GEMEENTE Medemblik

GEMEENTEBLAD

Officiële uitgave van de gemeente Medemblik

Nr. 175289

22 april

2025

Informatiebeveiligingsbeleid 2024-2027

Intentieverklaring
De inwoners gaan ervan uit dat de gemeente zorgvuldig omgaan met hun gegevens. Het college en de gemeentesecretaris erkennen dat de gemeente een maatschappelijke en ethische taak heeft om informatie beschikbaar, integer en vertrouwelijk te houden. Om de hoogste kwaliteit te kunnen garanderen voor onze burgers is informatiebeveiliging van cruciaal belang en het college en de gemeentesecretaris onderstrepen dit volledig. Wegens die reden committeren zij zich aan dit beleid en zorgen zij ervoor dat beschikbare middelen zo goed mogelijk ingezet worden en dat indien meer middelen noodzakelijk zijn dit gecommuniceerd wordt aan de raad.

Verder onderstrepen de ondergetekenden het belang van onafhankelijke controle en advisering door de interne auditor en de CISO en zullen zij ervoor zorgen dat die onafhankelijkheid wordt gewaarborgd.

Dit beleid wordt actief uitgedragen en is geborgd in de processen binnen de gemeente. Om dit belang naar de buitenwereld te onderstrepen zal de gemeente jaarlijks verantwoording afleggen middels een externe audit.

Tot slot, committeert men zich aan het doorvoeren van verbeteringen waar dit noodzakelijk wordt geacht.

Aldus vastgesteld door burgemeester en wethouders van de gemeente Medemblik op 3 september 2024.

De secretaris,
Chantal Minnaert

De burgemeester,
Michiel Pijl

Managementsamenvatting

Het beveiligen van informatie van onze inwoners, ondernemers en medewerkers wordt steeds belangrijker. De impact bij een (digitaal)incident, zoals het gijzelen van de gemeentelijke informatiesystemen of het lekken van persoonsgegevens, heeft een steeds grotere impact op onze bedrijfsvoering maar ook een steeds grotere maatschappelijke impact. Gemeente Medemblik heeft een grote verantwoordelijkheid om deze informatie adequaat te beschermen.

Informatiebeveiliging vormt een belangrijk kwaliteitsaspect van de informatievoorziening van de gemeente. Het beveiligen van informatie is echter geen eenmalige zaak, maar een proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen. Het doorlopen van dit proces is een verantwoordelijkheid van het lijnmanagement. Om te voorkomen dat informatie en informatiesystemen te licht of te zwaar worden beveiligd, vormt risicomanagement een belangrijk onderdeel in dit proces.

Dit beleid is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO) versie 1.04zv. De BIO beschrijft het basisniveau voor informatiebeveiliging en wordt gehanteerd binnen de Nederlandse overheid, door het Rijk, Gemeenten, Waterschappen en Provincies. Dit is één basisniveau voor informatiebeveiliging, één gezamenlijke taal voor alle overheidsorganisaties

Het beleid geeft een concrete invulling voor gemeente Medemblik hoe informatiebeveiliging optimaal ingezet kan worden voor de categorieën organisatie, mens, fysiek en techniek.

In dit beleid worden organisatorische maatregelen voor informatiebeveiliging beschreven. In deze maatregelen staat centraal hoe informatiebeveiliging binnen gemeente Medemblik vormgegeven wordt. Dit betreft onder andere waar welke verantwoordelijkheden liggen binnen de ambtelijke lijnorganisatie. Maar ook hoe om te gaan met informatiebeveiligingsincidenten, leveranciersmanagement toegangscontrole en onafhankelijke reviews van informatiebeveiliging.

Daarnaast worden eisen gesteld aan de processen van personeelszaken. Het gaat hierom maatregelen van de instroom tot de uitstroomprocessen en alles wat daartussen gebeurt, en ervoor maar ook erna. Hierbij moet gedacht worden aan eisen voor screening, arbeidsvoorwaarden, sanctiebeleid, gedragscode, thuiswerken, rapporteren van incidenten, bewustwordingstrainingen, doorstroom en uitdienst.

Ook worden maatregelen beschreven voor de fysieke beveiliging. De fysieke beveiliging is van belang om te voorkomen dat apparatuur of bijvoorbeeld dossiers met informatie gestolen worden. Hiervoor worden eisen gesteld aan maatregelen zoals beveiliging van gevoelige ruimten, clear desk en clear screen, bekabeling, veilig werken, beschikbaarheid nutsvoorzieningen, apparatuur buiten het gemeentehuis en vernietiging van apparatuur.

Aan de technische maatregelen worden ook eisen gesteld. Deze maatregelen zijn van toepassing voor zowel gemeente Medemblik als mede leveranciers waar producten en diensten worden afgenomen. Zo worden eisen gesteld aan maatregelen zoals identiteiten, authenticatie, wachtwoorden, autorisaties, logging, monitoring, verhoogde rechten, netwerk afscherming, netwerk beveiliging, cryptografie, beheersing van technische kwetsbaarheden, configuratiemanagement, patching, hardening, wijzigingen beheer, capaciteit beheer, redundantie, back-ups, bescherming tegen malware en het veilig ontwikkelen van software.

Terminologie

Term	Afkorting van	Eventuele uitleg
BIO	Baseline Informatiebeveiliging Overheid	Verplichte standaard, gebaseerd op de ISO27001, en specifiek gericht op Nederlandse overheidsorganisaties.
BRP	Basisregistratie Personen	-
Cbw	Cyberbeveiligingswet	De Cyberbeveiligingswet (Cbw) is er op gericht om de digitale weerbaarheid van Nederland te vergroten, de gevolgen van cyberincidenten te beperken en zo maatschappelijke ontwrichting te voorkomen.
CERT	Computer Emergency Response Team	Een Computer Emergency Response Team (CERT) is een gespecialiseerd team van ICT-professionals, dat in staat is snel te handelen in het geval van een beveiligingsincident met computers of netwerken. In het geval van de gemeente is dit de IBD.
CIP	Centrum Informatiebeveiliging en Privacybescherming	Een publiek-private netwerkorganisatie met participanten en kennispartners. Participanten zijn medewerkers uit de overheid, semioverheid en zorg. Kennispartners zijn medewerkers van marktpartijen, die een convenant met CIP zijn aangegaan om bij te dragen aan de kennisdeling.
CISO	Chief Information Security Officer	-
DT	Directie Team	-
FG	Functionaris Gegevensbescherming	-
HR	Human Resources	Ook wel bekend als personeelszaken of Personeel & Organisatie (P&O)
IBD	Informatiebeveiligingsdienst	De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en onderdeel van de Vereniging van Nederlandse Gemeenten. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy.
Incident Response Team	-	Het team dat voor informatiebeveiligingsincidenten wordt aangesteld om deze op te lossen. Voor incidenten met grote impact (bijzondere incidenten) betreft dit het crisis team.
Informatievoorziening		
ISO	Information Security Officer	-
ISO27001	-	Internationale standaard voor vormgeving informatiebeveiliging managementsysteem.
OOV	Openbare Orde en Veiligheid	

Raad	De gemeenteraad van gemeente Medemblik.	
SMT	Strategisch managementteam	-
SUWI	Wet structuur uitvoeringsorganisaties werk en inkomen	-
Systeemeigenaar	-	Medewerker binnen de gemeente belast met het eigenaarschap van een specifiek systeem.
VNG	Vereniging Nederlandse Gemeenten	-
Wdo	Wet digitale overheid	-
Woo	Wet open overheid	-

1. Inleiding

Het beveiligen van informatie van onze inwoners, ondernemers en medewerkers wordt steeds belangrijker. De impact bij een (digitaal)incident, zoals het gijzelen van de gemeentelijke informatie systemen of het lekken van persoonsgegevens, heeft een steeds groteren impact op onze bedrijfsvoering maar ook een steeds grotere maatschappelijke impact. Gemeente Medemblik heeft een grote verantwoordelijkheid om deze informatie adequaat te beschermen.

In het 2022 heeft de Rekenkamer van gemeente Medemblik een onderzoek uitgevoerd naar de staat van informatiebeveiliging binnen de gemeente Medemblik. Tijdens de Gemeenteraad van 29 september 2022 is de rapportage “Rekenkamerrapportage Informatieveiligheid gemeente Medemblik” behandeld. De raad heeft besloten om de gedane aanbevelingen over te nemen. Dit informatiebeveiligingsbeleid geeft verdere kaders hieraan.

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

Vanuit de Rijksoverheid is in 2020 vastgesteld dat overheidsorganisaties (inclusief gemeenten) moeten voldoen aan de Baseline Informatiebeveiliging Overheid (BIO) welke is gebaseerd op de internationaal erkende ISO27001 en ISO27002 standaarden.

1.1. Maatschappelijk belang

De inwoner gaat ervan uit dat de gemeente zorgvuldig omgaat met zijn of haar gegevens. De gemeente heeft een maatschappelijke en ethische taak om informatie beschikbaar, integer en vertrouwelijk te houden. Mogelijke gevolgen wanneer dit niet geborgd is:

- Beveiligingsincident;
- Datalek;
- Identiteitsfraude;
- Imagoschade: verlies van vertrouwen in de gemeente;
- Financiële risico’s: boetes en herstelkosten.

1.2. Wat is informatiebeveiliging

Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket aan maatregelen en processen om de betrouwbaarheid en kwaliteit van de informatievoorziening te waarborgen. Dit wordt onderverdeeld in:

- Beschikbaarheid:
  - de mate waarin informatie en/of functionaliteit op de juiste momenten beschikbaar zijn voor belanghebbende. Informatie en functionaliteit dienen voor belanghebbenden zodanig beschikbaar te zijn dat zij hun taken optimaal kunnen uitvoeren.

- Integriteit:
  - het in overeenstemming zijn van informatie met de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen (juistheid, volledigheid en tijdigheid). De juistheid van informatie en functionaliteit dient te voldoen aan de daarvoor gestelde normen, wet- en regelgeving.

- Vertrouwelijkheid:

- de mate waarin de toegang tot informatie of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn. Belangrijk hierbij is de controleerbaarheid van de maatregelen die genomen zijn om de betrouwbaarheid te borgen.

Informatiebeveiliging betreft alle vormen van informatie (analoog, digitaal, tekst, video, geluid, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, DVD, gesprekken, et cetera) en alle informatie verwerkende systemen (IT-systemen, databases, hardware, bijbehorende bedrijfsmiddelen, archiefkasten) en alle informatie houdende partijen (werknemers, leveranciers, bestuurders, et cetera).

2. Informatiebeveiligingsbeleid

2.1. Doel van dit beleid

Het doel van dit beleid is om de gemeente in staat te stellen de vertrouwelijkheid, beschikbaarheid en integriteit van informatie(systemen) aantoonbaar te waarborgen, en schade en andere ernstige gevolgen te minimaliseren. Het beleid stelt de gemeente hiertoe in staat door een kader te bieden met passende personele, organisatorische en technische maatregelen, waarmee de gemeente voldoet aan relevante wet- en regelgeving.

2.2. Scope

De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

2.3. Bestuurlijke principes

Informatiebeveiliging is een gemeente breed onderwerp, het betreft een kwaliteitsaspect in alle processen van de gemeente. Informatiebeveiliging is derhalve niet een geïsoleerd onderwerp. Informatiebeveiliging creëert waarde, voorkomt schade en draagt bij aan de bedrijfsdoelstellingen van de gemeente. Om dat te bewerkstelligen conformeert de gemeente zich aan de door de VNG[1] opgestelde 10 principes:

1. Bestuurders bevorderen een veilige cultuur;
2. Informatiebeveiliging is van iedereen;
3. Informatiebeveiliging is risicomanagement;
4. Risicomanagement is onderdeel van de besluitvorming;
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking;
6. Informatiebeveiliging is een proces;
7. Informatiebeveiliging kost geld;
8. Onzekerheid dient te worden ingecalculeerd;
9. Verbetering komt voort uit leren en ervaring;
10. Het bestuur controleert en evalueert.

Het bestuur dient de gemeente te faciliteren in het op orde brengen van de informatiebeveiliging.

Referentie: *BIO versie 1.04zv beheersmaatregel 5.1.1.1.f.*

2.4. Verantwoordelijkheden

De raad van gemeente Medemblik is verantwoordelijk voor de vaststelling van kaders voor het informatiebeveiligingsbeleid en het beschikbaar stellen van voldoende middelen aan de gemeente om te voldoen aan dit beleid.

De ambtelijke organisatie van verantwoordelijkheden ten aanzien van informatiebeveiliging staat beschreven in “hoofdstuk 3 Organiseren van informatiebeveiliging” van dit beleid.

Referentie: *BIO versie 1.04zv beheersmaatregel 5.1.1.1.b & 5.1.1.1.c.*

2.5. Strategische uitgangspunten

Het uitgangspunt betreffende informatiebeveiliging voor de gemeente is om te voldoen aan relevante wet- en regelgeving, in het bijzonder de Baseline Informatie Beveiligingsbeleid (BIO), en hierbij in te zetten op een ‘voldoende’. Een voldoende betekent dat niveau 3 van de BIO (zie afbeelding hieronder) wordt behaald binnen de gemeente.

1) de-10-bestuurlijke-principes-voor_20190109.pdf (vng.nl)

Figuur 1: Niveaus Baseline Informatiebeveiliging Overheid

Het BIO niveau van de informatiebeveiliging van de gemeente dient jaarlijks gemeten te worden middels een onafhankelijke audit van een externe partij. De CISO is verantwoordelijk voor de coördinatie van de audit en het bestuur is verantwoordelijk voor het doorvoeren van aanpassingen n.a.v. de resultaten uit deze meting.

Verdere uitgangspunten voor de informatiebeveiliging zijn:
- Het informatiebeveiligingsbeleid is gebaseerd op de meest recente versie van de Baseline Informatiebeveiliging Overheid (BIO);
- Het informatiebeveiligingsbeleid is vastgelegd in dit document en is goedgekeurd door de raad, het college van de gemeente als eindverantwoordelijke ten aanzien van het beleid. In het beleidsdocument wordt verwezen naar aanvullende documenten;
- Het beleidsdocument en de hieruit volgende producten zijn beschikbaar voor alle medewerkers van de gemeente en worden gepubliceerd via het intranet;
- Informatie moet beschikbaar, integer en vertrouwelijk zijn. De mate hiervan hangt af van het belang van de informatie voor de gemeente of haar inwoners.

Referentie: *BIO versie 1.04zv beheersmaatregel 5.1.1.1.a & 5.1.1.1.d.*

2.6. Randvoorwaarden
Randvoorwaarden ten aanzien van een efficiënte en effectieve uitvoering van dit beleid zijn:
- De maatregelen moeten standaard onderdeel worden van de werkzaamheden en gemeentelijke processen;
- Het niet naleven van de maatregelen wordt niet getolereerd en zal geadresseerd worden, waar nodig middels een disciplinaire procedure;
- Het college, het DT, de strategisch managers en de teamleiders dienen het goede voorbeeld te geven;
- Aan periodieke toetsing en controles dient actief meegewerkt te worden. Bij uitblijven of tegenwerking dient hier door leidinggevende direct op te worden geacteerd;
- Het college en het DT geven ieder jaar expliciet aandacht aan informatiebeveiliging en committeren zich opnieuw aan dit beleid en de uitvoering en naleving hiervan;
- Er moeten voldoende middelen en capaciteit beschikbaar zijn om de maatregelen van dit beleid te implementeren, te onderhouden en na te leven.

Referentie: *BIO versie 1.04zv beheersmaatregel 5.1.1.1.a.*

2.7. Relevante Wet- en Regelgeving
Dit informatiebeveiligingsbeleid dekt tevens aanvullende beveiligingseisen uit lokale, nationale en Europese wet- en regelgeving af. Dit betreft onder andere, en is niet gelimiteerd tot, de wetgeving voor de BRP, SUWI, Woo, Wdo, Archiefwet, AVG, en de Cbw. Aanpassingen in lokale, nationale en Europese wet- en regelgeving zal leiden tot een herziening van dit beleid.

2.8. Beoordeling van informatiebeveiligingsbeleid
Het beleid dient periodiek beoordeeld te worden. Vragen die minimaal in iedere beoordeling worden gesteld zijn:

1. Zijn er nieuwe ontwikkelingen die een bedreiging vormen voor de informatiebeveiliging van de gemeente?
   a. Zo ja, dient dit beleid hiervoor aangepast te worden?
   b. Zo nee, onderbouw waarom niet.

2. Zijn er door dit beleid hinderingen binnen de werkprocessen in de gemeente?
   a. Zo ja, dient dit beleid hiervoor aangepast te worden?
   b. Zo nee, onderbouw waarom niet.

3. Zijn er andere redenen om dit beleid aan te passen?
   a. Zo ja, welke?
   b. Zo nee, onderbouw waarom niet.

Beoordelingen worden uitgevoerd door de CISO en de ISO en worden schriftelijk vastgelegd op een locatie die voor alle betrokken rollen is te benaderen. Voor de beoordeling van het informatiebeveiligingsbeleid zijn er formele contactmomenten vastgesteld.

Tabel 1: Beoordeling van informatiebeveiligingsbeleid

Contactmoment	Omschrijving	Frequentie	Betrokken rollen
Beoordeling informatiebeveiligingsbeleid	Overleg om het beleid te beoordelen en eventueel te wijzigen.	2x per jaar	CISO & ISO
Terugkoppeling college en definitieve goedkeuring voorgestelde wijzigingen.	Terugkoppeling van de resultaten van de beoordeling en eventueel voorstellen wijzigingen ter definitieve goedkeuring (na goedkeuring SMT en DT).	2x per jaar	College, gemeentesecretaris & CISO
Interne Audit	Interne beoordeling die controleert of de gemeente voldoet aan het informatiebeveiligingsbeleid.	1x per jaar	Interne auditor
Terugkoppeling interne audit	De interne auditor rapporteert de bevindingen direct aan de directie, het SMT en de CISO.	1x per jaar	Interne auditor, CISO & gemeentesecretaris
SMT-overleg	Overleg om de resultaten vanuit de beoordeling terug te koppelen aan de directie en strategisch managers. Het SMT kan dan tevens aangeven of het beleid nog voldoende aansluit bij de werkzaamheden van de afdelingen.	4x per jaar	Directieteam, strategisch managers & CISO
Terugkoppeling beoordeling CISO en eventuele goedkeuring voorgestelde wijzigingen door het college.	Informatieve terugkoppeling van de beoordelingen van het beleid door de CISO. Na goedkeuring van de directie in het SMT-overleg dienen eventuele wijzigingen te worden voorgesteld aan het college en door hun goedgekeurd te worden.	2x per jaar	CISO, gemeentesecretaris en college

Indien door externe ontwikkelingen aanpassingen niet kunnen wachten tot de formele beoordelingsmomenten, kan de CISO het SMT, het DT, het college en de raad te allen tijde benaderen met een voorstel tot aanpassing. De CISO is verantwoordelijk voor de aanpassing van het informatiebeveiligingsbeleid, het college is verantwoordelijk voor de vaststelling van de aanpassing(en). De raad dient te worden geïnformeerd na vaststelling van de aanpassing(en).

Referentie: *BIO versie 1.04zv beheersmaatregel 5.1.1.1.e & 5.1.2.*

2.9. Bijhouden deelproducten
Een tabel met bijbehorende deelproducten is opgenomen in "Bijlage 1: Deelproducten behorende bij het informatiebeveiligingsbeleid".

2.10. Inwerkingtreding
Dit informatiebeveiligingsbeleid treedt in werking na vaststelling en ondertekening door de raad. Hiermee vervallen alle informatiebeveiligingsbeleidsstukken die voor dit beleid waren besloten.

2.11. Hardheidsclausule
In uitzonderlijke gevallen kan het college besluiten om af te wijken van de bepalingen in dit informatiebeveiligingsbeleid, indien strikte naleving ervan leidt tot onredelijke belemmeringen voor de uitvoering van gemeentelijke taken of andere dringende belangen in het algemeen belang.

Een dergelijke afwijking kan slechts plaatsvinden na zorgvuldige afweging van de risico's voor informatiebeveiliging op advies van de CISO en na goedkeuring van de gemeentesecretaris Het besluit tot afwijking en de redenen daarvoor worden gedocumenteerd en indien nodig gecommuniceerd naar relevante belanghebbenden, met inachtneming van de geldende wet- en regelgeving.

3. Organiseren van informatiebeveiliging
3.1. Interne organisatie

3.1.1. Rollen en verantwoordelijkheden bij informatiebeveiliging
In dit document worden enkel de functieprofielen benoemd die direct betrokken zijn bij het opstellen, uitvoeren en controleren van het informatiebeveiligingsbeleid.

Tabel 2: Rollen en verantwoordelijkheden bij informatiebeveiliging

Rol	Verantwoordelijkheden
Gemeenteraad	Verantwoordelijk voor de vaststelling van het informatiebeveiligingsbeleid en het beschikbaar stellen van voldoende middelen aan de gemeente om te voldoen aan dit beleid.
College van B&W	Verantwoordelijk voor de uitvoering en naleving van dit informatiebeveiligingsbeleid op het hoogste niveau. Daarnaast is het college gedurende de looptijd van het informatiebeveiligingsbeleid gemandateerd tot het doorvoeren van tussentijdse wijzigingen.
Gemeentesecretaris	Verantwoordelijk voor de operationele naleving van dit beleid en het voldoende toekennen van de beschikbare middelen.
Strategisch manager	Verantwoordelijk voor de uitvoering en naleving van dit beleid op afdelingsniveau én zijn, conform de BIO, verantwoordelijk voor de ketens van informatiesystemen die onder hun afdeling vallen. Indien een keten van informatiesystemen niet onder één afdeling valt zijn beide strategisch managers verantwoordelijk.
Chief Information Security Officer (CISO)	Verantwoordelijk voor de onafhankelijke controle op de uitvoering en naleving van dit beleid én dient tijdig de verantwoordelijken te wijzen op eventuele misstanden. Tevens is de CISO verantwoordelijk voor de aanpassingen van dit beleid.
Information Security Officer (ISO)	Ondersteunt de CISO en de gemeente met betrekking tot informatiebeveiliging.
Proceseigenaar	Verantwoordelijk voor een proces binnen de gemeente en de uitvoering en naleving van dit beleid binnen dat proces.
Teamleider	Verantwoordelijk voor de uitvoering en naleving van dit beleid in de processen die binnen hun team worden gehanteerd.
Budgethouder	Verantwoordelijk voor de uitvoering en naleving van dit beleid bij de door hen gecontracteerde leveranciers.
Systeemeigenaar	Verantwoordelijk voor de uitvoering en naleving van dit beleid voor het systeem waarvan zij eigenaar zijn. Ieder systeem (dus ook Cloud systemen) dienen een systeemeigenaar te hebben.
Interne Auditor	Verantwoordelijk voor de interne toetsing van het informatiebeveiligingsbeleid.
Privacy Officer (PO)	De PO houdt onder verantwoordelijkheid van de organisatie toezicht op de interne naleving van de AVG en, adviseert en ondersteund het lijnmanage-

	ment en medewerkers over de juiste en zorgvuldige omgang met persoonsgegevens zoals de AVG voorschrijft.
Functionaris Gegevensbescherming (FG)	De FG is de onafhankelijke interne toezichthouder. De FG controleert of de organisatie de AVG, en WPG, goed toepast en ziet erop toe dat betrokkenen hun privacy rechten kunnen uitoefenen.
Medewerker	Verantwoordelijk voor het uitvoeren van het informatiebeveiligingsbeleid binnen zijn / haar werkzaamheden.

Referentie: *BIO versie 1.04zv beheersmaatregel 6.1.1, 5.1.1.1.b & 5.1.1.1.c.*

3.1.2. Scheiding van taken

Conflicterende taken en verantwoordelijkheden dienen van elkaar te worden gescheiden zodat het risico van ongewenste wijzigingen of misbruik van bedrijfsmiddelen wordt verminderd.

In ieder onderdeel van dit beleid staan de verantwoordelijken benoemt. De verantwoordelijkheden zijn gekoppeld aan functies op een wijze waardoor men nooit de gehele cyclus van een proces kan beïnvloeden.

Deze functies dienen nimmer bij eenzelfde persoon belegd te worden. In onderstaande tabel staan de functies die niet tegelijktijdig bij een eenzelfde persoon mogen worden belegd. De 'x' geeft aan dat deze functies niet belegd mogen zijn bij dezelfde persoon.

Tabel 3: Functies die niet bij eenzelfde persoon belegd mogen zijn

Functies die niet bij eenzelfde persoon belegd mogen zijn						
	Proceseigenaar	Systeemeigenaar	Teamleider	CISO	Interne Auditor	SMT lid
Proceseigenaar		x		x	x	
Systeemeigenaar	x			x	x	x
Teamleider				x	x	x
CISO	x	x	x		x	x
Interne Auditor	x	x	x	x		x
SMT lid		x	x	x	1. x	

Referentie: *BIO versie 1.04zv beheersmaatregel 6.1.2.*

3.1.3. Contact met overheidsinstanties

In het kader van informatiebeveiliging is de CISO verantwoordelijk voor de contacten met toezichthouders en andere overheidsinstanties, waaronder de Informatiebeveiligingsdienst (IBD). Uitzondering op bovenstaande is het contact met de Autoriteit Persoonsgegevens (AP), waar de Functionaris Gegevensbescherming verantwoordelijk voor is.

Ten aanzien van de contacten met de overheidsinstanties dient een contactoverzicht te worden opgesteld door de CISO, die dit overzicht jaarlijks actualiseert. Het contactoverzicht wordt vastgelegd bij het informatiebeveiligingsbeleid en bevat de volgende onderdelen:

- Relevante overheidsinstanties waarmee contact onderhouden dient te worden;
- Contactgegevens overheidsinstanties, zoals postadres, e-mail, telefoon;
- Verantwoordelijke vanuit de gemeente voor het contact;
- In welk geval contact opgenomen moet worden met de overheidsinstantie;
- Datum van meest recente actualisatie contactoverzicht.

In het geval van incidenten en calamiteiten kan er afgeweken worden van bovenstaande. Het Bedrijfscontinuïteitsplan (BCP) en Incident Response Plan omvatten de verantwoordelijkheden in het geval van calamiteiten en incidenten.

Referentie: *BIO versie 1.04zv beheersmaatregel 6.1.3.*

3.1.4. Informatiebeveiliging in projectbeheer
Informatiebeveiliging is onderdeel van **alle** projecten.

Voorafgaand aan een project
Voorafgaand aan een project wordt de informatie die noodzakelijk is voor het project geclassificeerd aan de hand van hoofdstuk 5 uit dit beleid. Vervolgens worden informatiebeveiligingsrisico's geïdentificeerd middels een risicoanalyse.

Maatregelen en risico acceptatie
Na identificatie moet er gekozen worden voor welke risico's maatregelen worden getroffen en welke risico's worden geaccepteerd. De verantwoordelijke voor deze keuzes wordt als volgt bepaald:

Indien het project één of een deel van één werkproces omvat, dient de proceseigenaar deze keuzes te maken.

Indien het project meer dan één werkproces bevat maar geen werkprocessen in andere afdelingen raakt, dan is de strategisch manager hiervoor verantwoordelijk.

Als het project meerdere afdelingen raakt dient de gemeentesecretaris deze keuzes maken.

Te allen tijde dient de verantwoordelijke advies te vragen aan de CISO.

Vastlegging
De risicoanalyse en onderverdeling in te accepteren risico's en te nemen maatregelen worden schriftelijk vastgelegd door de verantwoordelijke en gedeeld met de CISO. Na vastlegging worden de project specifieke beveiligingsmaatregelen, in overleg met de CISO of ISO, uitgewerkt en opgenomen in de acceptatiecriteria én de kosten in de financiële verantwoording van het project.

Tijdens de uitvoering van het project
Tijdens uitvoering van projecten dient te allen tijde conform dit beleid gewerkt te worden. Tevens dienen de uitgewerkte project specifieke beveiligingsmaatregelen zo vroeg mogelijk aantoonbaar in het project te worden geïmplementeerd. De projectleider is verantwoordelijk voor de naleving en monitoring hiervan.

Referentie: *BIO versie 1.04zv beheersmaatregel 6.1.5.*

3.2. Mobiele apparaten en telewerken
Onder mobiele apparaten worden alle apparaten verstaan die niet gebonden zijn aan een vaste locatie. Een server, vaste telefoon of desktop vallen hierbuiten. Populaire mobiele apparaten zijn laptops, mobiele telefoons en tablets.

De volgende maatregelen gelden ten aanzien van mobiele apparaten en telewerken:
- Alle medewerkers, raadsleden, stagiaires en ingehuurde externen dienen te werken op een mobiel apparaat verstrekt door de gemeente;
- Voor alle verstrekte mobiele apparaten moet een bruikleenovereenkomst (zie hoofdstuk 6) getekend worden;
- Bij uitgifte van een mobiel apparaat ontvangt de gebruiker een document waarin de gedragsaspecten van veilig mobiel werken aan de orde komen;
- De toegang tot gegevens moet beperkt worden door middel van specifieke toegangsrechten voor elke gebruiker;
- Alle data op alle mobiele apparaten dient door middel van versleuteling beveiligd te zijn (zie hoofdstuk 8);
- Het moet medewerkers door technische maatregelen onmogelijk gemaakt worden om applicaties / programma's te installeren zonder toestemming van de gemeente;
- Mobiele apparatuur dient de mogelijkheid te hebben om op afstand onbruikbaar gemaakt te worden waarbij alle gegevens onomkeerbaar worden vernietigd;
- Alle mobiele apparaten dienen onder beheer te zijn van de gemeente en te voldoen aan dit informatiebeveiligingsbeleid;
- De verbinding tussen de telewerklocatie en de gemeente dient beveiligd te zijn middels versleuteling (zie hoofdstuk 8);
- Alle verstrekte mobiele apparaten worden na het beëindigen van de werkzaamheden voor de gemeente teruggegeven aan de gemeente en door de gemeente op een veilige manier gereset waarbij alle data verwijderd wordt (zie paragraaf 9.2.7).

Telewerken
Telewerken betreft het op afstand werken op het netwerk van de gemeente. De gemeente staat telewerken toe voor de netwerken waarin informatie bereikbaar (zie hoofdstuk 11) is met een informatieclassificatieniveau 'Laag' en 'Midden', voor 'Hoog' is telewerken niet toegestaan. Telewerken dient uitsluitend mogelijk te zijn via een beveiligde verbinding (zie hoofdstuk 8) die enkel werkt vanaf een beveiligde omgeving van de gemeente.

Referentie: *BIO versie 1.04zv beheersmaatregel 6.2.1 en 6.2.2.*

4. Veilig Personeel
4.1. Voorafgaand aan het dienstverband

4.1.1. Screening
Voor aanvang werkzaamheden
Alle medewerkers, stagiaires en extern ingehuurde overleggen voor de aanvang van werkzaamheden een Verklaring Omtrent het Gedrag (VOG) specifiek voor de te vervullen functie.

Registratie
Team HR registreert het overleggen van de VOG waarbij de registratie minimaal de volgende punten bevat:
- Naam medewerker;
- Datum indiensttreding;
- Functie medewerker;
- Datum overlegde functie specifieke VOG;
- Verwachte datum voor vernieuwde VOG-aanvraag.

Functiewijziging
Bij functiewijziging dient een nieuwe VOG aangevraagd te worden voor de te vervullen functie. Team HR is verantwoordelijk voor het verzamelen van de aangevraagde VOG's.

Vernieuwing VOG
Iedere vijf jaar dient de VOG opnieuw aangevraagd en overlegd te worden voor iemand die een kwetsbare of risicovolle functie en/ of taak uitvoert. De criteria hiervoor zijn vastgelegd in een screeningsbeleid.

Niet kunnen overleggen VOG
Bij het niet kunnen overleggen van een VOG zijn overeenkomsten niet geldig (zie paragraaf 4.1.2).

Opslag VOG's
VOG's zijn geclassificeerd als informatie met classificatieniveau 'Midden' (zie hoofdstuk 5). De eisen voor deze classificatie gelden voor de opslag, het beheer en andere zaken omtrent VOG's. Aanvullend geldt dat de VOG na 5 jaar onomkeerbaar verwijderd wordt.

Referentie: *BIO versie 1.04zv beheersmaatregel 7.1.1.*

4.1.2. Arbeidsvoorwaarden
Arbeidsovereenkomsten en inhuurovereenkomsten dienen de volgende punten te bevatten:
1. De plichten en verantwoordelijkheden van de ondertekende ten aanzien van informatiebeveiliging;
2. De disciplinaire procedure (paragraaf 4.2.4), met te nemen maatregelen voor wanneer:
   a. Geheimhouding geschonden wordt;
   b. Het informatiebeveiligingsbeleid niet wordt nageleefd;
   c. De plichten en verantwoordelijkheden niet worden nageleefd;

3. De randvoorwaarde dat men enkel voor de gemeente kan werken indien iedere vijf jaar een geldige VOG overlegt kan worden.

Medewerkers in dienst van de gemeente
Arbeidsovereenkomsten voor medewerkers in dienst van de gemeenten dienen een verwijzing naar de Ambtenarenwet te bevatten én alvorens aanvang van de werkzaamheden dient de ambtelijke eed ter geheimhouding te worden vastgelegd.

Inhuur, externen en stagiaires
Inhuur, externen en stagiaires dienen voor aanvang van de werkzaamheden een geheimhoudingsverklaring te ondertekenen. De plicht ter geheimhouding blijft na het beëindigen van de werkzaamheden van kracht (zie paragraaf 4.2.5).

Tevens dienen de gedragsregels voor het gebruik van bedrijfsmiddelen voor extern personeel in het contract vastgelegd te zijn.

Referentie: *BIO versie 1.04zv beheersmaatregel 7.1.2 & 8.1.3.2.*

4.1.3. Personeelsreglement

Het personeelsreglement bevat minimaal:

- De verantwoordelijkheden van medewerkers, stagiaires en extern ingehuurde ten aanzien van informatiebeveiliging.
- De plicht dat iedereen het informatiebeveiligingsbeleid en de maatregelen die van toepassing zijn dient te kennen.
- De plicht dat iedereen de verantwoordelijkheid heeft de gemeentelijke informatie te beschermen.

Referentie: *BIO versie 1.04zv beheersmaatregel 7.1.2.*

4.2. Tijdens het dienstverband

4.2.1. Directieverantwoordelijkheden

De directie heeft de verantwoordelijkheid ervoor te zorgen dat het informatiebeveiligingsbeleid van de gemeente wordt nageleefd door iedereen die werkzaam is voor de gemeente. De directie dient daarom:

1. Periodiek, ten minste per kwartaal, te controleren of regels en procedures worden nageleefd;
2. Opleidingen en trainingen beschikbaar stellen aan medewerkers over hoe ze informatiebeveiliging moeten toepassen;
3. Voor een duidelijk communicatiemiddel omtrent informatiebeveiliging te zorgen.

Referentie: *BIO versie 1.04vz beheersmaatregel 7.2.1.*

4.2.2. Klokkenluidersregeling

Wanneer afspraken rondom informatiebeveiliging niet of onvoldoende worden nagekomen, dient de directie te zorgen voor een klokkenluidersregeling conform de Wet bescherming klokkenluiders. Hiervoor is het noodzakelijk dat specifiek voor informatiebeveiliging de volgende punten worden gewaarborgd:

- Medewerkers moeten anoniem melding kunnen doen, zonder dat de melding is terug te traceren naar de melder;
- Klokkenluidersmeldingen zijn geclassificeerd als informatie met informatieclassificatie ‘Hoog’. Alle eisen ten aanzien van deze informatieclassificatie gelden voor deze meldingen;
- De melding komt alleen terecht bij degene die verantwoordelijk zijn voor het behandelen van beveiligingsincidenten om de vertrouwelijkheid van de melder te beschermen;
- Het meldpunt dient onafhankelijk van de rest van de gemeente te opereren;
- Medewerkers dienen terugkoppeling te krijgen van de behandelaar van de melding over hoe hun melding is behandeld en wat er met de informatie is gedaan;
- Medewerkers die melding maken dienen te worden beschermd tegen de consequenties van het doen van de melding;
- De procedure ten aanzien van de klokkenluidersregeling dient duidelijk gecommuniceerd te worden naar de medewerkers, zodat inzichtelijk is hoe een beveiligingsissue gemeld moet worden en wat er vervolgens mee gebeurt.

Referentie: *BIO versie 1.04vz beheersmaatregel 7.2.1.1.*

4.2.3. Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Beschikbaar stellen van informatie

Informatie met betrekking tot het informatiebeveiligingsbeleid wordt beschikbaar gesteld op het intranet en bestaat minimaal uit de beleidsdocumenten, de gehouden presentaties en andere relevante documenten gerelateerd aan dit beleid.

Binnen 3 maanden na aanvang werkzaamheden

Iedereen die werkzaam is voor de gemeente dient binnen drie maanden na aanvang van de werkzaamheden een bewustzijnstraining succesvol te hebben gevolgd. De training eindigt met een toets om het kennisniveau van de personen te bepalen.

Aanvullend wordt de presentatie van de voorgaande sessie verstrekt binnen één maand na aanvang van de werkzaamheden.

Registratie initiële training

Van de deelname aan de bewustzijnstraining dient een registratie te worden bijgehouden door de teamleider in het centrale register voor bewustzijnstrainingen. Deze registratie moet ten minste de volgende onderdelen bevatten:
- Naam deelnemer;
- Functie deelnemer;
- Datum indiensttreding deelnemer;
- Datum van succesvol afronden bewustzijnstraining.

Deze registratie maakt inzichtelijk welke medewerkers de training nog moeten volgen en welke medewerkers de training succesvol hebben afgerond.

Geen succesvolle afronding
Indien uit de toets blijkt dat een persoon een onvoldoende kennisniveau heeft dan dient deze persoon deel te nemen aan de volgende bewustzijnstraining.

Periodieke training
Om iedereen bewust te laten omgaan met informatiebeveiliging wordt ten minste halfjaarlijks een verplichte bewustzijnstraining gehouden. In onderstaande tabel staan de verantwoordelijkheden ten aanzien van de verplichte trainingen:

Tabel 4: Periodieke training

Doelgroep	**Verantwoordelijke**	**Ondersteund door**	**Frequentie**
De raad	Gemeentesecretaris	CISO	Jaarlijks
Directie, college en strategisch managementteam	Gemeentesecretaris	CISO	Halfjaarlijks
Teamleiders	Strategisch manager	ISO	Halfjaarlijks
Medewerkers	Teamleider	ISO	Halfjaarlijks

De CISO of ISO bereidt de presentatie voor en ondersteunt de verantwoordelijke in de sessie. De presentaties worden samen met de verantwoordelijke gegeven.

Gemiste training door omstandigheden
Als een persoon niet bij een periodieke bewustzijnstraining aanwezig kan zijn, dient deze zich te melden bij de ISO. De ISO plant een vervangende training in voor de personen die niet aanwezig waren. Deze training dient binnen één maand van de originele training plaats te vinden.

Referentie: *BIO versie 1.04zv beheersmaatregel 7.2.2.*

4.2.4. Disciplinaire procedure
Er is een formele disciplinaire procedure voor de gevallen waarin:
1. Het geheimhoudingsbeding is geschonden;
2. Het informatiebeveiligingsbeleid niet is nageleefd;
3. Er onrechtmatig inbreuk is gepleegd op de informatiebeveiliging.

De procedure wordt gebruikt om men tot verantwoording te roepen en om te zorgen dat dergelijke, vergelijkbare, overtredingen in de toekomst worden voorkomen. Het college is eindverantwoordelijk voor het opstellen, uitvoeren en handhaven van de disciplinaire procedure.

Meldingen
De directie stelt een team of persoon aan die verantwoordelijk is voor het ontvangen en onderzoeken van meldingen, het vaststellen van de verantwoordelijkheid van de overtreder, het opleggen van de straffen en het handhaven van de procedure.

Eisen aan de procedure
De disciplinaire procedure dient ten minste de volgende onderdelen te bevatten:
- Beschrijving van hoe een melding van een inbreuk op de informatiebeveiliging moet worden gemaakt;
- Beschrijving van hoe de melding vervolgens wordt behandeld;
- Beschrijving van hoe een melding wordt onderzocht;
- Wie verantwoordelijk is voor het onderzoeken van de melding;
- Hoe bewijs wordt verzameld en vastgelegd;
- Beschrijving van welke straffen er opgelegd kunnen worden voor de inbreuken;

- Beschrijving hoe de straf wordt bepaald;
- Beschrijving wie verantwoordelijk is voor het opleggen van de straf;
- Hoe de beslissingen over de inbreuken worden gecommuniceerd naar de verantwoordelijke;
- Wie verantwoordelijk is voor de communicatie en hoe de communicatie wordt gemonitord;
- Hoe de straffen worden gehandhaafd;
- Beschrijving van hoe de procedure periodiek wordt geëvalueerd en verbeterd.

Opslag van meldingen én vervolgacties
Informatie omtrent meldingen en onderzoeken ten aanzien van de disciplinaire procedure hebben het classificatieniveau 'Hoog'. Alle eisen van dit classificatieniveau zijn van toepassing op de opslag, verwerking en communicatie van deze informatie.

Kennisname van de procedure
De directie, strategisch managers en teamleiders dienen ervoor te zorgen dat de disciplinaire procedure bekend is bij de medewerkers. De procedure dient ook opgenomen te zijn in alle overeenkomsten.

Referentie: *BIO versie 1.04zv beheersmaatregel 7.2.3.*

4.2.5. Beëindiging en wijziging van dienstverband
Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband zijn gedefinieerd in het geheimhoudingsbeding en worden bij in- en uitdiensttreding gecommuniceerd aan de medewerker of contractant door team HR. Het geheimhoudingsbeding blijft permanent van kracht, ook als de werkzaamheden voor de gemeente zijn beëindigd.

Referentie: *BIO versie 1.04zv beheersmaatregel 7.3.*

5. Informatieclassificatie

Het is noodzakelijk dat informatie een passend beschermingsniveau krijgt. Om te bepalen welke beveiligingsmaatregelen worden getroffen ten aanzien van processen en informatiesystemen worden informatieclassificatieniveaus gebruikt. Een classificatie maakt het vereiste beschermingsniveau eenduidig zichtbaar en maakt direct inzichtelijk welke maatregelen minimaal noodzakelijk zijn.

Er wordt geclassificeerd op de drie betrouwbaarheidsaspecten van informatie: beschikbaarheid, integriteit (juistheid en volledigheid) en vertrouwelijkheid. Om te bepalen om welk classificatieniveau het gaat, wordt de classificatietoets BIO[2] van de VNG gebruikt.

Er zijn drie beschermingsniveaus: 'Hoog', 'Midden' en 'Laag'. Daarnaast is er nog het niveau 'Openbaar'. Het niveau 'Openbaar' geeft aan dat er enkel basismaatregelen worden geëist.

De niveaus zijn in onderstaande tabel weergegeven:

Tabel 5: Classificatie matrix van informatie

Classificatie	Beschikbaarheid	Integriteit	Vertrouwelijkheid
3 – Hoog	**Essentieel** Informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten *(vb.: basisregistraties)*	**Desastreus** Het bedrijfsproces staat geen fouten toe *(vb.: informatie op de website)*	**Geheim** Informatie is alleen toegankelijk voor direct geadresseerde(n) *(vb.: zorggegevens en strafrechtelijke informatie)*
2 – Midden	**Noodzakelijk** Informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk *(vb.: primaire proces informatie)*	**Ernstig** Het bedrijfsproces staat zeer weinig fouten toe *(vb.: bedrijfsvoeringinformatie en primaire procesinformatie zoals vergunningen)*	**Vertrouwelijk** Informatie is alleen toegankelijk voor een beperkte groep gebruikers *(vb.: persoonsgegevens, financiële gegevens)*

2) https://www.informatiebeveiligingsdienst.nl/product/handreiking-dataclassificatie-2/

1 – Laag	**Belangrijk** Informatie mag incidenteel niet beschikbaar zijn *(vb.: administratieve gegevens)*	**Gering** Het bedrijfsproces staat enkele (integriteits-)fouten toe *(vb.: rapportages)*	**Intern** Informatie is toegankelijk voor alle medewerkers van de gemeente *(vb.: informatie op het intranet)*
0 – Openbaar	**Niet zeker** Gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn *(vb.: ondersteunende tools)*	**Verwaarloosbaar** Informatie mag worden veranderd *(vb.: templates en sjablonen)*	**Openbaar** Informatie mag door iedereen worden ingezien *(vb.: algemene informatie op de externe website van gemeente Medemblik)*

5.1. Verantwoordelijkheden
De proceseigenaar classificeert alle informatie in het proces conform bovenstaande toets. De CISO kan te allen tijde een nieuwe classificatie uitvoeren. De proceseigenaar dient bij de CISO te consulteren over passende beveiligingsmaatregelen per classificatieniveau. Daarnaast evalueert de CISO de beveiligingsmaatregelen periodiek, voor classificatieniveau 'Hoog' minimaal halfjaarlijks en voor classificatieniveau 'Midden' minimaal jaarlijks.

De interne auditor evalueert de werking van de beveiligingsmaatregelen periodiek, voor classificatieniveau 'Hoog' minimaal halfjaarlijks en voor classificatieniveau 'Midden' minimaal jaarlijks.

Referentie: *BIO versie 1.04zv beheersmaatregel 8.2.1, 8.2.2 & 8.2.3.*

5.2. Niet geclassificeerde informatie
In de regel mag het niet voorkomen dat informatie (nog) niet geclassificeerd is. In de praktijk zal dit echter zeker voorkomen. Niet geclassificeerde informatie dient zo snel mogelijk geclassificeerd te worden.

Zolang informatie nog niet geclassificeerd is dient er gecontroleerd te worden of de informatie persoonsgegevens bevat. Indien dit zo is geldt de classificatie 'Hoog' totdat de classificatie is uitgevoerd. Indien er geen persoonsgegevens aanwezig zijn betreft het classificatie 'Midden' totdat de classificatie is uitgevoerd.

5.3. Informatie en data eigenaarschap
Het eigenaarschap en bepaalde hierbij behorende verantwoordelijkheden ten behoeve van data en informatie zijn vastgelegd in het Data Governance beleid. Dit beleid dient vastgesteld te worden door het college en dient drie jaarlijks geëvalueerd te worden door het SMT met advies van de CISO en proceseigenaren.

6. Beheer van bedrijfsmiddelen
6.1. Verantwoordelijkheid voor bedrijfsmiddelen

6.1.1. Inventariseren van bedrijfsmiddelen
Per afdeling zijn alle bedrijfsmiddelen die samenhangen met informatie of informatie verwerkende faciliteiten vastgelegd in een inventaris. De inventaris wordt ieder kwartaal bijgewerkt. De strategisch manager is verantwoordelijk voor de vastlegging en het onderhoud van de inventaris op afdelingsniveau.

Indien een bedrijfsmiddel op teamniveau beheerd wordt, is de teamleider verantwoordelijk voor de vastlegging en het onderhoud van de inventaris op teamniveau. Deze inventaris dient onderdeel te zijn van de inventaris op afdelingsniveau.

Bedrijfsmiddelen die gedeeld worden door afdelingen worden in een gemeente brede inventaris opgenomen. Het gehele strategisch managementteam (SMT) is hiervoor verantwoordelijk.

De inventaris dient opgesteld te worden aan de hand van een gemeente brede standaard waarin minimaal de volgende zaken worden vastgelegd:
- Wat het bedrijfsmiddel is;
- Om welk type bedrijfsmiddel het gaat;
- Onder welke afdeling het valt;
- Indien van toepassing, onder welk team het valt;
- Wie de eigenaar (verantwoordelijke) is van het bedrijfsmiddel;
- Wie de gebruikers (functies) zijn van het bedrijfsmiddel.

Referentie: *BIO versie 1.04zv beheersmaatregel 8.1.1 en 8.1.2.*

6.1.2. Aanvaardbaar gebruik van bedrijfsmiddelen

Voordat bedrijfsmiddelen verstrekt worden, dient aan een aantal voorwaarden te worden voldaan:

1. Middels de risicoanalyse 'Aanvaardbaar gebruik bedrijfsmiddelen' stelt de gemeente vast dat de ontvangende partij het gebruik van de bedrijfsmiddelen toevertrouwd kan worden;
2. De verantwoordelijke voor de bedrijfsmiddelen geeft expliciet toestemming voor het verstrekken van de bedrijfsmiddelen aan de ontvangende partij voor het beoogde doel;
3. De ontvangende partij heeft een dienstverband, contract of overeenkomst met de gemeente;
4. De ontvangende partij ondertekent voor de bedrijfsmiddelen een bruikleenovereenkomst conform de standaard van de gemeente (zie paragraaf 6.1.3);
5. De bruikleenovereenkomst is ondertekend en vastgelegd voordat de bedrijfsmiddelen worden verstrekt.

Referentie: *BIO versie 1.04zv beheersmaatregel 8.1.3 & 6.1.2.1.*

6.1.3. Bruikleenovereenkomst

De ontvangende partij ondertekent voor de bedrijfsmiddelen een bruikleenovereenkomst conform de standaard van de gemeente. In de bruikleenovereenkomst moeten minimaal de volgende onderdelen opgenomen zijn:

- Omschrijving van het bedrijfsmiddel dat in bruikleen wordt genomen;
- Omschrijving waarvoor het bedrijfsmiddel gebruikt mag worden;
- Omschrijving van welke gegevens uit het bedrijfsmiddel worden opgeslagen en gedeeld;
- Voorwaarden waaronder het bedrijfsmiddel in bruikleen wordt gegeven;
- Inwerkingtreding van de bruikleenovereenkomst;
- Looptijd van de bruikleenovereenkomst;
- De gevolgen indien het in bruikleen gegeven bedrijfsmiddel tijdens de bruikleenperiode verloren gaat of beschadigd raakt;
- Inleverprocedure;
- Contactgegevens van de verantwoordelijke voor het bedrijfsmiddel, inclusief functie;
- Contactgegevens van de gebruiker van het bedrijfsmiddel, inclusief functie;
- Handtekeningen van de verantwoordelijke voor het bedrijfsmiddel en de gebruiker;
- Gedragsregels behorende bij het bedrijfsmiddel.

De verantwoordelijke voor het bedrijfsmiddel is verantwoordelijk voor de afsluiting van de bruikleenovereenkomst (zie paragraaf 6.1.2). De bruikleenovereenkomst dient centraal te worden opgeslagen en dient toegankelijk te zijn voor de betrokken partijen.

Referentie: *BIO versie 1.04zv beheersmaatregel 6.1.2.1 & 8.1.3.1.*

6.1.4. Registratie uitgifte bedrijfsmiddelen

De uitgifte van bedrijfsmiddelen dient geregistreerd te worden. De registratie dient centraal bijgehouden te worden en is enkel inzichtelijk voor geautoriseerde personen. De registratie bevat minimaal de volgende zaken:

- Ontvanger van het bedrijfsmiddel, inclusief naam, functie en contactgegevens van de ontvanger;
- Verstrekker van het bedrijfsmiddel, inclusief naam, functie en contactgegevens van de verstrekker;
- Identificatie bedrijfsmiddel, inclusief type, merk, model en serienummer van het bedrijfsmiddel en eventueel de softwareversie van het bedrijfsmiddel;
- Datum van uitgifte;
- Datum van inname;
- Door wie en wanneer en in welke staat het bedrijfsmiddel retour is ingenomen;
- Bewijs dat de bruikleenovereenkomst door beide partijen is getekend;
- Indien van toepassing, beveiligingsinstellingen die zijn toegepast op het bedrijfsmiddel (zoals versleuteling of kunstmatige limitatie);
- Indien van toepassing, incidenten (bijvoorbeeld schade) die zich hebben voorgedaan met het bedrijfsmiddel.

De registratie van bedrijfsmiddelen dient periodiek, ten minste per kwartaal, gecontroleerd te worden door de strategisch manager.

Referentie: *BIO versie 1.04zv beheersmaatregel 6.1.2.1.*

6.1.5. Teruggeven van bedrijfsmiddelen

Alle bedrijfsmiddelen worden teruggegeven aan de gemeente wanneer deze voor de uit te voeren werkzaamheden niet meer noodzakelijk zijn of bij beëindiging van het dienstverband, contract of

overeenkomst. De gemeente geeft een schriftelijke bevestiging van inlevering van bedrijfsmiddelen aan de ontvangende partij en registreert de inname in de inventaris. De inname status van de inventaris dient maandelijks door de verantwoordelijke te worden beoordeeld. In de beoordeling wordt minimaal geverifieerd of:

- De staat van het ingenomen bedrijfsmiddel voldoende is;
- Het bedrijfsmiddel is ingenomen binnen de gestelde looptijd van de bruikleenovereenkomst.

Referentie: *BIO versie 1.04zv beheersmaatregel 8.1.4.*

6.2. Behandelen van media

De definitie van media in dit beleid is 'middelen om informatie over te dragen' ofwel gegevensdragers. Dit is niet gelimiteerd tot digitale gegevensdragers, fysieke gegevensdragers zoals papier vallen hier ook onder.

6.2.1. Beheer van verwijderbare media

Verwijderbare media kan informatie bevatten die in onbevoegde handen kan vallen bij onjuist gebruik, verlies of diefstal. Voor het beheren van verwijderbare media geldt dat:

- Digitale verwijderbare media (bijv. USB-sticks) zijn bedrijfsmiddelen, bij uitwisseling dient er te worden voldaan aan de eisen van paragraaf 6.2.3.
- Vernietiging vindt plaats conform het reglement 'Vernietiging opslagmedia' (zie paragraaf 9.2.7).
- Versleutelingseisen conform hoofdstuk 8 zijn ten alle tijden van toepassing.
- Hergebruik geldt alleen voor digitale media waarbij de eisen van paragraaf 9.2.7 te allen tijde van toepassing zijn.
- Verwijderbare media (zowel papier als digitale media) worden na werktijd altijd achter slot en grendel opgeborgen. Verder gelden de eisen van paragraaf 9.2.9.

Referentie: *BIO versie 1.04zv beheersmaatregel 8.3.1.*

6.2.2. Verwijderen van media

Media die vertrouwelijke informatie bevatten, zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden. Media die niet langer nodig zijn, behoren op een veilige en beveiligde manier te worden verwijderd (zie paragraaf 9.2.7).

Eisen omtrent het hergebruik van verwijderbare media (opslagmedia) staan beschreven in paragraaf 9.2.7.

Referentie: *BIO versie 1.04zv beheersmaatregel 8.3.2.*

6.2.3. Media fysiek overdragen

Media die informatie bevatten, dienen te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens de overdracht. Voor het uitwisselen en overdragen van media dient een uitwisselingsbeleid te worden opgesteld. Dit beleid moet worden vastgesteld door het college. In dit beleid dienen ten minste de volgende onderdelen te worden opgenomen:

- Welke typen media kunnen worden overgedragen;
- Wie media kan overdragen;
- Aan wie de media overgedragen mag worden;
- Binnen welke termijn de media worden overgedragen;
- Wat de gevolgen zijn als media onjuist of onrechtmatig wordt overgedragen;
- Op welke wijze de media overgedragen mag worden;
- Per classificatieniveau informatie eisen omtrent het gebruik van koeriers of transporteurs;
- Wie verantwoordelijk is voor het fysiek transport van de media.

Referentie: *BIO versie 1.04zv beheersmaatregel 8.3.3.*

7. Logische toegangsbeveiliging

7.1. Bedrijfseisen voor logische toegangsbeveiliging

7.1.1. Beleid voor logische toegangsbeveiliging

De gemeente heeft een 'Logisch toegangsbeveiligingsbeleid' vastgesteld en gedocumenteerd. Het toegangsbeveiligingsbeleid is bekend gemaakt aan iedereen die werkzaam is voor de gemeente. Het toegangsbeveiligingsbeleid wordt periodiek, minimaal jaarlijks, geëvalueerd door de CISO.
In het toegangsbeveiligingsbeleid dienen ten minste de volgende aspecten aan de orde te komen:

- Algemene identiteiten (groepsaccounts)

- Er worden in de regel geen ‘algemene’ identiteiten (groepsaccounts) gebruikt. Indien er gewerkt moet worden met ‘algemene’ identiteiten dient hiervoor de procedure ‘Aanvraag algemene identiteiten’ gevolgd te worden;
- Indien er een ‘algemene’ identiteit wordt aangemaakt is de proceseigenaar van het proces waarbinnen de identiteit wordt gehanteerd tevens de eigenaar van deze identiteit.

- Monitoring
  - Voor herleidbaarheid en transparantie dient er middels logging vastgelegd te worden wie een bepaalde actie heeft uitgevoerd binnen een systeem of netwerk.

- Standaarden
  - De gemeente maakt, waar mogelijk, gebruik van bestaande (landelijke) voorzieningen voor authenticatie, autorisatie en informatiebeveiliging (bijv. DigiD en eHerkenning);
  - De gemeente hanteert zoveel mogelijk geaccepteerde standaarden voor de informatiebeveiliging;
  - Indien afgeweken wordt van een standaard dient de motivatie hiervoor centraal vastgelegd te worden.

- Autorisaties
  - Alle toegekende bevoegdheden worden per functieprofiel en per systeem geregistreerd en beheerd in een autorisatiematrix.
  - Gebruikers krijgen alleen autorisaties die benoemd zijn in de autorisatiematrix behorende bij het functieprofiel.
  - In de autorisatiematrix dient vastgelegd te worden wie toegang heeft tot welke informatiesystemen, welke gegevens binnen het systeem en welke acties de gebruiker mag uitvoeren.
  - Systemen kunnen tevens gebruiker zijn van een ander systeem, hiervoor dienen aparte autorisatiematrixen opgesteld te worden.
  - Aanvragen voor toegang worden geautoriseerd door gemandateerde werknemers middels een gestandaardiseerd aanvraagformulier;
  - De gemandateerde werknemer dient met behulp van een gestandaardiseerd formulier schriftelijk een autorisatieverzoek in voor een nieuwe of gewijzigde autorisatie bij de systeemeigenaar;
  - Autorisaties worden doorgevoerd in de systemen door de systeemeigenaren op last van de gemandateerde en na controle van het aanvraagformulier (zie paragraaf 7.2);
  - De systeemeigenaar registreert deze aanvraag of wijziging in een registratiesysteem en voegt daar de originele aanvraag bij;
  - De aanvragen dienen conform de wettelijke bewaartermijn bewaard te worden;
  - Voor iedere deelprocedure, zoals beschreven in paragraaf 7.2, is een gestandaardiseerd formulier beschikbaar;
  - Het toekennen van speciale bevoegdheden wordt beperkt en beheerd door het SMT (zie paragraaf 7.2.3).

- Mandaat
  - Het SMT wijst medewerkers aan die gemandateerd zijn tot het aanvragen van toegang tot systemen.
  - Een mandaat geldt óf voor één proces of voor één systeem.
  - Gemandateerde werknemers en de voor welke processen of systemen zij mandaat hebben wordt centraal bijgehouden in een register. Alleen het SMT mag hier wijzigingen in aanbrengen. Het mandaatregister wordt ieder kwartaal geëvalueerd.
  - Systeemeigenaren mogen alleen leesrechten hebben op het mandaatregister ter controle van het mandaatrecht van de indiener van het autorisatieverzoek.

- Wachtwoorden
  - Bij het beheer van gebruikerswachtwoorden is vastgelegd op welke wijze het initiële wachtwoord aan de gebruiker kenbaar wordt gemaakt en hoe gehandeld wordt bij het vergeten van het wachtwoord;
  - Verstrekte wachtwoorden moeten onmiddellijk na het eerste gebruik door de gebruiker worden gewijzigd.

Verder gelden alle eisen benoemt in dit hoofdstuk.

Referentie: *BIO versie 1.04zv beheersmaatregel 9.1.1, 9.2.1, 9.2.1.1, 9.2.1.2, 9.2.2, 9.2.2.1 & 9.2.2.3.*

7.1.2. Toegang tot netwerken en netwerkdiensten

Gebruikers

Men krijgt alleen toegang tot de netwerken en de netwerkdiensten waarvoor zij conform het functieprofiel bevoegd zijn. De gemeente hanteert hiervoor de procedure 'Autorisatieprocedure toegang netwerken en netwerkdiensten'. Deze procedure dient te bestaan uit de volgende deelprocedures:
- Aanvragen;
- Vrijgeven;
- Wijzigen;
- Spoed;
- Blokkeren;
- Verwijderen.

Apparatuur
Alleen geautoriseerde apparatuur kan toegang krijgen tot een netwerk met gemeentelijke informatie (zie hoofdstuk 11).

Bring Your Own Device
Het gebruik van persoonlijke apparatuur is niet toegestaan voor gemeentelijke werkzaamheden. Ongeautoriseerde apparatuur krijgt enkel toegang tot het openbare netwerk waar gemeentelijke informatie niet toegankelijk is (zie hoofdstuk 11).

Referentie: *BIO versie 1.04zv beheersmaatregel 9.1.2, 9.1.2.1 & 9.1.2.2.*

7.2. Beheer van toegangsrechten van gebruikers
Voor het beheer van toegangsrechten voor gebruikers zijn in het 'Logisch toegangsbeveiligingsbeleid' procedures vastgesteld waarin de gehele beheercyclus is opgenomen. Minimaal moeten de volgende procedures zijn beschreven:
- Aanvragen (registreren);
- Vrijgeven;
- Wijzigen;
- Spoed;
- Blokkeren;
- Verwijderen (afmelden).

Gebruikers krijgen uitsluitend toegang tot diensten en systemen middels eerdergenoemde procedures. Onder gebruikers kunnen ook andere systemen vallen.

Referentie: *BIO versie 1.04zv beheersmaatregel 9.2.1, 9.2.1.1 & 9.2.2.*

7.2.1. Controle autorisatieverzoek
De systeemeigenaar beoordeelt het autorisatieverzoek waarbij in ieder geval wordt gecontroleerd of:
1. Het aanvraag- of wijzigingsformulier volledig en op de juiste manier is ingevuld;
2. Het aanvraag- of wijzigingsformulier door een autorisatiebevoegde medewerker is ingediend en ondertekend;
3. Het autorisatieverzoek in overeenstemming is met de beveiligingseisen zoals vastgelegd in het overzicht van wel en niet toegestane combinaties van taken, zodat er geen met elkaar conflicterende bevoegdheden ontstaan die niet aan één gebruiker gekoppeld mogen worden;

Referentie: *BIO versie 1.04zv beheersmaatregel 9.2.1 & 9.2.1.1.*

7.2.2. Functieprofielen en autorisatiematrixen
Functieprofiel
Per functieprofiel dient er een autorisatiematrix aanwezig te zijn waar per systeem is vastgelegd wie toegang heeft tot welke informatiesystemen, welke gegevens binnen het systeem en welke acties de gebruiker mag uitvoeren.

Autorisatiematrixen worden bepaald op basis van een risicoanalyse. Functiescheiding is een verplicht onderdeel van deze analyse.

Autorisatiematrixen voor systemen
Systemen kunnen tevens gebruiker zijn van een ander systeem, hiervoor dienen aparte autorisatiematrixen opgesteld te worden op basis van een risicoanalyse.

Voor alle autorisaties geldt dat deze zo beperkt mogelijk gehouden moeten worden. Indien enkel leesrechten benodigd zijn worden enkel leesrechten gegeven.

Referentie: *BIO versie 1.04zv beheersmaatregel 9.2.2, 9.2.2.2 & 9.2.2.3.*

7.2.3. Beheren van speciale toegangsrechten

Het toewijzen en gebruik van speciale toegangsrechten dienen te worden beperkt en beheerst. Speciale toegangsrechten zijn vastgelegd in het deelproduct 'Risicovolle Profielen'. Gebruikers hebben toegang tot speciale bevoegdheden voor zover dat voor de uitoefening van hun taak noodzakelijk is. Dit wordt bepaald door het strategisch management (SMT). Gebruikers krijgen slechts toegang tot een noodzakelijk geachte set van applicaties. De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld door het strategisch management (SMT). Indien de speciale bevoegdheden niet meer noodzakelijk zijn voor het uitoefenen van de functie, worden de speciale bevoegdheden weer ingetrokken.

De volgende stappen behoren in overweging te worden genomen:

1. De speciale toegangsrechten behorend bij elk systeem of proces en de gebruikers aan wie ze moeten worden toegewezen, dienen te worden geïdentificeerd;
2. Speciale toegangsrechten dienen op basis van noodzaak tot gebruik per gebeurtenis aan gebruikers te worden toegekend in overeenstemming met het toegangsbeveiligingsbeleid;
3. Er dient een autorisatieprocedure en een verslaglegging van alle toegekende speciale toegangsrechten te worden bijgehouden. Speciale toegangsrechten worden niet verleend voordat de autorisatieprocedure is afgerond;
4. Voor het vervallen van speciale toegangsrechten dienen eisen te worden gedefinieerd;
5. Speciale toegangsrechten dienen te worden toekend aan een gebruikersidentificatie die verschilt van identiteiten die voor reguliere bedrijfsactiviteiten worden gebruikt;
6. De competenties van gebruikers met speciale toegangsrechten dienen regelmatig te worden beoordeeld om te verifiëren of ze in overeenstemming zijn met hun taken;
7. Toewijzingen van speciale toegangsrechten dienen regelmatig, ten minste maandelijks, te worden gecontroleerd om te waarborgen dat speciale toegangsrechten niet onbevoegd zijn verkregen;
8. Wijzigingen in speciale accounts dienen bijgehouden te worden in logbestanden voor de periodieke beoordeling;
9. Specifieke procedures dienen te worden vastgesteld en onderhouden om onbevoegd gebruik van gebruikersidentificaties voor algemeen beheer te voorkomen, in overeenstemming met de configuratiecapaciteiten van het systeem;
10. Voor gebruikersidentificaties voor algemeen beheer dient de geheimhouding van geheime authenticatie-informatie in acht te worden genomen als deze wordt gedeeld.

Referentie: *BIO versie 1.04zv beheersmaatregel 9.2.3 & 9.2.5.*

7.2.4. Beoordeling van toegangsrechten van gebruikers

Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen. Bij het beoordelen van toegangsrechten van gebruikers worden de volgende onderdelen in acht genomen:

- Toegangsrechten van gebruikers dienen regelmatig, ten minste eenmaal per halfjaar, en na wijzigingen, zoals promotie, degradatie of beëindiging van het dienstverband, te worden beoordeeld door de systeemeigenaar nadat de teamleider deze heeft geïnformeerd over personele wijzigingen;
- Indien de gebruiker een andere functie krijgt binnen de gemeente, dienen de toegangsrechten van de gebruiker te worden beoordeeld en opnieuw te worden toegekend;
- Toewijzingen van speciale toegangsrechten dienen regelmatig, ten minste maandelijks, te worden gecontroleerd om te waarborgen dat speciale toegangsrechten niet onbevoegd zijn verkregen;
- Wijzigingen in accounts dienen bijgehouden te worden in logbestanden voor de periodieke beoordeling;
- De opvolging van bevindingen is gedocumenteerd in centraal registratiesysteem en wordt behandeld als beveiligingsincident.

Referentie: *BIO versie 1.04zv beheersmaatregel 9.2.5.*

7.2.5. Toegangsrechten intrekken of aanpassen

De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast. De teamleider is verantwoordelijk voor de coördinatie hiervan.

Bij beëindiging van het dienstverband worden alle toegangsrechten van een persoon voor informatie en bedrijfsmiddelen ingetrokken. Dit bevat tevens de fysieke en logische toegangsrechten. Intrekking of aanpassing vindt plaats door verwijdering, intrekking of vervanging van sleutels, identificatiekaarten, informatie verwerkende faciliteiten of abonnementen.

Indien een medewerker die uit dienst treedt of een externe gebruiker wachtwoorden kent van gebruikersidentificaties die actief blijven, dan behoren deze bij beëindiging of wijziging van het dienstverband, contract of overeenkomst te worden gewijzigd. De teamleider informeert de eigenaar van de algemene identiteit dat een persoon die gebruik maakte van deze identiteit uit dienst is of een andere functie vervult. De eigenaar van de identiteit is verantwoordelijk voor het doorvoeren van de noodzakelijke wijzigingen.

Referentie: *BIO versie 1.04zv beheersmaatregel 9.2.6.*

7.3. Verantwoordelijkheden van gebruikers
Gebruikers zijn verantwoordelijk voor het beschermen van hun authenticatie-informatie. Hiermee wordt onbevoegde toegang door gebruikers, en van beschadiging of diefstal van informatie en IT-voorzieningen beperkt.

Gebruikers behoren beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden. Aan de medewerkers is een set gedragsregels aangereikt met daarin minimaal het volgende:
- Wachtwoorden worden niet opgeschreven;
- Gebruikers delen wachtwoorden nooit met anderen;
- Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde;
- Gebruikers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordkluis.

Referentie: *BIO versie 1.04zv beheersmaatregel 9.3.1.*

7.4. Toegangsbeveiliging van systemen en toepassing

7.4.1. Beperking toegang tot informatie
Standaard dient toegang tot informatie beperkt te worden tot personen die zonder de informatie hun werk niet kunnen uitvoeren, het zogenaamde 'need-to-know' principe. De toegang tot informatie dient gekoppeld te zijn aan functieprofielen (rollen) waarbij personen aan de rollen gekoppeld worden. Voor digitale informatie dient de toegang beperking, na toekenning van de rollen, automatisch te geschieden.

Per functieprofiel dient er per informatiebron, waar de functie toegang tot moet krijgen, een autorisatieprocedure worden opgesteld waarin staat:
- Wat de acties zijn met betrekking tot de informatie;
  - *Bijvoorbeeld: alleen lezen of ook bewerken.*
- Hoe lang de toegang tot de informatiebron geldt;
- Hoe vaak de informatiebron mag worden geraadpleegd per gedefinieerde periode;
  - *Bijvoorbeeld: 10x per jaar of onbeperkt.*
- Wat de reden is dat het functieprofiel de gedefinieerde acties mag uitvoeren op de informatiebron.

De proceseigenaars zijn verantwoordelijk voor het opstellen van de autorisaties per functieprofiel en dienen deze aan te leveren bij het team Informatiemanagement, HR en de CISO. Jaarlijks dienen de autorisaties door de teamleiders geëvalueerd te worden. De CISO / ISO dient jaarlijks steekproefsgewijs de autorisaties te controleren vanuit het oogpunt informatiebeveiliging. In geval het een digitale informatiebron betreft, is de systeemeigenaar verantwoordelijk voor de inregeling van de autorisaties. Indien het een fysieke informatiebron betreft is de eigenaar van de informatiebron verantwoordelijk voor de controle van de autorisaties.

Referentie: *BIO versie 1.04zv beheersmaatregel 9.4.1.*

7.4.2a Beveiligde inlogprocedure
Op basis van het beleid voor logische toegangsbeveiliging behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure. Deze inlogprocedure dient:
- Geen systeem- of toepassingsidentificatoren te tonen voordat het inlogproces met succes is afgerond;
- Een algemene waarschuwing te tonen dat de computer alleen toegankelijk is voor bevoegde gebruikers;
- Tijdens de inlogprocedure geen hulpboodschappen weer te geven waarmee onbevoegde gebruikers hun doel kunnen bereiken;
- De inloginformatie pas na invoer van alle gegevens te valideren. Indien zich een fout voordoet, dient het systeem niet aan te geven welk deel van de gegevens juist of onjuist is;

- Bescherming te bieden tegen inlogpogingen die met grove middelen worden uitgevoerd;
- Niet-succesvolle en succesvolle pogingen te registreren;
- Een informatiebeveiligingsgebeurtenis te initiëren als een poging tot of een succesvolle schending van de inlogbeheersmaatregelen is vastgesteld;
- De volgende informatie te tonen nadat het inloggen met succes is voltooid:
  - Datum en tijdstip waarop de vorige keer met succes is ingelogd;
  - Details van niet-succesvolle pogingen om in te loggen sinds de vorige succesvolle poging om in te loggen;

- Een wachtwoord dat wordt ingevoerd niet weer te geven;
- Geen ongecodeerde wachtwoorden via een netwerk te versturen;
- Inactieve sessies na een bepaalde tijd van inactiviteit te beëindigen, vooral op locaties met een hoog risico, zoals openbare of externe locaties die buiten het beveiligingsbeheer van de gemeente vallen, of op mobiele appraten;
- De verbindingstijd te beperken om extra beveiliging te bieden voor toepassingen met een hoog risico en de mogelijkheden voor onbevoegde toegang te verkleinen.

Als vanuit een niet vertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van multi-factor authenticatie.

Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.

Referentie: *BIO versie 1.04zv beheersmaatregel 9.4.2.*

7.4.3. Systeem voor wachtwoordbeheer

Vanuit de CISO dient een voorschrift met betrekking tot het wachtwoordbeheer te worden opgesteld en jaarlijks te worden geëvalueerd. Het voorschrift is verplicht voor alle technische componenten waar middels wachtwoorden toegang gegeven wordt aan informatie. Het voorschrift dient ten minste het volgende te bevatten:

- Alle onderstaande eisen dienen minimaal te voldoen aan de richtlijnen zoals aangegeven in de nieuwste of nieuwst aangekondigde BIO versie;
- Eisen aan de minimale lengte van het wachtwoord;
  - Waarbij onderscheid gemaakt mag worden tussen het wel en niet hanteren van multi-factor authenticatie.

- Eisen aan het maximaal aantal foutieve inlogpogingen;
- Eisen aan de tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen;
- Eisen aan de periode waarna een wachtwoord opnieuw ingesteld moet worden;
  - Waarbij onderscheid gemaakt mag worden tussen het wel en niet hanteren van multi-factor authenticatie.

- Eisen aan de geldigheidsduur van initiële wachtwoorden en wachtwoorden die gereset zijn;
- Eisen aan de geldigheidsduur van wachtwoorden die voldoen aan het beleid;
- Eisen aan de geldigheidsduur van wachtwoorden gebruikt in systemen die technisch niet kunnen voldoen aan dit beleid.

Indien gebruik wordt gemaakt van een wachtwoordkluis dient deze aan de volgende voorwaarden te voldoen:
- De wachtwoordenkluis dient voor ieder systeem/ applicatie een ander wachtwoord te hanteren;
- De wachtwoordenkluis mag de gegevens niet opslaan buiten het grondgebied van de Europese Unie;
- De wachtwoorden in de wachtwoordenkluis dienen versleuteld opgeslagen te worden conform een versleutelingsmethode benoemt in het hoofdstuk 8 (Cryptografie) van dit beleid.

Referentie: *BIO versie 1.04zv beheersmaatregel 9.4.3.*

7.4.4. Speciale systeemhulpmiddelen gebruiken

Met systeemhulpmiddelen worden software- en hardwarecomponenten, zoals firewalls, encryptiesoftware, antivirussoftware en toegangscontrole, bedoeld die gebruikt worden om de IT-infrastructuur en IT-processen te ondersteunen en te beheren. Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moet worden beperkt en nauw-

keurig worden gecontroleerd. Alle onnodige systeemhulpmiddelen moeten worden verwijderd of onbruikbaar worden gemaakt.

Alleen bevoegd personeel heeft toegang tot de systeemhulpmiddelen. Bevoegdheid wordt voorgeschreven vanuit het functieprofiel en dient te worden bekrachtigd door het SMT.

Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is minimaal twee jaar beschikbaar voor onderzoek.

Referentie: *BIO versie 1.04zv beheersmaatregel 9.4.4.*

7.4.5. Toegangsbeveiliging op programmabroncode

Toegang tot de programmabroncode behoort te worden beperkt zodat introductie van onbevoegde functionaliteit en onbedoelde wijzigingen te voorkomen, alsmede om de vertrouwelijkheid van waardevolle intellectuele eigendom te handhaven. Dit wordt bereikt door de code gecontroleerd centraal op te slaan, waarbij het volgende in acht wordt genomen:

- Broncodebibliotheken worden niet in operationele systemen opgeslagen;
- De programmabroncode en de broncodebibliotheek worden beheerd in overeenstemming met de vastgestelde procedures;
- Ondersteunend personeel heeft geen onbeperkte toegang tot broncodebibliotheken;
- Het updaten van broncodebibliotheken en samenhangende items en het verstrekken van broncodes aan programmeurs vindt alleen plaats na ontvangst van een passende autorisatie;
- Programma-uitdraaien worden in een beveiligde omgeving bewaard;
- Van elke toegang tot broncodebibliotheken wordt een auditlogbestand bijgehouden;
- Onderhouden en kopiëren van broncodebibliotheken worden aan strike procedures voor wijzigingsbeheer te worden onderworpen.

Referentie: *BIO versie 1.04zv beheersmaatregel 9.4.5.*

8. Cryptografie

8.1. Beleid inzake het gebruik van cryptografische beheersmaatregelen

Voor het beoordelen of cryptografische maatregelen ingezet moeten worden, dient informatie te zijn geclassificeerd volgens de informatieclassificatie methode benoemt in hoofdstuk 5. Voor cryptografische maatregelen wordt onderscheid gemaakt tussen communicatie van informatie en opslag van informatie.

De door de gemeentelijke CISO goedgekeurde lijst van encryptiemaatregelen dient te voldoen aan of moeten expliciet aansluiten bij de standaarden op de ‘pas toe of leg uit’-lijst van het Forum Standaardisatie[3].

8.1.1. Communicatie van informatie

Alleen voor digitale communicatie van informatie gelden de cryptografische maatregelen.

Netwerkcommunicatie

Alle informatie die via netwerken gecommuniceerd wordt dient, waar technisch mogelijk, met TLS te worden beveiligd. Voor ieder systeem dient het stappenplan uit de nieuwste versie van het ‘ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)[4] de NCSC te worden doorlopen. De gehanteerde instellingen dienen in een centraal register per systeem vastgelegd te worden waarbij de instellingen geclassificeerd worden aan de hand van de in het ‘ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)’. Instellingen met classificatie ‘onvoldoende’ zijn niet toegestaan.

De systeemeigenaar is verantwoordelijk voor de instelling van de systemen en de vastlegging in het centrale instellingen register. De CISO of ISO voert een jaarlijkse controle uit op het register. Indien de CISO wijzigingen in de instellingen noodzakelijk acht dient de systeemeigenaar dit door te voeren.

Uitzonderingen waarbij geen gebruik gemaakt kan worden van TLS of van adequate instellingen dient er een uitzondering aangevraagd te worden bij de CISO. De CISO registreert eventuele uitzonderingen inclusief reden en eventuele additionele maatregelen in het centrale register.

Andere vormen van digitale communicatie

3) https://www.forumstandaardisatie.nl/open-standaarden
4) https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1

Voor andere vormen van digitale communicatie geldt dat voor de classificatieniveaus 'Midden' en 'Hoog' gebruik gemaakt dient te worden van cryptografische beheersmaatregelen.

Verwijderbare media
Verwijderbare media (bijvoorbeeld usb-sticks of Dvd's) dienen volledig versleuteld te zijn met een versleutelingstechniek die op de lijst van door de gemeentelijke CISO goedgekeurde versleutelingstechnieken staat.

Chatapplicaties
Er wordt geen gebruik gemaakt van niet goedgekeurde chatapplicaties.

Digitaal telefoneren
Voor digitaal telefoneren dient, waar technisch mogelijk, gebruik gemaakt te worden van 'end-to-end' encryptie. Deze encryptie dient in de betrokken programma's aangezet te worden.

Elektronische berichtenuitwisseling
Het bericht mag bij digitale berichtenuitwisseling (bijvoorbeeld e-mail) geen informatie met classificatie 'Midden' of 'Hoog' bevatten. Een eventuele bijlage mag deze informatie wel bevatten indien de bijlage middels encryptiemaatregelen wordt verstuurd. De encryptiemaatregelen en hulpapplicaties die hiervoor van toepassing zijn worden bijgehouden door de CISO op de lijst met goedgekeurde versleutelingstechnieken.

Referentie: *BIO versie 1.04zv beheersmaatregel 10.1.1.*

8.1.2. Opslag van informatie
Digitale informatie die wordt opgeslagen dient beveiligd te worden. Qua cryptografische maatregelen wordt onderscheid gemaakt tussen apparaten die door de gemeente worden gehanteerd en systemen die worden afgenomen.

Apparaten
Van alle apparaten die de gemeente hanteert, en waar informatie op kan worden opgeslagen, dient het opslagmedium volledig versleuteld te zijn. Hieronder vallen bijvoorbeeld laptops, mobiele telefoons, servers, IoT apparaten en vaste computers. Deze encryptiemaatregel dient automatisch afgedwongen te worden op alle apparaten waar de gemeente eigenaar van is of die voor gemeentelijke werkzaamheden worden gebruikt. De proceseigenaar belast met het uitgeven van apparaten is verantwoordelijk voor het voldoen aan bovenstaande.

Systemen
Informatie die buiten apparaten wordt opgeslagen waar de gemeente eigenaar van is en die geclassificeerd zijn als 'Midden' of 'Hoog', dient versleuteld te worden opgeslagen. De encryptiemaatregelen die hiervoor van toepassing zijn worden bijgehouden door de CISO op de lijst met goedgekeurde versleutelingstechnieken.

Referentie: *BIO versie 1.04zv beheersmaatregel 10.1.1.*

8.2. Sleutelbeheer
Cryptografische sleutels dienen beheerd te worden conform de ISO11770 standaard. Een sleutelbeheersysteem dient te zijn gebaseerd op een overeengekomen pakket van normen, procedures en beveiligingsmethoden voor:

- Het aanmaken van sleutels voor verschillende cryptografische systemen en toepassingen;
- Het verstrekken en verkrijgen van openbare sleutelcertificaten;
- Het verspreiden van sleutels onder de beoogde entiteiten en een instructie hoe de sleutels na ontvangst dienen te worden geactiveerd;
- Het opslaan van sleutels en de wijze waarop bevoegde gebruikers toegang tot sleutels krijgen;
- Het wijzigen of updaten van sleutels, met inbegrip van regels over wanneer en hoe sleutels dienen te worden gewijzigd;
- Het omgaan met gecompromitteerde sleutels;
- Het intrekken van sleutels, met inbegrip van hoe sleutels dienen te worden teruggetrokken of gedeactiveerd;
- Het herstellen van sleutels die verloren of gecorrumpeerd zijn;
- Een back-up maken of archiveren van sleutels;
- Het vernietigen van sleutels;
- Het registreren en auditen van aan sleutelbeheer gerelateerde activiteiten.

Referentie: *BIO versie 1.04zv beheersmaatregel 10.1.2 & 10.1.2.1.*

8.2.1. Reservecertificaten
Voor alle benodigde certificaten dient een risicoanalyse aanwezig te zijn. De risicoanalyse dient minimaal de volgende zaken te bevatten:
- Is de aanwezigheid van het certificaat cruciaal voor de kritische bedrijfsprocessen.

Aan de hand van de risicoanalyse dient de afweging gemaakt te worden om contractuele afspraken op te nemen over reserve certificaten van een alternatieve leverancier.

Referentie: *BIO versie 1.04zv beheersmaatregel 10.1.2.2.*

8.2.2. PKI-overheidscertificaten
Het gebruik van PKI-overheidscertificaten is niet langer toegestaan daar deze in december 2022 landelijk zijn ingetrokken. Voor informatie met classificatieniveaus 'Midden' en 'Hoog' zijn zogenaamde 'self-signed' certificaten eveneens niet toegestaan.

Referentie: *BIO versie 1.04zv beheersmaatregel 10.1.2.1.*

9. Fysieke beveiliging en beveiliging van de omgeving
9.1. Beveiligde gebieden

9.1.1. Fysieke beveiligingszone
De fysieke ruimten binnen de gemeente moeten zijn ingedeeld conform 'Handreiking toegangsbeleid v2.01' waarbij onderstaande zonering is voorgeschreven:

Tabel 6:Beschrijving fysieke beveiligingszone

Zone	Beschrijving
Zone 0	Het terrein Het terrein om het gebouw is vrij toegankelijk binnen vastgestelde toegangstijden. Toegang tot binnenterrein, rijwielstalling via slagboom/identificatie.
Zone 1	Publiekszone en Restaurant De publiekshal. In de hal is een receptie; hier wordt permissie gegeven voor het betreden van de volgende veiligheidszone.
Zone 2	Raadszaal, vergaderruimten en Balie Burgerzaken Het vergadercentrum dat regelmatig toegankelijk moet zijn voor het publiek, zoals de Raadszaal, de fractiekamers en de perskamer. Op vertoon van een afspraakbevestiging krijgt publiek toegang tot de balie van Burgerzaken van gemeente Medemblik.
Zone 3	Standaard werkgebied Dit betreft zones die uitsluitend bereikbaar zijn met toegangspassen voor geautoriseerde medewerkers. De kantoorwerkplekken voor de ambtelijke organisatie (inclusief de werkplekken Publiekszaken).
Zone 4	Bijzonder werkgebied Er zijn meerdere ondersteunende ruimten, waarbij de toegang geregeld wordt met een sleutelplan of een elektronische toegangsbeveiliging en alarmering. Het gaat om: • Laad- en losvoorzieningen (logistieke ruimten); • Kluis paspoorten, contant geld (specifieke ruimtelijke beveiliging conform wet- en regelgeving BRP); • Archiefruimtes; • Server en netwerkruimten (op dit moment in beheer van SSC DeSom); • Off-site back-up locatie (op dit moment in beheer van SSC DeSom);

	• Technische ruimtes die onderdelen bevatten die onderdelen bevatten die cruciaal zijn voor de dienstverlening, als voorbeeld de aansluitingen voor nutsvoorzieningen.

Uitwerking van de exacte inrichting van de locaties van gemeente Medemblik zijn vastgelegd in een door het college vastgesteld 'Plan fysieke toegangsbeveiliging'. Dit plan dient te voldoen aan de eisen zoals beschreven in dit hoofdstuk. Het plan heeft een maximale geldigheidsduur van 3 jaar.

Beoordeling en advisering ten aanzien van fysieke beveiligingszones is belegd bij de CISO.

Referentie: *BIO versie 1.04zv beheersmaatregel 11.1.1 en 11.1.1.1.*

9.1.2. Fysieke toegangsbeveiliging

De verschillende zones worden beschermd door passende toegangsbeveiliging die ervoor zorgen dat alleen bevoegd personeel toegang krijgt. De volgende eisen gelden minimaal met betrekking tot het fysieke toegangsbeleid:

Alle zones:
- Concrete beveiligingsrisico's worden conform afspraken, gecommuniceerd aan relevante collega's binnen het (informatie)beveiligingsdomein van de gemeente;
- Fysieke toegangsmiddelen vallen onder verantwoordelijkheid van HR, Facilitaire Zaken en gebouwenbeheer.

Vanaf zone 1 (Publiekszone):
- Iedereen die werkzaamheden voor de gemeente verricht (zoals; medewerkers, contractanten en externen) dragen zichtbare gemeentelijke identificatie;
- Aankomst- en vertrektijden van alle aanwezigen worden geregistreerd inclusief datum.

Zone 2 (Regelmatig toegankelijke publiekszone):
- Op vertoon van een afspraakbevestiging krijgt publiek toegang tot de balie van Burgerzaken van gemeente Medemblik;
- Raadzalen en fractiekamers worden beschikbaar gesteld voor het publiek wanneer er een vergadering is die publiek bijgewoond dient te worden;
    - In alle gevallen zijn de raadzalen en fractiekamers alleen toegankelijk voor geautoriseerde personen met geldige toegangspassen.

Zone 3 (Standaard werkgebied):
- Zone 3 is alleen toegankelijk voor geautoriseerde medewerkers met geldige toegangspassen.
- Alle toegangsacties van personeel worden gelogd;
- De gemeentewerven vallen onder zone 3;
- Het werkgebied Publiekszaken is alleen toegankelijk voor medewerkers van team Publiekszaken en de BHV;
- Fysieke informatie die geclassificeerd is als 'Midden' dienen te worden opgeborgen in brandkasten die zijn verankerd aan het pand. Op basis van de classificatie en de verantwoordelijkheden omtrent de informatie heeft alleen bevoegd personeel toegang tot de beveiligde brandkasten;
- Bij toegang tot zone 3 of hoger wordt gebruik gemaakt van beperking in de toegang die waarborgt dat enkel de geautoriseerde personen toegang krijgen en dat ongeautoriseerde niet kunnen meelopen met de geautoriseerde persoon.

Zone 4 (Bijzonder werkgebied):
- Fysieke informatie die geclassificeerd is met 'Hoog' dienen te worden opgeborgen in een brandwerende kluis die verankerd is aan het pand. De kluis dient voor een zeer beperkt aantal medewerkers toegankelijk te zijn. Hiervoor dient een toegangsprocedure zone 4 te zijn;
- Toegang behoort te worden goedgekeurd en periodiek te worden gemonitord;
- Alle toegangsacties worden gelogd in een logboek dat dagelijks geëvalueerd moet worden door de teamleider Facilitair. Omissies dienen per direct te worden gecommuniceerd met de teamleiders werkzaam in zone 4 en de CISO;
- Iedereen die enkel voor kortdurende werkzaamheden aanwezig dienen te zijn in zone 4 (bijv. onderhoudsmonteurs) mogen alleen werken onder permanente aanwezigheid van één van de geautoriseerde medewerkers en mogen niet zelfstandig de zone betreden of verlaten. Dit dient te worden vastgelegd in de toegangsprocedure voor zone 4.

Referentie: *BIO versie 1.04zv beheersmaatregel 11.1.2 en 11.1.2.1.*

9.1.3. Kantoren, ruimten en faciliteiten beveiligen

Fysieke beveiliging

Voor kantoren, ruimten en faciliteiten zijn maatregelen ontworpen en vastgelegd in het fysieke beveiligingsplan van de gemeente. De beveiliging van faciliteiten dient in het fysieke beveiligingsplan minimaal de volgende elementen te bevatten:

Faciliteiten

- Faciliteiten die toegang geven tot gemeentelijke informatie met classificatie niveau 'Laag' of hoger, of deze informatie bevatten, dienen minimaal te zijn gelegen in zone 3;
- Faciliteiten die gemeentelijke informatie bevatten met classificatie niveau 'Hoog' dienen te zijn gelegen in zone 4;
- Locaties van faciliteiten die informatie bevatten of verwerken dienen enkel kenbaar gemaakt te worden aan medewerkers geautoriseerd voor die specifieke informatie;
- Adresboeken, interne telefoonboeken en niet publiekelijke e-mailadressen zijn niet vrij toegankelijk voor onbevoegden;
- Niet uitgegeven toegangsmiddelen die toegang geven tot zone 3 worden zodanig veilig opgeborgen dat deze enkel toegankelijk zijn voor medewerkers van Facilitaire Zaken die de toegangsmiddelen uitgeven en de teamleider van Facilitaire Zaken is verantwoordelijk voor het toezicht hierop;
- Niet uitgegeven toegangsmiddelen die toegang geven tot zone 4 worden zodanig veilig opgeborgen dat deze enkel toegankelijk zijn voor de strategisch manager verantwoordelijk voor de teams in zone 4;
- Niet uitgegeven toegangsmiddelen die toegang geven tot de bij zone 3 genoemde brandkasten dienen enkel toegankelijk te zijn voor de teamleider verantwoordelijk voor de in de brandkast opgeslagen informatie;
- Niet uitgegeven toegangsmiddelen die toegang geven tot de bij zone 4 genoemde kluizen dienen enkel toegankelijk te zijn voor de teamleider verantwoordelijk voor de in de die specifieke kluis opgeslagen informatie;
- De toegangsmiddelen zijn ingericht op basis van een sleutelplan en vallen onder de procedure 'Sleutelbeheer' waarvoor de teamleider Facilitaire Zaken verantwoordelijk is.

Ruimten

- Werkplekken die zichtbaar zijn vanuit de publieke ruimte dienen te worden voorzien van maatregelen die de zichtbaarheid dusdanig belemmeren dat de werkplek niet meer zichtbaar is;
- Ruimten waarin gewerkt wordt met informatie met classificatieniveau 'Laag' of hoger dienen zodanig ingericht te zijn dat wordt voorkomen dat vanuit publiek beschikbare ruimten informatieoverdracht of activiteiten hoorbaar of zichtbaar zijn.

Referentie : *BIO versie 1.04zv beheersmaatregel 11.1.3 en 11.1.3.1.*

9.1.4. Sleutelplan

Toegangsmiddelen worden in dit hoofdstuk aangeduid als sleutels en betreffen bedrijfsmiddelen die dienen te voldoen aan het bedrijfsmiddelen beleid in hoofdstuk 5.

Voor zone 3, zone 4, de zone 3 brandkasten én de zone 4 kluizen dienen in totaal 4 sleutelplannen opgesteld te worden. De verantwoordelijkheid is als volgt belegt:

- Teamleider Inkoop, JZ en FaZa is verantwoordelijk voor 'sleutelplan zone 3' en 'sleutelplan brandkasten zone 3';
- De teamleider van het betreffende team in zone 4 is verantwoordelijk voor 'sleutelplan zone 4';
- De teamleider verantwoordelijk voor de informatie in de zone 4 kluis is verantwoordelijk voor 'sleutelplan kluizen zone 4'.

Alle sleutelplannen dienen minimaal te voldoen aan de volgende eisen:

- De verantwoordelijke is verantwoordelijk voor het opstellen en het bijwerken van het sleutelplan;
- Het sleutelplan wordt drie jaarlijks geëvalueerd door de verantwoordelijke. De evaluatie en diens resultaten worden vastgelegd en de betrokkenen worden hierover geïnformeerd;
- Het sleutelplan is goedgekeurd door het SMT met advies van de CISO;
- In het sleutelplan is mimimaal opgenomen:
  - Wie verantwoordelijk is voor de uitgifte en inname van fysieke sleutels;
  - Wie de centrale registratie van sleutels in omloop bijhoudt;
  - Wanneer en aan wie fysieke sleutels mogen worden uitgereikt;
  - Wie de periodieke controle op de centrale registratie en de voorraad sleutels uitvoert om de volledigheid van de sleutels vast te stellen.

Referentie: *BIO versie 1.04zv beheersmaatregel 11.1.3 en 11.1.3.1.*

9.1.5. Beschermen tegen bedreigingen van buitenaf

De gemeente moet een centrale inventarisatie bijhouden waarin per dienstverleningsproces is beschreven welke (papieren) archieven en apparatuur kritisch zijn. De inventarisatie dient jaarlijks geëvalueerd te worden, het strategisch managementteam (SMT) is hiervoor verantwoordelijk. In het plan fysieke toegangsbeveiliging dienen de volgende zaken minimaal te zijn vastgelegd:

- Welke dienstverleningsprocessen absoluut niet verstoord mogen worden;
  - Welke apparatuur en papieren archieven hierin kritisch zijn.

- Per bovengenoemde apparatuur en papierarchief welke maatregelen worden genomen ter voorkoming van verstoringen in het geval van natuurrampen, ongewenste menselijke handelingen en andere bedreigingen van buitenaf aan de hand van een risicoanalyse.;
- Periodieke herbeoordeling van de risicoanalyse en bovengenoemde maatregelen.

Verder dient informatie geclassificeerd als 'Midden' of 'Hoog' redundant opgeslagen te worden in geografisch en logisch gescheiden locaties.

Referentie: *BIO versie 1.04zv beheersmaatregel 11.1.4, 11.1.4.1 en 11.1.4.2.*

9.1.6. Werken in beveiligde gebieden

Zone 4 gebieden worden beschouwd als beveiligde gebieden, alsmede andere gebieden die de gemeente aanwijst als beveiligd. Voor het werken in beveiligde gebieden dienen procedures te zijn ontwikkeld die actief worden toegepast. De procedures dienen minimaal aan de volgende eisen te voldoen:

- Personeel behoort alleen dankzij 'need-to-know' bekend te zijn met het bestaan van of de activiteiten binnen een beveiligd gebied;
  - De procedure dient concrete toetsbare eisen te stellen aan het begrip 'need-to-know'.

- Zonder toezicht wordt niet gewerkt in beveiligde gebieden, zowel om veiligheidsredenen als om geen gelegenheid te bieden voor kwaadaardige activiteiten;
- Leegstaande beveiligde ruimten behoren fysiek te zijn afgesloten en periodiek geïnspecteerd te worden;
- Beeld- en geluidsopnameapparatuur, zoals in mobiele apparatuur, wordt niet toegelaten in de beveiligde ruimten, tenzij goedgekeurd;
- Bezoekers van kritieke faciliteiten:
  - Worden slechts toegang geboden voor vastgestelde doeleinden;
  - Worden continu aan toezicht onderworpen;
  - Worden gemonitord bij aankomst en vertrek;
  - Krijgen instructie over de beveiliging van de omgeving en van de noodprocedures en worden bewust gemaakt van de beveiligingsregels;
  - Wordt verteld dat het gebruik van beeld- en geluidopnamemateriaal/apparatuur niet is toegestaan;
  - Dragen verplicht een badge.

De verantwoordelijkheid van het bijhouden van de procedures ligt bij de strategisch manager wiens afdeling of teamleider onder de beveiligde gebieden vallen.

Referentie: *BIO versie 1.04zv beheersmaatregel 11.1.5.*

9.1.7. Laad- en loslocaties

De inrichting en maatregelen van laad- en loslocaties dienen te worden vastgelegd in het plan fysieke toegangsbeveiliging waarbij de onderstaande aandachtpunten terug moeten komen:

- Verdachte brieven en pakketten in postkamers en laad- en loslocaties dienen conform een vooraf opgestelde procedure afgehandeld te worden;
- Laad- en loslocaties zijn beperkt tot geïdentificeerd en bevoegd personeel;
- Laad- en loslocaties zijn zo ontworpen dat goederen geladen en gelost kunnen worden, zonder dat de leverancier toegang heeft tot andere delen van het gebouw;
- Buitendeuren van laad- en loslocaties zijn beveiligd als de binnendeuren open zijn;
- Materialen worden bij binnenkomst alleen aangenomen indien hier een inkooporder voor is die overeenkomt met de bestelbon;
- Materialen worden bij binnenkomst gecontroleerd en onderzocht op explosieven, chemicaliën of andere gevaarlijke materialen voordat ze vanaf ene laad- en loslocatie worden overbracht;
- Materialen worden bij binnenkomst geregistreerd en de desbetreffende verantwoordelijke voor het materiaal wordt op de hoogte gebracht;
- Inkomende en uitgaande zendingen zijn fysiek gescheiden;

- Inkomende materialen worden gecontroleerd op mogelijk aanwijzingen voor vervalsing tijdens het transport. Bij ontdekte vervalsing wordt dit direct aan beveiligingspersoneel gemeld.

Referentie: *BIO versie 1.04zv beheersmaatregel 11.1.6.*

9.2. Apparatuur

9.2.1. Plaatsing en bescherming apparatuur

Alle apparatuur die geplaatst is dient beschermt te zijn tegen toegang tot onbevoegden of bedreigingen van buitenaf. De proceseigenaar is verantwoordelijk voor de adequate bescherming van deze apparatuur, dit geldt zowel voor apparatuur die geplaatst is binnen de huisvesting van de gemeente als apparatuur dat buiten op locatie is. Per apparaat categorie dient vastgelegd te zijn welke maatregelen zijn genomen tegen:

- Diefstal;
- Weglekken van informatie;
- Blikseminslag indien apparatuur op een buitenlocatie wordt geplaatst;
- Overspanningen waardoor apparatuur beschadigd kan raken.

Referentie: *BIO versie 1.04zv beheersmaatregel 11.2.1.*

9.2.2. Nutsvoorzieningen

Onder nutsvoorzieningen vallen alle voorzieningen zoals beschreven door de Nederlandse Overheid Referentie Architectuur (NORA)[5].

De Specialist Gebouwen is belast met de verantwoordelijkheid over nutsvoorzieningen en draagt zorg voor een opgesteld, beheerd en geaccordeerd nutsvoorzieningen plan, waarin onderstaande minimaal is beschreven en geïmplementeerd:

- Nutsvoorzieningen zijn conform technische beschrijving van de fabrikant en de lokale wettelijke eisen geïnstalleerd;
- Nutsvoorzieningen zijn centraal geregistreerd;
- Nutsvoorzieningen worden regelmatig onderzocht naar de toereikendheid van de capaciteit, interactie met andere nutsvoorzieningen en de toereikendheid met het oog op de groei en toekomst van de gemeente;
- Nutsvoorzieningen worden periodiek geïnspecteerd en getest, om na te gaan dat deze nutsvoorzieningen correct functioneren;
- Alarmsystemen zijn geïmplementeerd om disfunctioneren van nutsvoorzieningen op te sporen;
- Nutsvoorzieningen hebben meervoudige voedingen met verschillende fysieke route om het risico op uitval tegen te gaan;
- Noodverlichting en (nood) communicatiemiddelen zijn aanwezig;
- Nabij nooduitgangen en ruimten waar apparatuur aanwezig is, zijn noodschakelaars en knoppen waarmee stroom, water, gas of andere voorzieningen kunnen worden uitgeschakeld;
- Netwerkverbindingen zijn redundant en hebben meerdere fysieke routes van meerdere aanbieders.

Referentie: *BIO versie 1.04zv beheersmaatregel 11.2.2.*

9.2.3. Beveiliging van communicatiekabels

Voedings- en telecommunicatiekabels dienen te worden beschermd tegen interceptie, verstoring of schade, waarbij:

- Communicatiekabels dienen bij voorkeur ondergronds aangelegd te worden;
- Voedings- en telecommunicatiekabels te allen tijde beveiligd zijn en niet toegankelijk voor onbevoegden;
- Wordt voldaan aan:
  - o TIA-942: Telecommunication Infrastructure Standard for Data Centers
  - o NEN-EN 50600: Europese normenreeks voor datacenters
  - o NPR 5313: Richtlijn voor datacenters (2014)
- Bovenstaande eisen gelden voor alle communicatiekabels die de gemeente gebruikt, zowel binnen als buiten het eigen terrein.

Referentie: *BIO versie 1.04zv beheersmaatregel 11.2.3.*

5) https://www.noraonline.nl/wiki/BIO_(Baseline_Informatiebeveiliging_Overheid)

9.2.4. Onderhoud apparatuur

Apparatuur wordt correct onderhouden om de beschikbaarheid en integriteit ervan te waarborgen.

Fysieke apparatuur

Bij het onderhouden van fysieke apparatuur wordt het volgende in acht genomen:

- Apparatuur wordt onderhouden volgens de door de leverancier aanbevolen intervallen voor servicebeurten en voorschriften;
- Reparaties en onderhoudsbeurten aan apparatuur worden alleen uitgevoerd door bevoegd onderhoudspersoneel;
- Reparaties van en onderhoud aan apparatuur (hardware) worden op locatie en door bevoegd personeel uitgevoerd, tenzij er geen data (meer) op het apparaat aanwezig is (zie paragraaf 9.2.7);
- Van alle vermeende en daadwerkelijke fouten en van al het preventieve en correctieve onderhoud worden op een centrale plek registraties bijgehouden;
- Voldaan wordt aan alle onderhoudseisen die door verzekeringspolissen zijn opgelegd;
- Voordat apparatuur na onderhoud weer in bedrijf wordt gesteld, wordt een inspectie uitgevoerd om te waarborgen dat niet met de apparatuur geknoeid is en dat deze voldoende functioneert.

Onderhoud van software op apparatuur

Wanneer de apparatuur software bevat wordt het volgende in acht genomen:

- Voor software is een updatebeleid van kracht waarin wordt aangegeven:
  - Hoe ver software mag achterlopen op de meest recente versie.
  - Hoe software bijgewerkt dient te worden.
  - Hoe men controleert dat deze tijdig bijgewerkt is.
  - Hoe de verantwoordelijkheden ten aanzien van updates zijn belegt.

Onderhoud van servers

In het kader van het onderhoud van servers zijn de volgende aanvullende eisen van kracht:

- Voor onderhoud vanuit interne of externe locaties worden passende maatregelen getroffen;
- Voordat servers na onderhoud weer in bedrijf worden gesteld, vindt een inspectie plaats om te waarborgen dat niet is geknoeid met de server en dat deze nog steeds of weer goed functioneert.

Referentie: *BIO versie 1.04zv beheersmaatregel 11.2.4.*

9.2.5. Verwijdering van bedrijfsmiddelen

Bedrijfsmiddelen (in het bijzonder apparatuur, informatie en software) worden niet meegenomen zonder voorafgaande goedkeuring via de in hoofdstuk 6 beschreven procedure.

Referentie: *BIO versie 1.04zv beheersmaatregel 11.2.5.*

9.2.6. Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein

Bedrijfsmiddelen die zich buiten het primaire werkterrein van de gemeente bevinden dienen te voldoen aan alle eisen in dit beleid. Voor iedere categorie van apparatuur, waarop gemeentelijke informatie is opgeslagen of wordt verwerkt, moet een plan zijn vastgelegd ter bescherming van de informatie buiten het primaire werkterrein.

Het brengen van apparatuur buiten het primaire werkterrein dient te worden goedgekeurd door de eigenaar van de apparatuur. Te allen tijde geldt dat:

- Apparatuur en media die buiten het terrein worden gebracht niet onbeheerd achtergelaten worden in de openbare ruimte;
- Voorschriften van de fabrikant voor het beschermen van de apparatuur worden te allen tijde in acht genomen;
- Van apparatuur die buiten het primaire werkterrein tussen verschillende personen of externe partijen wordt uitgewisseld dient ten alle tijden, door de verantwoordelijke, bijgehouden te worden wie op dat moment de apparatuur voor handen heeft (zie paragraaf 6.2.3);
- Voor digitale communicatie gelden de regels ten aanzien van telewerken;
- Niet digitale informatie met classificatieniveau Midden of hoger mag niet meegenomen worden van de primaire werklocatie.
- Bij thuiswerken dient men zich te houden aan het reglement 'Thuiswerken gemeente Medemblik' dat jaarlijks door het strategisch managementteam met advies van de CISO wordt geëvalueerd.

  Het reglement dient minimaal de adviezen[6] van de NCSC te bevatten.

6) https://www.ncsc.nl/documenten/publicaties/2020/april/1/factsheet-uw-thuiswerkfaciliteiten-zijn-nu-onmisbaar

Referentie: *BIO versie 1.04zv beheersmaatregel 11.2.6.*

9.2.7. Veilig verwijderen of hergebruiken van apparatuur en opslagmedia

Definitie

In deze paragraaf worden de termen verwijdering en vernietiging gebruikt. Deze termen hebben verschillende betekenissen:

- Verwijdering
  - Onder verwijdering wordt verstaan dat de apparatuur niet langer gebruikt wordt voor werkzaamheden voor de gemeente en bijvoorbeeld verkocht of gedoneerd kan worden. Bij verwijdering van apparatuur wordt de apparatuur niet fysiek onklaar gemaakt.

- Vernietiging
  - Vernietiging betreft het onklaar maken van de apparatuur. Dit betreft fysieke vernietiging van de apparatuur.

Tevens wordt de term opslagmedia gebruikt. Opslagmedia zijn alle soorten gegevensdragers zoals bijvoorbeeld harde schijven, papieren documenten, notities, telefoons et cetera.

9.2.7.1. Licenties

Alvorens er wordt overgegaan tot verwijdering of vernietiging van apparatuur dient de apparatuur te worden ontdaan van eventuele daaraan toegekende licenties. Deze licenties dienen binnen de gemeente te worden hergebruikt.

9.2.7.2. Opslagmedia

Opslagmedia, zowel digitaal als fysiek, dat informatie (heeft) bevat met classificatieniveau Midden of hoger dient door een gecertificeerd bedrijf vernietigd te worden conform het reglement 'Vernietiging opslagmedia', conform de wettelijke bewaartermijnen.

Digitale opslagmedia

Digitale opslagmedia (bijv. harde schijven of telefoons) met classificatieniveau Laag of lager mag worden hergebruikt mits deze worden geformatteerd middels de 'zero-fill' methodiek en er wordt voldaan aan het reglement 'Verwijdering opslagmedia' en de wettelijke bewaartermijnen in acht worden genomen

Fysieke opslagmedia

Fysieke opslagmedia (bijv. papier) met classificatieniveau Laag of lager dient te worden vernietigd door versnippering of dient te worden gedeponeerd in een door de gemeente aangewezen container ter vernietiging.

Reglementen

De reglementen 'Vernietiging opslagmedia' en 'Verwijdering opslagmedia' dienen drie jaarlijks door het SMT, met advies van de CISO, te worden geëvalueerd. Het reglement 'Vernietiging opslagmedia' moet voldoen aan de ISO / IEC 21964.

9.2.7.3. Verwijderen apparatuur

Voor het verwijderen van apparatuur is het reglement 'Verwijderen apparatuur' vastgesteld door het SMT. Tevens dient dit reglement jaarlijks door het SMT, met advies van de CISO, te worden geëvalueerd.

Het reglement dient te voldoen aan alle eisen in deze paragraaf.

Te verwijderen apparatuur en opslagmedia

Apparatuur met een afneembaar opslagmedium mag enkel hergebruikt worden buiten de gemeente (d.m.v. bijv. verkoop of donatie) mits het opslagmedium niet meer aanwezig is in de apparatuur.

Apparatuur waar het opslagmedium niet uit het apparaat gehaald kan worden én waar enkel informatie met classificatieniveau Laag of lager opgeslagen is dienen te worden hersteld naar de fabrieksinstellingen waarbij alle gegevens gewist worden.

In het geval dat 'zero-fill' formattering toegepast kan worden mogen apparaten met een opslagmedium waar enkel informatie met classificatieniveau Midden of lager opgeslagen is geweest hergebruikt worden na formattering middels deze methode.

Verwijderbesluit

Voor alle te verwijderen apparatuur dient de verantwoordelijke voor het bedrijfsmiddel én de strategisch manager van de betreffende afdeling een verwijderbesluit te ondertekenen. In het verwijderbesluit dienen minimaal de volgende zaken te staan:

- Welke apparatuur wordt verwijderd;
- Waarom deze apparatuur wordt verwijderd;
- Of de apparatuur ontdaan is van opslagmedia;
  - Zo ja, zijn deze vernietigd conform procedure?
  - Zo nee, zijn deze verantwoord geschikt gemaakt voor hergebruik?

- Waar de apparatuur naar toe gaat.

Het verwijderbesluit dient centraal vastgelegd te worden en dient inzichtelijk te zijn voor alle betrokkenen.

Beschadigde apparatuur
Beschadigde apparatuur dat een opslagmedium bevat mag enkel ter reparatie worden aangeboden nadat het opslagmedium is verwijderd. Indien het opslagmedium niet verwijderd kan worden en de apparatuur het niet toelaat om het opslagmedium op een veilige manier te wissen (zie bovenstaande 'verwijderen apparatuur') dan dient de apparatuur vernietigd te worden. Indien het opslagmedium voor het ter reparatie aan wordt geboden veilig gewist kan worden dient dit te gebeuren.

Inleveren apparatuur
Apparatuur zijn bedrijfsmiddelen en worden ingeleverd volgens de procedure (zie paragraaf 6.1.5).

Servers
Voor servers geldt:
- Bij buitengebruikstelling van servers/opslagmedia wordt te allen tijde informatie op deze servers/opslagmedia verwijderd dan wel vernietigd;
- Er worden technieken gebruikt waarmee informatie die niet meer nodig is, wordt vernietigd, overschreven, zodat oorspronkelijke informatie niet meer is terug te halen (zero-fill);
- Opslagmedia die niet meer nodig zijn en waar vertrouwelijke informatie dan wel auteursrechten op staan worden te allen tijde fysiek vernietigd. Van de fysieke vernietiging is altijd een bewijs en wordt centraal opgeslagen.

Referentie: *BIO versie 1.04zv beheersmaatregel 11.2.7.*

9.2.8. Onbeheerde gebruiksapparatuur
Gebruikers dienen ervoor te zorgen dat apparatuur te allen tijde voldoende beschermd is. Alle gebruikers dienen op de hoogte te worden gebracht van de beveiligingseisen en de procedures voor het beschermen van onbeheerde apparatuur, en van hun verantwoordelijkheden voor het implementeren van die bescherming. Gebruikers dienen geïnformeerd te worden dat zij:
- Apparatuur niet onbeheerd achterlaten;
- Actieve sessies na beëindiging afsluiten, tenzij de sessies kunnen worden beveiligd door een geschikte vergrendeling;
- Uitloggen uit toepassingen of netwerkdiensten die niet langer nodig zijn;
- Computers of mobiele apparatuur beveiligd worden tegen onbevoegd gebruik door middel van toets vergrendeling of toegang via wachtwoord, als de apparatuur niet in gebruik is.

Referentie: *BIO versie 1.04zv beheersmaatregel 11.2.8.*

9.2.9. 'Clean desk'- en 'clear-screen'-beleid
Binnen de gemeente hanteren medewerkers een 'clean desk'-beleid voor alle fysieke media en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatie verwerkende faciliteiten.

Te allen tijde geldt dat:
- Onbemande apparatuur zijn altijd vergrendeld;
  - Bij het verlaten van de werkplek dient de medewerker alle apparatuur te vergrendelen.

- Informatie wordt in een afgesloten ruimte bewaard wanneer deze informatie niet vereist is;
- Na kantooruren dient alle informatie in afgesloten ruimte te worden opgeborgen;
- Schermen worden automatisch vergrendeld na inactiviteit van een gebruiker van maximaal 5 minuten;
- Sessies middels remote desktop worden na inactiviteit van een gebruiker van maximaal 5 minuten onderbroken en vergrendeld;
- Het is alleen mogelijk om in te loggen op een remote desktop omgeving via een beveiligde inlogprocedure;
- Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van het token de toegangsbeveiligingsslot automatisch geactiveerd;
- Media dient vernietigd te worden conform de eisen in paragraaf 9.2.7.

Voor informatie met classificatie 'Midden of 'Hoog' geldt additioneel:
- Media dienen na het afdrukken onmiddellijk van printers te worden verwijderd.

Referentie: *BIO versie 1.04zv beheersmaatregel 11.2.9.*

10. Beveiliging bedrijfsvoering
10.1. Bedieningsprocedure en verantwoordelijkheden

10.1.1. Gedocumenteerde bedieningsprocedures
Bedrijfsprocessen voor servers dienen te zijn beschreven. De systeemeigenaar is samen met de proceseigenaar verantwoordelijk voor de opstelling hiervan. Wijzigingen aan bedieningsprocedures voor systeemactiviteiten worden formeel door de proceseigenaar goedgekeurd.

In de bedieningsprocedures zijn de bedieningsvoorschriften opgenomen, onder andere voor:
- de installatie en configuratie van systemen;
- de verwerking en behandeling van informatie, zowel geautomatiseerd als handmatig;
- de back-up;
- de eisen voor de planning, met inbegrip van onderlinge verbondenheid met andere systemen;
- de voorschriften voor de afhandeling van fouten of andere uitzonderlijke omstandigheden die tijdens de uitvoering van de taak kunnen optreden, waaronder beperkingen van het gebruik van systeemhulpmiddelen;
- de ondersteunings- en escalatiecontacten, waaronder externe ondersteuningscontacten door onverwachte bedienings- of technische moeilijkheden;
- het beheer van audit- en systeemlogbestandinformatie;
- de procedures voor het monitoren van activiteiten.

Referentie: *BIO versie 1.04zv beheersmaatregel 12.1.1.*

10.1.2. Wijzigingsbeheer
Veranderingen in de gemeente, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst. In de procedure 'Wijzigingsbeheer' dienen ten minste de volgende onderdelen zijn opgenomen:
- Identificatie en registratie van (significante) wijzigingen;
  - Oorzaak, doel en gevolg betreffende de wijzigingen.
  - Tijdlijn van doorvoering van de wijziging.

- Planning en testen van wijzigingen;
- Risicoanalyse ten aanzien van de informatiebeveiliging als gevolg van de wijzigingen;
  - Risico acceptatie, te nemen maatregelen en te accepteren restrisico's.

- Goedkeuringsprocedure voor wijzigingen;
- Communicatie van de wijzigingen aan betrokkenen;
- Uitwijkprocedures, waaronder de procedures en verantwoordelijkheden ten aanzien van het afbreken en herstellen van niet-geslaagde wijzigingen en onvoorziene gebeurtenissen.

Referentie: *BIO versie 1.04zv beheersmaatregel 12.1.2.*

10.1.3. Capaciteitsbeheer
Het gebruik van middelen behoort te worden gemonitord en afgestemd en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereisten systeemprestaties te waarborgen. Uit monitoring moet blijken dat de beschikbaarheid en doelmatigheid van systemen voldoende zijn en niet worden gehinderd door onvoldoende capaciteit. De monitoring dient tevens preventief te zijn.

De juiste afstemming van capaciteit kan worden bereikt door de capaciteit te verhogen of door de vraag te verlagen. De vraag wordt beheerst door:
- Verwijderen van oude gegevens;
- Het buiten gebruik stellen van toepassingen, systemen, databases of omgevingen;
- Geautomatiseerde workflow- en batchprocessen en -schema's te optimaliseren;
- Specialistische hardware toe te passen voor bepaalde bewerkingen;
- Toepassingslogica of databasevragen te optimaliseren;
- De bandbreedte voor diensten die veel energie of capaciteit verbruiken te weigeren of te beperken als deze niet van groot bedrijfsbelang zijn.

Referentie: *BIO versie 1.04zv beheersmaatregel 12.1.3.*

10.1.4. Scheiding van ontwikkel-, test- en productieomgevingen

Ontwikkel-, test-, acceptatie- en productieomgevingen zijn gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen. In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan kan er worden afgeweken.

Wijzigingen in de productieomgeving worden altijd getest in de testomgeving én acceptatieomgeving voordat zij in productie worden gebracht. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.

Referentie: *BIO versie 1.04zv beheersmaatregel 12.1.4.*

10.2. Bescherming tegen malware

Informatie en informatie verwerkende faciliteiten dienen beschermd te zijn tegen malware. Onder malware wordt software verstaan die specifiek is ontwikkeld om schade toe te brengen aan een computer en andere IT-systemen.

10.2.1. Beheersmaatregelen tegen malware

Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.

- De mogelijkheid van het downloaden en uitvoeren van (typen) bestanden is beperkt op alle apparaten die worden gebruikt voor gemeentelijke werkzaamheden. De beperkingen staan beschreven in de procedure ‘Downloaden en uitvoeren bestanden’.
- Gebruikers zijn voorgelicht over de risico’s ten aanzien van surfgedrag en het klikken op onbekende links;
- Alle apparaten die worden ingezet voor de dienstverlening van de gemeente dienen te zijn voorzien van anti-malwaresoftware die dagelijkse updates ontvangt.
- Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan behoort te omvatten:
  - Alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen;
  - Minimaal 1x per 3 dagen het gehele apparaat.

Referentie: *BIO versie 1.04zv beheersmaatregel 12.2.1.*

10.3. Back-up van informatie

Er dient een gemeente breed back-up beleid te zijn die jaarlijks wordt geëvalueerd. Dit beleid dient minimaal de volgende onderwerpen te bevatten:

- Specifieke eisen m.b.t. geaccepteerde periode van dataverlies en hersteltijd per informatieclassificatieniveau gebaseerd op een expliciete risico afweging.
  - Ongeacht het informatieclassificatieniveau:
    - Bedraagt het dataverlies maximaal 28 uur;
    - Is de hersteltijd in het geval van incidenten maximaal 16 werkuren (twee dagen van 8 uur) voor 85% van de gevallen.

- Het back-upproces voorziet in opslag van de back-ups op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere locatie (geografische scheiding van redundante opslag).
- De herstel procedure wordt minimaal jaarlijks getest (of na een grote wijziging) om de goede werking te waarborgen als deze in noodgevallen moet worden uitgevoerd.
- Back-ups dienen per informatieclassificatieniveau te worden gemaakt waarbij back-ups van het ene classificatieniveau geen gevolgen mogen hebben voor back-ups van het andere classificatieniveau.
- Procedures voor vernietiging van de back-ups.

Referentie: *BIO versie 1.04zv beheersmaatregel 12.3.1.*

10.4. Verslaglegging en monitoring

10.4.1. Beheersmaatregelen tegen malware

Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, worden gemaakt, bewaard en regelmatig, ten minste maandelijks, te worden beoordeeld door de systeemeigenaar. Een logregel bevat minimaal:

- De gebeurtenis;
- Gebruikersidentiteit;
- Het gebruikte apparaat;
- Registraties van geslaagde en geweigerde pogingen om toegang te krijgen tot het systeem;
- Registraties van geslaagde en geweigerde gegevens en andere pogingen om toegang te krijgen;
- Gebruik van speciale bevoegdheden;
- Gebruik van systeemhulpprogramma's en -toepassingen;
- Het resultaat van de handeling;
- Datum en tijdstip van de gebeurtenis.

Een logregel bevat geen gegevens die tot het doorbreken van de beveiliging kunnen leiden. De informatie verwerkende omgeving wordt geautomatiseerd gemonitord. Monitoring wordt ingezet op basis van een risico-inschatting, zodat aanvallen kunnen worden gedetecteerd.

Alle firewalls zijn voorzien van logging en monitoring die afwijkende gebeurtenissen kunnen waarnemen en daarop kunnen reageren.

Bij ontdekte nieuwe dreigingen (aanvallen) via de detectie-voorziening worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder via het sectorale CERT middels threat intelligence sharing mechanismen.

Referentie: *BIO versie 1.04zv beheersmaatregel 12.4.1.*

10.4.2. Beschermen van informatie in logbestanden

Er is een centraal overzicht van logbestanden die worden gegenereerd. Hierin worden ook de activiteiten van gebruikers met speciale toegangsrechten en operators in vastgelegd. In de logbestanden worden ten minste de volgende onderdelen vastgelegd:

- Het tijdstip waarop een gebeurtenis (succesvol of storing) is opgetreden;
- Informatie over de gebeurtenis of storing;
- Welk account en welke beheerder of operator erbij betrokken was;
- Welke processen erbij betrokken waren.

De logbestanden worden minimaal één jaar bewaard. Er is een interne audit procedure die minimaal halfjaarlijks toetst op het ongewijzigd bestaan van logbestanden. Oneigenlijk wijzigen of verwijderen van loggegevens of pogingen daartoe worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform paragraaf 14.1.2.

Referentie: *BIO versie 1.04zv beheersmaatregel 12.4.2 en 12.4.3.*

10.4.3. Kloksynchronisatie

De klokken van alle relevante informatie verwerkende systemen binnen de gemeente Medemblik worden gesynchroniseerd met één referentietijdbron: Central European Time (CET, Amsterdam). De systeemeigenaar van het kloksysteem is hiervoor verantwoordelijk.

Referentie: *BIO versie 1.04zv beheersmaatregel 12.4.4.*

10.5. Beheersing van operationele software

De integriteit van operationele systemen dient gewaarborgd te worden door procedures te implementeren ten aanzien van het installeren van software op de operationele systemen. Hierbij is vereist dat:

- De productieprogrammatuur, -toepassingen en -programmabibliotheken worden uitgevoerd door beheerders na goedkeuring door de directie;
- Op productiesystemen is uitsluitend goedgekeurde uitvoerbare programmatuur aanwezig (zie paragraaf 10.7);
- Toepassingen en besturingssysteemprogrammatuur wordt pas geïmplementeerd na tests op bruikbaarheid, beveiliging, effecten of andere systemen en gebruikersvriendelijkheid. De test dienen op gescheiden systemen te worden uitgevoerd (zie paragraaf 12.3);
- Alle bijbehorende broncodebibliotheken zijn geüpdatet;

- Er wordt een configuratiebeheerssysteem gebruikt om alle geïnstalleerde programmatuur en de systeemdocumentatie te beheersen;
- Er is een terugdraaistrategie vastgesteld voordat wijzigingen worden doorgevoerd (zie paragraaf 10.1.2);
- Er is een auditlogbestand bijgehouden van elke update van besturingsprogrammabibliotheken;
- Oude versies van programmatuur worden gearchiveerd, samen met alle vereiste informatie en parameters, procedures, configuratiedetails en ondersteunende programmatuur zolang er gegevens dienen te worden gearchiveerd of zolang het nodig kan zijn dat de gegevens worden geraadpleegd (zie paragraaf 10.3);
- De activiteiten van de leverancier worden gecontroleerd (zie paragraaf 13.1.1).

Referentie: *BIO versie 1.04zv beheersmaatregel 12.5.*

10.6. Beheer van technische kwetsbaarheden
Systeemeigenaren en de CISO dienen actief informatie te vergaren over technische kwetsbaarheden. Technische kwetsbaarheden dienen geclassificeerd te zijn aan de hand van de NCSC-classificatie kwetsbaarheidswaarschuwingen. Indien uit deze classificatie blijkt dat de kans op misbruik en de verwachte schade beide hoog zijn dienen eventueel beschikbare patches binnen 48 uur geïnstalleerd te worden en dient de CISO onmiddellijk op de hoogte gesteld te worden. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen. Hiervoor is de systeemeigenaar van het specifieke systeem verantwoordelijk.

Maandelijks rapporteren systeemeigenaren naar de CISO over technische kwetsbaarheden en genomen mitigerende maatregelen. De rapportages dienen minimaal onderstaande te bevatten:
- Omschrijving technische kwetsbaarheid (inclusief eventueel CVE-nummer);
- Bron van technische kwetsbaarheid;
- Datum van ontdekking technische kwetsbaarheid;
- NCSC-classificatie kwetsbaarheidswaarschuwingen;
- De genomen maatregelen.

De CISO rapporteert in hoofdlijnen de gerapporteerde kwetsbaarheden, risico's en genomen maatregelen minimaal halfjaarlijks naar het directieteam.

Referentie: *BIO versie 1.04zv beheersmaatregel 12.6.1.*

10.7. Beperkingen voor het installeren van software
Uitgangspunt
Gebruikers kunnen op apparaten die voor gemeentelijke werkzaamheden worden gebruikt niets zelf installeren. Geautomatiseerd moet afgedwongen worden dat geen andere software geïnstalleerd kan worden.

Whitelist
Software dient voor uitlevering van het apparaat geïnstalleerd te worden. Software die op de 'Geautoriseerde Software Whitelist' staat mag geïnstalleerd worden. De te installeren software is afhankelijk van het functieprofiel van de eindgebruiker. De verantwoordelijke voor de functieprofielen bepaalt aan de hand van de whitelist welke software voor welke functie geïnstalleerd mag worden in samenspraak met de teamleider Informatiemanagement.

Blacklist
Software die nimmer geïnstalleerd mag worden is vastgelegd in de 'Software Blacklist'. Geautomatiseerd moet afgedwongen worden dat deze software nimmer op apparatuur die voor gemeentelijke werkzaamheden wordt gebruikt wordt uitgevoerd.

Verantwoordelijkheden
De strategisch manager bedrijfsvoering is verantwoordelijk voor de 'Geautoriseerde Software Whitelist' en de 'Software Blacklist'. Op aanvraag van de teamleider Informatiemanagement en de CISO kan de strategisch manager besluiten om de lijsten te herzien.

Er dient een installatiemanager(s) aangesteld te zijn wie rechten heeft tot het installeren van software. Na goedkeuring van de teamleider Informatiemanagement mag deze persoon software van de whitelist installeren op de apparaten die voor de gemeentelijke werkzaamheden worden gebruikt. De installatiemanager legt de installatie vast in een centraal installatieregister waarbij de teamleider Informatiemanagement zijn goedkeuring tevens vastlegt.

Referentie: *BIO versie 1.04zv beheersmaatregel 12.6.2.*

10.8. Beheersing van operationele software

- De impact van auditactiviteiten op uitvoeringssystemen moet zo gering mogelijk zijn. Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, worden zorgvuldig gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren. Hierbij wordt in acht genomen dat:
- De auditeisen met de juiste verantwoordelijke zijn overeengekomen;
- De reikwijdte van de controles vooraf wordt overeengekomen;
- De controles worden beperkt tot alleen-lezen-toegang tot programmatuur en gegevens;
- Andere toegang dan 'alleen lezen' wordt uitsluitend toegelaten voor geïsoleerde kopieën van systeembestanden die na beëindiging van de audit aantoonbaar worden gewist of op een juiste wijze worden beschermd indien de auditdocumentatie dit vereist;
- Hulpmiddelen voor de uitvoering van controles worden vooraf expliciet vastgesteld;
- Eisen voor bijzondere of aanvullende verwerking worden vastgesteld en overeengekomen;
- Alle toegang wordt gecontroleerd en vastgelegd in een logbestand om een audittrail te produceren, en voor kritische gegevens of systemen wordt een 'reference trail' met tijdregistratie bijgehouden;
- Alle procedures, eisen en verantwoordelijkheden zijn gedocumenteerd;
- De persoon of personen die de audit uitvoert hebben geen belangen bij de activiteiten die worden geaudit.

Referentie: *BIO versie 1.04zv beheersmaatregel 12.7.*

11. Communicatiebeveiliging

11.1. Beheer van netwerkbeveiliging

11.1.1. Beheersmaatregelen voor netwerken

Er behoren beheersmaatregelen te worden geïmplementeerd om de veiligheid van informatie in netwerken te waarborgen en aangesloten diensten tegen onbevoegde toegang te beschermen.

Voor alle netwerken gelden ten minste de volgende eisen:

Netwerkapparatuur

- Apparatuur die binnen het netwerk wordt gebruikt en in het beheer van de gemeente is mag niet afkomstig zijn van bedrijven die de op de lijst van 'NDAA Prohibited Manufacturers'[7] en/ of op lijst van 'Early Detection and Exclusion System (EDES)'[8] staan;
- Apparatuur die binnen netwerken wordt gebruikt waarin informatie met classificatie 'hoog' wordt uitgewisseld mag niet afkomstig zijn van leveranciers die op de lijst van 'NDAA Prohibited Manufacturers' staan;
- Apparatuur die binnen netwerken wordt gebruikt waarin informatie met classificatie 'midden' en 'hoog' wordt uitgewisseld dient gedurende de tijd dat deze in het netwerk aanwezig is door de fabrikant softwarematig ondersteund te worden en te draaien op de nieuwste softwareversie die door de fabrikant beschikbaar is gesteld. Indien dit niet het geval is dient de apparatuur vervangen te worden door apparatuur die wel aan bovenstaande voldoet;
- Niet mobiele apparatuur die binnen het netwerk wordt gebruikt dient de fysieke toegang beperkt te worden conform de eisen uit het hoofdstuk 9.
    - Additioneel dient de apparatuur te voldoen aan de eisen conform hoofdstuk 6 en hoofdstuk 7.

Netwerk toegang

- Alle netwerken dienen beveiligd te zijn:
    - middels een firewall die geautomatiseerd up-to-date gehouden wordt;
    - door alle netwerkpoorten te blokkeren die niet noodzakelijk zijn;
    - door een geautomatiseerde blokkade te hanteren van IP-adressen en domeinen die niet benaderd mogen worden;
    - netwerken mogen niet van buiten de fysieke locatie benaderd worden tenzij dit noodzakelijk wordt geacht;
    - door alleen geauthentiseerde apparaten toe te staan te verbinden.

7) NDAA Prohibited Manufacturers (ucsd.edu)

8) https://commission.europa.eu/strategy-and-policy/eu-budget/how-it-works/annual-lifecycle/implementation/anti-fraud-measures/edes/edes-database_en

Noodzakelijkheid deblokkeren netwerkpoorten
Systeemeigenaren dienen bij team Informatiemanagement aan te geven welke netwerkpoorten noodzakelijk zijn voor de werking van het systeem. Informatiemanagement en informatiebeveiliging dienen overeen te komen welke netwerkpoorten gedeblokkeerd dienen te worden. De technische netwerkbeheerder mag enkel op advies van de CISO een netwerkpoort deblokkeren. De gedeblokkeerde netwerkpoorten dienen per netwerk geregistreerd te worden waarbij ten minste het systeem en de reden voor deblokkeren benoemd wordt. De registratieplicht is belegd bij informatiebeveiliging.

Noodzakelijkheid deblokkeren externe netwerktoegang
Informatiemanagement en informatiebeveiliging dienen overeen te komen welke netwerken (of delen van) extern benaderd mogen worden. De technische netwerkbeheerder mag enkel op advies van de CISO een netwerk extern toegankelijk maken. De mate van externe toegankelijkheid dient per netwerk geregistreerd te worden waarbij ten minste de te benaderen systemen en de reden voor deblokkeren benoemd wordt. De registratieplicht is belegd bij informatiebeveiliging.

Netwerken monitoring
- Netwerkmonitoring dient te voldoen aan het voorschrift netwerkmonitoring waarin minimaal de volgende zaken in moet worden beschreven:
  - Per informatieclassificatie niveau worden de monitoringseisen beschreven en hoe hieraan moet worden voldaan. Waarin tenminste aan de volgende eisen moet worden voldaan:
    - Per classificatieniveau dient aangegeven te worden:
      - welke informatie rechtmatig opgeslagen (bewaard) mag worden;
      - de tijdsduur van de bewaring;
      - welke informatie rechtmatig ingezien mag worden.
    - De monitoring dient te allen tijde te voldoen aan de eisen conform hoofdstuk 6 en hoofdstuk 7.
    - Voor de monitoring gelden dezelfde cryptografische eisen als het hoogste classificatieniveau van de informatie die in het netwerk wordt gecommuniceerd.
  - Wie verantwoordelijk is voor de implementatie van de monitoring;
  - De periodieke controle van het voorschrift.

Het voorschrift netwerkmonitoring wordt opgesteld en onderhouden door de CISO / ISO.

In het geval van verstoringen
Onder verstoringen vallen alle verstoringen van de netwerkdienstverlening, waaronder: migratie, technische wijzigingen, uitval van apparaten, et cetera. In het geval van verstoringen mag er niet afgeweken worden van alle in deze paragraaf benoemde eisen.

Beschikbaarheidseisen
Netwerken dienen jaarlijks minimaal een beschikbaarheidspercentage van 99,99% te hebben. Deze eis dient bij uitbesteding van netwerkdiensten contractueel vastgelegd te worden.

Beheeractiviteiten
Beheeractiviteiten dienen afgestemd te worden met Team Informatiemanagement alvorens deze plaats mogen vinden. Beheeractiviteiten dienen plaats te vinden buiten de standaard kantooruren (van 08:00 tot 18:00) tenzij Team Informatiemanagement het noodzakelijk acht dat dit binnen kantooruren plaats vindt.

Beheeractiviteiten die potentiële gevolgen hebben voor de beschikbaarheid van een systeem dienen afgestemd te worden met de systeemeigenaar waarbij de systeemeigenaar de plicht heeft om het systeem na de activiteiten te testen en de bevindingen van de test door te geven aan Team Informatiemanagement binnen 24 uur na afronding van de beheeractiviteiten.

Referentie: *BIO versie 1.04zv beheersmaatregel 13.1.1.*

11.1.2. Beveiliging van netwerkdiensten
Netwerkdiensten
Netwerkdiensten zijn een verzameling van: apparatuur en software die het mogelijk maken voor andere apparaten om via kabels of draadloos met elkaar te communiceren.

Dienstverleningsovereenkomsten
Voor alle netwerkdiensten, zowel voor intern als voor uitbestede diensten, dient er een dienstverleningsovereenkomst te worden aangegaan waarin tenminste de volgende eisen zijn verwerkt:

- alle eisen van paragraaf 11.1 en alle onderliggende paragrafen.
- de informatieclassificatie van de informatie die in het netwerk wordt gecommuniceerd.
- de wijze waarop verantwoording wordt afgelegd over de conformiteit van de eisen.
- de concrete maatregelen die getroffen worden om aan bovenstaande eisen te voldoen.
- alle eisen van paragraaf 13.1.2.

Referentie: *BIO versie 1.04zv beheersmaatregel 13.1.2.*

11.1.2.1. Netwerkdetectievoorzieningen
Het dataverkeer binnen de netwerken die worden gebruikt moet worden geanalyseerd op kwaadaardige elementen middels (geautomatiseerde) detectievoorzieningen. De detectievoorzieningen worden ingezet op basis van een risico-inschatting door de CISO / ISO. De detectievoorzieningen worden beschreven in het 'Voorschrift detectievoorzieningen gemeente Medemblik'. Dit voorschrift dient aan de volgende eisen voldoen:

- Per netwerk dient een risicoanalyse te zijn uitgevoerd waarbij de volgende onderdelen zijn inbegrepen:
  - Classificatie van informatie binnen het netwerk.
  - Systemen binnen het netwerk.
  - Aanvalsoppervlak van het netwerk.
  - (Fysieke) locatie van het netwerk en diens gegevens.
  - Relevante wet- en regelgeving.

- Jaarlijkse evaluatie van het voorschrift en de daarin beschreven risicoanalyses.
- Verantwoordelijkheden dienen duidelijk te zijn beschreven.
- De detectievoorzieningen dienen te worden gespecificeerd inclusief de kwaadaardige elementen die zij moeten detecteren.
- Procedures voor gedetecteerde kwaadaardige elementen dient te zijn beschreven.
- Restrisico's na implementatie detectievoorzieningen.
- Toegangsbeheer betreffende eventuele logging en detectievoorzieningen.
- Procedures voor inzage en vernietiging van eventuele persoonsgegevens.

Referentie: *BIO versie 1.04zv beheersmaatregel 13.1.2.1.*

11.1.2.2. Melden ontdekte dreigingen
Indien een dreiging wordt ontdekt in de beveiliging van de gebruikte netwerken zal de CISO de sectorale CERT op de hoogte stellen binnen 48 uur na detectie. Bij afwezigheid van de CISO neemt de ISO deze taak waar. De CISO / ISO houdt tevens een registratie bij van het aantal ontdekte dreigingen en de correspondentie hierover met de sectorale CERT.

Referentie: *BIO versie 1.04zv beheersmaatregel 13.1.2.2.*

11.1.2.3. Versleutelingstechnieken netwerken
Alle draadloze én bedrade verbindingen waar gebruik van wordt gemaakt dienen te zijn beveiligd conform de eisen in het hoofdstuk 7, hoofdstuk 8 en paragraaf 11.2.

Referentie: *BIO versie 1.04zv beheersmaatregel 13.1.2.3.*

11.1.2.4. Beschikbaarheidsaanvallen
Voor alle netwerken waarin informatie met classificatie Midden of Hoog wordt gecommuniceerd dienen preventiemaatregelen te zijn genomen om aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden te voorkomen. Deze preventieve maatregelen worden doorgevoerd op last van de CISO. De jaarlijkse beoordeling van deze maatregelen is belegd bij de CISO. De preventieve maatregelen en de daarmee te voorkomen type aanvallen dienen te zijn vastgelegd.

Referentie: *BIO versie 1.04zv beheersmaatregel 13.1.2.4.*

11.1.3. Scheiding in netwerken

Informatiediensten
Onder informatiediensten vallen alle systemen en bestanden. Informatiediensten dienen te zijn gegroepeerd op basis van het informatieclassificatieniveau van de informatie waar zij toegang tot hebben. Informatiediensten dienen infrastructureel gescheiden te zijn van informatiediensten met een andere informatieclassificatie.

Gebruikers

Alle gebruikers van netwerken dienen te zijn ingedeeld in groepen op basis van het informatieclassificatieniveau waartoe zij toegang mogen krijgen. Het classificatieniveau van de groep bepaalt de toegang tot de verschillende netwerken. Gebruikers in groepen met classificatieniveau Midden of Hoog mogen alleen de informatiediensten bereiken waartoe zij specifiek of via hun rol zijn geautoriseerd.

Netwerken
Netwerken dienen te zijn ingedeeld op basis van het informatieclassificatieniveau van de informatie die in het netwerk wordt gecommuniceerd. Informatiediensten zijn geplaatst in het netwerk met hetzelfde informatieclassificatieniveau. Netwerken met verschillende informatieclassificatieniveaus mogen niet de mogelijkheid hebben om met elkaar te communiceren.

Daarnaast gelden de volgende specifieke eisen per informatieclassificatieniveau:

Informatieclassificatieniveau Openbaar.
- Netwerken waarbij geen onderscheidt wordt gemaakt met welke specifieke apparaten mogen verbinden dienen een maximale duur aan de verbinding te stellen van 1 uur.
- De gebruiker van het apparaat dient akkoord te geven op de voorwaarden die ten grondslag liggen aan het gebruik van het netwerk. De voorwaarden dienen minimaal te bevatten:
  - Akkoord voor monitoring en opslag:
    - van uniek apparaat kenmerk;
    - hoeveelheid bandbreedte die wordt gebruikt;
    - duur van verbinding;
    - tijd en datum van verbinding;
    - bezochte webadressen;
    - duur van opslag van minimaal 24 uur en maximaal 1 week.
  - Maximale bandbreedte die per gebruiker geboden wordt.
  - De gemeente is niet aansprakelijk voor alle gevolgen inzake het gebruik van de verbinding en de gebruiker zich hiervan bewust is en akkoord geeft.
  - De gebruiker zich conformeert aan het volgen van de wet- en regelgeving die toepasselijk is op deze dienst.

Informatieclassificatieniveau Laag
- Netwerken waarbij geen onderscheidt wordt gemaakt met welke specifieke apparaten mogen verbinden zijn niet toegestaan.
- Gebruikers die met het netwerk willen verbinden mogen dit alleen na identificatie en autorisatie middels een door de gemeente verstrekt account én apparaat.
  - Het apparaat dient in beheer te zijn van de gemeente.
- Informatiediensten dienen te zijn geautoriseerd om met het netwerkverbinding te maken.

Informatieclassificatieniveau Midden
- Alle eisen van classificatieniveau Laag.
- Het netwerk mag enkel beschikbaar zijn binnen de fysieke locaties van gemeente Medemblik daar waar de werkzaamheden het noodzakelijk achtten.
  - Uitzondering hierop is een versleutelde beveiligde verbinding waarmee alleen vooraf geautoriseerde personen toegang mogen krijgen tot het netwerk. Deze versleutelde beveiligde verbinding mag enkel gebruikt worden vanaf andere locaties in Nederland.
- Voor het verbinden met het netwerk is voor gebruikers verplicht om gebruik te maken van een door de gemeente voorgeschreven multi-factor authenticatie techniek.

Informatieclassificatieniveau Hoog
- Alle eisen van classificatieniveau Midden.
- Voor het verbinden met het netwerk dient een door de gemeente beheerde hardware token gebruikt te worden ten behoeve van de multi-factor authenticatie.
  - De hardware tokens gelden als bedrijfsmiddelen (zie hoofdstuk 6). Het eigenaarschap is belegd bij CISO.

Enkel geautoriseerde apparaten mogen verbindingen maken met het netwerk van de gemeente.

Referentie: *BIO versie 1.04zv beheersmaatregel 13.1.3.*

11.2. Informatietransport

11.2.1. Beleid en procedures informatietransport
Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.

In de soorten transport wordt onderscheid gemaakt in digitaal- en fysiektransport, voor beiden zijn handreikingen beschikbaar. De handreikingen dienen te voldoen aan:

Handreiking Digitaal Informatietransport
- De eisen van paragraaf 10.1, paragraaf 11.1 & paragraaf 11.2 inclusief alle onderliggende paragrafen.
- De eisen van hoofdstuk Cryptografie (hoofdstuk 8).

Handreiking Fysiek Informatietransport
- De eisen van paragraaf 9.2.7.
- De eisen van paragraaf 6.2.

Tot slot dienen beide handreikingen procedures te beschrijven die informatie beveiligen tegen onderscheppen, kopiëren, wijzigen, foutieve routering en vernietiging. Hierin dient onderscheidt gemaakt te worden tussen de verschillende informatieclassificatieniveaus.

Referentie: *BIO versie 1.04zv beheersmaatregel 13.2.1.*

11.2.2. Beleid en procedures informatietransport
Overeenkomsten omtrent informatietransport dienen onderdeel te zijn van alle contracten waar gemeentelijke informatie wordt getransporteerd. In de overeenkomst dienen ten minste de onderstaande onderdelen aan bod te komen:
- directieverantwoordelijkheden voor het beheersen en notificeren van overdracht, verzending en ontvangst;
- procedures voor het waarborgen van de traceerbaarheid en onweerlegbaarheid;
- speciale en vereiste beheersmaatregelen voor het beschermen van gevoelige informatie, waarbij moet worden voldaan aan de eisen van hoofdstuk 7 van dit beleid;
- het handhaven van een bewakingsketen voor informatie tijdens de verzending;
- acceptabele niveaus van toegangsbeveiliging, waarbij moet worden voldaan aan alle eisen in dit beleid omtrent het toepasselijke informatieclassificatieniveau.
- In de overeenkomst behoren alle betrokken partijen én diens rol in de overeenkomst expliciet te zijn genoemd.
- Verwijzing naar de 'in gebreke procedure' (zie paragraaf 13.1) bij het niet nakomen van de afspraken.

Referentie: *BIO versie 1.04zv beheersmaatregel 13.2.2.*

11.2.3. Elektronische berichten
Voor elektronische berichten gelden te allen tijde de eisen uit dit hoofdstuk en hoofdstuk 8 i.c.m. de eisen van het Forum Standaardisatie m.b.t. 'Veilig Internet'[9]. Zonder schriftelijke toestemming inclusief uitgebreide uitleg van de CISO mag er niet afgeweken worden van de eisen.

Verder dient er voorafgaand aan het verzenden van elektronische berichten een (automatische) controle plaats te vinden of het bericht alleen aan geautoriseerde personen verstuurd wordt. Verder mogen elektronische berichten enkel via geautoriseerde media en software (zie paragraaf 10.7) verstuurd worden.

Referentie: *BIO versie 1.04zv beheersmaatregel 13.2.3.1.*

11.2.3.1. Elektronische berichten met basisregistratie
Elektronische berichten met basisregistraties dienen, naast het voldoen aan de bovenstaande eisen, altijd gebruik te maken van de meest actuele versie van de Digikoppeling.

Referentie: *BIO versie 1.04zv beheersmaatregel 13.2.3.2.*

11.2.3.2. Elektronische berichten met certificaten

9) https://www.forumstandaardisatie.nl/open-standaarden/verplicht?domein=125

Elektronische berichten waarin informatie staat met classificatie Midden of hoger dient er te alle tijde gebruik gemaakt te worden van PKI-certificaten ter beveiliging. Dit geldt tevens voor intern web-verkeer.

Indien noodzakelijk kunnen hogere eisen aan certificaten voortvloeien uit een risicoanalyse, aansluitvoorwaarden of wetgeving. Elektronische berichten met classificatie Midden of hoger mogen niet verzonden worden over niet vertrouwde netwerken.

Referentie: *BIO versie 1.04zv beheersmaatregel 13.2.3.3.*

11.2.3.3. Elektronische handtekening
Daar waar een elektronisch handtekening noodzakelijk is en de ontvangende partij het ondersteund dient er gebruik te worden gemaakt van de Ades Baseline Profiles [10] van het Forum Standaardisatie.

Referentie: *BIO versie 1.04zv beheersmaatregel 13.2.3.4.*

11.2.4. Vertrouwelijkheids- of geheimhoudingsovereenkomst
Informatietransport is onderdeel van de geheimhoudingsovereenkomst die moet worden afgesloten met iedereen die werkzaamheden voor de gemeente verricht of een product / dienst levert waarin informatie een rol speelt.

Referentie: *BIO versie 1.04zv beheersmaatregel 13.2.4.*

11.3. Transacties op toepassingen beschermen
Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen. Bij het beschermen van de transacties op toepassingen, dienen de volgende aspecten in acht te worden genomen:

- Het gebruik van elektronische handtekeningen door alle partijen die bij de transactie betrokken zijn;
- Alle aspecten van de transitie, dat wil zeggen waarborgen dat:
  - Geheime authenticatie-informatie van gebruikers van alle partijen geldig en geverifieerd is;
  - De transactie vertrouwelijk blijft;
  - De privacy van alle betrokken partijen behouden blijft;
- Versleuteling van de communicatiepaden tussen alle betrokken partijen;
- Bewerkstelligen dat de opslaglocatie van transactiegegevens zich buiten een publiek toegankelijke omgeving bevindt en niet wordt bewaard en getoond op een opslagmedium dat direct vanuit internet toegankelijk is;
- Als een vertrouwde instantie wordt gebruikt, beveiliging integreren en inbedden in het gehele beheerproces van certificaten/handtekeningen.

Transacties dienen te voldoen aan de eisen van wet- en regelgeving van het rechtsgebied waarin de transactie is gegenereerd, verwerkt, uitgevoerd of opgeslagen.

Referentie: *BIO versie 1.04zv beheersmaatregel 14.1.3.*

11.4. Toepassingen op openbare netwerken beveiligen
Werken via openbare netwerken
Op het primaire werkterrein van de gemeente mag niet gewerkt worden via onbeveiligde en / of openbare (Wi-Fi) netwerken. Buiten het primaire werkterrein gelden de eisen van de handreiking Telewerken (zie paragraaf 3.2).

Toepassingen
Indien toepassingen via openbare netwerken gemeentelijke informatie communiceren dienen er maatregelen worden genomen om te voldoen aan alle eisen uit dit beleid. Zo dient informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.

Referentie: *BIO versie 1.04zv beheersmaatregel 14.1.2.*

10) https://www.forumstandaardisatie.nl/open-standaarden/ades-baseline-profiles#_Detailinformatie_

12. Ontwikkeling en onderhoud van informatiesystemen
12.1. Ontwikkeling van informatiesystemen

12.1.1. Beleid voor beveiligd ontwikkelen
Voor het ontwikkelen van software en systemen zijn regels vastgesteld in het 'Beleid Beveiligd Ontwikkelen' van de gemeente. In dit beleid dienen ten minste de volgende onderdelen te zijn opgenomen:
- Hoe de ontwikkelomgeving dient te worden beveiligd (zie paragraaf 12.1.3);
- Broncode;
  - Toegang en autorisaties m.b.t. de broncode (zie paragraaf 7.4.5);
  - Locatie van opslag van de broncode;
  - Doorvoeren van wijzigingen in de broncode (zie paragraaf 7.4.5);
- Welke beveiligingseisen worden gesteld t.a.v. de ontwikkelfasen;
  - Beveiligingscontrolepunten binnen de mijlpalen van het project.
- Waarborging voldoende kennis van informatiebeveiliging bij de ontwikkelende personen;
  - Vermogen van de ontwikkelaar(s) om kwetsbaarheden te vermijden, te vinden en te repareren (kennis van secure software development);
  - Beveiligingseisen m.b.t. de software ontwikkelmethodologie (secure-by-design);
  - Principes voor de ontwikkeling van beveiligde systemen (zie paragraaf 12.1.2).
  - Kennis van informatiebeveiligingsrisico's omtrent in productie nemen van het ontwikkelde systeem;
  - Kennis van informatiebeveiligingsrisico's omtrent testdata.
    - Testen met echte (productie) data is niet toegestaan.
- Richtlijnen betreffende beveiliging in de levenscyclus van softwareontwikkeling;
- Testen van informatiebeveiliging.
  - Onafhankelijke technische broncode audit conform beveiligde coderingsrichtlijnen specifiek voor de programmeertaal die wordt gebruikt.
  - Onafhankelijke penetratietest op de acceptatieomgeving alvorens het ontwikkelde in productie te nemen.
- Eisen omtrent het in productie brengen van het ontwikkelde systeem.
  - Gescheiden ontwikkel-, test-, acceptatie- en productieomgevingen.
  - Beveiligingseisen omtrent infrastructuur;

Van bovenstaand beleid mag niet afgeweken worden en deze gelden eveneens voor uitbesteedde ontwikkeling van informatiesystemen (zie hoofdstuk 13).

Referentie: *BIO versie 1.04zv beheersmaatregel 14.2.1, 14.2.1.1 & 14.2.8.*

12.1.2. Principes voor de ontwikkeling van beveiligde systemen
Principes voor de ontwikkeling van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen. Deze principes dienen regelmatig, ten jaarlijks, te worden beoordeeld door de CISO om te waarborgen dat ze doelmatig bijdragen aan verbeterde normen voor beveiliging binnen het engineeringproces.

Referentie: *BIO versie 1.04zv beheersmaatregel 14.2.5.*

12.1.3. Beveiligde ontwikkelomgeving
De gemeente dient in het beleid 'Beleid Beveiligd Ontwikkelen' eisen te stellen aan de beveiligde ontwikkelomgevingen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling. Een beveiligde ontwikkelomgeving omvat personen, processen en technologie die in verband staan met systeemontwikkeling en integratie.

De gemeente dient risico's die samenhangen met individuele verrichtingen betreffende systeemontwikkeling en beveiligde ontwikkelomgevingen vast te stellen voor specifieke verrichtingen op het gebied van systeemontwikkeling, rekening houdend met:
- De gevoeligheid van de gegevens die door het systeem worden verwerkt, opgeslagen en verstuurd;
- Toepasselijke externe en interne eisen;
- Beheersmaatregelen voor beveiliging die al door de gemeente zijn geïmplementeerd ter ondersteuning van systeemontwikkeling;

- Betrouwbaarheid van personeel dat in de omgeving werkt;
- De graad van uitbesteding met betrekking tot systeemontwikkeling;
- De behoefte aan scheiding tussen verschillende ontwikkelomgevingen;
- Toegangsbeveiliging voor de ontwikkelomgeving;
- Monitoren van veranderingen aan de omgeving en de daarin opgeslagen codes;
- De beheersmaatregel dat back-ups worden bewaard op veilige externe locaties;
- Controle over bewegingen van gegevens van en naar de omgeving.

Systeemontwikkelomgevingen worden passend beveiligd op basis van een expliciete risicoafweging per ontwikkeltraject.

Referentie: *BIO versie 1.04zv beheersmaatregel 14.2.6.*

12.2. Onderhoud en wijzigingen

12.2.1. Procedures voor het wijzigingsbeheer met betrekking tot systemen

Wijzigingen aan systemen binnen de levenscyclus behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer (zie paragraaf 10.1.2). In deze procedure dienen ten minste de volgende onderdelen te worden opgenomen:

- Verslaglegging bijhouden van overeengekomen autorisatieniveaus;
- Waarborgen dat wijzigingen worden doorgevoerd door bevoegde gebruikers;
- Beheersmaatregelen en integriteitsprocedures beoordelen om te waarborgen dat deze niet worden gecompromitteerd door de wijzigingen;
- Alle software, informatie, database en hardware identificeren die wijziging behoeven;
- Beveiliging kritische codes identificeren en controleren om de waarschijnlijkheid van bekende zwakke plekken in de beveiliging zo gering mogelijk te houden;
- Formele goedkeuring voor gedetailleerde voorstellen verkrijgen voor aanvang van de werkzaamheden;
- Waarborgen dat bevoegde gebruikers de wijzigingen voorafgaand aan implementatie accepteren;
- Waarborgen dat de systeemdocumentatie na elke wijziging wordt geüpdatet en dat oude documentatie wordt gearchiveerd of verwijderd;
- Een audittraject voor alle wijzigingsverzoeken bijhouden;
- Waarborgen dat bedieningsdocumentatie en gebruikersprocedures indien nodig worden gewijzigd om ze toepasbaar te houden;
- Waarborgen dat het implementeren van wijzigingen op het juiste moment plaatsvindt en de betrokken bedrijfsprocessen niet verstoort.

Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheer raamwerk.

De introductie van nieuwe systemen en belangrijke wijzigingen aan bestaande systemen dient een formeel proces te volgen van documentatie, specificatie, testen, kwaliteitscontrole en beheerde implementatie. Dit proces dient een risicoanalyse, een analyse van de gevolgen van wijzigingen en een specificatie van de nodige beveiligingsbeheersmaatregelen te bevatten.

Referentie: *BIO versie 1.04zv beheersmaatregel 14.2.2 en 14.2.2.1.*

12.2.2. Technische beoordeling van toepassingen na wijzigen besturingsplatform

Besturingsplatforms bevatten besturingssystemen, databases en middlewareplatforms. Als besturingsplatforms zijn veranderd, behoren bedrijf kritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de gemeente. Voor de technische beoordeling dient een procedure opgesteld te worden waarin ten minste de volgende onderdelen zijn opgenomen:

- Beoordelen van procedures voor toepassingscontrole en integriteit om te waarborgen dat ze niet zijn gecompromitteerd door veranderingen aan het besturingsplatform;
- Waarborgen dat notificatie van veranderingen aan het besturingsplatform tijdig plaatsvindt zodat de aangewezen tests en beoordelingen voorafgaand aan implementatie plaats kunnen vinden;
- Bewerkstelligen dat de juiste veranderingen plaatsvinden aan de bedrijfscontinuïteitsplannen en bedieningsprocedures.

Referentie: *BIO versie 1.04zv beheersmaatregel 14.2.3.*

12.3. Testen

12.3.1. Bescherming van testgegevens

Het uitgangspunt is dat er niet getest mag worden met echte gegevens (lees: productiegegevens). Testgegevens dienen te worden gemaakt en mogen niet, zelfs bij toeval, herleidbaar zijn naar mensen.

Indien, wegens dwingende redenen, het noodzakelijk is dat er getest wordt met echte gegevens dienen hiervoor de volgende eisen te worden toegepast:

- Voorafgaand aan het overleggen van gegevens dient de proceseigenaar en systeemeigenaar schriftelijk toestemming te geven voor een zeer beperkte subset van deze gegevens middels het standaardformulier 'Autorisatie Testgegevens uit productie'. Deze toestemming dient centraal te worden vastgelegd waarbij de proces- en systeemeigenaar (automatisch) geïnformeerd worden bij het aflopen van de autorisatie.
- Productiegegevens mogen niet overgedragen worden aan een externe partij waar geen geheimhoudingsverklaring mee is aangegaan.

Standaardformulier Autorisatie Testgegevens uit productie
De volgende eisen zijn van toepassing op het formulier:

- De omvang van de subset dient vooraf te worden bepaald en te zijn afgestemd met de proceseigenaar en systeemeigenaar.
- De autorisatie heeft een begin- en einddatum.
  - o De einddatum is de datum waarop de testen zijn afgerond.

- Het formulier specifieert welke systemen en processen betrokken zijn.
- Het formulier specificeert hoe de gegevens worden overgedragen én welke goedgekeurde encryptiemiddelen worden toegepast.
- Het formulier specificeert hoe de gegevens aantoonbaar onomkeerbaar worden verwijderd direct na het verstrijken van de einddatum.
- Het formulier specificeert de maatregelen die worden genomen om het ongeautoriseerd kopiëren van de gegevens te verhinderen.

Voor testgegevens omtrent BSN's dient er te allen tijde gebruik te worden gemaakt van de 'Test Burgerservicenummers (BSN) en A-nummers (inclusief omnummertabel)' van de rijksoverheid.

Referentie: *BIO versie 1.04zv beheersmaatregel 14.3.1.*

12.3.2. Testen van systeembeveiliging

Systemen niet ontwikkeld door of in opdracht van de gemeente
Systemen die informatie bevatten met informatieclassificatieniveau 'Midden' of hoger dienen jaarlijks te worden getest qua beveiliging d.m.v. een penetratietest. De systeemeigenaar is verantwoordelijk voor het jaarlijks laten testen van de informatiebeveiliging.

Systemen ontwikkeld door of in opdracht van de gemeente
Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.

Referentie: *BIO versie 1.04zv beheersmaatregel 14.2.8.*

12.3.3. Systeemacceptatietesten

Systeemeigenaren dienen, in samenspraak met de proceseigenaren, voor alle systemen acceptatietesten en specifieke meetbare test criteria in een testplan vast te leggen. Voor acceptatietesten worden gestructureerde testmethodieken gebruikt die worden vastgelegd in het testplan. Acceptatietesten dienen de informatiebeveiligingseisen te bevatten als testcriteria.

Acceptatietesten dienen te worden uitgevoerd voor upgrades, substantiële wijzigingen en nieuwe versies van bestaande informatiesystemen én voor nieuwe informatiesystemen. De testen worden uitgevoerd op de acceptatieomgeving en bij voorkeur geautomatiseerd.

De testen dienen tevens te worden uitgevoerd op ontvangen componenten en geïntegreerde systemen.

Van de resultaten van de testen wordt een verslag gemaakt door de systeemeigenaar. Dit verslag wordt opgeslagen in een centraal registratiesysteem. De verslagen worden door de systeemeigenaar kenbaar gemaakt aan de proceseigenaar, team Informatiemanagement en de CISO.

Referentie: *BIO versie 1.04zv beheersmaatregel 14.2.9.*

13. Acquisitie en leveranciersrelaties

Leveranciers van diensten en producten dienen aan het informatiebeveiligingsbeleid van de gemeente te voldoen.

13.1. Informatiebeveiligingsbeleid voor leveranciers

13.1.1. Eisen aan offertes, aanbestedingen en (uitbreiding van) contracten

Voorafgaand aan het aanvragen van een offerte of aanbesteding of het afsluiten van (een uitbreiding van) een contract dient er bepaald te worden of informatie een rol speelt in de te leveren dienst / product. Indien informatie een rol speelt worden er eisen gesteld aan de leverancier en de dienst of product. Om te bepalen welke eisen gesteld moeten worden dient de informatie allereerst geclassificeerd te worden. Indien meerdere soorten informatie met verschillende classificaties in dezelfde dienst / product gebruikt worden dan geldt de hoogste classificatie.

De volgende eisen dienen te allen tijde gesteld te worden bij uitvraag van een aanbesteding, offerte en in de vastlegging van de uiteindelijke contracten:

- Er dient vastgesteld te worden of een verwerkersovereenkomst noodzakelijk is.
- Er dient een geheimhoudingsclausule opgenomen worden die voor alle betrokkenen geldt.
- Applicaties en IT-systemen dienen minimaal 95% van de tijd bereikbaar te zijn.
- De gemeente wordt binnen 24 uur op de hoogte gesteld van een datalek of beveiligingsincident bij de leverancier.
- Informatie van de gemeente of daaruit af te leiden informatie mag niet gebruikt worden voor andere doeleinden dan expliciet in de offerte zijn benoemd.
- Het eigenaarschap van de informatie dient vastgelegd te zijn in offertes en contracten. De gemeente is standaard eigenaar van de informatie.
- Commercieel verhandelen van informatie van de gemeente is niet toegestaan tenzij expliciet aangegeven in de offerte en het contract.
- De gemeente houdt zich het recht voor om audits uit te voeren op de leverancier om te beoordelen of de leverancier conform de opgenomen eisen in de offerte en dit beleid werkt.
- In de offerte wordt de bewaartermijn van de informatie expliciet benoemd. De leverancier toont aan dat de informatie na de bewaartermijn onomkeerbaar verwijderd is.
- De leverancier verplicht zich om mee te werken met de jaarlijkse beoordeling van de dienstverlening conform de afgesproken informatiebeveiligingseisen. Dit doet de leverancier door periodiek (maandelijks of jaarlijks) verantwoordingsrapportages op te leveren. De exacte periodieke verantwoordingstermijn dient opgenomen te worden in de offerte en het contract.
- Consequenties voor de leverancier voor het niet nakomen van de afspraken betreffende informatiebeveiliging dienen opgenomen te zijn in de ‘boeteclausule’.
- Bij IT gerelateerde diensten en producten zijn de meest recente GIBIT-voorwaarden van toepassing.
- Bij aanschaf van een dienst / product wordt een dienstverleningsovereenkomst gesloten (zie paragraaf 13.1.2).
- De leverancier verplicht zich te voldoen aan de geldende eisen omtrent informatietransport (zie paragraaf 11.2).
- De leverancier van software dient jaarlijks een ‘bill of material’ aan te leveren waarin de geleverde software inclusief de versies van deelproducten staan benoemt.

De volgende eisen dienen minimaal additioneel gesteld te worden per classificatieniveau:

Classificatie: Laag

- Voorafgaand aan verlening van de opdracht dient een verwerkersovereenkomst (waar nodig) te zijn afgesloten.
- Voorafgaand aan verlening van de opdracht dient een dienstverleningsovereenkomst (DVO) te zijn afgesloten.

Classificatie: Midden

- Alle eisen van classificatie Laag.
- Medewerkers van de leverancier mogen zonder expliciete toestemming (per medewerker) geen toegang hebben tot de informatie van de gemeente. Hiervoor dient de systeemeigenaar het modeldocument ‘Toestemming toegang informatie gemeente Medemblik’ te laten ondertekenen door de medewerker van de leverancier en het op de daarvoor bestemde centrale plek te registreren.

- De leverancier dient aantoonbaar te voldoen aan informatiebeveiligingseisen. Minimale eisen zijn een assurance rapport conform ISO27001 (of certificaat) of de meest recente Baseline Informatiebeveiliging Overheid (BIO) die niet ouder is dan 1 jaar.
- Applicaties en IT-systemen dienen minimaal 99,95% van de tijd bereikbaar te zijn.
- Alle informatie wordt versleuteld opgeslagen en gecommuniceerd conform moderne versleutelingsstandaarden (zie hoofdstuk 8). De leverancier informeert de CISO van de gemeente over de toegepaste encryptie én past de door gemeente voorgeschreven versleutelingsstandaarden toe. De leverancier verplicht zich tevens tot medewerking voor het bijwerken van versleutelingsstandaarden wanneer de gemeente dit noodzakelijk acht.

Classificatie: Hoog
- Alle eisen van classificaties Laag en Midden.
- Alle eisen zoals benoemt in het 'Incident Response Plan' in het kader van classificatie Hoog.
- De leverancier levert maandelijkse verantwoordingsrapportages aan ten aanzien van de informatiebeveiliging conform het reglement 'Verantwoordingsrapportages gemeente Medemblik'.
- Applicaties en IT-systemen dienen minimaal 99,99% van de tijd bereikbaar te zijn.
- De gemeente wordt binnen 12 uur op de hoogte gesteld van een datalek of beveiligingsincident bij de leverancier.

Referentie: *BIO versie 1.04zv beheersmaatregel 15.1.1.*

13.1.2. Dienstverleningsovereenkomsten
Dienstverleningsovereenkomsten dienen minimaal de volgende onderdelen te bevatten:
- scope van de dienstverlening.
- omschrijving van de te verlenen dienst.
- de duur van de te verlenen dienst.
  - Inclusief ingangsdatum en datum einde dienstverlening.

- de betrokken partijen (inclusief onderaannemers) van de te verlenen dienst.
- de contactpersoon bij incidenten van de te verlenen dienst.
- concrete verantwoording hoe de leverancier gaat voldoen aan de eisen.
- geheimhoudingsclausule.
- exit clausule / strategie.
- eigenaarschap van de informatie (data).

13.1.3. Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
Alvorens een contract mag worden afgesloten waarin informatie een rol heeft dient er aan de volgende eisen te zijn voldaan:
1. De beveiligingseisen die in de paragraaf 13.1.1 van toepassing zijn dienen te worden opgenomen in de definitieve contracten.
2. Voordat een contract wordt afgesloten, wordt in een risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is. Een vast onderdeel van het contract is een expliciete uitwerking van de exit-strategie.
3. Er dient opgenomen te zijn wat de procedure is in geval de leverancier in gebreke blijft.
4. Eisen die zijn afgeleid van de bedrijfsprocessen, zoals het registreren en monitoren van transacties dienen opgenomen te worden.
5. Eisen die verplicht zijn gesteld door andere beheersmaatregelen met betrekking tot beveiliging dienen te worden opgenomen.
6. Procedures voor het verlenen van toegang en autorisatie, voor zakelijke en voor bevoorrechte of technische gebruikers dienen te zijn vastgelegd.
7. Bij het kopen van producten behoort een formele test- en acquisitieprocedure te worden gevolgd.
8. De vereiste beschermingsbehoeften van de betrokken bedrijfsmiddelen, in het bijzonder met betrekking tot de beschikbaarheid, vertrouwelijkheid en integriteit zijn meetbaar vastgelegd.
9. Bij nieuwe informatiesystemen en bij wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging worden uitgevoerd ten behoeve van het vaststellen van de beveiligingseisen middels een risicoanalyse. Resultaten van de risicoanalyse worden schriftelijk gedocumenteerd en beoordeeld door alle belanghebbenden.
10. Na afsluiting dienen gebruikers en operators geïnformeerd te worden over hun plichten en verantwoordelijkheden.

Referentie: *BIO versie 1.04zv beheersmaatregel 14.1.1 & 15.1.2.*

13.2. Uitbesteding softwareontwikkeling

Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de gemeente. Een voorwaarde voor uitbestedingstrajecten is een expliciete risicoafweging. De noodzakelijke beveiligingsmaatregelen die daaruit volgen worden aan de leverancier opgelegd. Bij het uitbesteden van de softwareontwikkeling dienen de volgende punten in de gehele externe toeleveringsketen van de gemeente in acht te worden genomen:

- Licentieovereenkomsten, eigendom van de broncode en intellectuele-eigendomsrechten in verband met de uitbestede inhoud (zie paragraaf 16.1);
- Contractuele eisen voor beveiligde ontwikkel-, coderings- en testpraktijken (zie ook paragraaf 12.2.1);
- Het goedgekeurde dreigingsmodel aan de externe ontwikkelaar beschikbaar stellen;
- Acceptatietests voor de kwaliteit en nauwkeurigheid van de leveringen;
- Bewijs leveren dat beveiligingsdrempels zijn gebruikt om minimumacceptatieniveaus voor de veiligheid en kwaliteit van privacy toe te passen;
- Bewijs leveren dat voldoende tests zijn uitgevoerd om te waken voor de aanwezigheid van bekende kwetsbaarheden;
- Contractueel recht om ontwikkelprocessen en beheersmaatregelen te auditen;
- Doeltreffende documentatie van de gebouwde omgeving die wordt gebruikt om af te leveren producten te creëren;
- De gemeente blijft verantwoordelijk voor naleving van toepasselijke wetten en verificatie van de doelmatigheid van de controle.

Referentie: *BIO versie 1.04zv beheersmaatregel 14.2.7.*

13.3. Beheer van dienstverlening van leveranciers

13.3.1. Monitoring en beoordeling van dienstverlening van leveranciers

Jaarlijks wordt de prestatie van leveranciers op het gebied van de informatiebeveiliging beoordeeld. De beoordeling bestaat uit het verifiëren of de dienstverlening van de leverancier afgelopen jaar heeft voldaan aan de gestelde eisen qua informatiebeveiliging. De beoordeling wordt uitgevoerd door de interne auditor. De beoordeling dient vastgelegd te worden in het zakensysteem van de gemeente en wordt gecontroleerd door de CISO / ISO. Indien de leveranciers niet aan de afgesproken eisen voldoen escaleert de CISO / ISO naar het verantwoordelijke budgethouder. De budgethouder dient opvolging te geven aan het advies wat de CISO / ISO uitbrengt en de 'in gebreke procedure' in werking te stellen.

Referentie: *BIO versie 1.04zv beheersmaatregel 15.2.1.*

13.3.2. Beheer van veranderingen in dienstverlening van leveranciers

Wanneer de dienstverlening van een leverancier wijzigt dient er een herbeoordeling plaats te vinden op de volgende onderwerpen:

1. Informatieclassificatie.
2. Risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is.
3. Beoordeling toepasselijkheid exit-strategie.

Indien nieuwe inzichten leiden tot aanpassingen in het informatiebeveiligingsbeleid van de gemeente die gevolgen hebben voor de geleverde dienstverlening dient er naar de volgende onderwerpen gekeken te worden:

1. Indien afspraken dat toelaten dient de leverancier eventuele technische wijzigingen met betrekking tot versleuteling op last van de gemeente door te voeren.

Referentie: *BIO versie 1.04zv beheersmaatregel 15.2.2.*

14. Beheer van informatiebeveiligingsincidenten

Voor het beheer van informatiebeveiligingsincidenten dient een 'Incident Response Plan' aanwezig te zijn conform de nieuwste versie van 'Handreiking Incident- en response management' van de VNG.

14.1. Beheer van informatiebeveiligingsincidenten en – verbeteringen

14.1.1. Verantwoordelijkheden en procedures

Reguliere incidenten

Onder reguliere incidenten worden informatiebeveiligingsincidenten verstaan die geen verregaande impact hebben op de dienstverlening en er geen sprake is van een hoge mate van urgentie.

Informatiebeveiligingsincidenten worden gemeld bij de CISO of de ISO. Iedereen die constateert dat er sprake is van een mogelijk incident dient dit te melden. Indien men incidenten niet meldt kan de disciplinaire procedure in gang gezet worden.

De CISO / ISO dient de systeemeigenaar van het getroffen systeem én de proceseigenaar van het getroffen proces te informeren over het incident. Indien er persoonsgegevens bij het incident zijn betrokken dient tevens de Privacy Officer en Functionaris Gegevensbescherming te worden geïnformeerd. De coördinatie van de afhandeling van informatiebeveiligingsincidenten is belegd bij de CISO. De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.

Op advies van de CISO / ISO voert de systeemeigenaar en proceseigenaar maatregelen door. De CISO is, in het kader van informatiebeveiligingsincidenten, verantwoordelijk om alle incidenten centraal te registeren.

In voortgangsrapportages naar het strategisch managementteam en het directieteam informeert de CISO op hoofdlijnen over de voorgedane informatiebeveiligingsincidenten, de gelopen risico's en of de risico's zijn gemitigeerd. Deze rapportage dient minimaal tweemaandelijks te worden verstrekt.

Bijzondere situaties
Indien de CISO constateert dat een incident verregaande impact heeft, zie paragraaf 14.1.2, op de dienstverlening of dat er een hoge mate van urgentie is dan wordt de directie op de hoogte gesteld. De directie is eindverantwoordelijk voor bijzondere situaties en dient actief op te treden. De directie stelt direct een 'incident response team' aan en stelt het 'Incident response plan' in werking.

Het 'incident response team' bestaat minimaal uit:
- De gemeentesecretaris.
- De CISO (of de ISO in geval de CISO niet beschikbaar is).
- De strategisch manager(s) van de afdeling(en) waarvan de dienstverlening wordt getroffen.
- De proceseigenaar van de getroffen processen.
- De systeemeigenaar van de getroffen systemen.

In de arbeidsvoorwaarden van bovenstaande functies dient opgenomen te worden dat men buiten kantooruren en in het weekend bereikbaar is in het geval van een bijzondere situatie omtrent de informatiebeveiliging. In deze clausule dient tevens te staan dat men verplicht is mee te werken aan het mitigeren van deze risico's buiten kantooruren.

Indien nodig wordt het team per casus uitgebreid met andere specialisten uit de gemeente.

Bijzondere situaties worden apart vastgelegd en dienen direct te worden gecommuniceerd naar het college én de afhandeling dient besproken te worden in de eerstvolgende vergaderingen van het DT en SMT.

Leveranciers
Leveranciers van de gemeente dienen, ongeacht van het classificatieniveau van de informatie, de contracteigenaar binnen de gemeente binnen 24 uur op de hoogte stellen van informatiebeveiligingsincidenten die zich bij hen of in de productieomgeving hebben voorgedaan. De contracteigenaar meldt dit direct bij het meldloket.

Verder dient de leverancier aantoonbaar in het bezit te zijn van een incident response plan die voldoet aan de ISO27001 en ISO27002 normen.

Referentie: *BIO versie 1.04zv beheersmaatregel 16.1.1.*

14.1.2. Rapportage van informatiebeveiligingsgebeurtenissen
Informatiebeveiligingsgebeurtenissen dienen zo snel mogelijk te worden gemeld. Hiervoor is het noodzakelijk dat:
- Er een meldloket is waar beveiligingsincidenten worden gemeld;
  - o De CISO ontvangt direct een kopie van elke melding die gedaan wordt.
- Er een meldprocedure is waarin de taken en verantwoordelijkheden van het meldloket staan beschreven;
- Iedereen die gemeentelijke werkzaamheden verricht aantoonbaar hebben kennisgenomen van de meldingsprocedure van incidenten;
- Incidenten zo snel mogelijk, maar in ieder geval binnen 24 uur na bekendwording, worden gemeld;
- De proceseigenaar verantwoordelijk is voor het oplossen van de beveiligingsincidenten;

- De opvolging van incidenten wordt minimaal tweemaandelijks gerapporteerd door de CISO aan het SMT en wanneer nodig aan de directie (zie paragraaf 14.1.1);
- Een Coordinated Vulnerability Disclosure (CVD) procedure is gepubliceerd en ingericht;
- Informatie afkomstig uit de Coordinated Vulnerability Disclosure procedure onderdeel is van de incidentrapportage.

Iedereen die werkzaamheden verricht voor de gemeente en die gebruikmaken van de informatiesystemen en -diensten van de gemeente dienen de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging te registreren en te rapporteren.

Referentie: *BIO versie 1.04zv beheersmaatregel 16.1.2 en 16.1.3.*

14.1.3. Beheer van informatiebeveiligingsincidenten en -verbeteringen

Informatiebeveiligingsgebeurtenissen dienen te worden beoordeeld of de gebeurtenis geclassificeerd wordt als informatiebeveiligingsincident conform de handreiking 'Classificatie Informatiebeveiligingsgebeurtenissen'.

Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatie verwerkende systemen, behoren zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd te worden gemeld aan de sectorale CERT.

Referentie: *BIO versie 1.04vz beheersmaatregel 16.1.4 & 16.1.4.1.*

14.1.4. Respons op informatiebeveiligingsincidenten

Nadat er beoordeeld is of een informatiegebeurtenis een incident is kan er gereageerd worden op het incident. Voor de respons op informatiebeveiligingsincidenten is een Incident Response Plan beschikbaar. Voor bijzondere incidenten zijn scenariokaarten voor specifieke situaties beschikbaar die i.p.v. het Incident Response Plan gevogld kunnen worden..

In het plan moeten minimaal de volgende eisen zijn beschreven:

- Diverse standaard scenario's dienen uitgewerkt te zijn waarbij:
  - Wie verantwoordelijk is voor opvolging van het incident en de te nemen maatregelen.
  - Wie geïnformeerd moet worden en bij wie advies ingewonnen moet worden.
  - Indien geen scenario toepasselijk is dan is standaard de proceseigenaar verantwoordelijk opvolging van het incident en de te nemen maatregelen.

- Dat de CISO bij ieder incident dient te worden geïnformeerd;
- Hoe bewijs zo snel mogelijk wordt verzameld en vastgelegd (zie paragraaf 14.1.5);
- Welke middelen beschikbaar zijn t.b.v. een forensische analyse van de informatiebeveiliging en hoe deze toegepast kunnen worden;
- Hoe er geëscaleerd kan worden en wanneer;
- Hoe de responsactiviteiten van het incident worden vastgelegd voor latere analyse;
- Welke tijdelijke noodmaatregelen kunnen worden toegepast om verdere schade van het incident te beperken;
- Hoe de formele afsluiting van het incident en de verslaglegging wordt afgehandeld zodra het incident succesvol is behaald.
  - Hoe zwakke plek(ken) in de informatiebeveiliging die ten grondslag lagen aan het incident in de toekomst worden voorkomen (zie paragraaf 14.1.6).

Referentie: *BIO versie 1.04vz beheersmaatregel 16.1.5.*

14.1.5. Verzamelen van bewijsmateriaal

In het Incident Response Plan dient de gemeente procedures en richtlijnen vast te stellen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen en voor analysedoeleinden kan worden gebruikt.

De verzamelde informatie van het informatiebeveiligingsincident dient minimaal drie jaren bewaard te worden op een centrale locatie en heeft informatieclassificatieniveau 'Hoog'.

Referentie: *BIO versie 1.04vz beheersmaatregel 16.1.7.*

14.1.6. Leren van informatiebeveiligingsincidenten

De gemeente dient een proces in te richten met het doel om te leren van incidenten. Onderdeel van dit proces is de handreiking 'Leren van informatiebeveiligingsincidenten'. In de handreiking moeten minimaal de volgende zaken terugkomen:

- De evaluatie procedure met betrekking tot de reactie op incidenten.
- De evaluatiecriteria.
- De afspraken betreffende evaluatie van reacties op incidenten door leveranciers.

Referentie: *BIO versie 1.04vz beheersmaatregel 16.1.6.*

15. Informatiebeveiligingsaspecten bedrijfscontinuïteitsbeheer

15.1. Informatiebeveiligingscontinuïteit plannen

De gemeente behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijvoorbeeld een crisis of een ramp, vast te stellen.

15.1.1. Inventarisatie belangrijkste bedrijfsprocessen

Om dit te waarborgen dient de gemeente in het bezit te zijn van een inventarisatie van haar belangrijkste bedrijfsprocessen. Per bedrijfsproces dienen de volgende zaken geïnventariseerd te zijn:

- de bijbehorende informatiesystemen;
- hoe de organisatie wordt beïnvloed door storingen van één systeem en storingen van een combinatie van systemen;
- welke contractuele verplichtingen er zijn per informatiesysteem en hoe deze ingezet kunnen worden in het geval van een storing;
- welke nalevingsproblemen onderkend kunnen worden t.a.v. informatiebeveiligingseisen;
- interne (functies / medewerkers) en externe afhankelijkheden identificeren.

De proceseigenaar is verantwoordelijk voor bovenstaande inventarisatie die periodiek, minimaal jaarlijks, moet worden geëvalueerd.

15.1.2. Strategisch plan

De directie in samenwerking met het SMT dient een strategisch plan op te stellen waarin de meest kritische bedrijfsprocessen en de verantwoordelijkheden worden gedefinieerd in het kader van bedrijfscontinuïteit.

De gemeentesecretaris dient te beslissen wat de prioriteiten zijn voor de gemeente en dit vast te leggen. De bedrijfsprocessen worden onderscheiden in:

- Bedrijfsprocessen die geen dag uitgesteld kunnen worden;
- Bedrijfsprocessen die maximaal 1 dag uitgesteld kunnen worden;
- Bedrijfsprocessen die maximaal 3 dagen uitgesteld kunnen worden;
- Bedrijfsprocessen die maximaal 1 week uitgesteld kunnen worden;

Bedrijfsprocessen die maximaal 1 maand uitgesteld kunnen worden.

15.1.3. Proces plannen

Per proces dient er een bedrijfscontinuïteitsplan te zijn waarbij minimaal aandacht wordt besteed aan:

- De scope van het plan.
- Verantwoordelijkheden;
- O.a. wie het bedrijfscontinuïteitsplan mag activeren en wanneer, maar ook wanneer er weer gecontroleerd wordt teruggegaan;
- Strategische factoren en middelen;
- De mate van impact die een verstoring kan veroorzaken en hierbij behorende impact analyse;
- Bedrijfscontinuïteitsafspraken met externe partijen;
- Risico's t.o.v. de continuïteit van het proces en hierbij behorende risicoanalyse;
- Identificatie van essentiële procedures voor bedrijfscontinuïteit;
- Veilig te stellen informatie (aanvaardbaarheid van verlies van informatie);
- Prioriteiten en volgorde van herstel en reconstructie;
- Documentatie van systemen en bedrijfsprocessen;
- Kennis en kundigheid van medewerkers om de bedrijfsprocessen weer op te starten.
- Incidentrespons en risicobehandeling;
- Periodieke testen van het BCP.

Referentie: *BIO versie 1.04vz beheersmaatregel 17.1.1 & 17.1.2.*

15.2. Informatiebeveiligingscontinuïteit Implementeren
Naar aanleiding van de bedrijfscontinuïteitsplannen dient de gemeenteprocessen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.

Zo dienen er adequate back-ups van alle systemen en gegevens te worden gemaakt en te worden opgeslagen op een veilige locatie. Hiervoor dient per informatieclassificatieniveau een back-up beleid aanwezig te zijn (zie paragraaf 10.3).

Er dienen minimaal jaarlijks oefeningen of testen uitgevoerd om de bedrijfscontinuïteitsplannen te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de bedrijfscontinuïteitsplannen bijgesteld.

In geval van een ongewenste situatie vindt communicatie richting medewerkers, klanten en andere belanghebbenden plaats, zodat zij op de hoogte worden gebracht van de situatie en wat er van hen verwacht wordt.

Referentie: *BIO versie 1.04vz beheersmaatregel 17.1.1, 17.1.2 en 17.1.3.*

15.3. Redundante componenten
Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen. Als de beschikbaarheid niet kan worden gegarandeerd door middel van de bestaande systeemarchitectuur, behoren redundante componenten of architecturen in overweging te worden genomen.

Het implementeren van redundante componenten kan risico's voor de integriteit of de vertrouwelijkheid van informatie en informatiesystemen introduceren, waarmee bij het ontwerpen van informatiesystemen rekening dient te worden gehouden.

Per proces dient aan de hand van de BCP's onderzocht te worden waar de redundantie moet worden ingebouwd. De teamleider Informatiemanagement, tezamen met de CISO, systeemeigenaar en proceseigenaar zijn hiervoor verantwoordelijk.

Referentie: *BIO versie 1.04vz beheersmaatregel 17.2.1.*

16. Naleving
16.1. Naleving van wettelijke en contractuele eisen

16.1.1. Vaststellen van toepasselijke wetgeving en contractuele eisen
Per proces dienen alle relevant wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de gemeente om aan deze eisen te voldoen behoren voor elk informatiesysteem en de gemeente expliciet te worden vastgesteld, gedocumenteerd en actueel te worden gehouden. De proceseigenaar is hiervoor verantwoordelijk.

De specifieke beheersmaatregelen en individuele verantwoordelijkheden om aan deze eisen te voldoen, dienen te worden gedefinieerd en gedocumenteerd. De proceseigenaar is ervoor verantwoordelijk om alle wetgeving die toepasselijk is voor het proces vast te stellen om te voldoen aan de eisen.

Referentie: *BIO versie 1.04vz beheersmaatregel 18.1.1.*

16.1.2. Intellectuele-eigendomsrechten
Onder intellectuele-eigendomsrechten vallen auteursrechten op software of documenten, ontwerprechten, handelsmerken, patenten en broncodelicenties. Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen behoren passende procedures te worden geïmplementeerd.

De volgende richtlijnen dienen te worden nageleefd om materiaal dat kan worden beschouwd als intellectuele eigendom te beschermen:
- Een beleid ten aanzien van de naleving van intellectuele-eigendomsrechten publiceren dat het wettig gebruik van software en informatieproducten definieert;
  - o vaststellen voor het handhaven van de juiste licentievoorwaarden;
  - o vaststellen voor het verwijderen van of aan anderen overdragen van software;
- Software alleen verkrijgen bij bekende bronnen met een goede reputatie, om te waarborgen dat het auteursrecht niet wordt geschonden;

- Het bewustzijn in stand houden van het beleid voor de bescherming van intellectuele-eigendomsrechten en bekendheid geven aan het voornemen om disciplinaire maatregelen te nemen tegen personeel dat deze rechten schendt;
- Geschikte registers van bedrijfsmiddelen bijhouden (zie hoofdstuk 6), en alle bedrijfsmiddelen waarbij bescherming van intellectuele-eigendomsrechten vereist is identificeren;
- Bewijs bijhouden van de eigendom van licenties op intellectuele eigendommen;
- Beheersmaatregelen implementeren om te bewerkstelligen dat een maximumaantal gebruikers dat door de licentie is toegestaan niet wordt overschreven;
- Beoordelingen uitvoeren om te controleren dat alleen goedgekeurde software en in licentie gegeven producten zijn geïnstalleerd;
- Voldoen aan voorwaarden voor software en informatie verkregen van openbare netwerken;
- Niet dupliceren, maar een ander formaat converteren of een uittreksel maken van commerciële opnamen, tenzij auteursrechtelijk is toegestaan;
- Geen boeken, artikelen, rapporten of software geheel of ten dele kopiëren, tenzij auteursrechtelijk toegestaan.

Schending van auteursrecht of andere intellectuele-eigendomsrechten kunnen leiden tot een geldboete of een strafproces voor de gemeente. De gemeente dient voor haar medewerkers de disciplinaire procedure te hanteren in het geval dat bovenstaande niet wordt nageleefd.

Referentie: *BIO versie 1.04vz beheersmaatregel 18.1.2.*

16.1.3. Beschermen van registraties

Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.
Bij besluitvorming over bescherming van specifieke registraties van de gemeente behoort de classificatie daarvan, gebaseerd op het classificatieschema van de gemeente, in overweging te worden genomen. Registraties worden gecategoriseerd naar type informatie. De proceseigenaar heeft per soort informatie inzichtelijk gemaakt wat de bewaartermijn is.

Met betrekking tot het veiligstellen van registraties dient binnen de gemeente de volgende stappen te worden genomen:

- Er dienen richtlijnen te worden verstrekt voor het bewaren, opslaan, behandelen en verwijderen van registraties en informatie;
- Er dient een bewaarschema opgesteld te worden waarin registraties en de periode dat deze moeten worden bewaard, zijn vastgelegd;
- Er dient een inventarisoverzicht van bronnen van belangrijke informatie te worden bijgehouden.

Referentie: *BIO versie 1.04vz beheersmaatregel 18.1.3.*

16.1.4. Privacy en bescherming van persoonsgegevens

Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassen, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving. Hiervoor heeft de gemeente een privacy beleid opgesteld.

In overeenstemming met de AVG heeft iedere gemeente een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren.

Gemeentes controleren regelmatig de naleving van de privacyregels en informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.

Referentie: *BIO versie 1.04vz beheersmaatregel 18.1.4.*

16.1.5. Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving. Hiervoor dient met de volgende punten rekening te worden gehouden:

- Beperkingen op de import of export van computer hardware en -software voor het uitvoeren van cryptografische functies;
- Beperkingen op de import of export van computer hardware en -software die zo zijn ontworpen dat er cryptografische functies aan kunnen worden toegevoegd;
- Beperkingen op de toepassing van codering;

- Verplichte of discretionaire toegang voor nationale autoriteiten tot informatie die door hardware of software is versleuteld om in de vertrouwelijkheid van de inhoud te voorzien.

Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de 'pas toe of leg uit'-lijst van het Forum, zie hiervoor hoofdstuk 8.

Referentie: *BIO versie 1.04vz beheersmaatregel 18.1.5.*

16.1.6. Naleving verplichtingen omtrent ENSIA, DigiD en Suwinet

ENSIA
In de voor ENSIA relevante functieprofielen dient medewerking tot de jaarlijks terugkerende self-assessment te worden opgenomen. Tevens dient (beperkte) toegang tot het online portaal van ENSIA in de autorisatiematrix voor deze functieprofielen te worden opgenomen. Voor deze functies dient tijd beschikbaar te worden gesteld om de self-assessment uit te voeren.

DigiD
Betreffende DigiD aansluitingen is de houder van de DigiD aansluiting de systeemeigenaar van het systeem waar de DigiD aansluiting wordt gebruikt tenzij er een aparte functie beschikbaar is waarin de verantwoordelijkheid voor de aansluiting anders wordt benoemd. Verder dient de gemeente in het bezit te zijn van een DigiD beleid.

Suwinet
Betreffende Suwinet is de houder van de Suwinet aansluiting de systeemeigenaar van het systeem waar de Suwinet aansluiting wordt gebruikt tenzij er een aparte functie beschikbaar is waarin de verantwoordelijkheid voor de aansluiting anders wordt benoemd. Verder dient de gemeente in het bezit te zijn van een Suwinet beleid.

16.2. Informatiebeveiligingsbeoordelingen

16.2.1. Onafhankelijke beoordeling van informatiebeveiliging

De aanpak van de gemeente ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld. De directie dient de onafhankelijke beoordeling te initiëren. Hiervoor is een vastgesteld auditplan waarin keuzes worden gemaakt voor welke systemen welk soort audits worden uitgevoerd.

De resultaten van de onafhankelijke beoordeling dienen vastgelegd en gerapporteerd te worden aan de directie die de beoordeling heeft geïnitieerd. Deze verslagen worden conform de wettelijke bewaartermijn bewaard.

De interne auditor is verantwoordelijk voor het uitvoeren van de onafhankelijke beoordeling. Eenmaal per jaar is een audit door een externe onafhankelijke auditor verplicht.

Indien in de onafhankelijke beoordeling wordt vastgesteld dat de aanpak en de implementatie van het beheer van informatiebeveiliging van de gemeente ontoereikend zijn, dient de directie corrigerende maatregelen te nemen.

Tot slot dient er een information securitymanagement system (ISMS) te zijn waarmee aantoonbaar de gehele plan-do-check-act cyclus op gestructureerde wijze wordt afgedekt.

Referentie: *BIO versie 1.04vz beheersmaatregel 18.2.1.*

16.2.2. Naleving van beveiligingsbeleid en normen

De directie behoort de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.

Voor de onderdelen waar dit beleid niet de wijze van beoordeling voorschrijft stelt het SMT, na inwinning van advies van de CISO, vast op welke manier er beoordeeld moet worden of er is voldaan aan de in dit beleid gestelde en hieruit voortvloeiende eisen.

De directie en het SMT zijn eindverantwoordelijk voor de beoordelingen en dienen erop toe te zien dat deze tijdig worden uitgevoerd. De proceseigenaren zijn verantwoordelijk voor de beoordelingen binnen de processen. De systeemeigenaren zijn verantwoordelijk voor beoordelingen binnen de systemen. En de teamleiders zijn verantwoordelijk voor de beoordelingen binnen hun teams.

Indien uit de beoordeling blijkt dat eisen of elementen hiervan niet worden nageleefd dienen de volgende stappen doorlopen te worden:

1. De oorzaken van de niet-naleving vaststellen;
2. De noodzaak evalueren tot het treffen van maatregelen om naleving te bewerkstelligen;
3. Een verbeterplan opstellen ongeacht de uitkomst van stap 2;
4. Passende corrigerende maatregelen implementeren uit het verbeterplan;
5. De getroffen corrigerende maatregelen beoordelen om de doeltreffendheid ervan te verifiëren en om gebreken of zwakke plekken te identificeren.
6. Van alle bovenstaande stappen dient een schriftelijke vastlegging op een centrale plaats te worden bijgehouden. De interne auditor wordt van iedere stap op de hoogte gehouden door de verantwoordelijke.

In de P&C-cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de reguliere, generieke verantwoording. Ieder kwartaal wordt het college op de hoogte gesteld van de resultaten en hieruit voortvloeiende acties van de beoordelingen door de interne auditor.

Referentie: *BIO versie 1.04vz beheersmaatregel 18.2.2.*

16.2.3. Beoordeling van technische naleving

Informatiesystemen behoren periodiek te worden gecontroleerd op technische naleving van de beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid door middel van technische kwetsbaarheidsanalyses of penetratietesten. Dergelijke tests behoren te worden gepland en gedocumenteerd en dienen herhaalbaar te zijn. De systeemeigenaar is hiervoor verantwoordelijk.

Van de informatiesystemen die geen informatie bevatten of verwerken met informatieclassificatieniveau 'Hoog' dienen jaarlijks een gedeelte van de systemen te worden gecontroleerd op technische naleving van de beveiligingsnormen. Geen enkel informatiesysteem mag langer dan 3 jaar niet gecontroleerd zijn.

Informatiesystemen die informatie bevatten of verwerken met informatieclassificatieniveau 'Hoog' dienen jaarlijks gecontroleerd te worden op technische naleving van de beveiligingsnormen.

Voor alle controles geldt dat dit aantoonbaar moet gebeuren. De systeemeigenaar levert nadat de controle is uitgevoerd een rapport of certificaat op naar de relevante proceseigenaren, de CISO en de interne auditor.

Beoordeling van technische naleving dient uitsluitend te worden uitgevoerd door competente, bevoegde personen of onder toezicht van dergelijke personen.

Referentie: *BIO versie 1.04vz beheersmaatregel 18.2.3.*

Bijlage 1: Deelproducten behorende bij het informatiebeveiligingsbeleid

Type document	Titel	Referentie in beleid	Eigenaar	Periodieke evaluatie
Risicoanalyse				
	Aanvaardbaar gebruik bedrijfsmiddelen	6.1.2	Strategisch Manager Bedrijfsvoering	Drie jaarlijks
	Risicoafweging toegang netwerk externe leveranciers	7.4.2	Teamleider Informatiemanagement	Jaarlijks
	Risicoanalyse reservecertificaten	8.2.1	Teamleider Informatiemanagement	Jaarlijks
Standaard document				
	Bruikleenovereenkomst bedrijfsmiddelen	6.1.2 6.1.3	Teamleider HR	Drie jaarlijks
	Aanvraagformulier logische toegang	7.1.1	Teamleider Informatiemanagement	Drie jaarlijks
	Verwijderbesluit apparatuur	9.2.7.3	Teamleider Informatiemanagement	Drie jaarlijks
	Autorisatie Testgegevens uit productie	12.3.1	Teamleider Informatiemanagement	Drie jaarlijks
	Toestemming toegang informatie gemeente Medemblik	13.1.1	Strategisch Manager Bedrijfsvoering	Drie jaarlijks
Reglement				
	Vernietiging opslagmedia	8.2.1 9.2.7.2	Teamleider Informatiemanagement	Drie jaarlijks
	Voorschrift wachtwoordbeheer	7.4.3	Chief Information Security Officer	Jaarlijks
	Goedgekeurde versleutelingstechnieken	Hoofdstuk 8	Chief Information Security Officer	Jaarlijks
	Plan fysieke toegangsbeveiliging	Hoofdstuk 9	College Burgemeester en Wethouders	Drie jaarlijks
	Sleutelplan zone 3	9.1.4	Teamleider Inkoop, JZ en FaZa	Drie jaarlijks
	Sleutelplan brandkasten zone 3	9.1.4	Teamleider Inkoop, JZ en FaZa	Drie jaarlijks
	Sleutelplan zone 4	9.1.4	Teamleider (betreffend team)	Drie jaarlijks
	Sleutelplan kluis zone 4	9.1.4	Teamleider (betreffend team)	Drie jaarlijks
	Nutsvoorzieningen plan	9.2.2	Teamleider Vastgoed en Grondzaken	Drie jaarlijks
	Thuiswerken gemeente Medemblik	9.2.6	Teamleider HR	Drie jaarlijks
	Geautoriseerde Software Whitelist	10.7	Strategisch Manager Bedrijfsvoering	Half jaarlijks
	Software Blacklist	10.7	Strategisch Manager Bedrijfsvoering	Half jaarlijks
	Voorschrift detectievoorzieningen gemeente Medemblik	11.1.2.1	Chief Information Security Officer	Jaarlijks
	Handreiking Telewerken	3.2 11.4	Teamleider HR	Drie jaarlijks
	Verantwoordingsrapportages gemeente Medemblik	13.1.1	Contracteigenaar	Jaarlijks
	Handreiking Classificatie Informatiebeveiligingsgebeurtenissen	145.1.3	Directie Team	Drie jaarlijks
	Handreiking Leren van informatiebeveiligingsincidenten	14.1.6	Directie Team	Drie jaarlijks

	Richtlijnen voor het bewaren, opslaan, behandelen en verwijderen van registraties en informatie;	16.1.3	Teamleider Informatiebeheer & Basisinformatie	Drie jaarlijks
	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	16.1.5	Teamleider Informatiemanagement	Drie jaarlijks
Beleid				
	Uitwisselingsbeleid media	6.2.3	Teamleider Informatiemanagement	Drie jaarlijks
	Logisch toegangsbeveiligingsbeleid	Hoofdstuk 7	Teamleider Informatiemanagement	Drie jaarlijks
	Cryptografisch sleutelbeheerbeleid	Hoofdstuk 8	Teamleider Informatiemanagement	Drie jaarlijks
	Bedrijfscontinuïteitsplan (BCP)	3.1.3 15.1.3	Verantwoordelijke teamleiders	Jaarlijks
	Incident Response Plan	3.1.3 14.1	Teamleider Informatiemanagement	Drie jaarlijks
	Updatebeleid software	9.2.4	Teamleider Informatiemanagement	Drie jaarlijks
	Back-up beleid	10.3	Teamleider Informatiemanagement	Drie jaarlijks
	Beleid Beveiligd Ontwikkelen	12.1.1	Teamleider Informatiemanagement	Drie jaarlijks
	Beleid ten aanzien van de naleving van intellectuele-eigendomsrechten	16.1.2	Teamleider Inkoop, JZ en FaZa	Drie jaarlijks
	Privacy beleid	16.1.4	College Burgemeester en Wethouders	Drie jaarlijks
	DigiD beleid	16.1.6	College Burgemeester en Wethouders	Drie jaarlijks
	Suwinet beleid	16.1.6	College Burgemeester en Wethouders	Drie jaarlijks
	Data Governance beleid.	5.3	Teamleider Informatiemanagement	Drie jaarlijks
Procedure				
	Aanvraag algemene identiteiten	7.1.1	Teamleider Informatiemanagement	Jaarlijks
	Autorisatieprocedure toegang netwerken en netwerkdiensten	7.1.2	Teamleider Informatiemanagement	Jaarlijks
	Autorisatieprocedure speciale toegangsrechten	7.2.3	Teamleider Informatiemanagement	Jaarlijks
	Autorisatieprocedure per functieprofiel per informatiebron	7.4.1	Teamleider Informatiemanagement	Jaarlijks
	Inlogprocedure	7.4.2	Teamleider Informatiemanagement	Jaarlijks
	Procedure broncode beheer	7.4.5	Teamleider Informatiemanagement	Jaarlijks
	Wijzigingsbeheer broncode	7.4.5 Hoofdstuk 12	Teamleider Informatiemanagement	Jaarlijks
	Toegangsprocedure zone 4 / werken in beveiligde gebieden	9.1.2 9.1.6	Teamleider (betreffende zone)	Jaarlijks
	Sleutelbeheer	9.1.2 9.1.3	Teamleider Vastgoed en Grondzaken	Jaarlijks
	Bescherming onbeheerde apparatuur	9.2.8	Teamleider Informatiemanagement	Jaarlijks

	Bedieningsprocedures systemen (specifiek server)	10.1.1	Verantwoordelijke teamleider	Jaarlijks
	Wijzigingsbeheer informatie verwerkende faciliteiten	10.1.2 12.2	Strategisch Manager Bedrijfsvoering	Jaarlijks
	Downloaden en uitvoeren bestanden	10.2.1	Teamleider Informatiemanagement	Jaarlijks
	Interne Audit procedure	10.4.2	Concern Controller Chief Information Security Officer	Jaarlijks
	Installeren Software	10.5	Teamleider Informatiemanagement	Jaarlijks
	Meldprocedure informatiebeveiligingsgebeurtenissen	14.1.2	Teamleider Informatiemanagement	Jaarlijks
	Coordinated Vulnerability Disclosure (CVD) procedure	14.1.2	Teamleider Informatiemanagement	Jaarlijks
	Technische beoordeling	12.2.2	Teamleider Informatiemanagement	Jaarlijks
Functieprofielen				
	Functieprofielen van alle functies met hierin de autorisatiematrix per functie per systeem	7.2.2	Strategisch Manager Bedrijfsvoering	Jaarlijks
	Risicovolle Profielen	7.2.3	Strategisch Manager Bedrijfsvoering	Jaarlijks
Gedragsregels				
	Gedragsregels informatiebeveiliging	4.1.2 6.1.3 7.3	College Burgemeester en Wethouders	Drie jaarlijks
Contactenoverzicht				
	Contactoverzicht overheidsinstanties	3.1.3	Chief Information Security Officer	Jaarlijks