.1.3 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.

6.2.1.4 Voorafgaand aan het afsluiten van een contract voor uitbesteding en externe inhuur is bepaald hoe geauthenticeerde en geautoriseerde toegang vastgesteld wordt.

6.2.1.5 Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een bewerkersovereenkomst (conform Wbp artikel 14) afgesloten.

6.2.1.6 Er is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd (zie ook 6.2.3.3).
Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits en penetratietests) en hoe het toezicht is geregeld.

6.2.1.7 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.

6.2.2.1 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.

~~Let op! Hier onder genoemde normen zijn van toepassing voor nieuwe door Syntrophos opgestelde contracten. Voor bestaande contracten blijft dit verantwoordelijkheid van de gemeenten.~~

6.2.3.1 De maatregelen behorend bij 6.2.1 zijn voorafgaand aan het afsluiten van het contract gedefinieerd en geïmplementeerd.

6.2.3.2 Uitbesteding (ontwikkelen en aanpassen) van software is geregeld volgens formele contracten waarin o.a. intellectueel eigendom, kwaliteitsaspecten, beveiligingsaspecten, aansprakelijkheid, escrow en reviews geregeld worden.

6.2.3.3 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.

6.2.3.4 In contracten met externe partijen is vastgelegd hoe wordt omgegaan met geheimhouding en de geheimhoudingsverklaring.

6.2.3.5 Er is een plan voor beëindiging van de ingehuurde diensten waarin aandacht wordt besteed aan beschikbaarheid, vertrouwelijkheid en integriteit.

6.2.3.6 In contracten met externe partijen is vastgelegd hoe escalaties en aansprakelijkheid geregeld zijn.

6.2.3.7 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.

6.2.3.8 De producten, diensten en daarbij geldende randvoorwaarden, rapporten en registraties die door een derde partij worden geleverd, worden beoordeeld op het nakomen van de afspraken in de overeenkomst. Verbeteracties worden geïnitieerd wanneer onder het afgesproken niveau wordt gepresteerd.

7 Beheer van bedrijfsmiddelen

7.1 Verantwoordelijkheid voor bedrijfsmiddelen

Doelstelling

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

7.1.1 Inventarisatie van bedrijfsmiddelen

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

7.1.1.1 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.

7.1.2.1 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 ICTvoorzieningen.

7.1.3.1 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.

7.1.3.2 Gebruikers hebben kennis van de regels.

7.1.3.3 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.

7.1.3.4 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.
Dit betreft zowel bedrijfsinformatie van Syntrophos als informatie van de door Syntrophos ondersteunde gemeenten. De bescherming van informatie wordt op basis van de door de gemeente aangegeven en overeengekomen classificatie voor beschikbaarheid geleverd.

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.

7.2.1.1 De organisatie heeft rubriceringrichtlijnen opgesteld.

7.2.1.2 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.

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

7.2.2.2 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.

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.

8.1.1.1 De taken en verantwoordelijkheden van een medewerker zijn opgenomen in de functiebeschrijving en worden onderhouden. In de functiebeschrijving wordt minimaal aandacht besteed aan:
- uitvoering van het informatiebeveiligingsbeleid
- bescherming van bedrijfsmiddelen
- rapportage van beveiligingsincidenten
- expliciete vermelding van de verantwoordelijkheden voor het beveiligen van persoonsgegevens

8.1.1.2 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.

8.1.1.3 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.

8.1.1.4 De algemene voorwaarden van het arbeidscontract van medewerkers bevatten de wederzijdse verantwoordelijkheden ten aanzien van informatiebeveiliging. Het is aantoonbaar dat medewerkers bekend zijn met hun verantwoordelijkheden op het gebied van informatiebeveiliging.

8.1.2 Screening

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

8.1.2.1 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.

8.1.2.2 Bij de aanstelling worden de gegevens die de medewerker heeft verstrekt over zijn arbeidsverleden en scholing geverifieerd.

8.1.2.3 Het is noodzakelijk om de VOG of screening periodiek te herhalen volgens de voorschriften.

8.1.3 Arbeidsvoorwaarden

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

8.2 Tijdens het dienstverband

Doelstelling

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

8.2.1 Directieverantwoordelijkheid

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

8.2.1.1 Het lijnmanagement heeft een strategie ontwikkeld en geïmplementeerd om blijvend over specialistische kennis en vaardigheden van medewerkers en ingehuurd personeel (onder andere die kritische bedrijfsactiviteiten op het gebied van IB uitoefenen) te kunnen beschikken.

8.2.1.2 Het lijnmanagement bevordert dat medewerkers, 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.

8.2.2.1 Alle medewerkers van de organisatie worden regelmatig attent gemaakt op het beveiligingsbeleid en de beveiligingsprocedures van de organisatie, voor zover relevant voor hun functie (Bewustwordingstrainingen zijn een van de meest effectieve maatregelen om de menselijke fouten tegen te gaan).

8.2.2.2 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.

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

8.3 Beëindiging of wijziging van het dienstverband

Doelstelling

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

8.3.1 Beëindiging van verantwoordelijkheden

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

8.3.1.1 Voor medewerkers 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.

8.3.1.2 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.

8.3.1.3 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.

8.3.2.1 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.

8.3.3.1 Zie 8.3.1.3

9 Fysieke beveiliging en beveiliging van de omgeving

9.1 Beveiligde ruimten

Doelstelling

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

9.1.1 Fysieke beveiliging van de omgeving

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

9.1.1.1 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.

9.1.1.2 Voor voorzieningen (binnen of buiten het gebouw) zijn duidelijke beveiligingsgrenzen bepaald.

9.1.1.3 Gebouwen bieden voldoende weerstand (bepaald op basis van een risicoafweging)
bij gewelddadige aanvallen zoals inbraak en ICT-gericht vandalisme.

9.1.1.4 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.

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

9.1.1.6 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.

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

9.1.1.8 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.

9.1.2.1 Toegang tot gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.

9.1.2.2 De beveiligingszones en toegangsbeveiliging daarvan zijn ingericht conform het gemeentelijk toegangsbeleid.

9.1.2.3 In gebouwen met beveiligde zones houdt beveiligingspersoneel toezicht op de toegang. Hiervan wordt een registratie bijhouden.

9.1.2.4 De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afgestemd op de zonering.

9.1.2.5 De uitgifte van toegangsmiddelen wordt geregistreerd.

9.1.2.6 Niet uitgegeven toegangsmiddelen worden opgeborgen in een beveiligd opbergmiddel.

9.1.2.7 Apparatuur en bekabeling in kabelverdeelruimtes en patchruimtes voldoen aan dezelfde eisen t.a.v. toegangsbeveiliging zoals die worden gesteld aan computerruimtes.

9.1.2.8 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.

9.1.3.1 Papieren documenten en mobiele gegevensdragers die vertrouwelijke informatie bevatten worden beveiligd opgeslagen, tenzij de vertrouwelijke informatie op de mobiele gegevensdrager voldoende versleuteld is.

9.1.3.2 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.

9.1.3.3 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.

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

9.1.4.2 Reserve apparatuur en back-ups zijn op een zodanige afstand ondergebracht dat één en dezelfde calamiteit er niet voor kan zorgen dat zowel de hoofdlocatie als de back-up/reserve locatie niet meer toegankelijk zijn.

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

9.1.4.4 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.

9.1.4.5 Gevaarlijke of brandbare materialen zijn op een zodanige afstand van een beveiligde ruimte opgeslagen dat een calamiteit met deze materialen geen invloed heeft op de beveiligde ruimte.

9.1.4.6 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.

9.1.5.1 Medewerkers die zelf niet geautoriseerd zijn mogen alleen onder begeleiding van bevoegd personeel en als er een duidelijke noodzaak voor is toegang krijgen tot fysiek beveiligde ruimten waarin ICT-voorzieningen zijn geplaatst of waarin met vertrouwelijke informatie wordt gewerkt.

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

9.1.5.3 Zonder expliciete toestemming mogen binnen beveiligde ruimten geen opnames (foto, video of geluid) worden gemaakt.

9.1.6 Openbare toegang en gebieden voor laden en lossen

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

9.1.6.1 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.

9.2.1.1 Apparatuur wordt opgesteld en aangesloten conform de voorschriften van de leverancier. Dit geldt minimaal voor temperatuur en luchtvochtigheid, aarding, spanningsstabiliteit en overspanningsbeveiliging.

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

9.2.1.3 Gebouwen zijn beveiligd tegen blikseminslag.

9.2.1.4 Eten en drinken zijn verboden in computerruimtes.

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

9.2.2 Nutsvoorzieningen

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

9.2.3 Beveiliging van kabels

9.2.3.1 Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, behoren tegen interceptie of beschadiging te worden beschermd conform de norm NEN 1010 (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/)

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.

9.2.4.1 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.

9.2.5.1 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.

9.2.6.1 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.(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.)

9.2.6.2 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 voor apparaten die dit ondersteunen (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). 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

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

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.

10.1.1.1 Bedieningsprocedures bevatten informatie over opstarten, afsluiten, back-up- en herstelacties, afhandelen van fouten, beheer van logs, contactpersonen, noodprocedures en speciale maatregelen voor beveiliging.

10.1.1.2 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.

10.1.2.1 In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan:
- het administreren van significante wijzigingen
- impactanalyse van mogelijke gevolgen van de wijzigingen
- goedkeuringsprocedure voor wijzigingen

10.1.2.2 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.

10.1.3.1 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.

10.1.3.2 Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerwerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.

10.1.3.3 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.

10.1.3.4 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.

10.1.4.1 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.

10.1.4.2 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.

10.1.4.3 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.

10.2.1.1 De uitbestedende partij blijft verantwoordelijk voor de betrouwbaarheid van uitbestede diensten.

10.2.1.2 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.

10.2.2.1 Er worden afspraken gemaakt over de inhoud van rapportages, zoals over het melden van incidenten en autorisatiebeheer.

10.2.2.2 De in dienstverleningscontracten vastgelegde betrouwbaarheidseisen worden gemonitord. Dit kan bijvoorbeeld middels audits of rapportages en gebeurt minimaal eens per jaar (voor ieder systeem).

10.2.2.3 Er zijn voor beide partijen eenduidige aanspreekpunten.

10.2.3 Beheer van wijzigingen in dienstverlening door een derde partij

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

10.2.3.1 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.

10.3.1.1 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.

10.3.1.2 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.

10.3.1.3 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. E.e.a. conform richtlijnen opgenomen in de NCSC aanbevelingen.

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.

10.3.2.1 Van acceptatietesten wordt een log bijgehouden.

10.3.2.2 Er zijn acceptatiecriteria vastgesteld voor het testen van de beveiliging. Dit betreft minimaal OWASP (Open Web Application Security Project) 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.

10.4.1.1 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.

10.4.1.2 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.

10.4.1.3 In verschillende schakels van een keten binnen de infrastructuur van een organisatie wordt bij voorkeur antivirusprogrammatuur van verschillende leveranciers toegepast.

10.4.1.4 Er zijn maatregelen om verspreiding van virussen tegen te gaan en daarmee schade te beperken (bijv. quarantaine en compartimentering).

10.4.1.5 Er zijn continuïteitsplannen voor herstel na aanvallen met virussen waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven.

10.4.1.6 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' is toegelaten, behoort de configuratie te bewerkstelligen dat de geautoriseerde 'mobile code' functioneert volgens een duidelijk vastgesteld beveiligingsbeleid, en behoort te worden voorkomen dat onbevoegde 'mobile code' wordt uitgevoerd 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.

10.4.2.1 '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.

10.4.2.2 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.

10.5.1.1 Er zijn (geteste) procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen.

10.5.1.2 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.

10.5.1.3 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.

10.5.1.4 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.

10.5.1.5 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.

10.6.1.1 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.

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

10.6.1.3 Bij transport van vertrouwelijke informatie over onvertrouwde netwerken, zoals het internet, dient altijd geschikte encryptie te worden toegepast. Zie hiertoe 12.3.1.3.

10.6.1.4 Er zijn procedures voor beheer van apparatuur op afstand.

10.6.2 Beveiliging van netwerkdiensten

10.6.2.1 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.

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

10.7.1.2 Verwijderbare media met vertrouwelijke informatie mogen niet onbeheerd worden achtergelaten op plaatsen die toegankelijk zijn zonder toegangscontrole.

10.7.1.3 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.

10.7.1.4 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.

10.7.2.1 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 (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.) 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

10.7.3.1 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.

10.7.4.1 Systeemdocumentatie die vertrouwelijke informatie bevat is niet vrij toegankelijk.

10.7.4.2 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.

10.8.1.1 Het meenemen van Departementaal Vertrouwelijke (Hier wordt verwezen naar een rijks classificatie zodat dit aansluit bij andere baselines en beveiligingsvoorschriften) of vergelijkbaar geclassificeerde informatie, of hogere, buiten de gemeente vindt uitsluitend plaats indien dit voor de uitoefening van de functie noodzakelijk is.

10.8.1.2 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.

10.8.1.3 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.

10.8.1.4 Medewerkers zijn geïnstrueerd om geen vertrouwelijke documenten bij de printer te laten liggen.

10.8.1.5 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.

10.8.2.1 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.

10.8.2.2 Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, alsmede procedures over melding van incidenten.

10.8.2.3 Het eigenaarschap van gegevens en programmatuur en de verantwoordelijkheid voor de gegevensbescherming, auteursrechten, licenties van programmatuur zijn vastgelegd. Nb: Gemeente verantwoordelijk voor de gegevens en de gegevensbescherming. Syntrophos voor de licenties.

10.8.2.4 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.

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

10.8.3.2 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.

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

10.8.4.2 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.

10.8.5.1 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. Nb: Aktie voor gemeenten. Syntrophos is deels adviserend, maar voornamelijk uitvoerend.

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.

10.9.1.1 Conform verplichting worden authentieke basisregistraties van de overheid gebruikt (bijvoorbeeld. GBA) (eenmalige vastlegging, meervoudig gebruik).
Nb: zowel gemeenten als Syntrophos. Syntrophos heeft daarnaast rol in bewaken ervan.

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.

10.9.2.1 Een transactie wordt bevestigd (geautoriseerd) door een (gekwalificeerde) elektronische handtekening of een andere wilsuiting (bijv. een TAN code) van de gebruiker.

10.9.2.2 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.

10.9.3.1 Er zijn procedures die waarborgen dat gepubliceerde informatie is aangeleverd door daartoe geautoriseerde medewerkers. Deze procedures worden door de gemeenten opgesteld en getoetst

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.

10.10.1.1 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 kanbijvoorbeeld per maand of kwartaal. De gemeenten stellen loginbeleid vast en voert controles uit.

10.10.1.2 Een log-regel bevat minimaal:
- een tot een natuurlijk persoon herleidbare gebruikersnaam of ID
- de gebeurtenis (zie 10.10.2.1)
- waar mogelijk de identiteit van het werkstation of de locatie
- het object waarop de handeling werd uitgevoerd
- het resultaat van de handeling
- de datum en het tijdstip van de gebeurtenis

10.10.1.3 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.).

10.10.1.4 Logberichten worden overzichtelijk samengevat. Daartoe zijn systemen die logberichten genereren bij voorkeur aangesloten op een Security Information and Event Management systeem (SIEM) waarmee meldingen en alarmoproepen aan de beheerorganisatie gegeven worden. Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen gegenereerd worden.
Nb: Voor kleinere gemeenten zal dit bijna ondoenlijk zijn, echter het is aan te bevelen om gebruik te maken van SIEM.
(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)

10.10.1.5 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.

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

10.10.3 Bescherming van informatie in logbestanden

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

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

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

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

10.10.3.4 De instellingen van logmechanismen worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingenaangepast

moeten worden zal daarbij altijd het vier ogen principe toegepast worden.

10.10.3.5 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.

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

10.10.4 Logbestanden van administrators en operators

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

10.10.4.1 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.

10.10.5.1 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.

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

11 Toegangsbeveiliging

11.1 Toegangsbeleid
Doelstelling
Beheersen van de toegang tot informatie.

11.1.1 Toegangsbeleid

11.1.1.1 *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.

11.2.1.1 Gebruikers worden vooraf geïdentificeerd en geautoriseerd. Van de registratie wordt een administratie bijgehouden.

11.2.1.2 Authenticatiegegevens worden bijgehouden in één bronbestand zodat consistentie is gegarandeerd.

11.2.1.3 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.

11.2.2.1 Gebruikers hebben toegang tot speciale bevoegdheden voor zover dat voor de uitoefening van hun taak noodzakelijk is (need-to-know, need-to-use).

11.2.2.2 Systeemprocessen draaien onder een eigen gebruikersnaam (een functioneel account), voor zover deze processen handelingen verrichten voor andere systemen of gebruikers.

11.2.2.3 Gebruikers krijgen slechts toegang tot een noodzakelijk geachte set van applicaties en commando’s.

11.2.2.4 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.

11.2.3.1 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.

11.2.3.2 Ten aanzien van wachtwoorden geldt:
• Wachtwoorden worden op een veilige manier uitgegeven (controle identiteit van de gebruiker).
• Tijdelijke wachtwoorden of wachtwoorden die standaard in software of hardware worden meegegeven worden bij eerste gebruik vervangen door een persoonlijk wachtwoord.
• Gebruikers bevestigen de ontvangst van een wachtwoord.
• Wachtwoorden zijn alleen bij de gebruiker bekend.
• Wachtwoorden bestaan uit minimaal 8 karakters, waarvan tenminste 1 hoofdletter, 1 cijfer en 1 vreemd teken.
• Wachtwoorden zijn maximaal 60 dagen geldig en mogen niet binnen 6 keer herhaald worden.

11.2.4 Beoordeling van toegangsrechten van gebruikers

Het management behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces.

11.2.4.1 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.

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

11.3.2 Onbeheerde gebruikersapparatuur

Gebruikers behoren te bewerkstelligen dat onbeheerde apparatuur passend is beschermd.

11.3.2.1 De gebruiker vergrendelt de werkplek tijdens afwezigheid. Zie ook: 11.5.5.

11.3.3 Clear desk en clear screen

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

11.3.3.1 In het clear desk-beleid staat minimaal dat de gebruiker geen vertrouwelijke informatie op het bureau mag laten liggen. Deze informatie moet altijd worden opgeborgen in een afsluitbare opbergmogelijkheid (kast, locker, bureau of kamer).

11.3.3.2 Bij afdrukken van gevoelige informatie wordt, wanneer mogelijk, gebruik gemaakt van de functie 'beveiligd afdrukken' (pincode verificatie).

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

11.3.3.4 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.

11.4.1.1 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.

11.4.2.1 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.

11.4.3.1 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.

11.4.4.1 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.

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

11.4.5.2 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.

11.4.5.3 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.

11.4.5.4 Beheer en audit van zones vindt plaats vanuit een minimaal logisch gescheiden, separate zone.

11.4.5.5 Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).

11.4.6 Beheersmaatregelen voor netwerkverbindingen

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

11.4.7 Beheersmaatregelen voor netwerkroutering

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

11.4.7.1 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.

11.5.1.1 Toegang tot kritische toepassingen of toepassingen met een hoog belang wordt verleend op basis van twee-factor authenticatie.

11.5.1.2 Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.

11.5.1.3 Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.

11.5.1.4 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.

11.5.1.5 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. Nb: is nu 5x

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.

11.5.2.1 Bij uitgifte van authenticatiemiddelen wordt minimaal de identiteit vastgesteld evenals het feit dat de gebruiker recht heeft op het authenticatiemiddel.

11.5.2.2 Bij het intern gebruik van ICT-voorzieningen worden gebruikers minimaal geauthenticeerd op basis van wachtwoorden.

11.5.2.3 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). Syntrophos is contractpartij en zal bij leveranciers deze normen moeten afdwingen. De actie die eruit volgt (update of andere leverancier) is een gezamenlijke met de gemeenten.

11.5.3 Systemen voor wachtwoordenbeheer

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

11.5.3.1 Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (o.a. voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord). (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).

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

11.5.3.3 Wachtwoorden die gereset zijn en initiële wachtwoorden hebben een zeer beperkte geldigheidsduur en moeten bij het eerste gebruik worden gewijzigd.

11.5.3.4 De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Hierbij geldt het volgende:
• voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geauthenticeerd;
• ter voorkoming van typefouten in het nieuw gekozen wachtwoord is er een bevestigingsprocedure.

11.5.4 Gebruik van systeemhulpmiddelen

11.5.4.1 *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.

11.5.5.1 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.
Nb: Vraagt afstemming met klant. RDS sessie is nu ingesteld op een langere tijd (2 uur). Voorstel tijdsduur naar 1 uur te zetten.

11.5.6 Beperking van verbindingstijd

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

11.5.6.1 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.

11.6.1.1 In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.

11.6.1.2 Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten.

11.6.1.3 Bij extern gebruik vanuit een onvertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.

11.6.1.4 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.

11.6.2.1 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.
Nb: invulling alleen logisch niveau. Fysiek is het op de 2 datacenter voor de server omgeving beveiligd. ~~Gemeenten dienen eventuele zwaarwegende argumenten om het daadwerkelijk fysiek gescheiden te moeten isoleren, aan te leveren.~~

11.7 Draagbare computers en telewerken

Doelstelling

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

11.7.1 Draagbare computers en communicatievoorzieningen

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

11.7.1.1 Het mobiele apparaat is waar mogelijk zo ingericht dat geen bedrijfsinformatie wordt opgeslagen (‘zero footprint’). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, geldt:
een mobiel apparaat (zoals een handheld computer, tablet, smartphone, PDA) biedt de mogelijkheid om de toegang te beschermen d.m.v. een wachtwoord en versleuteling van die gegevens. Voor printen in onvertrouwde omgevingen vindt een risicoafweging plaats.

11.7.1.2 Er zijn, waar mogelijk, voorzieningen om de actualiteit van anti-malware programmatuur op mobiele apparaten te garanderen.

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

11.7.2 Telewerken

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

11.7.2.1 Er wordt een beleid met gedragsregels en een geschikte implementatie van de techniek opgesteld t.a.v. telewerken.

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

11.7.2.3 De telewerkvoorzieningen zijn waar mogelijk zo ingericht dat op de werkplek (thuis of op een andere locatie) geen bedrijfsinformatie wordt opgeslagen (‘zero footprint’) en mogelijke malware vanaf de werkplek niet in het vertrouwde deel terecht kan komen.
Voor printen in onvertrouwde omgevingen vindt vooraf een risicoafweging plaats door de verantwoordelijk manager.

12 Verwerving, ontwikkeling en onderhoud van Informatiesystemen

12.1 Beveiligingseisen voor informatiesystemen

Doelstelling

Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.

12.1.1 Analyse en specificatie van beveiligingseisen

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

12.1.1.1 In projecten worden een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen.

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

12.1.1.3 Bij aanschaf van producten wordt een proces gevolgd waarbij beveiliging een onderdeel is van de specificatie.

12.1.1.4 Waar het gaat om beveiligingsrelevante producten wordt de keuze voor een bepaald product verantwoord onderbouwd.

12.1.1.5 Voor beveiliging worden componenten gebruikt die aantoonbaar voldoen aan geaccepteerde beveiligingscriteria zoals NBV (NBV: Nationaal Bureau voor Verbindingsbeveiliging, onderdeel van het ministerie van BZK.) goedkeuring of certificering volgens ISO/IEC 15408 (common criteria).

12.1.1.6 Er is expliciet aandacht voor leveranciers accounts, hardcoded wachtwoorden en mogelijke 'achterdeurtjes'. Syntrophos zal deze norm handhaven bij de leveranciers. Eventuele conseqenties als gevolg van het door de leverancier niet kunnen voldoen aan deze normen zullen worden voorgelegd aan het bestuur.

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. Syntrophos zal deze norm handhaven bij de leveranciers. Eventuele conseqenties als gevolg van het door de leverancier niet kunnen voldoen aan deze normen zullen worden voorgelegd aan het bestuur.

12.2.1.1 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. Syntrophos zal deze norm handhaven bij de leveranciers. Eventuele conseqenties als gevolg van het door de leverancier niet kunnen voldoen aan deze normen zullen worden voorgelegd aan het bestuur.

12.2.2.1 Er bestaan voldoende mogelijkheden om reeds ingevoerde gegevens te kunnen corrigeren door er gegevens aan te kunnen toevoegen.

12.2.2.2 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.

12.2.2.3 Stapelen van fouten wordt voorkomen door toepassing van 'noodstop' mechanismen.

12.2.2.4 Verwerkingen zijn bij voorkeur herstelbaar zodat bij het optreden van fouten en/of wegraken van informatie dit hersteld kan worden door het opnieuw verwerken van de informatie.

12.2.3 Integriteit van berichten

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

12.2.4 Validatie van uitvoergegevens

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

12.2.4.1 De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijv. door checksums).

12.2.4.2 Bij uitvoer van gegevens wordt gegarandeerd dat deze met het juiste niveau van vertrouwelijkheid beschikbaar gesteld worden (bijv. beveiligd printen).

12.2.4.3 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.

12.3.1.1 De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst.

12.3.1.2 Bij de inzet van cryptografische producten volgt een afweging van de risico's aangaande locaties, processen en behandelende partijen.

12.3.1.3 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.

12.3.2.1 In het sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden.

12.3.2.2 De geldigheidsduur van cryptografische sleutels wordt bepaald aan de hand van de beoogde toepassing en is vastgelegd in het cryptografisch beleid.

12.3.2.3 De vertrouwelijkheid van cryptografische sleutels dient te zijn gewaarborgd tijdens generatie, gebruik, transport en opslag van de sleutels.

12.3.2.4 Er is een procedure vastgesteld waarin is bepaald hoe wordt omgegaan met gecompromitteerde sleutels.

12.3.2.5 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.

12.4.1.1 Alleen geautoriseerd personeel kan functies en software installeren of activeren

12.4.1.2 Programmatuur behoort pas te worden geïnstalleerd op een productieomgeving na een succesvolle test en acceptatie.

12.4.1.3 Geïnstalleerde programmatuur, configuraties en documentatie worden bijgehouden in een configuratiedatabase.

12.4.1.4 Er worden alleen door de leverancier (Dit kan ook een interne leverancier zijn.) onderhouden (versies van) software gebruikt.

12.4.1.5 Van updates wordt een log bijgehouden.

12.4.1.6 Er is een rollbackstrategie.

12.4.2 Bescherming van testdata

Testgegevens behoren zorgvuldig te worden gekozen, beschermd en beheerst.

12.4.2.1 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.

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

12.4.3.2 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.

12.5.1.1 Er is aantoonbaar wijzigingsmanagement ingericht volgens gangbare best practices zoals ITIL 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.

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

12.5.3 Restricties op wijzigingen in programmatuurpakketten

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

12.5.3.1 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.

12.5.4.1 Op het grensvlak van een vertrouwde en een onvertrouwde omgeving vindt content-scanning plaats. Het gaat hier dan om informatie die zich daar voor leent. Encrypted informatie is niet zondermeer te scannen.

12.5.4.2 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.

12.5.5.1 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.

12.6.1.1 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.

12.6.1.2 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.

12.6.1.3 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).

12.6.1.4 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.

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

13 Beheer van Informatiebeveiligingsincidenten

13.1 Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken

Doelstelling

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

13.1.1 Rapportage van informatiebeveiligingsgebeurtenissen

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

13.1.1.1 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.

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

13.1.1.3 Er is een contactpersoon (Deelnemer Security Contact (DSC). Lees ook als: Vertrouwde Contactpersoon Informatiebeveiliging (VCIB) of Algemeen Contactpersoon Informatiebeveiliging (ACIB) of CISO of gelijkwaardig) aangewezen voor het rapporteren van beveiligingsincidenten. Voor integriteitsschendingen is ook een vertrouwenspersoon aangewezen die meldingen in ontvangst neemt.

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

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

13.1.1.6 Informatie over de beveiligingsrelevante handelingen, bijvoorbeeld loggegevens, foutieve inlogpogingen, van de gebruiker wordt regelmatig nagekeken. De Beveiligingsfunctionarisbekijkt 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.

13.1.2.1 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.

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

13.2.2 Leren van informatiebeveiligingsincidenten

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

13.2.2.1 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.

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

14 Bedrijfscontinuïteitsbeheer

14.1 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Doelstelling

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

14.1.1 Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer

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

14.1.1.1 Calamiteitenplannen worden gebruikt in de jaarlijkse bewustwording-, trainingen testactiviteiten.

14.1.2 Bedrijfscontinuïteit en risicobeoordeling

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

14.1.2.1 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.

14.1.3.1 In de continuïteitsplannen wordt minimaal aandacht besteed aan:
- identificatie van essentiële procedures voor bedrijfscontinuïteit
- wie mag het continuïteitsplan wanneer activeren
- wanneer wordt er gecontroleerd teruggaan naar de standaard situatie
- veilig te stellen informatie (aanvaardbaarheid van verlies van informatie)
- prioriteiten en volgorde van herstel en reconstructie
- documentatie van systemen en processen
- kennis en kundigheid van personeel om de processen weer op te starten.

14.1.4 Kader voor de bedrijfscontinuïteitsplanning

14.1.4.1 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.

14.1.5.1 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.

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.

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

Deze lijst is in conceptvorm te vinden op: https://www.ibdgemeenten.nl/wpcontent/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.

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

15.1.3 Bescherming van bedrijfsdocumenten

15.1.3.1 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

15.1.4.1 De bescherming van gegevens en privacy behoort te worden bewerkstelligd overeenkomstig relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen (Zie artikel 12 WBP).

15.1.5 Voorkomen van misbruik van ICT-voorzieningen
Gebruikers behoren ervan te worden weerhouden ICT-voorzieningen te gebruiken voor onbevoegde doeleinden.

15.1.5.1 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.

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

15.2 Naleving van beveiligingsbeleid en -normen en technische naleving
Doelstelling
Bewerkstelligen dat systemen voldoen aan het beveiligingsbeleid en de beveiligingsnormen van de organisatie.

15.2.1 Naleving van beveiligingsbeleid en -normen

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

15.2.1.1 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 Beveiligingsfunctionaris, namens het MT , voor het toezicht op de uitvoering van het beveiligingsbeleid.
Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door of vanwege de Beveiligingsfunctionaris, de deelnemers, dan wel door interne of externe auditteams.

15.2.1.2 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.

15.2.2.1 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

15.3.1.1 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

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