Informatiebeveiligingsbeleid 2025

Gemeente Boekel

GEMEENTE BOEKEL
gastvrij & actief

Versiebeheer

Versie	Datum	Omschrijving	Auteur
0.9.6	25-11-2024	Conceptversie intern gedeeld	Frank Schaap
1.0	14-1-2025	Feedback verwerkt	Frank Schaap
1.0	21-1-2025	Vastgesteld	DT

Inhoud

Leeswijzer

Dit document volgt globaal de hoofdstukindeling van de Baseline Informatiebeveiliging Overheid (BIO 1.04zv) omdat die meer beschrijvende hoofdstuktitels heeft dan de BIO2. Alle relevante onderdelen en (aanvullende) maatregelen van de BIO2 zijn hierin verwerkt. Na inwerkingtreding van de Cyberbeveiligingswet in 2025 zal de BIO2 het vigerende normenkader zijn. Logius hanteert daarnaast het “Normenkader 3.0 voor ICT-beveiligingsassessments DigiD” wat voor de gemeente van toepassing is.

In dit document wordt op verschillende plaatsen gerefereerd naar specifieke documenten anders dan dit beleid. Waar dit voor de gemeente interne documenten betreft, zullen deze documenten in veel gevallen bij vaststelling van het beleid nog niet bestaan. Deze documenten moeten dus als onderdeel van de implementatie van het informatiebeveiligingsbeleid door de organisatie opgesteld worden.

In dit document wordt verwezen naar de rol van teamleider, ISO en Interne Auditor. Deze functies of rollen bestaan op moment van schrijven in de organisatie van gemeente Boekel niet. Dit wordt nader toegelicht in Hoofdstuk 3.

Terminologie

Term	**Afkorting van**	**Eventuele uitleg**
DT	Directieteam	-
CISO	Chief Information Security Officer	-
ISO	Information Security Officer	-
FG	Functionaris Gegevensbescherming	-
PO	Privacy Officer	
Proceseigenaar	-	Directeur of gemandateerde medewerker die eindverantwoordelijk is voor alle aspecten van een bedrijfsproces, van planning en uitvoering tot beheersing en controle.
Systeemeigenaar	-	Directeur of gemandateerde medewerker belast met het eigenaarschap van een specifiek systeem.
Functioneel beheerder	-	Medewerker verantwoordelijk voor de functionele beheerstaken van een applicatie of dienst, contact met en controle van de leverancier, eerste aanspreekpunt voor de eigen organisatie m.b.t. de applicatie.
Verbijzonderde Interne Controleur		Onafhankelijke persoon of afdeling buiten de reguliere lijn die de

		Verbijzonderde Interne Controles uitvoert.
VIC	Verbijzonderde Interne Controle	Een audit op de opzet, het bestaan en de werking van reguliere interne controles en beheersmaatregelen met als doel het verbeteren van interne processen, ondersteunen van risicomanagement en vergroten van transparantie.
ISO27001	-	Internationale standaard voor inrichting van beheersysteem voor informatiebeveiliging.
BIO / BIO 2	Baseline Informatiebeveiliging Overheid	Verplichtend normenkader specifiek gericht op Nederlandse overheidsorganisaties, gebaseerd op de internationale standaard ISO27001.
NIS / NIS 2	Network and Information Security directive	Europese richtlijn ter bevordering van de cyberbeveiliging en (cyber)weerbaarheid. De NIS 2 richtlijn wordt in Nederland als de Cyberbeveiligingswet geïmplementeerd en heeft geleid tot het opstellen van de BIO 2.
ENSIA	Eenduidige Normatiek Single Information Audit	Het systeem voor de jaarlijkse audit waarmee de gemeente verantwoording aflegt aan de toezichthouders over de mate van naleving van de wet- en regelgeving omtrent informatiebeveiliging. De DigiD-audit van Logius maakt hier onderdeel van uit.
DigiD	-	Het digitale authenticatiesysteem van de Nederlandse overheid.
Suwinet	-	Extra beveiligd netwerk van de Nederlandse overheid voor het uitwisselen van zeer gevoelige persoonsgegevens tussen de verschillende overheden.
VNG	Vereniging Nederlandse Gemeenten	-
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.
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.
RDI	Rijksdienst voor Digitale Infrastructuur	Toezichthouder op de wet- en regelgeving namens het ministerie van Binnenlandse Zaken.

1 Inleiding

1.1 Doel

Het **doel** van informatiebeveiliging is zorgen dat de processen van de organisatie ongestoord en veilig kunnen worden uitgevoerd en dat de gegevens die de gemeente van en namens inwoners en ondernemers verwerkt veilig en vertrouwelijk blijven. Het gaat dus om het waarborgen van de bedrijfscontinuïteit en daarmee is informatiebeveiliging een integraal onderdeel van de bedrijfsvoering.

De focus van informatiebeveiliging ligt daarbij op het beschermen van de (digitale) gegevensbronnen en informatieverwerkende systemen omdat de primaire processen van de gemeente daar in hoge mate van afhankelijk zijn. De essentiële processen van informatiebeveiliging zijn:

- identificeren van bedreigingen;
- inschatten welke risico's dit oplevert;
- opstellen van en adviseren over beheersmaatregelen om risico's te verkleinen;
- controleren en verbeteren van de effectiviteit van de beheersmaatregelen.

De uitvoering van de beheersmaatregelen vindt altijd plaats **in** de processen van de organisatie en is dus geen uitvoeringstaak van informatiebeveiliging an sich.

De Rijksoverheid heeft in 2020 vastgesteld dat overheidsorganisaties moeten voldoen aan het normenkader Baseline Informatiebeveiliging Overheid (BIO). Dit normenkader wordt in 2025 opgevolgd door de BIO2 en aangevuld met de Cyberbeveiligingswet. Hiermee geeft Nederland invulling aan de Europese Richtlijn NIS2.

In de Cyberbeveiligingswet is een **zorgplicht** voor de gemeente opgenomen: de gemeente moet risico's conform de BIO2-normen beheersen. Ook voert de Cyberbeveiligingswet een **meldplicht** in voor de incidenten die de gemeente treffen. Tenslotte regelt de Cyberbeveiligingswet op welke wijze jaarlijks **verantwoording** moet worden afgelegd aan de toezichthouder(s).

Dit informatiebeveiligingsbeleid schept voor gemeente Boekel de kaders voor het opstellen, implementeren, controleren en verbeteren van een samenhangend pakket aan beheersmaatregelen om de betrouwbaarheid en kwaliteit van de informatievoorziening te waarborgen conform de wet- en regelgeving.

1.2 Ambitie

Onze ambities voor informatieveiligheid zijn:

- We zijn aantoonbaar een betrouwbare partner voor de burgers, ondernemers en ketenpartners van de gemeente op het gebied van informatieveiligheid.
- We verwerken gegevens van burgers en ondernemers op een veilige manier door het implementeren van organisatorische en technische beveiligingsmaatregelen, conform wet- en regelgeving, waaronder BIO2, AVG, Wet BRP, WPG en CBW.
- We dragen bij aan het voorkomen en bestrijden van digitale criminaliteit en ondersteunen de samenleving bij het optreden van digitale incidenten.

1.3 Maatschappelijk belang

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

- Datalekken;
- Identiteitsfraude;
- Verlies van vertrouwen in de gemeente;
- Boetes, losgeld en herstelkosten.

1.4 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 de 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 gaat over:

- **Alle vormen van informatie:** analoog, digitaal, tekst, video, geluid, kennis, etc.
- **Alle mogelijke informatiedragers:** papier, elektronisch, foto, film, DVD, gesprekken, etc.
- **Alle informatie verwerkende systemen:** IT-systemen, databases, hardware, cloud diensten, communicatiemiddelen, bedrijfsmiddelen, archiefkasten, etc.
- **Alle informatie houdende partijen:** werknemers, bestuurders, ketenpartners, leveranciers, etc.

2 Informatiebeveiligingsbeleid

2.1 Doel van dit beleid

Het doel van dit beleid is om de gemeente in staat te stellen de beschikbaarheid, integriteit en vertrouwelijkheid 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, waarbij de gemeente voldoet aan relevante wet- en regelgeving.

Essentieel aan de implementatie van het beleid is een sluitende administratie van beslissingen en handelingen zodat bij interne en externe audits verantwoording afgelegd kan worden over de werking van de bedrijfsvoering en de effectiviteit van beheersmaatregelen. Het doel van de audits is om als organisatie te leren en te verbeteren en dus de bedrijfsvoering als geheel te verbeteren.

2.2 Scope

Dit beleid is van toepassing op de ambtelijke organisatie en het college van B&W van de gemeente Boekel. 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 Zorgplicht, meldplicht en toezicht

De Europese Richtlijn NIS2 wordt in Nederland omgezet in de Cyberbeveiligingswet. Gemeenten moeten voldoen aan de bepalingen voor ‘essentiële entiteiten’ onder de NIS2. Dat houdt onder andere in: een zorgplicht, meldplicht en toezicht.

De zorgplicht houdt in dat de gemeente:

- Moet zorgen voor een adequaat niveau van informatiebeveiliging;
- Proactief cyberbeveiligingsrisico's moet identificeren en aanpakken;
- Maatregelen moet implementeren om de weerbaarheid tegen cyberaanvallen te vergroten.

De meldplicht houdt in dat de gemeente informatiebeveiligingsincidenten met ‘aanzienlijke gevolgen’ moet melden:

- Incidenten moeten binnen 24 uur gemeld worden bij de toezichthouder (Rijksinspectie voor Digitale Infrastructuur, RDI) via de Informatiebeveiligingsdienst van de VNG;
- De exacte drempelwaarden voor wat geldt als ‘aanzienlijke gevolgen’ moeten nog worden vastgesteld in nadere regelgeving.

Het toezicht houdt in dat:

- Er toezicht komt op de beveiliging van de gemeentelijke ICT;
- De Rijksinspectie voor Digitale Infrastructuur (RDI) wordt aangewezen als toezichthouder voor de overheid, inclusief gemeenten;

- Er wordt onderzocht hoe ENSIA kan worden aangepast om te voldoen aan de eisen van NIS2-toezicht.

2.4 Bestuurlijke principes

Informatiebeveiliging is een gemeentebreed onderwerp, het betreft een kwaliteitsaspect in alle processen van de gemeente. Informatiebeveiliging is dus 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 opgestelde 10 principes:

- Bestuurders bevorderen een veilige cultuur;
- Informatiebeveiliging is van iedereen;
- Informatiebeveiliging is risicomanagement;
- Risicomanagement is onderdeel van de besluitvorming;
- Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking;
- Informatiebeveiliging is een proces;
- Informatiebeveiliging kost geld;
- Onzekerheid dient te worden ingecalculeerd;
- Verbetering komt voort uit leren en ervaring;
- Het bestuur controleert en evalueert.

Het bestuur faciliteert de gemeente in het op orde brengen en houden van de informatiebeveiliging.

Referentie		
BIO versie 2.0	beheersmaatregel	5.01.01
ISO 27001:2023	beheersmaatregel	5.1
BIO versie 1.04zv	beheersmaatregel	5.1.1.1.f

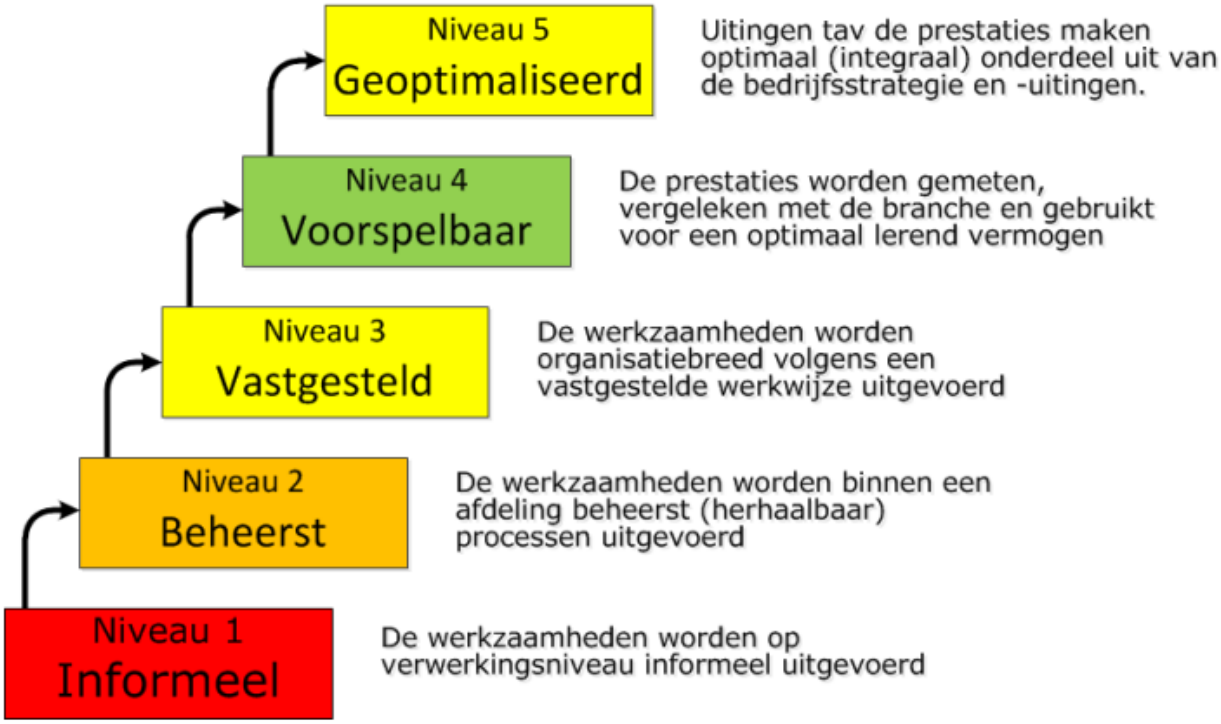
2.5 Verantwoordelijkheden

De organisatie van verantwoordelijkheden ten aanzien van informatiebeveiliging staat beschreven in hoofdstuk 3 van dit beleid.

Referentie		
BIO versie 2.0	beheersmaatregel	5.01.01, 5.02.01
ISO 27001:2023	beheersmaatregel	5.2
BIO versie 1.04zv	beheersmaatregel	5.1.1.1.b en 5.1.1.1.c

2.6 Strategische uitgangspunten

Het uitgangspunt voor de informatiebeveiliging voor gemeente Boekel is om te voldoen aan relevante wet- en regelgeving, in het bijzonder de Baseline Informatiebeveiliging Overheid (BIO/BIO2). Hierbij zetten we in om als organisatie duurzaam op een ‘voldoende’ niveau te functioneren. Een voldoende betekent dat niveau 3 van de BIO (zie afbeelding hieronder) wordt behaald binnen de gemeente.



Afbeelding: 1 - Niveaus Baseline Informatiebeveiliging Overheid.

Het duurzaam functioneren op niveau 3 wordt door veel gemeenten op dit moment als substantieel maar haalbaar doel gehanteerd. Als de organisatie enkele jaren op niveau 3 heeft gefunctioneerd, kan het nut en inspanning voor het stijgen naar een hoger niveau overwogen worden.

Het BIO niveau van de informatiebeveiliging van de gemeente wordt jaarlijks gemeten door middel van een onafhankelijke audit van een externe partij. De CISO is verantwoordelijk voor de coördinatie van de audit en stelt op basis van de resultaten een jaarplan met verbeteringen op. De directie is verantwoordelijk voor het doorvoeren van aanpassingen.

Verdere uitgangspunten voor de informatiebeveiliging zijn:

- Het informatiebeveiligingsbeleid is gebaseerd op de meest recente versie van de Baseline Informatiebeveiliging Overheid (BIO);
- Het informatiebeveiligingsbeleid wordt jaarlijks geëvalueerd en waar nodig herzien;
- Het informatiebeveiligingsbeleid is vastgelegd in dit document en is goedgekeurd door het college van B&W als eindverantwoordelijke ten aanzien van het beleid;
- Het beleidsdocument en de hieruit volgende producten zijn beschikbaar voor alle medewerkers van de gemeente en worden ontsloten via het intranet;
- De organisatie werkt risicogebaseerd aan informatiebeveiliging, voert periodiek risicoanalyses uit en bepaalt of bestaande beheersmaatregelen nog voldoen of dat er aanpassingen of nieuwe maatregelen nodig zijn;
- De informatie van en informatieverwerking door de gemeente moet beschikbaar, integer en vertrouwelijk zijn. De mate hiervan hangt af van het belang van de informatie voor de gemeente of haar inwoners en wordt vastgesteld door middel van dataclassificatie.

Referentie		
BIO versie 2.0	beheersmaatregel	5.01.01
ISO 27001:2023	beheersmaatregel	5.1
BIO versie 1.04zv	beheersmaatregel	5.1.1.1.a en 5.1.1.1.d

2.7 Randvoorwaarden

Randvoorwaarden ten aanzien van een efficiënte en effectieve uitvoering van dit beleid zijn:

- Het bestuur geeft ieder jaar expliciet aandacht aan informatiebeveiliging en committeert zich aan de uitvoering en naleving hiervan;
- Het bestuur en directie dragen zorg voor voldoende middelen en capaciteit om de maatregelen van dit beleid te implementeren, te onderhouden en na te leven;
- Het bestuur en de directieleden geven het goede voorbeeld en dragen het beleid uit waar en wanneer nodig;
- De directie voert een gestructureerde bedrijfsvoering:
    - (werk)processen van de organisatie zijn inzichtelijk en beschreven;
    - proceseigenaarschap en verantwoordelijkheden zijn belegd;
- De maatregelen worden een standaard onderdeel van de werkzaamheden en gemeentelijke processen gemaakt;
- Het niet naleven van de maatregelen dient middels een disciplinaire procedure niet getolereerd te worden;
- Uitvoering en naleving wordt periodiek getoetst verbeteringen worden geïmplementeerd.

Sommige informatiebeveiligingsmaatregelen vergen het monitoren en analyseren van netwerkverkeer, authenticatiegegevens en/of andere gebruiksgegevens van systemen, applicaties en diensten van de gemeente. Voor een groot deel betreft dit gegevens die ontstaan door het gebruik en werkzaamheden van de medewerkers. Bijzondere aandacht moet daarom gegeven worden aan het waarborgen van de privacy bij het monitoren en analyseren van die gegevens. Ook moeten medewerkers goed geïnformeerd zijn over hoe de monitoring en analyse werkt. De Ondernemingsraad moet betrokken zijn bij het opstellen en implementeren van deze maatregelen. Het privacybeleid van de gemeente is van toepassing.

Referentie		
BIO versie 2.0	beheersmaatregel	5.01.01
ISO 27001:2023	beheersmaatregel	5.1
BIO versie 1.04zv	beheersmaatregel	5.1.1.1.a en 5.1.1.1.d

2.8 Beoordeling van informatiebeveiligingsbeleid

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

- Zijn er nieuwe ontwikkelingen die een bedreiging vormen voor de informatiebeveiliging van de gemeente?
    - Zo ja, dient dit beleid hiervoor aangepast te worden?

    - Zo nee, onderbouw waarom niet.
- Zijn er door dit beleid hinderingen binnen de werkprocessen in de gemeente?
    - Zo ja, dient dit beleid hiervoor aangepast te worden?
    - Zo nee, onderbouw waarom niet.
- Zijn er andere redenen om dit beleid aan te passen?
    - Zo ja, welke?
    - Zo nee, onderbouw waarom niet.

Beoordelingen worden onder verantwoordelijkheid van de CISO uitgevoerd 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.

Contactmoment	Omschrijving	Frequentie	Betrokken rollen
Directieoverleg	Overleg om de maandelijkse rapportage toe te lichten en nieuwe of gewijzigde procedures en beheersmaatregelen af te stemmen	1x per maand	Directieteam & CISO
Beoordeling informatiebeveiligingsbeleid	Overleg om het beleid te beoordelen en eventueel te wijzigen	1x per jaar	CISO (& ISO)
GAP-analyse	Terugkoppeling BIO zelfevaluatie	1x per jaar	Directieteam & CISO
Interne audit (VIC)	Terugkoppeling van de Verbijzonderde Interne Controle	1x per jaar	Directieteam, CISO & Verbijzonderde Interne Controleur
Externe audit	Terugkoppeling van de externe audit	1x per jaar	Directieteam, CISO & Externe auditor
Informatiebeveiligingsbeleid vaststellen	Informatiebeveiligingsbeleid met wijzigingen en verbeteringen vaststellen	1x per jaar	College van B&W
ENSIA-rapportage	Vaststellen van de ENSIA-rapportage	1x per jaar	College van B&W

Als door ontwikkelingen aanpassingen niet kunnen wachten tot de formele beoordelingsmomenten, kan het DT het college 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.

Referentie		
BIO versie 2.0	beheersmaatregel	5.01.02
ISO 27001:2023	beheersmaatregel	5.1
BIO versie 1.04zv	beheersmaatregel	5.1.1.1.e en 5.1.2

2.9 Implementatie, ISMS en risicogebaseerd werken

Het informatiebeveiligingsbeleid wordt jaarlijks als een Plan-Do-Check-Act (PDCA) cyclus uitgevoerd en haakt aan bij de P&C-cyclus. We gebruiken een Information Security Management System (ISMS)[1], gebaseerd op de ISO 27001 standaard, om de verbetercyclus op een gestructureerde en aantoonbare wijze te doorlopen. Als onderdeel van de cyclus wordt jaarlijks een plan gemaakt welke verbeteringen en audits worden uitgevoerd.

Het belangrijkste bij het opstellen van beheersmaatregelen op basis van dit beleid is dat:

- Het (werk)proces goed is beschreven zodat een risicoanalyse uitgevoerd kan worden en een beheersmaatregel opgesteld kan worden;
- De maatregel het risico afdekt tot het niveau dat de proceseigenaar acceptabel vindt;
- Een maatregel in de praktijk goed, gebruiksvriendelijk en effectief uitgevoerd kan worden;
- Interne controle, evaluatie en verbetering integraal onderdeel uitmaken van de maatregelen en de processen waar ze op van toepassing zijn.

De beste informatiebeveiliging is wat je *doet,* niet wat je zou moeten doen.

2.9.1 Risicogebaseerd werken

Dit informatiebeveiligingsbeleid is gebaseerd op het principe van risicogebaseerd werken. De essentie van risicogebaseerd werken is het erkennen van onzekerheden en het in beeld brengen van mogelijke dreigingen en kwetsbaarheden in de processen en middelen van de organisatie. Het doel is **bewust** omgaan met risico's, beheersmaatregelen treffen en/of (rest)risico's accepteren. Hiermee komt de organisatie **in control** op de vlakken informatiebeveiliging en bedrijfscontinuïteit.

In control zijn betekent dat de organisatie in staat is om de bedrijfsprocessen beheerst te laten verlopen en voorspelbaar te handelen. Voorwaarde voor het beheersen van processen en voorspelbaar handelen, is dat de kaders en normen waar processen binnen moeten plaatsvinden helder beschreven zijn. Het "in control zijn" is zelf een continu proces van (bij)sturen, beheersen en toezicht houden.

De volgende stappen geven puntsgewijs de onderdelen van risicogebaseerd werken weer:

Risicoanalyse
Een grondige risicoanalyse vormt de basis van een risicogebaseerde aanpak. Dit omvat:

- Het identificeren van potentiële dreigingen en kwetsbaarheden die de processen en informatiesystemen van de organisatie kunnen beïnvloeden.
- Het in kaart brengen van alle bedrijfsprocessen, betrokkenen, informatiesystemen en -bronnen.
- Het classificeren van bedrijfsinformatie op basis van beschikbaarheid, integriteit en vertrouwelijkheid.

[1] Een ISMS is niet een specifieke applicatie, maar het samenhangende geheel van beleid, procedures, overlegstructuren, verantwoordelijkheden en controles die ervoor zorgen dat het informatiebeleid tot uitvoer wordt gebracht. De gemeente zet ook een ISMS-applicatie in om dit proces te ondersteunen.

Het uitvoeren van de risicoanalyse is een verantwoordelijkheid van de proceseigenaar en de eerste lijn: de medewerkers die het proces kennen en uitvoeren.

Risicobeoordeling en -prioritering

Na de identificatie van risico's moet een beoordeling plaatsvinden om:

- De impact en waarschijnlijkheid van elk risico te beoordelen en categoriseren.
- Risico's te prioriteren op basis van hun potentiële impact op de organisatie.
- Te bepalen welke risico's het meest kritiek zijn en onmiddellijke aandacht vereisen.

Risicomanagement

Op basis van de risicoanalyse en -beoordeling:

- Wordt voor elk geïdentificeerd risico bepaald of het beheerst, overgedragen, ontweken of geaccepteerd moet worden.
    - De proceseigenaar bepaalt op welke wijze en de mate waarin met het risico wordt omgegaan.
- Ontwikkelen en implementeren we passende beveiligingsmaatregelen om de geïdentificeerde risico's te beheersen.

Beleid en procedures

Het informatiebeveiligingsbeleid, procesbeschrijvingen en procedures bieden:

- Duidelijke richtlijnen voor het verwerken en beschermen van gevoelige informatie;
- Regels voor gegevensbescherming, beveiligingsmaatregelen en incidentrespons;
- Worden periodiek geëvalueerd en waar nodig herzien.

Implementatie van maatregelen

Implementatie van de gekozen beveiligingsmaatregelen, waarbij:

- De focus ligt op de meest kritieke gebieden, gebaseerd op de risicoanalyse.
- Maatregelen worden afgestemd op de specifieke behoeften en risico's van de organisatie en dat wordt bepaald door de proceseigenaar.

Bewustwording en training

De bewustwording onder medewerkers vergroten:

- Kennis en begrip van bedreigingen, risico's en maatregelen.
- Training over het informatiebeveiligingsbeleid en -procedures.
- Het belang van informatiebeveiliging en ieders rol daarin te benadrukken.

Continu proces en evaluatie

Informatiebeveiliging is een doorlopend proces dat vereist:

- Regelmatige evaluatie en herijking van bedreigingen, risico's en beheersmaatregelen.
- Implementatie van hulpmiddelen zoals een Information Security Management System (ISMS) om de PDCA-cyclus inzichtelijk en uitvoerbaar te maken.
- Interne controles om nieuwe risico's tijdig te signaleren en de beveiliging voortdurend te verbeteren.
- Actieve sturing op het beheerst en voorspelbaar uitvoeren van de (werk)processen en dit toetsen door (interne) controles.

Compliance en certificering/verantwoording

Het (kunnen) aantonen dat het ISMS en de verbetercyclus daadwerkelijk worden uitgevoerd en effectief zijn:

- Interne controles en rapportages.
- Audits en verantwoording aan toezichthouders conform de ENSIA.
- Mogelijk een certificering conform industrienormen zoals ISO 27001, die aantonen dat de organisatie *in control* is op informatiebeveiliging

Referentie		
BIO versie 2.0	beheersmaatregel	5.01.02, 5.35.01 en 5.35.02
ISO 27001:2023	beheersmaatregel	5.1 en 5.35
BIO versie 1.04zv	beheersmaatregel	18.2.1.1 en 18.2.1.2

2.10 Inwerkingtreding

Dit informatiebeveiligingsbeleid treedt in werking na vaststelling en ondertekening door college van B&W. Hiermee vervalt het Informatiebeveiligingsbeleid 2020.

3 Organiseren van informatiebeveiliging

3.1 Interne organisatie

Gemeente Boekel is een kleine organisatie met een platte organisatiestructuur. Voldoende personele capaciteit voor de taken is daarom een uitdaging, maar ook het aanbrengen van voldoende scheiding tussen rollen en verantwoordelijkheden. Functiescheiding is belangrijk om de integriteit van de processen te waarborgen. Als een persoon in een proces zowel kan controleren en besluiten of accorderen, dan ontstaat er een risico op onbedoelde of bedoelde fouten of het overslaan of uitstellen van noodzakelijke stappen en controles.

In dit beleid wordt verwezen naar de rol van teamleider, ISO en Interne Auditor. Deze functies of rollen bestaan op moment van schrijven in de organisatie van gemeente Boekel niet.

- Waar teamleider wordt geschreven, vallen voor gemeente Boekel de taken en verantwoordelijkheden toe aan de directeur, tenzij die bij een gemandateerde medewerker worden belegd. Mandatering kan in het kader van functiescheiding problematisch zijn.
- De rol Information Security Officer (ISO) verschijnt naast de CISO daar waar de omvang van de taken groot is, een vier-ogen-principe of domeinspecifieke kennis gewenst is.
- De interne controle is in de organisatie (nog) niet in een onafhankelijke rol buiten de lijn belegd.

Kortom, in de implementatie van dit beleid naar de procedures voor uitvoering moet extra aandacht zijn voor:

- Omvang en aantal van taken die bij één persoon kunnen liggen;
- Functiescheiding en afdoende verantwoordingsstructuur;
- Interne controle.

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.

Rol	Verantwoordelijkheden
Gemeenteraad	Controlerende functie en eindverantwoordelijk voor het beschikbaar stellen van voldoende middelen aan de gemeente om te voldoen aan dit beleid middels de begroting.
College van B&W	Verantwoordelijk voor de vaststelling, uitvoering en naleving van dit informatiebeveiligingsbeleid op het hoogste niveau.
Gemeentesecretaris	Verantwoordelijk voor de operationele naleving van dit beleid en het toekennen van voldoende middelen.
Sectordirecteur	Verantwoordelijk voor de uitvoering en naleving van dit beleid op sectorniveau én verantwoordelijk voor de ketens van informatiesystemen die onder hun afdeling vallen. Indien een keten van informatiesystemen niet onder één afdeling valt, zijn meerdere sectordirecteuren verantwoordelijk.
Chief Information Security Officer (CISO)	Kennishouder en verantwoordelijk voor advisering over bedreigingen, risico's en maatregelen. voor de controle op de uitvoering en naleving

	van dit beleid én dient tijdig de verantwoordelijken te wijzen op eventuele onvolkomenheden. Tevens is de CISO verantwoordelijk voor aanpassingen van dit beleid, advisering over informatiebeveiliging en beheersmaatregelen.
Information Security Officer (ISO)	Ondersteunt de CISO en de gemeente met betrekking tot operationele en beleidsmatige taken ten behoeve van de informatiebeveiliging.
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.
Proceseigenaar	Verantwoordelijk voor een proces binnen de gemeente.
Functioneel Applicatie Beheerder	Verantwoordelijk voor het beheer en de inrichting van een specifieke applicatie, onder andere het (de)activeren van gebruikers, het toekennen van rollen/rechten, wijzigingsbeheer en incidentenbeheer m.b.t. die applicatie.
Teamleider (c.q. coördinator of manager)	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.
Interne Auditor	Verantwoordelijk voor de interne toetsing van het informatiebeveiligingsbeleid (Verbijzonderde Interne Controleur).
Privacy Officer	De Privacy Officer is verantwoordelijk voor de controle van de naleving van de AVG en de privacyregels uit dit beleid.
Functionaris Gegevensbescherming (FG)	De FG is verantwoordelijk voor het houden van toezicht op de toepassing en naleving van de AVG en de Wpg.
ENSIA-coördinator	Verantwoordelijk voor de coördinatie en het indienen van de jaarlijkse ENSIA-verantwoording en DigiD-audits.
Medewerker	Verantwoordelijk voor het uitvoeren van het informatiebeveiligingsbeleid binnen haar of zijn werkzaamheden.

3.1.1.1 *CISO*

De CISO dient aangesteld te zijn conform een door het college vastgesteld CISO-functieprofiel. In dit functieprofiel zijn de rol en de verantwoordelijkheden van de CISO vastgelegd. De directie is verantwoordelijk voor het aanstellen van een CISO conform een vastgesteld CISO-functieprofiel.

3.1.1.2 *Besluitvorming*

De verantwoordelijkheden voor het vaststellen van beleid, procedures en maatregelen die voortvloeien uit of samenhangen met dit informatiebeveiligingsbeleid zijn als volgt belegd:

Besluitvormingsstuk	Verantwoordelijke
Informatiebeveiligingsbeleid	College van B&W
Beleid met een publieke of mogelijk politiek gevoelige strekking	College van B&W
Intern beleid, procedure of maatregel organisatiebreed	Directieteam
Intern beleid, procedure of maatregel van toepassing binnen één sector	Sectordirecteur
Intern beleid, procedure of maatregel van toepassing binnen één proces	Proceseigenaar

Referentie

BIO versie 2.0	beheersmaatregel	5.01.01, 5.02.01, 5.02.03
ISO 27001:2023	beheersmaatregel	5.1 en 5.2
BIO versie 1.04zv	beheersmaatregel	5.1.1.1.f , 5.1.1.1.c en 6.1.1

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 niet 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.

Functies die niet bij eenzelfde persoon belegd mogen zijn								
	Proces-eigenaar	Systeem-eigenaar	Teamleider	CISO	Interne Auditor	DT lid	Func. Beheerder	Procesmedewerker
Proces-eigenaar	v	x	x	x	x	v	x	x
Systeem-eigenaar	x	v	v	x	x	v	x	x
Teamleider	x	v	v	x	x	x	x	x
CISO	x	x	x	v	x	x	x	x
Interne Auditor	x	x	x	x	v	x	x	x
DT lid	x	x	x	x	x	v	x	x
Func. Beheerder	x	x	x	x	x	x	v	v
Procesmedewerker	x	x	x	x	x	x	v	v

Referentie		
BIO versie 2.0	beheersmaatregel	5.03.01
ISO 27001:2023	beheersmaatregel	5.3
BIO versie 1.04zv	beheersmaatregel	6.1.2

3.1.3 Contact met overheidsinstanties en belangengroepen

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

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 2.0	beheersmaatregel	5.05.01 en 5.06.01
ISO 27001:2023	beheersmaatregel	5.5 en 5.6
BIO versie 1.04zv	beheersmaatregel	6.1.3 en 6.1.4

3.1.4 Informatiebeveiliging in projectbeheer en samenwerkingen

Informatiebeveiliging is onderdeel van **alle** projecten en samenwerkingen.

Een project is een tijdelijke en georganiseerde inspanning met een duidelijke opdrachtgever die gericht is op het realiseren van een specifiek resultaat of product binnen vooraf bepaalde kaders, zoals tijd, geld en middelen. Het onderscheidt zich van routinematige werkzaamheden door een uniek karakter en de noodzaak om verschillende disciplines en specialisten samen te brengen.

Een samenwerking ontstaat als medewerkers van de gemeentelijke organisatie een project, staande of nieuwe taken gaan uitvoeren. Dit kan zijn in samenwerking met medewerkers van een andere organisatie of bedrijf. Dit kan gebeuren op basis van een formele overeenkomst of op meer informele wijze geregeld zijn.

3.1.4.1 *Voorafgaand aan een project of samenwerking*

Voorafgaand wordt de informatie die noodzakelijk is voor het project geclassificeerd aan de hand van hoofdstuk 5 uit dit beleid. Ook worden (werk)processen, (ict) middelen en gegevensuitwisselingen in kaart gebracht. Vervolgens worden informatiebeveiligingsrisico's geïdentificeerd middels een risicoanalyse. Maken persoonsgegevens onderdeel uit van de gegevensuitwisseling, dan wordt een DPIA uitgevoerd.

3.1.4.2 *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 sectordirecteur hiervoor verantwoordelijk.

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

De verantwoordelijke moet altijd advies vragen aan de CISO.

3.1.4.3 *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 of de samenwerking.

3.1.4.4 *Tijdens de uitvoering van het project of samenwerking*

Tijdens uitvoering dient te allen tijde conform dit beleid gewerkt te worden. Tevens dienen de uitgewerkte specifieke beveiligingsmaatregelen zo vroeg mogelijk aantoonbaar te worden geïmplementeerd. De projectleider of proceseigenaar is verantwoordelijk voor de naleving, monitoring en rapportage hiervan.

Referentie		
BIO versie 2.0	beheersmaatregel	5.08.01
ISO 27001:2023	beheersmaatregel	5.8
BIO versie 1.04zv	beheersmaatregel	6.1.5

3.1.5 Informatie over en analyses van dreigingen

Er moet een proces ingericht te zijn waarmee de organisatie informatie verzameld over bestaande en opkomende dreigingen. Deze informatie moet geanalyseerd worden om weloverwogen maatregelen op te kunnen stellen en de impact van dreigingen te beperken. Bij verzameling en analyse wordt onderscheid gemaakt in strategische, tactische en operationele dreigingen. De resulterende dreigingsanalyse en maatregelen worden periodiek met het DT gedeeld en besproken.

Referentie		
BIO versie 2.0	beheersmaatregel	5.07.01
ISO 27001:2023	beheersmaatregel	5.7
BIO versie 1.04zv	beheersmaatregel	-

3.2 Inrichting en beheer van netwerk, apparaten en toegang

De principes voor de inrichting en beheer van netwerk, apparaten en toegang zijn *Zero Trust* en *Zero Footprint*.

In plaats van het (impliciet) geven van vertrouwen (meestal wanneer een bepaald controlepunt, zoals inloggen, is gepasseerd), moet elke verbinding met of via het netwerk, met apparaten en toegang tot systemen, applicaties of diensten gecontroleerd en (geautomatiseerd) gemonitord worden. Accounts, apparaten, software en netwerk worden geconfigureerd met minimaal mogelijke functionaliteit en rechten, waarbij gewaarborgd wordt dat gegevens niet of alleen volledig versleuteld op een apparaat aanwezig kunnen zijn.

- Het netwerk wordt door middel van (micro)segmentatie ingedeeld in logische, afzonderlijk beveiligde delen.
- Accounts krijgen op basis van *Least Privilege* alleen toegang tot die delen van het netwerk en bronnen, systemen, applicaties of diensten die noodzakelijk zijn voor de werkzaamheden.
- Enkel door de gemeente uitgegeven en beheerde apparaten worden op *whitelist* basis toegang tot het netwerk verleend.
- Apparaten en netwerkcomponenten zijn dusdanig geconfigureerd ze vanuit een centrale omgeving op afstand beheerd kunnen worden.
    - Netwerkcomponenten en servers kunnen alleen beheerd worden vanuit een afgescheiden, beveiligd netwerk waarop toegang voorbehouden is aan personen met autorisatie voor het gebruik van speciale systeemhulpmiddelen en elke toegang tot dit netwerk wordt gelogd en gemonitord;
    - Er is dus geen enkele toegang tot beheer- of configuratie-instellingen vanuit publieke en medewerkersnetwerken of segmenten, ook geen open poorten of inlog prompts.
- Apparaten en netwerkcomponenten zijn dusdanig geconfigureerd dat:
    - Alleen goedgekeurde en geverifieerde besturingssystemen uitgevoerd kunnen worden;
    - Firmware, apparaat- en systeeminstellingen niet zonder authenticatie van een passend niveau gewijzigd kunnen worden;
    - Wijzigingen aan firmware, apparaat- en systeeminstellingen conform het wijzigingsbeleid uitgevoerd worden;
    - Voor beheertoegang tot apparaten, netwerkcomponenten en firmware geen groeps- of generieke beheeraccounts en/of wachtwoorden worden gebruikt;
- Apparaten zijn dusdanig geconfigureerd dat de volledige opslag inclusief systeempartities is versleuteld (*Full Disk Encryption*);
- Apparaten en netwerkcomponenten zijn dusdanig geconfigureerd dat eenmaal gegenereerde loggegevens niet (alleen) op het apparaat zelf worden opgeslagen;
- Apparaten en netwerkcomponenten zijn dusdanig geconfigureerd dat eenmaal gegenereerde loggegevens niet meer gewijzigd kunnen worden;
- Apparaten en netwerkcomponenten zijn dusdanig geconfigureerd dat adequate log- en monitoringgegevens worden gegenereerd om incidenten waar te kunnen nemen;
- Apparaten zijn dusdanig geconfigureerd dat niet gebruikte functionaliteit en (software)componenten zijn uitgeschakeld. Gebruikers kunnen uitgeschakelde functionaliteit en (software)componenten niet zelf weer inschakelen;
- Gebruikers kunnen niet zelf applicaties installeren of losstaande uitvoerbare bestanden uitvoeren buiten de toegestane en door de gemeente beheerde applicaties;
- Netwerk, apparaten, besturingssystemen en applicaties zijn dusdanig geconfigureerd dat deze geen (identificerende) gegevens kunnen versturen of doorlaten naar derden, zoals telemetrie, gebruiksgegevens, crashlogs, etc.;
- Netwerk, apparaten, besturingssystemen en applicaties zijn met openbare en ‘curated’ lijsten dusdanig geconfigureerd toegang wordt geblokkeerd tot advertenties/advertentienetwerken, bekende bronnen van malware, phishing, etc. en deze lijsten worden minimaal 1 keer per 24 uur geüpdatet.

Accounts voor werkgerelateerde zaken waarvoor geen door de gemeente gecontroleerde authenticatie mogelijk is (bijvoorbeeld VNG forums, support accounts, etc.) worden centraal aangemeld en geregistreerd.

Netwerkcomponenten, apparaten, besturingsssystemen, applicaties/apps en diensten uit landen met een offensief cyberprogramma worden beoordeeld op risico's voor de bedrijfsvoering en als die er zijn, worden deze als onwenselijk op een blacklist gezet die automatisch wordt afgedwongen. Overheidsspecifieke blacklists worden hierbij als basis ingezet.

Netwerkcomponenten, systemen of diensten die via publieke netwerken toegankelijk zijn, zijn zodanig geconfigureerd dat ze middels de tests van Internet.nl en Basisbeveiliging.nl 100% scoren, waarbij ook volledig wordt voldaan aan de aanbevolen standaarden en tests; certificaten en de configuratie van de cryptografische maatregelen scoren een A+ op de Qualys SSL Labs SSL Server Test.

Referentie		
BIO versie 2.0	beheersmaatregel	7.10.02, 7.14.01, 8.01.01, 8.01.02, 8.03.01, 8.03.02, 8.07.01, 8.12.01, 8.16.03, 8.16.04, 8.19.01, 8.20.01 en 8.23.01
ISO 27001:2023	beheersmaatregel	7.10, 7.14, 8.1, 8.7, 8.12, 8.16,8.19, 8.20 en 8.23
BIO versie 1.04zv	beheersmaatregel	6.2.1.1, 6.2.1.2, 8.3.2.1, 9.4.1.1, 9.4.1.2, 11.2.7, 12.2.1, 12.4.1, 12.6.1 en 13.1.1

3.3 Gebruik van privé apparaten of programmatuur

Het is niet toegestaan om privé apparaten of programmatuur te gebruiken voor werkzaamheden voor de gemeente. Het is niet toegestaan om niet geautoriseerde apps of webdiensten te gebruiken voor werkzaamheden voor de gemeente, waaronder het versturen of beschikbaar stellen van gegevens of berichten via accounts of diensten die niet onder beheer van de gemeente staan.

3.4 Mobiele apparaten en telewerken

Onder mobiele apparaten worden alle apparaten verstaan die niet gebonden zijn aan een vaste locatie, meestal: laptops, mobiele telefoons en tablets.

Telewerken betreft het op afstand werken via het netwerk en/of met de systemen, applicaties en diensten van de gemeente. De gemeente staat telewerken toe voor de netwerken, systemen en diensten waarin informatie bereikbaar is met een informatieclassificatieniveau ‘Laag’ en ‘Midden’. Voor informatieclassificatieniveau ‘Hoog’ is telewerken niet toegestaan.

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 getekend worden;
- Voor alle verstrekte mobiele apparaten wordt een registratie bijgehouden: welk apparaat op welke datum aan welke persoon is uitgegeven en een kopie van de getekende bruikleenovereenkomst;

- 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 functionaliteit en 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;
- 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;
- Telewerken is uitsluitend mogelijk via een beveiligde verbinding (VPN) tussen de telewerklocatie en de omgeving van de gemeente. De authenticiteit van het VPN-endpoint wordt door de client geverifieerd;
- 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.

Referentie		
BIO versie 2.0	beheersmaatregel	6.07.01, 8.01.01 en 8.01.02
ISO 27001:2023	beheersmaatregel	6.7 en 8.1
BIO versie 1.04zv	beheersmaatregel	6.2.1 en 6.2.2

3.5 Informatiebeveiliging voor het gebruik van clouddiensten

Er dient beleid te zijn dat toeziet op het inventariseren, classificeren, uitvoeren van risicoanalyses, selecteren, beoordelen en managen van cloudserviceproviders (CSP) en het beëindigen van dienstverlening met of door CSPs. Dit beleid wordt tenminste elke 3 jaar herzien.

In contracten met CSPs dient opgenomen te worden welke situaties aanleiding kunnen zijn tot ontbinding van het contract. De exit-strategie, het eigendomsrecht van de gegevens en mogelijke bewerkingen of verwerkingen door de CSP dienen onderdeel uit te maken van de contractvorming. Wanneer belangrijke wijzigingen bij de leverancier optreden, worden de risico's daarvan beoordeeld en worden passende maatregelen genomen.

Referentie		
BIO versie 2.0	beheersmaatregel	5.23.01
ISO 27001:2023	beheersmaatregel	5.23
BIO versie 1.04zv	beheersmaatregel	-

4 Veilig Personeel

4.1 Voorafgaand aan het dienstverband

4.1.1 Screening

Alle medewerkers, stagiair(e)s en extern ingehuurden overleggen vóór aanvang van werkzaamheden een Verklaring Omtrent het Gedrag (VOG) specifiek voor de te vervullen functie. Voor functies met een verhoogd risico wordt een VOG-P gevraagd. Identiteit, opleiding, referenties en specifieke competenties worden door team P&O geverifieerd.

Voor stagiair(e)s, extern ingehuurden en/of gedetacheerden wordt gecontroleerd of de overeenkomst getekend is en past bij de geplande werkzaamheden en functie/toegangsrechten.

4.1.1.1 *Registratie*

Team P&O 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.

Team P&O registreert de uitkomst van de verificaties en de overeenkomsten van stagiair(e)s, extern ingehuurden en/of gedetacheerden.

4.1.1.2 *Functiewijziging*

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

4.1.1.3 *Vernieuwing VOG*

Tenminste iedere vijf jaar dient de VOG opnieuw aangevraagd en overlegd te worden.

4.1.1.4 *Niet kunnen overleggen VOG*

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

4.1.1.5 *Opslag*

VOG's hebben classificatieniveau 'Midden'. 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.

Overeenkomsten voor stagiair(e)s, extern ingehuurden en/of gedetacheerden hebben classificatieniveau 'Midden' en worden tot 1 jaar na het verlopen van de overeenkomst bewaard conform de eisen voor dit classificatieniveau.

Referentie		
BIO versie 2.0	beheersmaatregel	6.01.01

ISO 27001:2023	beheersmaatregel	6.1
BIO versie 1.04zv	beheersmaatregel	7.1.1

4.1.2 Arbeidsvoorwaarden

Arbeidsovereenkomsten en inhuurovereenkomsten dienen de volgende punten te bevatten:

- De plichten en verantwoordelijkheden van de ondertekende ten aanzien van informatiebeveiliging;
- De disciplinaire procedure met te nemen maatregelen voor wanneer:
  - Geheimhouding geschonden wordt;
  - Het informatiebeveiligingsbeleid niet wordt nageleefd;
  - De plichten en verantwoordelijkheden niet worden nageleefd;
  - De randvoorwaarde dat men enkel voor de gemeente kan werken indien iedere vijf jaar een geldige VOG overlegt kan worden.

Als onderdeel van de arbeidsovereenkomst wordt de geheimhoudingsverklaring en gedragscode van de gemeente door de werknemer getekend.

4.1.2.1 *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.

4.1.2.2 *Inhuur, externen en stagiaires*

Inhuur, externen en stagiaires dienen voor aanvang van de werkzaamheden dezelfde gedragscode en geheimhoudingsverklaring als medewerkers te ondertekenen. De plicht ter geheimhouding blijft na het beëindigen van de werkzaamheden van kracht.

Referentie		
BIO versie 2.0	beheersmaatregel	5.10.01 en 6.2.01
ISO 27001:2023	beheersmaatregel	5.10 en 6.2
BIO versie 1.04zv	beheersmaatregel	7.1.2 en 8.1.3.2

4.1.3 Personeelsreglement

Het personeelsreglement bevat minimaal:

- De verantwoordelijkheden van medewerkers, stagiaires en extern ingehuurden 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.
- De plicht dat incidenten direct volgens de daarvoor geldende procedure worden gemeld.

Referentie

BIO versie 2.0	beheersmaatregel	6.2.01
ISO 27001:2023	beheersmaatregel	6.2
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:

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

Referentie		
BIO versie 2.0	beheersmaatregel	5.4.01
ISO 27001:2023	beheersmaatregel	5.4
BIO versie 1.04zv	beheersmaatregel	7.2.1

4.2.2 Klokkenluidersregeling

De directie zorgt 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 2.0	beheersmaatregel	6.2.01
ISO 27001:2023	beheersmaatregel	6.2

BIO versie 1.04zv	beheersmaatregel	7.2.1.1

4.2.3 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

4.2.3.1 *Beschikbaar stellen van informatie*

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

4.2.3.2 *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.

4.2.3.3 *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 te 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.

4.2.3.4 *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.

4.2.3.5 *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:

Doelgroep	Verantwoordelijke	Ondersteund door	Frequentie
Gemeenteraad	Gemeentesecretaris	CISO	Jaarlijks
College B&W en DT	Gemeentesecretaris	CISO	Halfjaarlijks
Medewerkers	Sectordirecteur	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.

4.2.3.6 *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 2.0	beheersmaatregel	6.03
ISO 27001:2023	beheersmaatregel	6.3
BIO versie 1.04zv	beheersmaatregel	7.2.2

4.2.4 Disciplinaire procedure

Er is een formele disciplinaire procedure voor de gevallen waarin:

- Het geheimhoudingsbeding is geschonden;
- Het informatiebeveiligingsbeleid niet is nageleefd;
- 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. De college van B&W is eindverantwoordelijk voor het opstellen, uitvoeren en handhaven van de disciplinaire procedure.

4.2.4.1 *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.

4.2.4.2 *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.

4.2.4.3 *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.

4.2.4.4 *Kennisname van de procedure*

De directieleden 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 2.0	beheersmaatregel	6.04.01
ISO 27001:2023	beheersmaatregel	6.4
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 de sectordirecteur. Het geheimhoudingsbeding blijft permanent van kracht, ook als de werkzaamheden voor de gemeente zijn beëindigd.

Referentie		
BIO versie 2.0	beheersmaatregel	6.05.01
ISO 27001:2023	beheersmaatregel	6.5
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 BIO2 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:

Classificatie	Beschikbaarheid	Integriteit	Vertrouwelijkheid
3 – Hoog	**Essentieel** Informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten.	**Desastreus** Het bedrijfsproces staat (hoegenaamd) geen fouten toe.	**Geheim** Informatie is alleen toegankelijk voor direct geadresseerde(n).
2 – Midden	**Noodzakelijk** Informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk.	**Ernstig** Het bedrijfsproces staat zeer weinig fouten toe.	**Vertrouwelijk** Informatie is alleen toegankelijk voor een beperkte groep gebruikers.
1 – Laag	**Belangrijk** Informatie mag incidenteel niet beschikbaar zijn.	**Normaal** Het bedrijfsproces staat enkele (integriteits-)fouten toe.	**Intern** Informatie is toegankelijk voor alle medewerkers van de gemeente.
0 – Openbaar	**Niet zeker** Gegevens kunnen zonder gevolgen enige tijd niet beschikbaar zijn.	**Gering** Belang van de informatie voor het bedrijfsproces is zeer beperkt.	**Openbaar** Informatie mag door iedereen worden ingezien.

Het hoogst toegekende niveau bepaalt de informatieclassificatie; daarbij maakt het niet uit op welk aspect het hoogste niveau wordt toegekend.

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 2.0	beheersmaatregel	5.12.01
ISO 27001:2023	beheersmaatregel	5.12
BIO versie 1.04zv	beheersmaatregel	8.2.1, 8.2.2, 8.2.3

6 Beheer van bedrijfsmiddelen

6.1 Verantwoordelijkheid voor bedrijfsmiddelen

6.1.1 Inventariseren van bedrijfsmiddelen

Alle bedrijfsmiddelen die samenhangen met informatie of informatie verwerkende faciliteiten of daar toegang toe geven zijn vastgelegd in een centraal inventaris. De sectordirecteur is verantwoordelijk voor de vastlegging en het onderhoud van de inventaris van bedrijfsmiddelen van de eigen sector.

Iedere sectordirecteur is verantwoordelijk voor het controleren of bedrijfsmiddelen die gedeeld worden door sectoren correct in de inventaris is opgenomen.

De inventaris dient opgesteld te worden aan de hand van een gemeentebrede 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 2.0	beheersmaatregel	5.09.01
ISO 27001:2023	beheersmaatregel	5.9
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:

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

Referentie		
BIO versie 2.0	beheersmaatregel	5.10.01
ISO 27001:2023	beheersmaatregel	5.10
BIO versie 1.04zv	beheersmaatregel	8.1.3

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 2.0	beheersmaatregel	5.10.01
ISO 27001:2023	beheersmaatregel	5.10
BIO versie 1.04zv	beheersmaatregel	8.1.3

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 sectordirecteur.

Referentie		
BIO versie 2.0	beheersmaatregel	5.10.01
ISO 27001:2023	beheersmaatregel	5.10
BIO versie 1.04zv	beheersmaatregel	6.1.2.1 en 8.1.3

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 2.0	beheersmaatregel	5.11.01
ISO 27001:2023	beheersmaatregel	5.11
BIO versie 1.04zv	beheersmaatregel	8.1.4

6.2 Behandelen van media

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:

- De standaard apparaten (laptop, tablet, telefoon) ondersteunen het gebruik van verwijderbare media niet (functionaliteit is uitgeschakeld);
- 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 te alle tijden van toepassing.
- Hergebruik geldt alleen voor digitale media waarbij de eisen van paragraaf 9.2.7 altijd 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 2.0	beheersmaatregel	7.10.1 en 7.10.2
ISO 27001:2023	beheersmaatregel	7.10
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 conform paragraaf 9.2.7.

Referentie		
BIO versie 2.0	beheersmaatregel	7.10.01
ISO 27001:2023	beheersmaatregel	7.10
BIO versie 1.04zv	beheersmaatregel	8.3.1.1

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 van B&W. 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 2.0	beheersmaatregel	7.10.03
ISO 27001:2023	beheersmaatregel	7.10
BIO versie 1.04zv	beheersmaatregel	8.3.3.1

7 Logische toegangsbeveiliging

7.1 Bedrijfseisen voor logische toegangsbeveiliging

7.1.1 Beleid voor logische toegangsbeveiliging

De gemeente moet een 'Logisch toegangsbeveiligingsbeleid' hebben vastgesteld. De werking van het beleid moet aangetoond kunnen worden aan de hand van de verslaglegging van de werkzaamheden in het proces. 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:

- Beveiliging en gebruiksvriendelijkheid
    - Alle accounts worden tenminste beveiligd met een wachtwoord conform het wachtwoordbeleid en een tweede onafhankelijke factor (MFA);
    - Het wachtwoord en tweede factor moeten minimaal eens per 24 uur ingevoerd worden ter controle;
    - Het gebruik van een biometrische factor (bijvoorbeeld vingerafdruk) wordt waar mogelijk geactiveerd. Gebruik hiervan is op vrijwillige basis en niet verplicht voor medewerkers;
    - Het apparaat of sessie waarop succesvol met MFA is ingelogd, blijft actief en kan gedurende 24 uur herhaaldelijk *locked* en *unlocked* worden met slechts 1 factor (bijvoorbeeld alleen wachtwoord of vingerafdruk);
    - Bij inactiviteit langer dan 2 uur vervalt de actieve inlog en moet opnieuw met MFA ingelogd worden;
    - Alternatieve authenticatiemethoden zoals bijvoorbeeld *passkeys* kunnen worden toegepast als het beveiligingsniveau tenminste vergelijkbaar is met MFA;
    - Er wordt een wachtwoordmanager ingezet voor alle wachtwoorden behalve het hoofdwachtwoord voor account-toegang (zie paragraaf 7.4.3).
- Service-/groepsaccounts
    - Medewerkers moeten, ook voor beheertaken, werken met 'named accounts';
        - Dit kan ook een *named* beheeraccount zijn anders dan het reguliere gebruikersaccount;
    - Er worden in de regel geen gedeelde service-/groepsaccounts gebruikt;
    - Als er gewerkt moet worden met service-/groepsaccounts dient hiervoor de procedure 'Aanvraag service-account' gevolgd te worden;
    - Indien er een service-/groepsaccount wordt aangemaakt is de proceseigenaar van het proces waarbinnen dat account wordt gehanteerd tevens de eigenaar van dit account.
- Monitoring
    - Voor herleidbaarheid en transparantie moet er met logging vastgelegd te worden welke authenticaties er op welk moment hebben plaats gevonden;
    - Systemen en applicaties moeten met logging vastleggen welke gebruikers welke acties hebben uitgevoerd;

  - Monitoring, logging en het verder verwerken van deze gegevens wordt getoetst aan de AVG, afgestemd met de OR en duidelijk gecommuniceerd met de medewerkers;
  - De loggegevens, voor zover deze persoonsgegevens bevatten of daartoe herleid kunnen worden, worden na een vastgestelde periode verwijderd of geanonimiseerd.
- Standaarden
  - De gemeente maakt, waar mogelijk, gebruik van bestaande (landelijke) voorzieningen voor authenticatie, autorisatie en informatiebeveiliging;
  - De gemeente hanteert zoveel mogelijk geaccepteerde standaard authenticatiemiddelen;
  - Als afgeweken wordt standaarden dient de motivatie hiervoor door de CISO 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.
  - Alle autorisatieverzoeken en goed- of afkeuringen worden in het centrale register autorisatieverzoeken opgeslagen.
  - Een autorisatieverzoek ontstaat als gevolg van het IDU-proces of wanneer een medewerker taken gaat uitvoeren die niet oorspronkelijk bij het functieprofiel horen.
  - De leidinggevende van de medewerker moet een autorisatieverzoek voor additionele rollen of rechten goedkeuren.
    - Autorisaties worden pas doorgevoerd na controle op de goedkeuring van de leidinggevende;
  - 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 DT (zie paragraaf 7.2.3).
- Mandaat
  - Het DT kan taken in het autorisatieproces aan medewerkers mandateren;
  - Bij mandatering dient rekening gehouden te worden met functiescheiding:
  - Goedkeuring voor een autorisatieverzoek kan niet verleend worden door een medewerker met actieve taken in het werkproces en/of toegang tot het systeem of de applicatie;
  - De verleende mandaten worden in het mandaatregister opgenomen. Het mandaatregister wordt ieder kwartaal door het DT geëvalueerd.
- Wachtwoorden

- Accounts worden aangemaakt zonder het invoeren van een initieel wachtwoord: de gebruiker ontvangt een uitnodiging om zelf het account te activeren en een wachtwoord in te stellen;
- Alleen als systemen of applicaties dit proces niet ondersteunen, mag gebruik gemaakt worden van een initieel wachtwoord:
  - Er wordt een veilig en willekeurig gegenereerd wachtwoord ingesteld;
  - Het wachtwoord wordt via een veilig kanaal met de gebruiker gedeeld op een moment dat bekend is dat de gebruiker hier direct mee gaat inloggen;
  - Verstrekte initiële wachtwoorden moeten onmiddellijk na het eerste gebruik door de gebruiker worden gewijzigd.

Verder gelden alle eisen benoemt in dit hoofdstuk.

Referentie		
BIO versie 2.0	beheersmaatregel	5.15.01, 5.17.01 en 5.18.01
ISO 27001:2023	beheersmaatregel	5.15, 5,17 en 5.18
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 en 9.2.2.3

7.1.2 Toegang tot netwerken en netwerkdiensten

7.1.2.1 *Gebruikers*

Medewerkers krijgen alleen toegang tot de netwerken en de netwerkdiensten waarvoor zij conform het functieprofiel bevoegd zijn. Noodzakelijke additionele toegangsrechten kunnen aangevraagd worden via de procedure Toegangsrechten.

7.1.2.2 *Apparatuur*

Alleen geautoriseerde apparatuur kan toegang krijgen tot een netwerk met gemeentelijke informatie.

7.1.2.3 *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.

Referentie		
BIO versie 2.0	beheersmaatregel	5.15.01
ISO 27001:2023	beheersmaatregel	5.15
BIO versie 1.04zv	beheersmaatregel	9.1.2

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);
- Wijzigen;
- Verwijderen (afmelden);

- Blokkeren;
- Vrijgeven.

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

Iedere gebruiker heeft toegang tot een wachtwoordmanager om het beheer van wachtwoorden veilig en gemakkelijker te maken. Het gebruik van de wachtwoordmanager en het toepassen van het wachtwoordbeleid is verplicht voor alle situaties waarin een wachtwoord wordt gebruikt. Voor het openen van de wachtwoordmanager moet minimaal één keer per 24 uur een tweede beveiligingsfactor ingevoerd worden.

Referentie		
BIO versie 2.0	beheersmaatregel	5.16.01, 5.17.02, 5.18.01
ISO 27001:2023	beheersmaatregel	5.16, 5.17, 5.18
BIO versie 1.04zv	beheersmaatregel	9.2.1, 9.2.1.1 en 9.2.2

7.2.1 Controle autorisatieverzoek

De systeemeigenaar beoordeelt het autorisatieverzoek waarbij in ieder geval wordt gecontroleerd of:

- Het aanvraag- of wijzigingsformulier volledig en op de juiste manier is ingevuld;
- Het aanvraag- of wijzigingsformulier door een autorisatiebevoegde medewerker is ingediend en ondertekend;
- 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 2.0	beheersmaatregel	5.16.01 en 5.16.02
ISO 27001:2023	beheersmaatregel	5.16
BIO versie 1.04zv	beheersmaatregel	9.2.1 en 9.2.1.1

7.2.2 Functieprofielen en autorisatiematrixen

7.2.2.1 *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.

7.2.2.2 *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 2.0	beheersmaatregel	5.18.01, 5.18.02, 8.02.01
ISO 27001:2023	beheersmaatregel	5.18 en 8.2
BIO versie 1.04zv	beheersmaatregel	9.2.2, 9.2.2.2 en 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 (DT). Gebruikers krijgen slechts toegang tot een noodzakelijk geachte set van applicaties. De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld door het strategisch management (DT). 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:

- De speciale toegangsrechten behorend bij elk systeem of proces en de gebruikers aan wie ze moeten worden toegewezen, dienen te worden geïdentificeerd;
- Speciale toegangsrechten dienen op basis van noodzaak tot gebruik per gebeurtenis aan gebruikers te worden toegekend in overeenstemming met het toegangsbeveiligingsbeleid;
- 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;
- Voor het vervallen van speciale toegangsrechten dienen eisen te worden gedefinieerd;
- Speciale toegangsrechten dienen te worden toekend aan een gebruikersidentificatie die verschilt van identiteiten die voor reguliere bedrijfsactiviteiten worden gebruikt;
- De competenties van gebruikers met speciale toegangsrechten dienen regelmatig te worden beoordeeld om te verifiëren of ze in overeenstemming zijn met hun taken;
- Toewijzingen van speciale toegangsrechten dienen regelmatig, ten minste maandelijks, te worden gecontroleerd om te waarborgen dat speciale toegangsrechten niet onbevoegd zijn verkregen;
- Wijzigingen in speciale accounts dienen bijgehouden te worden in logbestanden voor de periodieke beoordeling;
- 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;
- Voor gebruikersidentificaties voor algemeen beheer dient de geheimhouding van geheime authenticatie-informatie in acht te worden genomen als deze wordt gedeeld.

Referentie		
BIO versie 2.0	beheersmaatregel	5.18.03 en 8.02.01

ISO 27001:2023	beheersmaatregel	5.18 en 8.2
BIO versie 1.04zv	beheersmaatregel	9.2.3 en 9.2.5

7.2.4 Beheren van geheime authenticatie-informatie van gebruikers

7.2.4.1 *Definitie*

Onder geheime authenticatie-informatie van gebruikers wordt verstaan: wachtwoorden, cryptografische sleutels, biometrische gegevens, tokens, 'druppels', apparaten of software die authenticatiecodes produceren en alle andere informatie die als authenticatie dient en niet publiekelijk bekend is.

7.2.4.2 *Procedure*

Het toewijzen of registreren van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces. In dit beheersproces is opgenomen wie verantwoordelijk is voor het toewijzen van geheime authenticatie-informatie. Het proces behoort de volgende eisen te bevatten:

- In de arbeidsvoorwaarden dient te worden opgenomen dat iedereen die werkt voor de gemeente persoonlijke geheime authenticatie-informatie geheimhouden en gedeelde geheime authenticatie-informatie niet verder delen;
- Er behoren procedures te worden vastgesteld om de identiteit van een gebruiker vast te stellen voordat nieuwe, vervangende of tijdelijke geheime authenticatie-informatie wordt verstrekt;
- Tijdelijke geheime authenticatie-informatie behoort op een veilige manier aan gebruikers te worden gegeven. Gebruikmaken van externe partijen of onbeschermde e-mailberichten behoort te worden vermeden;
- Tijdelijke geheime authenticatie-informatie behoort uniek voor één persoon te zijn en behoort minimaal te voldoen aan de specifieke eisen voor het type authenticatie-informatie zoals benoemt in dit beleid;
- Gebruikers bevestigen de ontvangst van geheime authenticatie-informatie;
- Gebruikers zijn niet verplicht biometrische gegevens als authenticatie-informatie te registreren: de gemeente voorziet medewerkers die afzien van het registreren van biometrische gegevens van een passend en gelijkwaardig alternatief voor authenticatie;
- Biometrische gegevens zijn bijzondere persoonsgegevens en worden door de gemeente dusdanig behandeld en beveiligd;
- Standaard geheime authenticatie-informatie van een leverancier moet direct worden gewijzigd na de installatie van systemen of software en standaard service- of groepsaccounts moeten worden gedeactiveerd en verwijderd.

Referentie		
BIO versie 2.0	beheersmaatregel	5.17.01
ISO 27001:2023	beheersmaatregel	5.17
BIO versie 1.04zv	beheersmaatregel	9.2.4

7.2.5 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 2.0	beheersmaatregel	5.18.03
ISO 27001:2023	beheersmaatregel	5.18
BIO versie 1.04zv	beheersmaatregel	9.2.5

7.2.6 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 2.0	beheersmaatregel	5.18
ISO 27001:2023	beheersmaatregel	5.18

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;
- Gebruik van de wachtwoordmanager (wachtwoordkluis) is verplicht voor alle situaties waarin een wachtwoord gebruikt wordt;
- Wachtwoorden moeten voldoen aan de vereisten in het Wachtwoordbeleid en moeten altijd met behulp van de wachtwoordmanager gegenereerd en beheerd worden.

Referentie		
BIO versie 2.0	beheersmaatregel	5.17.02 en 5.17.03
ISO 27001:2023	beheersmaatregel	5.17
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 team Informatiemanagement, P&O of 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 2.0	beheersmaatregel	8.03
ISO 27001:2023	beheersmaatregel	8.3
BIO versie 1.04zv	beheersmaatregel	9.4.1

7.4.2 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 2.0	beheersmaatregel	8.05.01
ISO 27001:2023	beheersmaatregel	8.5
BIO versie 1.04zv	beheersmaatregel	9.4.2

7.4.3 Systeem voor wachtwoordbeheer

De CISO moet een voorschrift met betrekking tot het wachtwoordbeheer opstellen en jaarlijks evalueren. Het voorschrift is verplicht voor alle situaties waar met wachtwoorden toegang wordt gegeven tot netwerken, systemen, applicaties, diensten en/of informatie. Het voorschrift moet tenminste het volgende te bevatten:

- Alle onderstaande eisen dienen minimaal te voldoen aan de richtlijnen zoals aangegeven in de vigerende BIO versie;
- Verplicht gebruik van de wachtwoordmanager-applicatie voor alle wachtwoorden;
- Verplicht laten genereren en beheren van wachtwoorden door de wachtwoordmanager-applicatie;
    - Eisen minimale lengte en complexiteit van de automatisch gegenereerde wachtwoorden;
- Verplicht 1 keer per 24 uur gebruik van tweede factor om de wachtwoordmanager-applicatie te openen/activeren;
- Eisen minimale lengte en complexiteit van het hoofdwachtwoord van de gebruiker;
- 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.

De wachtwoordmanager-applicatie dient deze aan de volgende voorwaarden te voldoen:

- De wachtwoordmanager dient voor ieder systeem, applicatie of dienst een ander wachtwoord te hanteren;
- De wachtwoordmanager mag de gegevens niet opslaan buiten het grondgebied van de Europese Unie;
- Alle gegevens in de wachtwoordmanager dienen versleuteld opgeslagen te worden conform een versleutelingsmethode benoemt in het hoofdstuk 8 (Cryptografie) van dit beleid;

- De wachtwoordmanager moet met hetzelfde niveau van beveiliging functioneren op alle apparaten van de medewerker en op elk apparaat toegang geven tot dezelfde set authenticatiegegevens.

Referentie		
BIO versie 2.0	beheersmaatregel	5.17.01
ISO 27001:2023	beheersmaatregel	5.17
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 beveiligen, ondersteunen en beheren. Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moet worden beperkt en nauwkeurig worden gecontroleerd. Alle onnodige systeemhulpmiddelen moeten worden verwijderd of onbruikbaar worden gemaakt voor gebruikers zonder autorisaties hiervoor.

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

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

Referentie		
BIO versie 2.0	beheersmaatregel	8.18.01 en 8.18.02
ISO 27001:2023	beheersmaatregel	8.18
BIO versie 1.04zv	beheersmaatregel	9.4.4

7.4.5 Toegangsbeveiliging op programmabroncode

Toegang tot de programmabroncode, softwarebibliotheken, ontwikkelinstrumenten en *build & deploy* systemen moet worden beperkt en controleerbaar zijn om de introductie van onbevoegde functionaliteit en onbedoelde wijzigingen te voorkomen, en om, waar geen open source licenties van toepassing zijn, de vertrouwelijkheid van het intellectuele eigendom te handhaven. Dit wordt bereikt door de code gecontroleerd centraal op te slaan en toegang te reguleren, 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
- Alle wijzigingen aan broncode en bibliotheken, maar ook configuratie van de gebruikte ontwikkelinstrumenten en build & deploy systemen worden in een wijzigingsbeheersysteem vastgelegd;
- Gebruik van en toegang tot alle systemen is alleen mogelijk op basis van een ‘named’ account.

Referentie		
BIO versie 2.0	beheersmaatregel	08.04.01
ISO 27001:2023	beheersmaatregel	8.4
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 het hoofdstuk Informatieclassificatie. Voor cryptografische maatregelen wordt onderscheid gemaakt tussen communicatie van informatie en opslag van informatie.

De door de gemeentelijke CISO goedgekeurde lijst van encryptiemaatregelen moet tenminste de standaarden op de ‘pas toe of leg uit‘-lijst van het Forum Standaardisatie bevatten.

8.1.1 Communicatie van informatie

De cryptografische maatregelen gelden alleen voor communicatie van digitale informatie.

8.1.1.1 *Netwerkcommunicatie*

Alle informatie die via netwerken gecommuniceerd wordt, moet tenminste met TLS te worden beveiligd. Voor ieder systeem dient het stappenplan uit de nieuwste versie van het ‘ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)’ van 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 / 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.

8.1.1.2 *Andere vormen van digitale communicatie*

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

8.1.1.3 *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.

8.1.1.4 *Chatapplicaties*

Er wordt geen gebruik gemaakt van niet goedgekeurde chatapplicaties.

8.1.1.5 *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.

8.1.1.6 *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 2.0	beheersmaatregel	8.24.01, 8.24.02, 8.24.03
ISO 27001:2023	beheersmaatregel	8.24
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. Alle opslagmedia, ook in afgenomen systemen, moeten vanaf het eerste gebruik door middel van ‘full disk encryption’ versleuteld zijn, zodanig dat de gegevens op het opslagmedium niet toegankelijk is zonder de bijbehorende sleutel; deze sleutel mag nooit op hetzelfde opslagmedium aanwezig zijn en wordt conform paragraaf 8.2 beheerd.

8.1.2.1 *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.

8.1.2.2 *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.

8.1.2.3 *Back-ups*

Back-ups worden altijd versleuteld opgeslagen c.q. op een versleuteld opslagvolume geplaatst. Sleutels voor back-ups verdienen extra aandacht en worden conform paragraaf 8.2 beheerd

Referentie		
BIO versie 2.0	beheersmaatregel	8.24
ISO 27001:2023	beheersmaatregel	8.24
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;
- Back-ups maken van sleutels conform een 3-2-1 back-up strategie;
- Meervoudig redundante toegang tot het sleutelbeheersysteem en de back-ups, verspreid over meerdere personen en apparaten/factoren;
- Het vernietigen van sleutels;
- Het registreren en auditen van aan sleutelbeheer gerelateerde activiteiten;
- Periodieke tests van systemen en processen, waaronder disaster recovery scenario's;
- Interne controle op de werking.

Referentie		
BIO versie 2.0	beheersmaatregel	8.24
ISO 27001:2023	beheersmaatregel	8.24
BIO versie 1.04zv	beheersmaatregel	10.1.2 en 10.1.2.1

8.2.1 Certificaten

Bij voorkeur wordt gebruik gemaakt van zichzelf automatisch vernieuwende certificaten met een levensduur van 3 maanden.

Voor alle overige certificaten geldt dat deze in een gemeentebreed register moeten zijn opgenomen. Van ieder certificaat wordt tenminste geregistreerd:

- Locatie / systeem / applicatie waar het certificaat wordt gebruikt
- Leverancier van systeem of applicatie indien van toepassing
- Vervaldatum
- Risicoanalyse
- Verantwoordelijke voor verlengen/vervangen van certificaat
- Contactgegevens verantwoordelijke
- Functioneel beheerder of systeemeigenaar

Er wordt maandelijks een rapportage gemaakt uit het register van certificaten die binnen 45 dagen verlopen. Deze rapportage wordt door de functioneel beheerders en/of systeemeigenaren gebruikt om de certificaten tijdig te (laten) vervangen en/of te controleren of certificaten tijdig zijn vervangen.

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 2.0	beheersmaatregel	8.24.05
ISO 27001:2023	beheersmaatregel	8.24
BIO versie 1.04zv	beheersmaatregel	10.1.2.2

8.2.2 PKI-overheidscertificaten

PKI-overheid wordt niet meer ingezet voor het uitgeven van publiek vertrouwde certificaten, bijvoorbeeld voor beveiliging van website-verbindingen. Voor enkele toepassingen worden (niet-publieke) PKI-overheid certificaten nog wel ingezet. Voor het beheer van PKI-overheid certificaten gelden dezelfde vereisten als voor overige certificaten. Hierbij zijn de bepalingen van Logius en de certificaatleverancier leidend.

Referentie		
BIO versie 2.0	beheersmaatregel	8.24
ISO 27001:2023	beheersmaatregel	8.24
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 de meest recente versie van de 'Handreiking toegangsbeleid' waarbij onderstaande zonering is voorgeschreven:

Zone 0	**Het terrein** Het terrein om het gebouw is vrij toegankelijk. Toegang tot binnenterrein verloopt via slagboom/identificatie.
Zone 1	**Publiekszone** De publiekshal en vluchtroute, waaronder het trappenhuis. In de hal is een receptie; hier wordt permissie gegeven voor het betreden van de volgende veiligheidszone. Hieronder valt ook de (fietsen)kelder toegankelijk via het trappenhuis (vluchtroute).
Zone 2	**Raadszaal en publieke vergaderruimten** De raadszaal, het keukentje en de vergaderruimten op de begane grond zijn toegankelijk na toestemming van de receptie. Leeszaal in het raadhuis. De leeszaal is echter alleen bereikbaar via Zone 3.
Zone 3	**Standaard werkgebied** Dit betreft zones in het gemeentekantoor, raadshuis, locatie Dorpsteam en werf die uitsluitend bereikbaar zijn met toegangspassen voor geautoriseerde medewerkers. De kantoorwerkplekken voor de ambtelijke organisatie, inclusief de werkplekken Receptie en Publiekszaken in de publiekshal. Hieronder vallen ook de vergaderruimten bereikbaar via het trappenhuis (vluchtroute).
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); • Archieven; • Server en netwerkruimten; • Technische ruimten; • Off-site back-up locatie.

Uitwerking van de exacte inrichting van de locaties van gemeente Boekel 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 2.0	beheersmaatregel	7.01.01 en 7.01.02
ISO 27001:2023	beheersmaatregel	7.1
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 Facilitaire Zaken.

Zone 1 (Publiekszone):

- Medewerkers, stagiair(e)s en ingehuurden dragen zichtbare gemeentelijke identificatie;
- Bezoekers die verder dan Zone 2 worden toegelaten:
    - Worden vooraf bij de Receptie aangemeld;
    - Krijgen een bezoekerspas die enkel binnendeuren in Zone 3 opent, maar geen buitendeuren;
    - Naam, contactgegevens, aankomst- en vertrektijden/datum van bezoekers worden geregistreerd;
    - Bezoekers worden in Zone 3 altijd door een medewerker vergezeld.
- In Zone 1 bevinden zich geen toegankelijke actieve netwerkpoorten of communicatiemiddelen van de gemeente.

Zone 2 (Regelmatig toegankelijke publiekszone):

- Raadszaal wordt beschikbaar gesteld voor het publiek wanneer er een vergadering is die publiek bijgewoond dient te worden;
- In Zone 2 bevinden zich geen toegankelijke actieve netwerkpoorten of communicatiemiddelen van de gemeente.

Zone 3 (Standaard werkgebied):

- Zone 3 is alleen toegankelijk voor geautoriseerde medewerkers met geldige toegangspassen.
- Alle toegangsacties van personeel worden gelogd;
- Het werkgebied Receptie en Publiekszaken is alleen toegankelijk voor medewerkers van team Receptie en Publiekszaken;

- 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 ongeautoriseerden 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;
- Externe inhuur die enkel voor een 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 2.0	beheersmaatregel	7.01.01, 7.01.02, 7.02.01, 7.03.01
ISO 27001:2023	beheersmaatregel	7.1, 7.2 en 7.3
BIO versie 1.04zv	beheersmaatregel	11.1.2 en 11.1.2.1

9.1.3 Kantoren, ruimten en faciliteiten beveiligen

9.1.3.1 *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:

9.1.3.2 *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 de teamleider van Facilitaire Zaken;

- Niet uitgegeven toegangsmiddelen die toegang geven tot zone 4 worden zodanig veilig opgeborgen dat deze enkel toegankelijk zijn voor de sectordirecteur 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.

9.1.3.3 *Ruimten*

- Werkplekken die zichtbaar zijn vanuit de publiek toegankelijke 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 toegankelijke ruimte informatieoverdracht of activiteiten hoorbaar of zichtbaar zijn.

Referentie		
BIO versie 2.0	beheersmaatregel	7.03.01
ISO 27001:2023	beheersmaatregel	7.3
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 bedrijfsmiddelenbeleid in hoofdstuk 6.

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 Facilitaire Zaken is verantwoordelijk voor ‘sleutelplan zone 3’ en ‘sleutelplan brandkasten zone 3’;
- Sectordirecteur verantwoordelijk voor de teams 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 moet het sleutelplan opstellen en actualiseren als nodig;
- Het sleutelplan wordt jaarlijks geëvalueerd door de verantwoordelijke. De evaluatie en diens resultaten worden vastgelegd en de betrokken worden hierover geïnformeerd;
- Het sleutelplan is goedgekeurd door het DT 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 2.0	beheersmaatregel	7.03.01
ISO 27001:2023	beheersmaatregel	7.3
BIO versie 1.04zv	beheersmaatregel	11.1.3 en 11.1.3.1

9.1.5 Monitoren van fysieke beveiliging

De gebouwen en terreinen van de gemeente moeten voortdurend worden gemonitord op onbevoegde fysieke toegang. Teamleider Facilitaire zaken is verantwoordelijk voor het opstellen, beheren en implementeren van de procedure Fysieke beveiliging. De procedure beschrijft tenminste:

- Methode en middelen voor het monitoren van toegang door onbevoegden of verdacht gedrag;
- Wijze waarop de ingezette middelen zijn afgeschermd tegen toegang of manipulatie door onbevoegden;
- Wijze van notificatie bij (mogelijke) incidenten;
- Wijze waarop notificaties direct en op een later tijdstip gecontroleerd of geanalyseerd (kunnen) worden;
- Reactietijden en reactiemogelijkheden bij een geconstateerd incident;
- Testplan voor het periodiek controleren van de werking van de middelen;
- Wijze waarop (persoons)gegevens verwerkt, opgeslagen en verwijderd worden, waarbij vermeld wordt hoe lang en op welke wijze gegevens opgeslagen worden.

De werkwijze en ingezette middelen moeten voldoen aan de geldende wet- en regelgeving, waaronder de AVG.

Referentie		
BIO versie 2.0	beheersmaatregel	7.04.01
ISO 27001:2023	beheersmaatregel	7.4
BIO versie 1.04zv	beheersmaatregel	-

9.1.6 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 DT 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 2.0	beheersmaatregel	7.05.01
ISO 27001:2023	beheersmaatregel	7.5
BIO versie 1.04zv	beheersmaatregel	11.1.4, 11.1.4.1 en 11.1.4.2

9.1.7 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 sectordirecteur wiens afdeling of teamleider onder de beveiligde gebieden vallen.

Referentie		
BIO versie 2.0	beheersmaatregel	7.06
ISO 27001:2023	beheersmaatregel	7.6
BIO versie 1.04zv	beheersmaatregel	11.1.5

9.1.8 Laad en loslocaties

De inrichting en maatregelen van laad en los locaties 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 losruimten 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 2.0	beheersmaatregel	7.02 en 7.03
ISO 27001:2023	beheersmaatregel	7.2 en 7.3
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 teamleider Facilitaire Zaken is verantwoordelijk voor de adequate beschermen 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 buiten locatie wordt geplaatst;
- Overspanningen waardoor apparatuur beschadigd kan raken.

Referentie		
BIO versie 2.0	beheersmaatregel	7.08
ISO 27001:2023	beheersmaatregel	7.8

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).

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 2.0	beheersmaatregel	7.11
ISO 27001:2023	beheersmaatregel	7.11
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:
- TIA-942: Telecommunication Infrastructure Standard for Data Centers
- NEN-EN 50600: Europese normenreeks voor datacenters

- 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 2.0	beheersmaatregel	7.12
ISO 27001:2023	beheersmaatregel	7.12
BIO versie 1.04zv	beheersmaatregel	11.2.3

9.2.4 Onderhoud apparatuur

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

9.2.4.1 *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 9.2.4);
- 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.

9.2.4.2 *Onderhoud van software op apparatuur*

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

- Besturingssystemen worden automatisch bijgewerkt en mogen niet meer dan één versie achterlopen op de meest recente versie. En de gebruikte versie dient te allen tijde ondersteund te worden door de fabrikant. Het automatisch bijwerken van besturingssystemen wordt automatisch afgedwongen op alle apparaten die voor gemeentelijke werkzaamheden worden gebruikt;
- Voor software, anders dan besturingssystemen, is een updatebeleid van kracht waarin per applicatie wordt aangegeven:
- Hoe ver deze mag achterlopen op de meest recente versie.
- Hoe deze bijgewerkt wordt.
- Hoe men controleert dat deze tijdig bijgewerkt is.

9.2.4.3 *Onderhoud van servers*

In het kader van het onderhoud van servers zijn 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 2.0	beheersmaatregel	7.13
ISO 27001:2023	beheersmaatregel	7.13
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 Beheer van bedrijfsmiddelen beschreven procedure.

Referentie		
BIO versie 2.0	beheersmaatregel	7.14
ISO 27001:2023	beheersmaatregel	7.14
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. Ten alle 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 regelement ‘Thuiswerken gemeente X’ dat jaarlijks door het strategisch managementteam met advies van de CISO wordt geëvalueerd. Het regelement dient minimaal de adviezen6 van de NCSC te bevatten.

Referentie

BIO versie 2.0	beheersmaatregel	7.09
ISO 27001:2023	beheersmaatregel	7.9
BIO versie 1.04zv	beheersmaatregel	11.2.6

9.2.7 Veilig verwijderen of hergebruiken van apparatuur en opslagmedia

9.2.7.1 *Controle licenties*

Alvorens er wordt overgegaan tot verwijdering / 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*

Digitale en fysieke opslagmedia dat informatie (heeft) bevat met classificatieniveau Midden of hoger dient door een gecertificeerd bedrijf vernietigd te worden conform het regelement ‘Vernietiging opslagmedia’, dat jaarlijks door het strategisch managementteam met advies van de CISO wordt geëvalueerd. Het regelement moet voldoen aan ISO / IEC 21964.

Digitale opslagmedia met classificatieniveau Laag of lager mag worden hergebruikt mits deze worden geformatteerd middels de ‘zero-fill’ methodiek.

Fysieke opslagmedia 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.

9.2.7.3 *Verwijderen apparatuur*

Apparatuur met een te verwijderen opslagmedium mag enkel hergebruikt worden buiten de gemeente (verkoop / donatie) mits het opslagmedium volledig is verwijderd uit de apparatuur.

Apparatuur waar het opslagmedium niet verwijderd 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.

Voor alle te verwijderen apparatuur dient de verantwoordelijke voor het bedrijfsmiddel én de sectordirecteur 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.

9.2.7.4 *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.

9.2.7.5 *Inleveren apparatuur*

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

9.2.7.6 *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 2.0	beheersmaatregel	7.14
ISO 27001:2023	beheersmaatregel	7.14
BIO versie 1.04zv	beheersmaatregel	11.2.7

9.2.8 Onbeheerde gebruikersapparatuur

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 2.0	beheersmaatregel	7.07
ISO 27001:2023	beheersmaatregel	7.7
BIO versie 1.04zv	beheersmaatregel	11.2.8

9.2.9 Clean desk en clear screen

Binnen de gemeente hanteren medewerkers een ‘clean desk’-beleid voor papieren documenten en verwijderbare opslagmedia en een ‘clear screen’-beleid voor informatie verwerkende faciliteiten.

Ten alle tijden 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 9.2.4.

Voor informatie met classificatie ‘Midden of ‘Hoog’ geldt additioneel:

- Media dienen na het afdrukken onmiddellijk van printers te worden verwijderd.

Referentie		
BIO versie 2.0	beheersmaatregel	7.07
ISO 27001:2023	beheersmaatregel	7.7
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 2.0	beheersmaatregel	5.37
ISO 27001:2023	beheersmaatregel	5.37
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 2.0	beheersmaatregel	8.32.01
ISO 27001:2023	beheersmaatregel	8.32
BIO versie 1.04zv	beheersmaatregel	12.1.2

10.1.3 Configuratiebeheer

Configuraties en wijzigingen op configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken behoren te worden vastgesteld, vastgelegd, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.

Het doel is dat de organisatie kan garanderen en controleren dat hardware, software, diensten en netwerken correct en met de vereiste beveiligingsinstellingen functioneren en de configuratie niet door ongeautoriseerde of foutief handelen wordt gewijzigd. Door documentatie en wijzigingen middels een versiebeheersysteem op te slaan en waar mogelijk geautomatiseerd uit te rollen, kan een foutief geconfigureerd of gecompromitteerd dan wel kapot systeem sneller hersteld worden.

De procedure Configuratiebeheer beschrijft tenminste:

- Processen en instrumenten om voor zowel nieuwe als bestaande netwerken, systemen, applicaties en diensten de volledige configuratie, waaronder de beveiligingsconfiguraties:
    - Geversioneerd op te slaan;
    - Te documenteren;
    - Gedurende de levensduur af te dwingen;
    - Te monitoren en periodiek te controleren;
- Rollen en verantwoordelijkheden om de procedure uit te voeren en afdoende beheersing van alle veranderingen aan configuraties te waarborgen.

Referentie		
BIO versie 2.0	beheersmaatregel	8.09.01
ISO 27001:2023	beheersmaatregel	8.9
BIO versie 1.04zv	beheersmaatregel	-

10.1.4 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 2.0	beheersmaatregel	8.06.01
ISO 27001:2023	beheersmaatregel	8.6
BIO versie 1.04zv	beheersmaatregel	12.1.3

10.1.5 Scheiding van ontwikkel-, test- en productieomgevingen

Ontwikkel-, test-, acceptatie- en productieomgevingen (OTAP) zijn gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving of -gegevens te verlagen. In de productieomgeving wordt niet getest, tenzij om gewijzigde functionaliteit te verifiëren: hierbij mogen in de productieomgeving gegevens niet daadwerkelijk gewijzigd worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan kan er worden afgeweken.

Het is leveranciers toegestaan om zonder voorafgaande toestemming wijzigingen aan Acceptatie- en Productieomgevingen door te voeren als niet-gemitigeerde kwetsbaarheden van niveau Hoog of Kritiek verholpen moeten worden om de beveiliging van het netwerk, systeem, applicatie of dienst te garanderen. Hierbij wordt de CVSS-schaal gehanteerd; een CVE of CVE-aanvraag is niet noodzakelijk, maar inschaling van de kwetsbaarheid wordt door de leverancier wel onderbouwd. Deze wijzigingen worden door de leverancier direct aan de gemeente gemeld en door een medewerker gecontroleerd.

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

- Het is niet toegestaan een kopie van de gegevens (database) van de Productie-omgeving op enige andere omgeving te plaatsen;
    - Voor ontwikkel-, test- en acceptatiedoeleinden worden representatieve set aan gegevens gebruikt;
    - Deze set mag standaard of generieke gegevens van het systeem bevatten;
    - Deze set mag géén persoonsgegevens bevatten;
    - Deze set mag géén gegevens bevatten die door medewerkers over personen of organisaties zijn ingevoerd of die door personen of organisaties zelf zijn ingevoerd of aangeleverd;
    - Deze set mag onomkeerbaar geanonimiseerde of gesubstitueerde gegevens bevatten die instaan voor de persoonsgegevens en/of gegevens over of van personen en organisaties;
- Het is niet toegestaan om verschillende omgevingen aan elkaar te koppelen of gegevens met elkaar te laten uitwisselen (bijvoorbeeld het koppelvlak van Acceptatieomgeving Systeem A verbinden met het koppelvlak Productieomgeving Systeem B).

Referentie

BIO versie 2.0	beheersmaatregel	8.31.02
ISO 27001:2023	beheersmaatregel	8.31
BIO versie 1.04zv	beheersmaatregel	12.1.4

10.2 Bescherming tegen malware, spam en phishing

Informatie en informatie verwerkende faciliteiten dienen beschermd te zijn tegen malware, spam en phishing.

- Malware is software die specifiek is ontwikkeld om schade toe te brengen aan een computer en andere IT-systemen, toegang hiertoe te forceren of het systeem op een oneigenlijke wijze te kunnen gebruiken;
- Spam zijn ongewenste berichten (via alle kanalen), meestal gericht op het aanprijzen of verkopen van al dan niet legale diensten of producten;
    - Ongevraagde (commerciële) berichten, waaronder nieuwsbrieven, enquêtes, aanbod van producten of diensten, etc. van bona fide partijen worden ook als spam beschouwd;
- Phishing zijn ongewenste berichten (via alle kanalen) die zijn gericht op het verkrijgen van toegang en/of toegangsgegevens van medewerkers tot netwerken, systemen, applicaties of diensten van de gemeente, meestal door het proberen te verleiden van de ontvanger te klikken op een malafide link of bijlage in het bericht.

10.2.1 Beheersmaatregelen tegen malware, spam en phishing

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

- Netwerk, apparaten, besturingssystemen en applicaties zijn met openbare en ‘curated’ lijsten dusdanig geconfigureerd toegang wordt geblokkeerd tot advertenties/advertentienetwerken, bekende bronnen van malware, spam, phishing, etc. en deze lijsten worden minimaal 1 keer per 24 uur geüpdatet;
- Netwerk, systemen en accounts worden (geautomatiseerd) gemonitord op signalen van malware, spam, phishing, compromitatie en/of oneigenlijk gebruik;
- Netwerken, systemen en accounts waarop verdachte signalen worden geconstateerd, worden direct in quarantaine geplaatst en nader onderzocht;
- Berichtenverkeer wordt automatisch gescand op malware, spam en phishing en verdachte berichten worden in quarantaine geplaatst en kunnen alleen door een daartoe bevoegde medewerker geraadpleegd en eventueel vrijgegeven worden;
- 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 dag wordt het gehele apparaat gescand
    - De scan mag de werkzaamheden van de medewerker niet onderbreken of vertragen.

Referentie		
BIO versie 2.0	beheersmaatregel	8.07.01, 8.07.02, 8.07.03 en 8.07.04
ISO 27001:2023	beheersmaatregel	8.7
BIO versie 1.04zv	beheersmaatregel	12.2.1

10.3 Back-up van informatie

Er moet een gemeentebreed back-upbeleid zijn dat jaarlijks wordt geëvalueerd. De sectordirecteur Publiekszaken en bedrijfsvoering is verantwoordelijk voor het vaststellen en implementeren van dit beleid. De coördinator I&A is verantwoordelijk voor het opstellen en updaten van dit beleid.

Het back-upbeleid bevat algemene bepalingen en waar nodig onderwerp- of systeemspecifieke bepalingen. De dataclassificatie en het belang van de beschikbaarheid van de informatie en/of het systeem voor de bedrijfscontinuïteit wegen mee in de eisen ten aanzien de back-ups. Het back-upbeleid is ook van toepassing op leveranciers en systemen die als dienst of ‘in de cloud’ geleverd worden.

Dit beleid dient minimaal de volgende onderwerpen te bevatten:

- Specifieke eisen met betrekking tot de hersteltijd en dataverlies per informatieclassificatieniveau gebaseerd op een expliciete risico-afweging.
    - Het beleid definieert de Recovery Time Objective (RTO): de maximale periode totdat de desbetreffende werkzaamheden weer volledig operationeel zijn;
    - Het beleid definieert de Recovery Point Objective (RPO): de maximale hoeveelheid transacties op of wijzigingen aan de gegevens die verloren mogen zijn gegaan na herstel.
- Specifieke eisen met betrekking tot de inhoud, retentie en rotatie van back-ups.
- 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).
- Het back-upproces voorziet in een periodieke offline opslag van back-ups.
- Ook gegevens uit cloudopslag en configuratiegegevens worden gebackupt.
- Eén backup-kopie is ondergebracht bij een onafhankelijke derde partij waar de gemeente zelf toegang toe kan autoriseren mocht de leverancier van de oorspronkelijke applicatie en/of opslag om enigerlei redenen de gewenste gegevens niet (tijdig genoeg) kunnen ontsluiten.
- De herstelprocedure wordt minimaal jaarlijks getest (of na een grote wijziging) om de goede werking te waarborgen als deze in noodgevallen moet worden uitgevoerd.
- Toegang tot back-ups wordt beveiligd door middel van versleuteling conform hoofdstuk 8.

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.

Referentie		
BIO versie 2.0	beheersmaatregel	8.13.01
ISO 27001:2023	beheersmaatregel	8.13
BIO versie 1.04zv	beheersmaatregel	12.3.1

10.4 Wissen van informatie

De gemeente moet beleid hebben voor het wissen van informatie. Informatie waar niet langer actief gebruik van gemaakt wordt, moet conform de Archiefwet gearchiveerd worden. Als informatie gearchiveerd is, moet de actieve kopie(ën) gewist worden. Als archivering niet nodig is of de vernietigingstermijn is bereikt, moet de gearchiveerde informatie gewist worden. Het doel is dat (gevoelige) informatie niet langer dan noodzakelijk opgeslagen wordt, zodat deze informatie niet op een oneigenlijke wijze gebruikt of openbaar gemaakt wordt.

Het beleid schrijft in ieder geval de volgende punten voor:

- Een algemene aanpak die rekening houdt met de Archiefwet en andere wettelijke archiveringsbepalingen, verschillende dataclassificaties en het gebruik van diensten en/of ‘cloud’ opslag;
- De bepaling dat opslagmedia vanaf eerste ingebruikname voorzien moeten zijn van ‘full disk encryption’, zie paragraaf 8.1.2;
- De toe te passen wismethode(n);
- Hoe resultaten van de wismethode(n) als bewijs van het wissen geregistreerd worden;
- Hoe een dienstverlenende partij of cloudleverancier bewijs van wissen van informatie aantoont;
- Periodieke controle op het wissen van informatie.

Referentie		
BIO versie 2.0	beheersmaatregel	8.10.01
ISO 27001:2023	beheersmaatregel	8.10
BIO versie 1.04zv	beheersmaatregel	-

10.5 Verslaglegging en monitoren

10.5.1 Gebeurtenissen registreren

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, toegangs- en authenticatiesystemen 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 2.0	beheersmaatregel	8.15.01, 8.15.02, 8.16.01, 8.16.04
ISO 27001:2023	beheersmaatregel	8.15 en 8.16
BIO versie 1.04zv	beheersmaatregel	12.4.1

10.5.2 Beschermen van informatie in logbestanden

Logbestanden worden beschermd tegen wijziging achteraf. 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 14.3.

Referentie		
BIO versie 2.0	beheersmaatregel	8.15.03, 8.15.03, 8.15.04, 8.15.05, 8.15.06
ISO 27001:2023	beheersmaatregel	8.15
BIO versie 1.04zv	beheersmaatregel	12.4.2 en 12.4.3

10.5.3 Kloksynchronisatie

Het accuraat voeren van de juiste datum en tijd is essentieel voor alle informatieverwerkende systemen om goed en veilig informatie op te slaan, uit te wisselen en logbestanden te genereren. Alle systemen van de gemeente en systemen of diensten van leveranciers dienen te voldoen aan de volgende eisen:

- Datum en tijd wordt middels het secure Network Time Protocol (NTP V4 of hoger) ingesteld en minimaal 1 keer per 24 uur geautomatiseerd gesynchroniseerd;
    - Systeemtijd en hardware tijd worden beiden gesynchroniseerd;
    - 'Clock drift' wordt gemeten en zonodig wordt het systeem vaker dan 1 keer per 24 uur gesynchroniseerd;
- Het systeem roept voor synchronisatie een redundante pool van publieke NTP-servers aan;
    - Bij voorkeur worden geen interne NTP-servers gebruikt, maar indien noodzakelijk zijn interne NTP-servers redundant uitgevoerd en roepen op hun beurt een redundante pool van publieke NTP-servers aan;
- De gehanteerde systeemtijd is UTC (Coordinated Universal Time);
    - Waar datum en tijd voor 'gewone' gebruikers zichtbaar is, worden deze door middel van conversie weergegeven als CET (Central European Time) waarbij rekening wordt gehouden met zomertijd/wintertijd;
    - Databases slaan in ieder geval de datum/tijd in UTC op en kunnen daarnaast een kolom met lokale tijd voeren;
    - Waar dit logisch of noodzakelijk is, kan een systeem als onderdeel van de gegevens/informatie de lokale tijd opslaan, echter altijd onder vermelding van de gebruikte tijdzone.

Systeemeigenaren zijn verantwoordelijk voor de juiste werking en synchronisatie van hun systemen.

Referentie		
BIO versie 2.0	beheersmaatregel	8.17.01
ISO 27001:2023	beheersmaatregel	8.17
BIO versie 1.04zv	beheersmaatregel	12.4.4

10.6 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 systeemeigenaar;
- Op productiesystemen is uitsluitend goedgekeurde uitvoerbare programmatuur aanwezig (zie paragraaf 10.8);
- 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 2.0	beheersmaatregel	8.19.01
ISO 27001:2023	beheersmaatregel	8.19
BIO versie 1.04zv	beheersmaatregel	12.5

10.7 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 24 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 2.0	beheersmaatregel	8.08.01
ISO 27001:2023	beheersmaatregel	8.8
BIO versie 1.04zv	beheersmaatregel	12.6.1

10.8 Beperkingen voor het installeren van software

10.8.1.1 *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. Ook zijn niet toegestane uitvoerbare bestanden niet uitvoerbaar.

10.8.1.2 *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.

10.8.1.3 *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.

10.8.1.4 *Verantwoordelijkheden*

De sectordirecteur Publiekszaken en Bedrijfsvoering is verantwoordelijk voor de 'Geautoriseerde Software Whitelist' en de 'Software Blacklist'. Op aanvraag van de Coördinator I&A en de CISO kan de sectordirecteur besluiten om de lijsten te herzien.

Er dient een installatiemanager(s) aangesteld te zijn die 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 2.0	beheersmaatregel	8.19.01
ISO 27001:2023	beheersmaatregel	8.19
BIO versie 1.04zv	beheersmaatregel	12.6.2

10.9 Overwegingen betreffende audits van informatiesystemen

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 2.0	beheersmaatregel	8.34.01
ISO 27001:2023	beheersmaatregel	8.34
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:

11.1.1.1 *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' staan;
- Apparatuur die binnen netwerken wordt gebruikt waarin informatie met classificatie 'hoog' wordt uitgewisseld mag niet afkomstig van die de 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 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 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 7.

11.1.1.2 *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.

11.1.1.3 *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.

11.1.1.4 *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.

11.1.1.5 *Netwerken monitoren*

Netwerkmonitoring dient te voldoen aan het voorschrift netwerkmonitoring waarin minimaal de volgende zaken in moeten 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 7 en 8.
- 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.

11.1.1.6 *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.

11.1.1.7 *Beschikbaarheidseisen*

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

11.1.1.8 *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 2.0	beheersmaatregel	8.20.01 en 8.20.02
ISO 27001:2023	beheersmaatregel	8.20

BIO versie 1.04zv	beheersmaatregel	13.1.1

11.1.2 Beveiliging van 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.

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 2.0	beheersmaatregel	8.21.01
ISO 27001:2023	beheersmaatregel	8.21
BIO versie 1.04zv	beheersmaatregel	13.1.2

11.1.2.1 *Netwerkdetectievoorzieningen*

Het dataverkeer binnen de netwerken moeten worden geanalyseerd op signalen van misbruik middels (geautomatiseerde) detectievoorzieningen. De detectievoorzieningen worden ingezet op basis van een risico-inschatting door de CISO. De detectievoorzieningen worden beschreven in het ‘Voorschrift detectievoorzieningen’. 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 2.0	beheersmaatregel	8.21.02

ISO 27001:2023	beheersmaatregel	8.21
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 24 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 2.0	beheersmaatregel	8.21.03
ISO 27001:2023	beheersmaatregel	8.21
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, 8 en paragraaf 11.2.

Referentie		
BIO versie 2.0	beheersmaatregel	8.21.04
ISO 27001:2023	beheersmaatregel	8.21
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 2.0	beheersmaatregel	8.21.01
ISO 27001:2023	beheersmaatregel	8.21
BIO versie 1.04zv	beheersmaatregel	13.1.2.4

11.1.3 Scheiding in netwerken

11.1.3.1 *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.

11.1.3.2 *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. Daarnaast zijn gebruikers ingedeeld in groepen op basis van werkgebied, wat mede bepaalt tot welke netwerken en/of informatiediensten zij toegang hebben. Tenslotte bepaalt het aan de functie van de medewerker gekoppelde standaard autorisatieprofiel tot welke netwerken en informatiediensten de medewerker toegang heeft.

11.1.3.3 *Netwerken*

Netwerken moeten zijn ingedeeld op basis van het informatieclassificatieniveau van de informatie die in het netwerk wordt gecommuniceerd. Daarnaast moeten netwerken gesegmenteerd worden op basis van logische of functionele verschillen. 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 Boekel 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 bedrijfsmiddelen). Het eigenaarschap is belegd bij CISO.

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

Referentie		
BIO versie 2.0	beheersmaatregel	8.22.01
ISO 27001:2023	beheersmaatregel	8.22
BIO versie 1.04zv	beheersmaatregel	13.1.3

11.1.4 Toepassen van (web)filters

De gemeente moet een richtlijn hebben voor het filteren van binnenkomende schadelijke inhoud en uitgaande (gevoelige) informatie. Webfilters worden primair toegepast om gebruikers en systemen te beschermen tegen blootstelling aan (functioneel) kwaadaardige inhoud en evident illegale bronnen. Het doel van webfiltering is dus niet het beperken van toegang tot bepaalde meningen of minder courante soorten informatie.

Voor het filteren wordt gebruikt gemaakt van publieke ‘blacklists’ van vertrouwde partijen. Deze lijsten combineren meestal bekende netwerkadressen, domeinnamen en patronen om te bepalen welke inhoud en bronnen worden geblokkeerd. Het blokkeren dient zowel op netwerkniveau (DNS, firewall) als op het apparaat van de gebruiker (browser addon, ‘endpoint protection’) te gebeuren. Te blokkeren inhoud en bronnen omvatten tenminste:

- Netwerkbronnen bekend om het verspreiden van malware, phishing, etc. inclusief advertenties en advertentienetwerken;
- Command-and-control servers of netwerken;
- Netwerkbronnen die evident illegale inhoud delen;
- Netwerkbronnen die op basis van informatie of analyse een dreiging vormen.

Netwerk, apparaten, besturingssystemen en applicaties zijn met openbare en ‘curated’ lijsten dusdanig geconfigureerd toegang wordt geblokkeerd tot advertenties/advertentienetwerken, bekende bronnen van malware, phishing, etc. en deze lijsten worden minimaal 1 keer per 24 uur geüpdatet.

Filtering dient, waar mogelijk, ook het onbedoeld of ongewenst versturen van informatie te voorkomen. Netwerk, apparaten, besturingssystemen en applicaties zijn dusdanig geconfigureerd dat deze geen (identificerende) gegevens kunnen versturen of doorlaten naar derden, zoals telemetrie, gebruiksgegevens, crashlogs, etc.

Medewerkers worden geacht gegevens van de gemeente alleen te delen of versturen zoals beschreven in het werkproces of op de voorgeschreven veilige methode aan/met vertrouwde personen. Mocht de praktijk er aanleiding toe geven, dan kunnen ook websites/diensten geblokkeerd worden waar gegevens van de gemeente kunnen worden geüpload en/of gedeeld.

De richtlijn omschrijft tenminste:

- Op welke wijze voor welke doeleinden welke filters worden ingezet;
- Welke filterlijsten worden gebruikt;
- Hoe met meldingen van false positives/negatives en verzoeken tot vrijgave van bronnen wordt omgegaan;
- Hoe de werking van de filters wordt gecontroleerd en geëvalueerd;
- Hoe gerapporteerd wordt over de werking en wijziging van filters.

Referentie		
BIO versie 2.0	beheersmaatregel	8.23.01
ISO 27001:2023	beheersmaatregel	8.23
BIO versie 1.04zv	beheersmaatregel	-

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 fysiek transport. Voor beiden zijn handreikingen beschikbaar. De handreikingen dienen te voldoen aan:

Handreiking Digitaal Informatietransport

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

Handreiking Fysiek Informatietransport

- De eisen van paragraaf 9.2.4.
- De eisen van paragraaf 6.2.

Het gebruik van een privé-apparaat voor werkgerelateerde zaken is niet toegestaan. Dat betekent ook dat het synchroniseren van de werkagenda of -mail met een privé apparaat of account niet is toegestaan, net zoals het versturen van werkgerelateerde informatie of documenten naar een privé (mail)account.

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

Referentie		
BIO versie 2.0	beheersmaatregel	5.14.01
ISO 27001:2023	beheersmaatregel	5.14
BIO versie 1.04zv	beheersmaatregel	13.2.1

11.2.2 Overeenkomst over 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 8 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 2.0	beheersmaatregel	5.14.01
ISO 27001:2023	beheersmaatregel	5.14
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’.

- Mailservers dienen 100% te scoren op de tests van Internet.nl en ook de niet-meewegende standaarden volledig te implementeren (op moment van schrijven: DANE);
- Ook servers van leveranciers/diensten die namens de gemeente onder het “boekel.nl” domein mail versturen dienen hier aan te voldoen: dit dient bij inkoop/aanbesteding contractueel vastgelegd te zijn;
- Zonder schriftelijke toestemming inclusief uitgebreide uitleg van de CISO mag er niet afgeweken worden van de eisen.

Verder dient er voorafgaand 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 2.0	beheersmaatregel	5.14.01
ISO 27001:2023	beheersmaatregel	5.14
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 2.0	beheersmaatregel	5.14.02
ISO 27001:2023	beheersmaatregel	5.14
BIO versie 1.04zv	beheersmaatregel	13.2.3.2

11.2.3.2 *Elektronische berichten met certificaten*

Elektronische berichten waarin informatie staat met classificatie Midden of hoger dient er te alle tijden gebruik gemaakt te worden van versleuteling en 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 2.0	beheersmaatregel	5.14.03
ISO 27001:2023	beheersmaatregel	5.14
BIO versie 1.04zv	beheersmaatregel	13.2.3.3

11.2.3.3 *Registratie van systemen die elektronische berichten verzenden en ontvangen*

Er moet een registratie zijn van alle systemen die elektronische berichten verzenden en ontvangen. Hieronder vallen alle systemen die:

- Open staan voor verbindingen op willekeurig welke poort of via welk protocol;
- Berichten versturen naar andere systemen via willekeurig welke poort of welk protocol.

Referentie		
BIO versie 2.0	beheersmaatregel	5.14.04
ISO 27001:2023	beheersmaatregel	5.14
BIO versie 1.04zv	beheersmaatregel	-

11.2.3.4 *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 van het Forum Standaardisatie.

Referentie		
BIO versie 2.0	beheersmaatregel	5.14.05
ISO 27001:2023	beheersmaatregel	5.14
BIO versie 1.04zv	beheersmaatregel	13.2.3.4

11.2.3.5 *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 2.0	beheersmaatregel	6.06.01
ISO 27001:2023	beheersmaatregel	6.6
BIO versie 1.04zv	beheersmaatregel	13.2.4

11.3 Informatie publiceren en delen

11.3.1 Voorkomen van gegevenslekken

Ongeoorloofde openbaarmaking of extractie van informatie door personen of systemen moet gedetecteerd en voorkomen worden. Hiervoor moet een richtlijn zijn. De richtlijn beschrijft tenminste:

- Dat informatie geïdentificeerd en geclassificeerd moet zijn;
- Hoe de kanalen worden gemonitord waarlangs de informatie bedoeld of onbedoeld gelekt kan worden;
- Welke maatregelen tegen het lekken worden genomen;
- De uitgangspunten en eisen zoals geformuleerd in paragrafen 3.2, 10.2 en 11.1.4.

De CISO is verantwoordelijk voor het opstellen en jaarlijks evalueren van de richtlijn. De richtlijn moet door het DT worden vastgesteld.

Referentie		
BIO versie 2.0	beheersmaatregel	8.12.01
ISO 27001:2023	beheersmaatregel	8.12
BIO versie 1.04zv	beheersmaatregel	-

11.3.2 Maskeren van gegevens

Het moet voorkomen worden dat persoons- en gevoelige gegevens mee openbaar worden gemaakt in informatie of documenten die wel openbaar gemaakt moeten of mogen worden waar dat niet toegestaan is. De richtlijn *Maskeren van gegevens* beschrijft tenminste:

- De algemene regels van de gemeente Boekel voor het maskeren van gegevens bij transport, (her)gebruik of openbaarmaking van informatie;
- Specifieke processen en taken waar openbaar te maken informatie gemaskeerd moet worden;
- Werkwijze en middelen om het maskeren van de gegevens te bewerkstelligen
- Toepasselijke (eisen van) wet- en regelgeving

In specifieke gevallen kan waar “maskeren” staat ook “pseudonimiseren” gelezen worden.

De Privacy officer is verantwoordelijk voor het opstellen en jaarlijks evalueren van de richtlijn. De richtlijn moet door het DT worden vastgesteld.

Referentie		
BIO versie 2.0	beheersmaatregel	8.11.01
ISO 27001:2023	beheersmaatregel	8.11
BIO versie 1.04zv	beheersmaatregel	-

11.4 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 2.0	beheersmaatregel	8.26.01
ISO 27001:2023	beheersmaatregel	8.26
BIO versie 1.04zv	beheersmaatregel	14.1.3

11.5 Toepassingen op openbare netwerken beveiligen

11.5.1 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).

11.5.2 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 2.0	beheersmaatregel	8.26.01
ISO 27001:2023	beheersmaatregel	8.26
BIO versie 1.04zv	beheersmaatregel	14.1.2

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 7.3.5);
    - Locatie van opslag van de broncode;
    - Doorvoeren van wijzigingen in de broncode (zie paragraaf 7.3.5);
- 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 2.0	beheersmaatregel	8.25.01
ISO 27001:2023	beheersmaatregel	8.25
BIO versie 1.04zv	beheersmaatregel	14.2.1, 14.2.1.1 en 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 2.0	beheersmaatregel	8.27.01
ISO 27001:2023	beheersmaatregel	8.27
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 2.0	beheersmaatregel	8.31.01
ISO 27001:2023	beheersmaatregel	8.31
BIO versie 1.04zv	beheersmaatregel	14.2.6

12.1.4 Veilig coderen

Het doel is bij het ontwikkelen van software zoveel mogelijk kwetsbaarheden en fouten te vermijden. De toe te passen maatregelen hiervoor zijn afhankelijk van het soort software, in welke context of systemen de software wordt toegepast, de gebruikte programmeertaal, etc. In geval de gemeente software zou ontwikkelen of laat ontwikkelen wordt voor dat project een Veilig coderen beleid opgesteld.

Het beleid beschrijft de maatregelen die tijdens de ontwikkeling genomen worden om software te ontwikkelen conform de principes van Security by Design, Privacy by Design en Accessibility by Design. Daarnaast worden de 'best practices' voor de te gebruiken programmeertaal, framework en/of community in het beleid meegenomen. Het beleid houdt rekening met bepalingen voor de voorbereidingsfase, de ontwikkelfase, de gebruiksfase (operationeel gebruik, onderhoud en doorontwikkeling).

Referentie		
BIO versie 2.0	beheersmaatregel	8.28.01
ISO 27001:2023	beheersmaatregel	8.28
BIO versie 1.04zv	beheersmaatregel	-

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 2.0	beheersmaatregel	8.25.01 en 8.32.02
ISO 27001:2023	beheersmaatregel	8.25 en 8.32
BIO versie 1.04zv	beheersmaatregel	14.2.2 en 14.2.2.1

12.2.2 Technische beoordeling van toepassingen na wijzigingen 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 2.0	beheersmaatregel	8.32.01
ISO 27001:2023	beheersmaatregel	8.32
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.
- 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 2.0	beheersmaatregel	8.33.01
ISO 27001:2023	beheersmaatregel	8.33
BIO versie 1.04zv	beheersmaatregel	14.3.1

12.3.2 Testen van systeembeveiliging

12.3.2.1 *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.

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

Referentie		
BIO versie 2.0	beheersmaatregel	8.29.01
ISO 27001:2023	beheersmaatregel	8.29
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 2.0	beheersmaatregel	8.29.01
ISO 27001:2023	beheersmaatregel	8.29
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. Leveranciers van diensten en producten dienen ook de gemeente in staat te stellen zelf aan het informatiebeveiligingsbeleid te voldoen en hier bij de toezichthouders met positief resultaat verantwoording over af te leggen.

13.1 Informatiebeveiligingsbeleid voor leveranciers

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

Voorafgaand aan het aanvragen van een offerte, aanbesteding of het afsluiten van (een uitbreiding van) een contract dient er bepaald te worden of er voor de uitvoering of levering sprake is van:

- (gebruik van) ICT-middelen of -diensten;
- een koppeling of integratie met de netwerken en/of ICT-omgeving van de gemeente;
- het verwerken of transporteren van gegevens van de gemeente.

Als dat het geval is, worden er eisen gesteld aan de leverancier en de dienst of product. Deze eisen moeten onderdeel zijn van het inkoop- en aanbestedingsproces en de leverancier moet hier contractueel mee instemmen.

Om te bepalen welke eisen gesteld moeten worden, moet:

- een risicoanalyse opgesteld te worden van het voorgeziene proces en ICT-middelen of -diensten, en een eventuele koppeling of integratie met de netwerken en/of ICT-omgeving van de gemeente;
- de te verwerken of transporteren informatie geclassificeerd te worden. Als meerdere soorten informatie met verschillende classificaties in dezelfde dienst / product gebruikt worden dan geldt de hoogste classificatie voor het vaststellen van de eisen.

De CISO of ISO worden betrokken bij het opstellen van de risicoanalyse en de informatieclassificatie. Als er ook persoonsgegevens worden verwerkt of getransporteerd, dan worden de PO en FG betrokken voor het uitvoeren van een DPIA.

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

- Op alle overeenkomsten zijn de meest recente versie van de Gibit inkoopvoorwaarden en het gemeentelijke inkoop- en aanbestedingsbeleid van toepassing;
- De leverancier is ISO 27001 gecertificeerd door een auditor onder accreditatie met een audit scope die de gehele dienstverlening van het aanbod dekt. Als er sprake is van samenwerking met onderaannemers, dienen alle partijen aan deze normen te voldoen;
- De leverancier moet jaarlijks een Third Party Memorandum (TPM) inclusief scope en Verklaring van Toepasselijkheid (VvT) aan te leveren van de actuele stand van de ISO 27001 certificering;
- Als persoonsgegevens verwerkt (kunnen) worden, levert de leverancier een ingevulde en ondertekende standaard verwerkersovereenkomst aan (VNG model);

- Als er sprake is van een dienst of product waarbij medewerkers van de leverancier (beheer)toegang hebben tot de dienst of product en/of de gegevens van de gemeente, dan:
    - Moet de leverancier een passende screeningsprocedure toepassen voor het werven en selecteren van nieuwe medewerkers;
    - Enkel medewerkers van de leverancier die een VOG aan de leverancier hebben overlegd, krijgen (beheer)toegang tot de systemen, applicaties en gegevens van de gemeente;
    - De leverancier laat de auditor een verklaring over compliance met deze eis in de jaarlijkse TPM-verklaring opnemen of bijvoegen;
    - De leverancier controleert minimaal iedere 5 jaar de VOG-status van de medewerkers die (beheers)toegang hebben tot de systemen, applicaties en gegevens van opdrachtgever;
- De toepassing van AI(-tools) en algoritmen is niet toegestaan zonder expliciete toestemming van de gemeente, een uitgevoerde DPIA en (verwerkers)overeenkomst betreffende de verwerking;
- De leverancier dient alle benodigde informatie over de AI(-tools) en/of algoritmen aan te leveren die noodzakelijk zijn voor het aanmelden hiervan bij het Algoritmeregister.
- Er moet een geheimhoudingsclausule opgenomen worden die voor alle betrokkenen geldt;
- Voor het type dienst of product en dataclassificatie wordt een passende uptime geëist;
- Voor het type dienst of product en dataclassificatie wordt een passende backup-procedure geëist conform paragraaf 10.3;
- Voor het type dienst of product en dataclassificatie wordt een passende exit-strategie geleverd:
    - Tenminste wordt beschreven hoe gegevens van de gemeente in een machine-leesbaar open standaardformaat geëxporteerd kunnen worden;
    - Hoe de gemeente dit zelf kan doen of dat de leverancier dit zonder meerkosten op verzoek uitvoert;
- De gemeente blijft te allen tijde eigenaar van de gegevens en metagegevens die met en via de systemen en diensten van de inschrijver worden verwerkt;
- (Meta)gegevens worden zonder expliciete toestemming van de opdrachtgever niet met derden gedeeld of door de inschrijver voor eigen of commerciële doeleinden verwerkt;
- De gemeente wordt binnen 12 uur op de hoogte gesteld van een datalek of beveiligingsincident bij de leverancier dat (ook) de dienst of systeem of gegevens van de gemeente raakt;
- Voor het type dienst of product en dataclassificatie wordt een passende incidentenprocedure geleverd;
    - Tenminste wordt beschreven hoe de samenwerking tussen de leverancier en de gemeente verloopt in geval van een informatiebeveiligingsincident, bijvoorbeeld door middel van een communicatie- en escalatiematrix;
- 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 (minimaal 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 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 leverancier levert verplicht een volledig functionele Acceptatie-omgeving van het systeem, applicatie of dienst;
    - De leverancier hanteert een wijzigingsbeleid dat voorziet in het testen en goedkeuren van wijzigingen door de gemeente vóórdat deze in productie worden genomen;
    - Het wijzigingsbeleid mag een uitzondering hanteren voor wijzigingen die kwetsbaarheden van niveau Hoog of Kritiek remediëren;
    - De systemen en procedures voldoen aan het in paragraaf 10.1.5 en hoofdstuk 12 gestelde;
    - Van deze bepaling kan, in de aanbesteding of bij implementatie, alleen met instemming van de CISO en de proceseigenaar afgeweken worden.

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

Classificatie: Laag

- Voorafgaand aan verlening van de opdracht moet een verwerkersovereenkomst op basis van de VNG-standaard zijn afgesloten als de leverancier (persoons)gegevens verwerkt of transporteert namens de gemeente.
- 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 Boekel' te laten ondertekenen door de medewerker van de leverancier en het op de daarvoor bestemde centrale plek te registreren.
- 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 (zie formulier bijlage 2) 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 regelement 'Verantwoordingsrapportages gemeente Boekel'.
- 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 2.0	beheersmaatregel	5.19.01
ISO 27001:2023	beheersmaatregel	5.19
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).

Referentie		
BIO versie 2.0	beheersmaatregel	8.20.01
ISO 27001:2023	beheersmaatregel	5.20
BIO versie 1.04zv	beheersmaatregel	15.1.2

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:

- De beveiligingseisen die in de paragraaf 13.1.1 van toepassing zijn dienen te worden opgenomen in de definitieve contracten.
- 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.
- Er dient opgenomen te zijn wat de procedure is in geval de leverancier in gebreke blijft.
- Eisen die zijn afgeleid van de bedrijfsprocessen, zoals het registreren en monitoren van transacties dienen opgenomen te worden.
- Eisen die verplicht zijn gesteld door andere beheersmaatregelen met betrekking tot beveiliging dienen te worden opgenomen.
- Procedures voor het verlenen van toegang en autorisatie, voor zakelijke en voor bevoorrechte of technische gebruikers dienen te zijn vastgelegd.
- Bij het kopen van producten behoort een formele test- en acquisitieprocedure te worden gevolgd.
- De vereiste beschermingsbehoeften van de betrokken bedrijfsmiddelen, in het bijzonder met betrekking tot de beschikbaarheid, vertrouwelijkheid en integriteit zijn meetbaar vastgelegd.
- 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.
- Na afsluiting dienen gebruikers en operators geïnformeerd te worden over hun plichten en verantwoordelijkheden.

Referentie		
BIO versie 2.0	beheersmaatregel	5.08.01 en 5.20
ISO 27001:2023	beheersmaatregel	5.8 en 5.20
BIO versie 1.04zv	beheersmaatregel	14.1.1 en 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 hoofdstuk 12);
- 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 2.0	beheersmaatregel	8.30.01
ISO 27001:2023	beheersmaatregel	8.30
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 2.0	beheersmaatregel	5.22.01
ISO 27001:2023	beheersmaatregel	5.22
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:

- Informatieclassificatie.
- Risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is.
- 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:

- 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 2.0	beheersmaatregel	5.22.02
ISO 27001:2023	beheersmaatregel	5.22
BIO versie 1.04zv	beheersmaatregel	15.2.2

14 Beheer van informatiebeveiligingsincidenten

Het doel is dat de organisatie een snelle, doeltreffende, consistente en geordende reactie kan geven wanneer informatiebeveiligingsincidenten zich voordoen en hierover zowel intern als met externe partijen kan communiceren en noodzakelijke gegevens kan verstrekken. Het beheer van informatiebeveiligingsincidenten is een continu proces dat gaat om voorbereiden, reageren en leren.

Er dient een incidentenbeheerprocedure te zijn (zie paragraaf 14.3) waarin de praktische inrichting en uitvoering van het beheer van informatiebeveiligingsincidenten beschreven staat. Ook dient er een crisisplan te zijn in geval van serieuze of kritieke informatiebeveiligingsincidenten.

14.1 Organisatie en verantwoordelijkheden

Het voorbereiden op en omgaan met informatiebeveiligingsincidenten vergt:

- Capaciteit in de staande organisatie;
- Een goede relatie en goede afspraken met de primaire ICT-dienstverlener en overige leveranciers van systemen, applicaties en diensten;
    - De werkwijze in geval van informatiebeveiligingsincidenten moet in de overeenkomst met de leveranciers opgenomen zijn;
- Afspraken om snel op te kunnen schalen en (kritieke) beslissingen te kunnen nemen.

Referentie		
BIO versie 2.0	beheersmaatregel	5.24
ISO 27001:2023	beheersmaatregel	5.24
BIO versie 1.04zv	beheersmaatregel	16.1

14.1.1 CERT

Het Computer Emergency Response Team (CERT) is het staande team dat verantwoordelijk is voor:

- de voorbereiding op incidenten;
- het ontvangen en beoordelen van meldingen;
- het initiëren van actie op een beveiligingsincident;
- het herstellen van een veilige situatie op de netwerken, systemen en diensten van de gemeente.

De te ondernemen actie is primair het stoppen van het incident en het beperken van de schade door het incident. Deze taak moet uitgevoerd worden ook als de eerste actie van het CERT het escaleren van het incident naar het IRT of IBD is.

Na de acute fase van een incident is het CERT verantwoordelijk voor:

- het veilig stellen, overdragen en/of analyseren van eventueel bewijsmateriaal;
- het opstellen en communiceren van de analyses en voorgestelde verbeteringen.

In geval van criminele activiteiten moeten altijd de IBD en het digitale forensisch team van de politie ingeschakeld worden voor het veilig stellen, overdragen en/of analyseren van bewijsmateriaal. In dit geval mag de gemeente dat niet zelf doen.

De incidentenbeheerprocedure beschrijft de samenstelling en werking van het CERT van de gemeente Boekel. De CISO en ISO maken per definitie onderdeel uit van het CERT.

De incidentenbeheerprocedure beschrijft hoe het CERT en leverancier(s) van getroffen systemen of diensten samenwerken in geval van een informatiebeveiligingsincident.

Referentie		
BIO versie 2.0	beheersmaatregel	5.24
ISO 27001:2023	beheersmaatregel	5.24
BIO versie 1.04zv	beheersmaatregel	16.1

14.1.2 IRT

Het Incident Response Team (IRT) wordt geformeerd zodra de omvang of impact van het incident hier om vraagt. De gemeentesecretaris formeert het IRT op advies van de CISO of de ISO. Het IRT bestaat tenminste uit:

- Directeur van de (meest) getroffen sector
- CISO en ISO
- Coördinator I&A
- Proceseigenaar van de getroffen processen
- Systeemeigenaar van de getroffen systemen
- Privacy officer en/of FG als ook persoonsgegevens zijn getroffen

De directeur fungeert als de incidentmanager. Het IRT coördineert de reactie van de gemeente in de acute fase van een incident en draagt zorg voor het inschakelen en/of informeren van derde partijen.

- Het IRT informeert de gemeentesecretaris en portefeuillehouder zo vaak als het incident vereist.
- Het IRT betrekt de gemeentesecretaris en portefeuillehouder bij de besluitvorming en/of communicatie als het incident dit vereist.

Het IRT is verantwoordelijk voor het initiëren van een respons op het incident en het herstellen van een veilige situatie op de netwerken, systemen en diensten van de gemeente. De te ondernemen actie is primair het stoppen van het incident en het beperken van de schade door het incident.

De incidentenbeheerprocedure beschrijft hoe het IRT en leverancier(s) van getroffen systemen of diensten samenwerken in geval van een informatiebeveiligingsincident.

Referentie		
BIO versie 2.0	beheersmaatregel	5.24
ISO 27001:2023	beheersmaatregel	5.24
BIO versie 1.04zv	beheersmaatregel	16.1

14.1.3 Herstel

Het CERT of het IRT is verantwoordelijk voor het herstellen van een veilige situatie in geval van een informatiebeveiligingsincident, maar is niet verantwoordelijk voor het herstel van systemen, gegevens of werkzaamheden.

De verantwoordelijkheid voor het herstel van systemen en werkzaamheden na de acute fase van een incident ligt bij de proces- en systeemeigenaren. De proces- en systeemeigenaren houden bij het herstel rekening met de eventuele noodzaak om bewijsmateriaal te verzamelen en veilig te stellen.

Referentie		
BIO versie 2.0	beheersmaatregel	5.24
ISO 27001:2023	beheersmaatregel	5.24
BIO versie 1.04zv	beheersmaatregel	16.1

14.1.4 Verantwoordelijkheden

De incidentenbeheerprocedure beschrijft op welke wijze bezetting en eventuele vervanging van de verantwoordelijkheden en/of mandatering is geregeld zodat het incidentenbeheer altijd doorgang kan vinden. De volgende verantwoordelijkheden zijn de basis voor het incidentenbeheer.

Taak	Verantwoordelijke
Waarborgen dat capaciteit en middelen van CERT voldoen, waaronder: • formeel toewijzen van functie en taken aan medewerkers • zorgen voor training/opleiding van medewerkers	Directieteam
Formeren van het IRT zodra noodzakelijk	Gemeentesecretaris
Leiding geven aan het IRT	Incidentmanager
Voorbereiding, ontvangen en direct beoordelen meldingen, initiëren actie, herstel veilige situatie	Leden CERT
Informeren naar eigen organisatie en derden	Leden CERT en IRT
Inschakelen IBD en/of politie	Leden CERT en IRT
Periodieke rapportage van incidenten aan DT	CISO
Direct melden van (vermoeden van) kwetsbaarheid of incident	Iedereen werkzaam voor de gemeente

Referentie		
BIO versie 2.0	beheersmaatregel	5.24
ISO 27001:2023	beheersmaatregel	5.24
BIO versie 1.04zv	beheersmaatregel	16.1

14.2 Voorbereiden op informatiebeveiligingsincidenten

De volgende voorbereidingen dienen te worden getroffen en periodiek te worden gecontroleerd en geëvalueerd:

- Het beleid, procedures, beheersmaatregelen, documentatie en hulpmiddelen zijn actueel;

- Het beleid, procedures, beheersmaatregelen, documentatie en hulpmiddelen zijn toegankelijk en beschikbaar voor de medewerkers van de organisatie, ook bij een grootschalige storing van ICT-diensten en -systemen;
- Er is een methode en procedure ingericht voor het monitoren en rapporteren van signalen in netwerken, systemen, applicaties en ruimtes van de gemeente die kunnen duiden op een incident;
- Er is een methode en procedure ingericht voor het inwinnen en evalueren van informatie over kwetsbaarheden die betrekking hebben op de netwerken, systemen, applicaties en ruimtes van de gemeente;
- Er is een methode en procedure ingericht voor het inwinnen en evalueren van informatie over dreigingen die impact kunnen hebben op de bedrijfsvoering van de gemeente;
- Door training, certificering en professionele ontwikkeling wordt gezorgd dat de kennis en kunde van medewerkers belast met het beheer van informatiebeveiligingsincidenten op het juiste niveau is en blijft.

Er zijn afspraken gemaakt over de bezetting, beschikbaarheid, bereikbaarheid en vervanging van de medewerkers van het CERT/IRT. Arbeidsrechtelijke aspecten zijn verwerkt in de arbeidsovereenkomst van deze medewerkers.

De procedures omvatten tenminste:

- Incidentenbeheerprocedure;
- Criteria voor informatiebeveiligingsincidenten;
- Classificatie- en prioriteringsschema voor informatiebeveiligingsincidenten;
- Crisisplan.

De documentatie omvat tenminste:

- Een actueel overzicht van alle mensen met een account en/of fysieke toegang, waarvan vermeld:
    - Functie;
    - Standaard autorisatieprofiel;
    - Extra toegekende rollen/rechten;
- Een actueel overzicht van alle systemen, applicaties en diensten, waarvan vermeld:
    - Locatie / (web)adres;
    - Versienummer(s) softwarecomponent(en);
    - Proceseigenaar;
    - Systeemeigenaar;
    - Functioneel beheerder;
    - Leverancier;
    - Contactgegevens incidentmanager leverancier;
    - Escalatieprocedure;
- Een actueel overzicht van alle uitgegeven apparaten, waarvan vermeld:
    - Type apparaat;
    - Identificatiegegevens voor (remote) beheer;
    - Gebruiker;

- Netwerkdiagram(men), waarin vermeld:
  - Structuur en segmentering van het netwerk;
  - Netwerk- en servercomponenten;
  - IP-nummering en routering;
  - Gebruikte poortnummers op/tussen segmenten en/of servers, applicaties en diensten.

Het CERT en IRT oefenen periodiek ter voorbereiding met de procedures. Het beleid, procedures, beheersmaatregelen, documentatie en hulpmiddelen worden na de oefening geëvalueerd en waar nodig bijgesteld.

Referentie		
BIO versie 2.0	beheersmaatregel	5.24
ISO 27001:2023	beheersmaatregel	5.24
BIO versie 1.04zv	beheersmaatregel	16.1

14.3 Incidentenbeheerprocedure

De kwaliteit en effectiviteit van het incidentenbeheer hangt in hoge mate af van de snelheid waarmee actie genomen wordt op meldingen. Het is daarom cruciaal dat meldingen van medewerkers of automatische systemen snel in behandeling worden genomen. Medewerkers moeten daarom goed op de hoogte zijn van het belang van direct melden en het melden moet snel en laagdrempelig zijn.

14.3.1 Procedure en meldpunt

Er moet één gemeentebrede procedure zijn voor het beheer van informatiebeveiligingsincidenten. Er moet één centraal meldpunt zijn voor het melden van informatiebeveiligingsincidenten. Het meldpunt is via meerdere kanalen bereikbaar. Het meldpunt is ook bereikbaar van buiten het interne netwerk.

Referentie		
BIO versie 2.0	beheersmaatregel	5.24 en 5.26
ISO 27001:2023	beheersmaatregel	5.24 en 5.26
BIO versie 1.04zv	beheersmaatregel	

14.3.2 Respons en beschikbaarheid

Er moet gewaarborgd zijn dat het CERT binnen het dagvenster van 07:00 – 22:00 uur snel en adequaat op meldingen kan reageren, inclusief de mogelijkheid om binnen en buiten de organisatie te escaleren. De incidentbeheerprocedure dient de responstijden van het CERT te specificeren. De incidentbeheerprocedure dient te beschrijven op welke wijze wordt omgegaan met meldingen buiten het dagvenster.

De NIS2/Cyberbeveiligingswet schrijft een meldplicht binnen 24 uur voor. Er moet daarom een voorziening getroffen worden voor het beheren van meldingen in weekenden en op feestdagen. Ook leveranciers moeten aan de meldplicht voldoen en dit moet in de overeenkomst zijn vastgelegd.

In de procedure dient de achtervang c.q. vervanging van de rollen en verantwoordelijkheden bij afwezigheid of onbereikbaarheid van medewerkers beschreven te zijn.

In de arbeidsovereenkomst van medewerkers belast met het incidentbeheer zijn bepalingen opgenomen over de beschikbaarheid en vergoeding passend bij de beschikbaarheidseisen.

Met de primaire ICT-dienstverlener zijn passende afspraken vastgelegd over beschikbaarheid en responstijden die het voor de gemeentelijke organisatie mogelijk maken om aan de responstijden en de meldplicht te kunnen voldoen.

De incidentbeheerprocedure beschrijft hoe het CERT van de gemeente samenwerkt en coördineert met de primaire ICT-dienstverlener. Deze beschrijving omvat tenminste de SLA en DAP van de leverancier en een beschrijving van de rollen, verantwoordelijkheden, contactgegevens en overleg- en escalatiematrix.

Kwetsbaarheden in systemen van de gemeente en/of leveranciers worden middels een *Coordinated Vulnerability Disclosure* bij de leveranciers, de sectorale CERT en zonodig NCSC openbaar gemaakt. De CVD-procedure moet beschreven zijn. Dit betekent ook dat informatie over kwetsbaarheden *niet* eerder of met derden buiten de CVD-procedure gedeeld mag worden dan dat er formeel over de kwetsbaarheid wordt gecommuniceerd.

De maandelijkse rapportage van de CISO aan het DT bevat een overzicht van de incidenten van die periode.

Referentie		
BIO versie 2.0	beheersmaatregel	5.24, 8.08.06
ISO 27001:2023	beheersmaatregel	5.24, 8.8
BIO versie 1.04zv	beheersmaatregel	16.1.1, 16.1.2 en 16.1.3

14.3.3 Melden van informatiebeveiligingsgebeurtenissen

Iedereen die werkzaamheden verricht voor de gemeente en die gebruik maakt van de netwerken, systemen, applicaties en diensten van de gemeente dient waargenomen of vermeende zwakke plekken in de informatiebeveiliging te melden via de incidentenbeheerprocedure. Deze bepaling is ook opgenomen in de overeenkomsten voor tijdelijke inhuur, stages en/of detachering.

De gemeente publiceert een *Responsible Disclosure* procedure op de website en stelt een veilig en ook anoniem te gebruiken kanaal in voor het door derden indienen van geconstateerde kwetsbaarheden. De gemeente zorgt dat van alle webdiensten de *security.txt* melding goed staat ingesteld.

Referentie		
BIO versie 2.0	beheersmaatregel	5.24, 8.08.06
ISO 27001:2023	beheersmaatregel	5.24, 8.8
BIO versie 1.04zv	beheersmaatregel	16.1.2 en 16.1.3

14.3.4 Beoordeling van informatiebeveiligingsgebeurtenissen

Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld conform de ‘Classificatie Informatiebeveiligingsgebeurtenissen’. De classificatie bepaalt de vervolgstappen in de respons op het incident en of het IRT geformeerd moet worden.

Referentie		
BIO versie 2.0	beheersmaatregel	5.25.01
ISO 27001:2023	beheersmaatregel	5.25
BIO versie 1.04zv	beheersmaatregel	16.1.4, 16.1.4.1

14.3.5 Respons op informatiebeveiligingsincidenten

De juiste respons op informatiebeveiligingsincidenten hangt af van de context en de omvang en is daarom vaak maatwerk. Het classificatieschema en vooraf opgestelde handreikingen of scenario's zijn hierbij hulpmiddelen, maar gezond verstand en rust bewaren zijn het belangrijkste om een doelmatige en doeltreffende reactie op het incident te bewerkstelligen.

De incidentbeheerprocedure beschrijft tenminste de aanpak om de volgende doelstellingen te realiseren:

- Vereiste responstijden en hoe die te realiseren;
- Het incident zo snel mogelijk beperken en beheersen, zodat het gevolgen van het incident beperkt worden;
- Bewijsmateriaal verzamelen en veilig stellen;
- Responsactiviteiten uitvoeren, maar ook vastleggen voor latere analyse en evaluatie;
- Zonodig intern en/of extern escaleren;
- Informatie over het incident waar nodig delen, maar niet meer dan noodzakelijk (need-to-know);
- Het incident formeel afsluiten en registeren in het Incidentenregister.

Ter ondersteuning van de respons worden enkele handreikingen of scenario's uitgewerkt, waarbij onder andere wordt beschreven:

- 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 van toepassing is, dan is standaard de proceseigenaar verantwoordelijk voor de opvolging van het incident en de te nemen maatregelen.
- Dat de CISO en/of ISO bij ieder incident dient te worden geïnformeerd;
- Hoe bewijs zo snel mogelijk wordt verzameld en vastgelegd;
- 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 de acute fase van het incident afgerond is.
- 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 2.0	beheersmaatregel	5.26.01
ISO 27001:2023	beheersmaatregel	5.26
BIO versie 1.04zv	beheersmaatregel	16.1.5

14.3.6 Verzamelen van bewijsmateriaal

Er moet een procedure zijn voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen en voor analysedoeleinden kan worden gebruikt.

In geval van criminele activiteiten moeten altijd de IBD en het digitale forensisch team van de politie ingeschakeld worden voor het veilig stellen, overdragen en/of analyseren van bewijsmateriaal. In dit geval mag de gemeente dat niet zelf doen.

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

Referentie		
BIO versie 2.0	beheersmaatregel	5.28.01
ISO 27001:2023	beheersmaatregel	5.28
BIO versie 1.04zv	beheersmaatregel	16.1.7

14.3.7 Leren van informatiebeveiligingsincidenten

De gemeente moet 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:

- Hoe het bewijs dat verzameld was tijdens het incident geanalyseerd moet worden.
    - Hierbij moet duidelijk zijn hoe men kan komen tot bevindingen die:
        - De oorsprong van het incident tonen;
        - De gebruikte kwetsbaarheden inzichtelijk maken voor zowel processen, techniek als het menselijke aspect.
- Hoe bepaald moet worden hoe de waarschijnlijkheid of impact van toekomstige incidenten wordt verkleind;
- Hoe analyses van de beveiligingsincidenten worden gedeeld met relevante partners om herhaling en toekomstige incidenten te voorkomen;
- Dat de beoordeling van de informatiebeveiligingsincidenten dienen te worden gearchiveerd op een centrale locatie en moeten worden gebruikt om terugkerende incidenten te identificeren en adequaat aan te pakken.

Referentie		
BIO versie 2.0	beheersmaatregel	5.27
ISO 27001:2023	beheersmaatregel	5.27
BIO versie 1.04zv	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 vast te stellen, bijvoorbeeld voor langdurige uitval van diensten of middelen, een cyberaanval, een crisis of een ramp.

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 DT 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 2.0	beheersmaatregel	5.30
ISO 27001:2023	beheersmaatregel	5.30
BIO versie 1.04zv	beheersmaatregel	17.1.1 en 17.1.2

15.1.4 ICT-gereedheid voor bedrijfscontinuïteit

BIO 2 5.30

Referentie		
BIO versie 2.0	beheersmaatregel	5.30.01 en 5.30.02
ISO 27001:2023	beheersmaatregel	5.30
BIO versie 1.04zv	beheersmaatregel	-

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 2.0	beheersmaatregel	5.30
ISO 27001:2023	beheersmaatregel	5.30
BIO versie 1.04zv	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 2.0	beheersmaatregel	8.14.01
ISO 27001:2023	beheersmaatregel	8.14
BIO versie 1.04zv	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 2.0	beheersmaatregel	5.31
ISO 27001:2023	beheersmaatregel	5.31
BIO versie 1.04zv	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;
- beleid vaststellen voor het handhaven van de juiste licentievoorwaarden;
- beleid 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 2.0	beheersmaatregel	5.32.01
ISO 27001:2023	beheersmaatregel	5.32
BIO versie 1.04zv	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 de ze moeten worden bewaard, zijn vastgelegd;
- Er dient een inventarisoverzicht van bronnen van belangrijke informatie te worden bijgehouden.

Referentie		
BIO versie 2.0	beheersmaatregel	5.33.01
ISO 27001:2023	beheersmaatregel	5.33
BIO versie 1.04zv	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 2.0	beheersmaatregel	5.34.01
ISO 27001:2023	beheersmaatregel	5.34
BIO versie 1.04zv	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 2.0	beheersmaatregel	5.31.01
ISO 27001:2023	beheersmaatregel	5.31
BIO versie 1.04zv	beheersmaatregel	18.1.5

16.1.6 Naleving verplichtingen omtrent ENSIA, DigiD en Suwinet

16.1.6.1 *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.

16.1.6.2 *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 benoemt. Verder dient de gemeente in het bezit te zijn van een DigiD beleid.

16.1.6.3 *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 benoemt. 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 (zie paragraaf 2.5).

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 2.0	beheersmaatregel	5.35.01
ISO 27001:2023	beheersmaatregel	5.35
BIO versie 1.04zv	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 DT, 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 DT 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 de beoordeling een constateert dat eisen of elementen hiervan niet worden nageleefd dienen de volgende stappen doorlopen te worden:

- De oorzaken van de niet-naleving vaststellen;
- De noodzaak evalueren tot het treffen van maatregelen om naleving te bewerkstelligen;
- Een verbeterplan opstellen ongeacht de uitkomst van stap 2;
- Passende corrigerende maatregelen implementeren uit het verbeterplan;
- De getroffen corrigerende maatregelen beoordelen om de doeltreffendheid ervan te verifiëren en om gebreken of zwakke plekken te identificeren.
- 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 regulieren, 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 2.0	beheersmaatregel	5.36.01
ISO 27001:2023	beheersmaatregel	5.36
BIO versie 1.04zv	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 2.0	beheersmaatregel	8.08
ISO 27001:2023	beheersmaatregel	8.08
BIO versie 1.04zv	beheersmaatregel	18.2.3