

Informatiebeveiligingsbeleid

2020 - 2023

Gemeente Drimmelen



Vastgesteld op 19 november 2019
door het College van B&W

Voorwoord

Voor u ligt het strategische informatiebeveiligingsbeleid (IB-beleid) 2020-2023 van de gemeente Drimmelen, vast te stellen door College van burgemeester en wethouders. Dit vervangt het in 2016 vastgestelde 'Informatiebeveiligingsbeleid Gemeente Drimmelen 2016-2019'. De vertaling van dit strategische beleid naar tactisch beleid is uitgewerkt in het Informatiebeveiligingsplan gemeente Drimmelen (IB-plan) en valt onder de verantwoordelijkheid van het management team. Het IB-plan wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

Drimmelen stemt haar bedrijfsvoering inzake informatiebeveiliging af op de norm NEN-EN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (in het vervolg: BIO¹). De daaruit voortkomende aspecten zijn aantoonbaar gemaakt in de bedrijfsvoering van Drimmelen.

Het beleid houdt rekening met onder andere:

- De Internationale norm voor informatiebeveiliging (NEN-EN-ISO/IEC 27001:2017²).
- De Code voor Informatiebeveiliging (NEN-EN-ISO/IEC 27002:2017³).
- Baseline Informatiebeveiliging Overheid (BIO)⁴ aangevuld met 'eigen' regelgeving die door college of MT specifiek voor Drimmelen van toepassing is verklaard.
- Eisen gesteld door derden aan de dienst- en productlevering.
- Eisen voortkomende uit van toepassing zijnde wet- en regelgeving (zie bijlage 1), waaronder:
 - artikel 213a van de gemeentewet;
 - de RODIN-richtlijnen voor digitale archivering en volledige substitutie (Referentiekader Opbouw Digitaal Informatiebeheer).
 - de beveiligingseisen en -richtlijnen voor:
 - Algemene Verordening Gegevensbescherming (AVG)
 - Archiefwet
 - Basisadministratie Persoonsgegevens en Reisdocumenten (BPR)
 - Basisregistraties Adressen en Gebouwen (BAG)
 - Basisregistratie Grootchalige Topografie (BGT)
 - Basisregistratie Ondergrond (BRO)
 - Basisregistratie personen (BRP)
 - ICT-beveiligingsrichtlijnen voor webapplicaties (DigiD)
 - Paspoorten en Nederlandse Identiteitskaarten (PNIK)
 - Paspoort Uitvoeringsregeling Nederland (PUN)
 - Reglement rijbewijzen
 - Wet structuur uitvoeringsorganisatie werk en inkomen (Suwi)

¹ De baseline is een instrument waarmee gemeenten in staat zijn om te meten of de organisatie 'in control' is op het gebied van informatiebeveiliging.

² Opgesteld door Technische Subcommissie ISO/IEC/JTC 1/SC 27 "Information security" van de Internationale Organisatie voor Standaardisatie (ISO) en het International Elektrotechnische Comité (IEC) en is overgenomen als EN ISO/IEC 27001: 2017 (ISO 27001).

³ Informatietechnologie – Beveiligingstechnieken – Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging EN ISO/IEC 27001: 2017 (ISO 27002)

⁴ In de buitengewone algemene ledenvergadering hebben gemeenten ingestemd met het proces van standaardverklaring. Het College van Dienstverleningszaken (CvD), dat het VNG Bestuur adviseert over standaarden voor de gemeentelijke uitvoering, heeft positief advies afgegeven over standaardisering. Het bestuur heeft hier positief op gereageerd en de BIO daarmee verbindend verklaard voor gemeenten per 1 januari 2020. De BIO is interbestuurlijk bekrachtigd in het Overheidsbrede overleg Digitale Overheid (OBDO).

Alle opvolgende wetgeving en richtlijnen worden van toepassing op het moment dat zij ingaan.

Om de uitgangspunten op een efficiënte en effectieve wijze te beheren, zijn de bijbehorende normen, controls en maatregelen geregistreerd in een 'Informatiebeveiligingsmanagementsysteem' (ook wel ISMS⁵ genoemd). Het ISMS is een integraal kwaliteitssysteem voor informatiebeveiliging conform ISO 27001:2017 en is samen met het tactisch beleid vastgelegd in het IB-plan gemeente Drimmelen. Het IB-plan is, samen met de handboeken met operationele procedures, onderdeel van het managementsysteem van de gemeente Drimmelen. Schematisch weergegeven:

College	• Informatiebeveiligingsbeleid
Management	• Informatiebeveiligingsplan • Informatiebeveiligingsmanagementsysteem
Medewerkers	• Handboek met procedures en richtlijnen etc.

⁵ ISMS staat voor Information Security Management System

Inhoudsopgave

1. Inleiding	6
Leeswijzer	7
2. Doelstelling en uitgangspunten informatiebeveiliging.....	8
2.1. Het belang van informatieveiligheid.....	8
2.2. Visie.....	8
2.3. Doelstelling	9
2.4. Uitgangspunten	9
2.5. Risicobenadering.....	10
2.6. Doelgroepen	11
2.7. De reikwijdte.....	12
2.8. Werking.....	12
2.9. Samenhang	12
3. Informatiebeveiliging managen	13
3.1. Beheersen maatregelen.....	13
3.2. Inrichten organisatie.....	14
3.3. 10 principes voor informatiebeveiliging	15
3.4. Plaats van beleid in de organisatie	16
3.5. Beoordeling en corrigerende maatregelen	17
3.6. Bescherming van informatie, classificatie	18
4. Aanpak van informatiebeveiliging	20
4.1. Risicobeoordeling en risico-afweging	20
4.2. Organiseren van informatiebeveiliging	21
4.3. Veilig personeel	21
4.4. Beheer van bedrijfsmiddelen.....	21
4.5. Toegangsbeveiliging.....	22
4.6. Cryptografie	22
4.7. Fysieke beveiliging en beveiliging van de omgeving	23
4.8. Beveiliging bedrijfsvoering.....	23
4.9. Communicatiebeveiliging	23
4.10. Acquisitie, ontwikkeling en onderhoud van informatiesystemen	24
4.11. Leveranciersrelaties	24
4.12. Beheer van beveiligingsincidenten	24
4.13. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	25
4.14. Naleving	25
5. Kwaliteitsbewaking.....	27
5.1. Communicatie.....	27
5.2. Borging.....	27
5.3. Geldigheid en evaluatie	27
5.4. Naleving	28
6. Informatiebeveiligingsbeleid gemeente Drimmelen	29
6.1. Algemeen	29
6.2. IB-beleid gemeente Drimmelen 2020 – 2023.....	29
Bijlage 1: Wet- en regelgeving	31

1. Inleiding

Gemeente Drimmelen erkent dat informatiebeveiliging steeds belangrijker wordt binnen de bedrijfsvoering vanuit:

- Het coalitieprogramma.
- De door de burger gestelde eisen en het vertrouwen van de burger in de gemeente.
- De naleving en opvolging van wet- en regelgeving.
- Maatschappelijke verantwoording.
- Het dreigingsbeeld van de Informatiebeveiligingsdienst (IBD)
- De uitkomsten van Eenduidige Normatiek Single Information Audit (ENSIA)

Drimmelen is een veilige gemeente waarin inwoners, bedrijven en organisaties/verenigingen samen leven, werken en genieten. De dienstverlening en service zijn zeer belangrijk. De gemeente is open en benaderbaar. We communiceren met een tijdige, duidelijke boodschap en zijn zo transparant mogelijk. Het dorpsgericht werken is meer dan een subsidieregeling en dit succes zetten we voort met een nadruk op burger- en overheidsparticipatie en een gezamenlijke Toekomstvisie.

Figuur 1.1 Bron: coalitieakkoord 2018-2022

De gemeente Drimmelen wil in alle opzichten een betrouwbare partner zijn. Zorg en respect zijn belangrijke waarden in het doen en laten van de medewerkers van de gemeente. Een betrouwbare informatievoorziening waarbij de informatie van inwoners wordt beschermd en de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens is geborgd, is hier onlosmakelijk mee verbonden. Niet alleen kan inadequate beveiliging leiden tot beschadiging van het vertrouwen, maar ook kunnen (de privacy van) inwoners geschaad worden als bijvoorbeeld privéinformatie openbaar wordt of identiteitsgegevens worden misbruikt.

Gemeente Drimmelen onderkent in haar bedrijfsprocessen aspecten van informatiebeveiliging die bewaakt en gecontroleerd dienen te worden; om zo 'in control' te zijn en daarover op professionele wijze verantwoording af te leggen. Het management speelt een cruciale rol bij het uitvoeren van dit IB-beleid. Zo maakt het management een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente hebben, van de risico's die de gemeente hiermee loopt en van welke van deze risico's onacceptabel hoog zijn.

Dit document legt de basis voor informatiebeveiliging binnen de gemeente en is - zoals hiervoor reeds is aangegeven - afgeleid van de BIO. Het normenkader⁶ is vastgesteld als basis voor de gemeente en is tevens van toepassing op rijksdienst, provincies en waterschappen. Wel is er de mogelijkheid voor afweging door middel van het 'pas toe of leg uit' principe. Het IB-beleid is naast de BIO in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving, zoals de basisregistraties, Suwi, Paspoorten en ID-bewijzen, maar ook de archiefwet en de Algemene Verordening Gegevensbescherming.

Gemeente Drimmelen waarborgt dat het beleid evenals de bijbehorende documenten regelmatig worden herzien. Zodanig dat deze, indien nodig, worden aangepast op organisatorische veranderingen en technologische ontwikkelingen. Dit om inwoners, partners, bedrijven en de interne organisatie van dienst te zijn en daarbij de informatiebeveiligingsaspecten te continueren en waar mogelijk te verbeteren.

⁶ Het normenkader BIO betreft maatregelen voor algemene informatiebeveiliging, voor de informatiebeveiligingsfunctionaris, voor ICT, HRM en Facilitair.

Leeswijzer

In hoofdstuk 2 staan de doelstelling en de uitgangspunten van dit IB-beleid genoemd, wordt de risicobenadering toegelicht en zijn de taken en verantwoordelijkheden in de organisatie benoemd. Verder is in dit hoofdstuk de reikwijdte van het IB-beleid gekaderd en is de werking van oud- voor nieuw beleid geduid.

In hoofdstuk 3 wordt de management cyclus van informatiebeveiliging toegelicht, staat uitgelegd hoe de IB-organisatie is ingericht en wordt uitgelegd hoe IB-controles werken en welke systematiek voor classificatie van informatie wordt toegepast.

In hoofdstuk 4 wordt de aanpak van de veertien beveiligingsaspecten uit de BIO beschreven zoals die door gemeente Drimmelen wordt toegepast.

In hoofdstuk 5 wordt de bewaking van de kwaliteit van IB-beleid uitgelegd op het vlak van communiceren over IB-beleid, borgen van processen e.d., actueel houden van en het toezien op naleving van het IB-beleid.

In hoofdstuk 6 staan de feitelijke beleidsregels voor informatiebeveiliging, die de gemeente Drimmelen heeft vastgesteld.

2. Doelstelling en uitgangspunten informatiebeveiliging

In dit hoofdstuk staan het belang, de visie, de doelstelling en de uitgangspunten van dit IB-beleid genoemd, wordt de risicobenadering toegelicht en staan de verantwoordelijkheden van de betrokkenen benoemd. Verder is de reikwijdte van het IB-beleid gekaderd en is de vaststelling van oud- voor nieuw beleid geduid. Waarom uitgangspunten? Om de uitvoering van informatiebeveiliging en de te nemen maatregelen te kaderen zijn er duidelijke uitgangspunten vastgesteld.

2.1. Het belang van informatieveiligheid

Gegevens t.b.v. informatievoorziening zijn één van de voornaamste bedrijfsmiddelen van Drimmelen. Het verlies van gegevens, uitval van ICT en/of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering. Informatieveiligheid is alleen daarom al van groot belang. Ernstige incidenten hebben mogelijk negatieve gevolgen voor inwoners, ondernemers, partners en de eigen organisatie met mogelijk ook politieke consequenties. Het kan ook leiden tot imago schade. De overheid erkent dat beveiliging van de informatie volledige aandacht moet krijgen van zowel de politiek als de ambtelijke organisatie en dat de informatie blijvend adequaat moet worden geborgd.

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie. Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politieke bestuur, alle medewerkers, inwoners, gasten, bezoekers en externe relaties.

2.2. Visie

Visie informatieveiligheid gemeente Drimmelen:

Een betrouwbare en veilige informatievoorziening is noodzakelijk voor het goed functioneren van de gemeentelijke organisatie en de basis voor het beschermen van rechten van medewerkers, inwoners, gasten, bezoekers en externe relaties. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Het proces van informatiebeveiliging is primair gericht op bescherming van gemeentelijke informatie. De focus is gericht op informatie(uitwisseling) in alle verschijningsvormen, zoals elektronisch, op papier en mondeling. Het gaat niet alleen over bescherming van privacy, maar ook over bescherming van vitale maatschappelijke functies die worden ondersteund met informatie (denk aan verkeerssystemen, vervoerssystemen, bestuurbare rioolgemalen etc.). Het gaat ook niet alleen over ICT.

Verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid.

2.3. Doelstelling

Doelstelling informatieveiligheid gemeente Drimmelen:

Beheersing van informatiebeveiligingsaspecten wordt bereikt door een stelsel van organisatorische en technische maatregelen. Gemeente Drimmelen heeft als streven om al die maatregelen te treffen die noodzakelijk zijn en die binnen alle redelijkheid en billijkheid voor de gemeente in economische zin haalbaar zijn. Dit om de veiligheid van de informatie en het personeel te waarborgen, om aan de relevante wet- en regelgeving te voldoen, om de continuïteit van de bedrijfsvoering te waarborgen en om de reputatie als betrouwbare partner te beschermen.

Dit IB-beleid is het kader voor passende organisatorische, procedurele en technische maatregelen om gemeentelijke informatie te beschermen en te waarborgen. Gemeente Drimmelen geeft met dit beleid een duidelijke richting aan op het gebied van informatiebeveiliging en streeft de volgende doelen na om een adequaat niveau van beveiliging conform de BIO en alle relevante wet- en regelgeving te bereiken:

- het garanderen van correcte en veilige informatievoorzieningen;
- het beschermen van kritieke bedrijfsprocessen;
- het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers;
- het minimaliseren van risico's;
- het adequaat reageren op incidenten;
- het bereiken van informatiebeveiligingsbewustzijn bij medewerkers, management, college en alle andere bij de gemeentelijke organisatie betrokken medewerkers, zoals inhuurkrachten, stagiaires en dienstverleners;
- het inbedden van het component informatiebeveiliging in de werkzaamheden van alle organisatieonderdelen;
- het 'in control' zijn op alle informatiebeveiligingsmaatregelen die genomen zijn en die nog nodig zijn, verankerd in een PDCA-cyclus⁷ met aansluiting bij de Planning en Control (P&C) cyclus;
- het waarborgen van de naleving van dit beleid.

2.4. Uitgangspunten

De uitgangspunten van het IB-beleid zijn:

- ✓ Het informatiebeveiligingsbeleid van de gemeente Drimmelen is in lijn met het algemeen beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.
- ✓ Het beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verwerkingen).
- ✓ Het beleid is gebaseerd op de Code voor Informatiebeveiliging (NEN-ISO 27001 en 27002) en de Baseline Informatiebeveiliging Overheid.
- ✓ Het strategisch IB-beleid wordt vastgesteld door het College van burgemeester en wethouders. Het management herijkt periodiek het strategisch IB-beleid.
- ✓ Het tactisch IB-beleid (het IB-plan) wordt vastgesteld door het management. Het management herijkt minimaal jaarlijks het tactische beleid.
- ✓ Het management is verantwoordelijk voor het (laten) uitwerken en uitvoeren van specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.

⁷ Uitleg over PDCA-cyclus volgt in paragraaf 3.1

- ✓ Afdelingsmanagers dienen erop toe te zien dat de controle op het veilig verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- ✓ De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Afdelingsmanagers beoordelen door de CISO en procesverantwoordelijke uitgevoerde analyses en/of onderzoeken op basis van de BIO om risicoafwegingen te kunnen maken.
- ✓ De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie (concern control) de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert met kennisgeving aan de concern controller hierover aan het management.
- ✓ Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.

2.5. Risicobenadering

De aanpak van informatiebeveiliging in de gemeente Drimmelen is 'risicogericht'. Dat wil zeggen: beveiligingsmaatregelen worden getroffen op basis van een toets (GAP-analyse⁸) op de BIO⁹ controls en maatregelen. Indien een proces of informatiesysteem privacy of security gevoelig is, kan het zijn dat er aanvullende maatregelen nodig zijn. Daartoe inventariseert de procesverantwoordelijke¹⁰ de kwetsbaarheid van haar/zijn werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beschermingseisen van de informatie.

Het risico is de kans op beveiligingsincidenten en de impact daarvan op het werkproces en wordt bepaald door de procesverantwoordelijke:

Risico	=	kans	x	impact
---------------	----------	-------------	----------	---------------

De BIO heeft een werkwijze welke gericht is op risicomanagement. De afdelingsmanagers werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt in dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid (BIV). De BIV-classificatie wordt nader toegelicht in hoofdstuk 3.6. Aan de hand van deze classificatie wordt het basisbeveiligingsniveau (BBN) bepaald. Is het beveiligingsniveau hoog dan wordt geadviseerd een diepgaande risicoanalyse uit te voeren.

⁸ Het doel van de GAP-analyse is om te controleren of en in welke mate de maatregelen uit de BIO geïmplementeerd zijn bij de gemeente die het onderzoek uitvoert of laat uitvoeren. De GAP-analyse (opgesteld door de IBD) bevat alle maatregelen uit de BIO met daarbij controlevragen. De GAP-analyse is een methode om een vergelijking te maken tussen een bestaande of huidige situatie en de gewenste situatie, de maatregelen uit de baseline.

⁹ De BIO kent een normenkader waarmee gemeenten in staat zijn om te meten of de organisatie 'in control' is op het gebied van informatiebeveiliging. De GAP-analyse is het instrument waarmee dit wordt gedaan.

¹⁰ Elk proces moet bestuurd en beheerd worden. Elk proces kent een eindverantwoordelijke. In het IB-plan wordt dit verder uitgewerkt.

2.6. Doelgroepen

Het gemeentelijk IB-beleid is bedoeld voor alle medewerkers van de gemeente Drimmelen, ongeacht aanstellingsvorm. Daarnaast zijn binnen en buiten de gemeentelijke organisatie specifieke IB-taakgerichte groepen en/of functionarissen.

Doelgroep	Relevantie / verantwoordelijkheid voor IB-beleid
Gemeenteraad	Controlerende taak t.a.v. informatieveiligheid
College van B&W	Bestuurlijke Integrale verantwoordelijkheid
Portefeuillehouder informatiebeveiliging	Bestuurlijk verantwoordelijk voor informatieveiligheid
Management	Organisatorische Integrale verantwoordelijkheid
Afdelingsmanagers	Sturing op informatieveiligheid en controle op naleving
Procesverantwoordelijke	Verantwoordelijk voor procesanalyse, classificeren van informatie en implementeren van maatregelen
Medewerkers	Gedrag en naleving
Gegevenseigenaren/ bronhouders (BRP, BAG, BGT, BRO etc)	Classificatie: bepalen beschermingseisen van informatie
Beleidsmakers	Planvorming binnen IB-kaders
Chief Information Security Officer (CISO), tevens Privacy Officer	Ontwikkelen van een visie en beleid op informatiebeveiliging, uitwerking daarvan in informatiebeveiligingsplan (tactisch) en handboeken (operationeel). Dagelijkse coördinatie van IB zaken. Deze functies zijn bij gemeente Drimmelen ondergebracht bij de Beleidsmedewerker informatiebeveiliging, privacy en interne controle
Functionaris Gegevensbescherming (FG)	Toezicht houden op toepassing en naleving van de Algemene Verordening Gegevensbescherming (AVG)
Personeelszaken	Arbeidsvoorwaardelijke zaken
Facilitaire zaken	Fysieke toegangsbeveiliging
ICT-diensten	Technische beveiliging
Auditors	Onafhankelijke toetsing
Informatiebeveiligingsdienst (IBD)	De IBD (onderdeel van VNG) ondersteunt gemeenten op het gebied van informatiebeveiliging en is het schakelpunt met het Nationaal Cyber Security Centrum (NCSC)
Leveranciers en ketenpartners	Alle leveranciers en ketenpartners waarmee gemeentelijke gegevens worden uitgewisseld, worden beheerd etc. ¹¹
Autoriteit Persoonsgegevens (AP)	Onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt.

¹¹ De veiligheid van gemeentelijke gegevens wordt geborgd door een met de leverancier af te sluiten verwerkingsovereenkomst, volgens het model van de IBD.

2.7. De reikwijdte

De reikwijdte van dit strategisch IB-beleid is dat:

- ✓ Dit beleid van toepassing is op alle gemeentelijke processen, op onderliggende informatiesystemen, op informatie en gegevens van de gemeente en op externe partijen; het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur;
- ✓ Dit beleid een overkoepelende organisatie brede werking heeft met als basis de BIO en waarvoor bepaalde kerntaken op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen gelden;
- ✓ Dit beleid in lijn is met het algemeen beleid van de gemeente en met de relevante landelijke en Europese wet- en regelgeving, zoals basisregistraties als BRP, BAG en BGT, maar ook Suwinet, Paspoorten en ID-bewijzen PNIK, DigiD, de archiefwet en de AVG.

2.8. Werking

Dit IB-beleid treedt na vaststelling door het college van B&W op 1 januari 2020 in werking. Hiermee komt het oude Informatie beveiligingsbeleid van de gemeente Drimmelen te vervallen met uitzondering van de bestaande gemeentelijke procedures.

Het beleidsdeel uit het beveiligingsplan van de BRP en Suwinet is opgenomen in dit overkoepelend IB-beleid. De betreffende beveiligingsplannen staan echter op zichzelf en dat blijft zo omdat daarin de specifieke maatregelen, procedures, regelingen en bijlagen zijn opgenomen. Dit beleid vormt de kapstok voor aanvullend beleid, procedures en standaarden binnen de gemeente.

2.9. Samenhang

Aan het IB-beleid van de gemeente Drimmelen wordt nadere invulling gegeven door het management op basis van het 'pas toe of leg uit principe'. In het IB-plan worden hiervoor beleidsregels opgenomen op alle aspecten van informatiebeveiliging uit de BIO. Het gaat hier om de volgende beveiligingsaspecten:

- Organiseren van informatiebeveiliging
- Veilig personeel
- Beheer van bedrijfsmiddelen
- Toegangsbeveiliging
- Cryptografie
- Fysieke beveiliging en beveiliging van de omgeving
- Beveiliging bedrijfsvoering
- Communicatiebeveiliging
- Acquisitie, ontwikkeling en onderhoud van informatiesystemen
- Leveranciersrelaties
- Beheer van beveiligingsincidenten
- Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
- Naleving

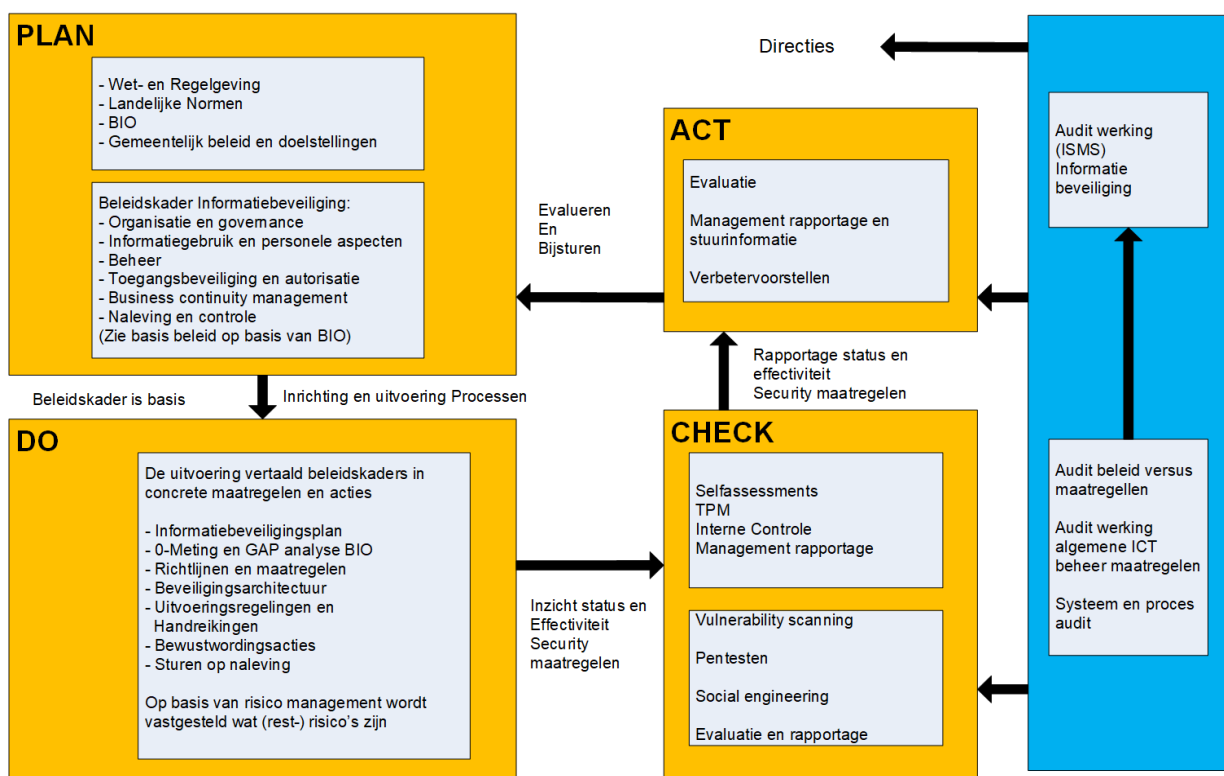
In hoofdstuk 4 'Aanpak van informatiebeveiliging' van dit beleidsdocument wordt de aanpak van bovenstaande beveiligingsaspecten beschreven zoals die door gemeente Drimmelen wordt gehanteerd.

3. Informatiebeveiliging managen

In dit hoofdstuk wordt de managementcyclus van informatiebeveiliging toegelicht; staat uitgelegd hoe de IB-organisatie is ingericht en wordt uitgelegd hoe IB-controles werken en welke systematiek voor classificatie van informatie wordt toegepast.

3.1. Beheersen maatregelen

Voor de beheersing van informatiebeveiligingsaspecten hanteert gemeente Drimmelen een Information Security Management System (ISMS). Het ISMS is gebaseerd op de internationale standaarden voor informatiebeveiligingsmanagementsystemen zoals opgesteld in de ISO 27001 door de International Standards Organization (ISO) die de basis vormt voor de BIO. Het ISMS bevat een informatiebeveiligingsmanagementproces dat is ingericht op basis van de PDCA-cyclus van Deming (Plan - Do - Check - Act). Door middel van het doorlopen van PDCA-cyclus wordt gemonitord of de genomen beheersmaatregelen nog effectief zijn en zich nieuwe of andere risico's voordoen die nog niet beheerst worden. Het zorgt er dus voor dat een passend beveiligingsniveau wordt gehandhaafd en het waarborgt een lerende gemeente.



Information Security Management System

Figuur 2.1: ISMS informatiebeveiliging (bron: InformatieBeveiligingsDienst gemeenten). Voor begrippen zie voetnoot.¹²

¹² TPM: Third Party Mededelingen is een rapportage van een onafhankelijke auditor bij een serviceorganisatie waar de gemeente diensten afneemt.

Een vulnerability scan controleert de website op malware, kwetsbaarheden en beveiligingslekken.

Een penetratietest of pentest (binnendringingstest) is een toets van een of meer computersystemen op kwetsbaarheden.

Self assessment is een zelfonderzoek naar het voldoen aan de gestelde eisen.

Concreet betekent bovenstaande dat in Drimmelen:

- ✓ Het management jaarlijks een plan laat opstellen voor het verbeteren van de informatiebeveiliging. Dit plan wordt vastgelegd in het IB-plan;
- ✓ Het management maatregelen treft om de beveiligingsrisico's te verminderen en om compliant te zijn aan wet- regelgeving, landelijke normen en de Baseline Informatiebeveiliging Overheid (BIO);
- ✓ De CISO jaarlijks vaststelt welke (rest-)risico's er zijn door middel van een risicoanalyse;
- ✓ Het management periodiek zelfonderzoeken en interne/externe audits laat uitvoeren voor de BRP, PNIK, BAG, BGT en BRO en Suwi en andere toekomstige wettelijke normenkaders;
- ✓ Het management jaarlijks het IB-beleid en het IB-plan evalueert en een verbeterplan naar aanleiding van interne/externe audits laat opstellen.

3.2. Inrichten organisatie

Door het inrichten van een informatiebeveiligingsorganisatie zorgt de gemeente Drimmelen voor passende aandacht en sturing. Het College is bestuurlijk integraal eindverantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeente. Het management is organisatorisch integraal eindverantwoordelijk voor de beveiliging van informatie en voor de werking van het ISMS en zal via delegatie naar medewerkers de taken en verantwoordelijkheden beleggen voor de implementatie en beheer van maatregelen die voortkomen uit dit beleid.

Specifieke rollen hierbij:

- ✓ De raad stelt de kaders voor het IB-beleid. Bepaalt het voor de gemeente toepasselijke niveau van basisbeveiliging ingevolge de BIO. Controleert de naleving daarvan op grond van de verantwoording door het college over dit onderwerp in bestuursrapportages en jaarstukken.
- ✓ Het college is verantwoordelijk voor het IB-beleid. Ze zullen volgens de 10 principes (zie 3.3) voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie;
- ✓ Portefeuillehouder bedrijfsvoering en dienstverlening: vanuit het College is de wethouder het aanspreekpunt. De portefeuillehouder wordt gevraagd en ongevraagd geïnformeerd over informatiebeveiliging;
- ✓ De afdelingsmanagers dragen het informatiebeveiligingsbeleid uit en zijn verantwoordelijk voor de informatiebeveiliging voor de eigen processen, data, applicaties, systemen en de daarbij behorende middelen. De afdelingsmanagers hebben een signaleringsfunctie voor dreigingen en incidenten, indien deze niet in eerste instantie zijn voorgelegd aan de CISO.
- ✓ De Chief Information Officer (CIO). Dit is de verantwoordelijke voor de informatievoorziening en is een rol op strategisch niveau binnen de gemeentelijke organisatie;
- ✓ de Chief Information Security Officer (CISO). De organisatie van informatiebeveiliging wordt namens het management aangestuurd door de CISO. De CISO ondersteunt, adviseert, coördineert en bewaakt. Tactische/operationele taken zullen gedelegeerd worden naar de security officers en/of verantwoordelijken binnen de afdelingen en processen;
- ✓ De ENSIA-coördinator legt verantwoording af over informatiebeveiliging volgens de ENSIA-systematiek¹³;
- ✓ Functionaris Gegevensbescherming (FG). Dit is de interne toezichthouder op de toepassing en naleving van de AVG;
- ✓ De Privacy Officer (PO). Deze rol is gericht op de uitvoering en de naleving van de privacy wetgeving en wordt gecombineerd met de rol van CISO. De PO adviseert over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.

¹³ Horizontale en verticale verantwoording

3.3. 10 principes voor informatiebeveiliging

De 10 principes¹⁴ voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:

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

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuursstafel.

Het toewijzen van overige rollen, taken en bevoegdheden is een managementverantwoordelijkheid en wordt verder uitgewerkt in het IB-plan.

Het management is verantwoordelijk voor kaderstelling en sturing. Het management stuurt op concern risico's, controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden en evalueert periodiek beleidskaders en stelt ze waar nodig bij.

De afdelingsmanagers binnen de gemeente zijn verantwoordelijk voor de integrale beveiliging van hun eigen organisatieonderdelen. Iedere afdelingsmanager:

- ✓ stelt op basis van een expliciete risicoafweging betrouwbaarheidseisen voor zijn of haar eigen informatiesystemen vast (classificatie);
- ✓ is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- ✓ stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- ✓ neemt kennis van de rapportages over naleving van wet- en regelgeving en algemeen beleid van de gemeente in de managementrapportages.

Alle medewerkers van gemeente Drimmelen hebben de verantwoording tot naleving van dit beleid en opvolging van de maatregelen die voortvloeien uit dit beleid. Identificatie van incidenten of het niet voldoen aan het gestelde in dit beleid dient gemeld te worden aan de CISO.

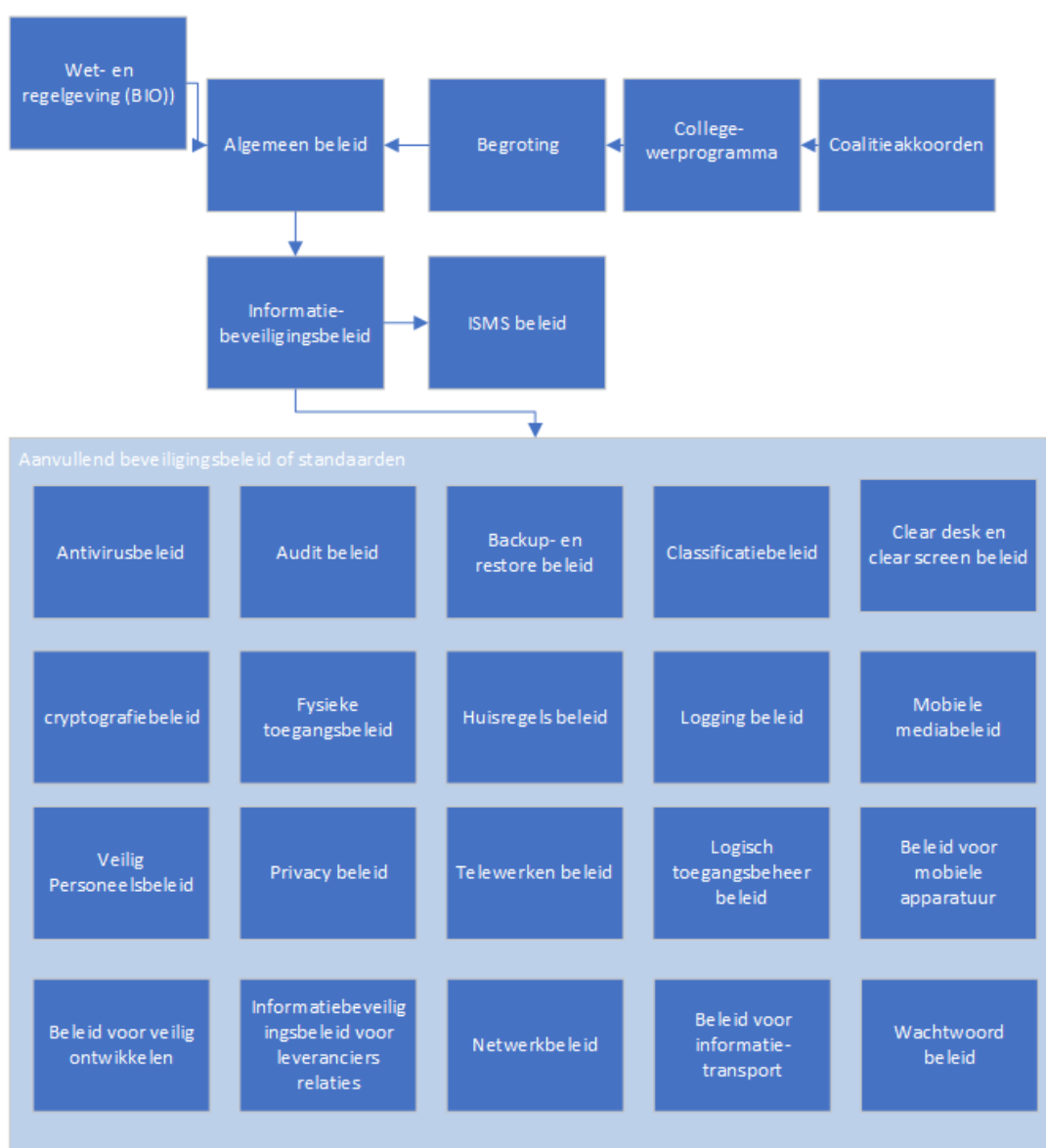
¹⁴ Deze principes zijn gelijk met de BIO van kracht

Informatiebeveiliging is opgenomen in de organisatieverordening en als competentie in fuwa-systeem. Op die manier wordt informatiebeveiliging en de eisen die hieraan worden gesteld richting medewerkers juridisch in één keer afgedicht. Alle medewerkers worden door het management actief geïnformeerd over dit informatiebeleid en worden verwacht kennis te nemen van de inhoud van dit informatiebeleid.

✓ Dit beleid maakt integraal deel uit van de arbeidsvoorwaarden van Gemeente Drimmelen.

3.4. Plaats van beleid in de organisatie

De BIO met verschillende beveiligingsdoelstellingen en beveiligingsonderwerpen in aanvullende beleidstukken ziet er grafisch als onderstaande figuur uit.



Figuur 3.1: structuur van beveiligingsbeleid

Aanvullend gemeentelijk beveiligingsbeleid, -plannen en -procedures mogen worden vastgesteld door een lager niveau in de organisatie, bijvoorbeeld het management.

Systeem-, proces- of afdelingsbeveiligingsbeleid

Het kan voorkomen dat het organisatiebrede beveiligingsbeleid en organisatiebrede aanvullende beveiligingsbeleid geen recht doen aan specifieke beveiligingseisen uit wetgeving, of die van een bedrijfskolom, proces of informatiesysteem. Dan is daar apart beveiligingsbeleid voor, omdat de beveiligingseisen zo (systeem) specifiek zijn dat dit noodzakelijk is. De verantwoordelijkheid voor dit specifieke beleid per bedrijfskolom, proces of informatiesysteem ligt dan bij de betreffende manager.

Gemeenten hebben te maken met aanvullende specifieke wetgeving waarvan onderdelen bij ENSIA worden uitgevraagd voor de jaarlijkse verticale verantwoording. Het gaat hierbij om wetgeving voor de basisregistraties, Suwi en DigiD.

Beveiligingsbeleid voor samenwerkingsverbanden en gemeenschappelijke regelingen

Gemeenten maken gebruik van gemeenschappelijke regelingen (GR) om gezamenlijk met andere gemeenten of partijen bepaalde taken en/of processen bij een derde partij te beleggen. In veel gevallen blijft de gemeente verantwoordelijk voor de beveiligingseisen en privacy afspraken. Dat betekent dat het IB-beleid ook van toepassing wordt verklaard op samenwerkingsverbanden en GR. Soms voeren meerdere taken uit en dan kunnen er ook per taak/proces andere beveiligingseisen zijn en dus ook andere beleidsdocumenten.

3.5. Beoordeling en corrigerende maatregelen

Gemeente Drimmelen controleert periodiek de maatregelen die voortkomen uit dit beleid door controles vanuit ENSIA en interne assessments en externe audits ten aanzien van (kosten)effectiviteit en informatieveiligheid.

Jaarlijks beoordeelt het management het informatiebeveiligingsmanagementproces op basis van verzamelde gegevens en informatie. Input voor deze beoordeling is o.a.:

- Registratie van incidenten en beveiligingsissues die niet worden nageleefd.
- Registratie van controles en interne en externe audits.
- Leveranciersbeoordelingen.
- Risicoanalyse¹⁵ output.
- Medewerkerscompetenties.
- Bewustwordingssessies en -trainingen.
- Wet- & regelgeving.

Op basis van de beoordelingen worden waar mogelijk corrigerende en/of preventieve maatregelen doorgevoerd. Maatregelen worden geselecteerd met het doel dat de kans op herhaling geminimaliseerd wordt. Of waardoor de doeltreffendheid van het informatiebeveiligingsmanagementsysteem wordt verbeterd en het geleverde product of dienst beter aansluit op de eisen van de burger, bedrijven en partners.

¹⁵ Een risicoanalyse bestaat uit/omvat: 1. Risicogebied vaststellen (context) door het vaststellen van kritieke processen en bedrijfsmiddelen. 2. Risico assessment en evaluatie door middel van een business impact analyse en dreigingsanalyse. Deze analyse wordt momenteel nog jaarlijks opgesteld/geactualiseerd vanuit het beveiligingsplan BRP en Waardedocumenten. Met de invoering van de BIO wordt deze analyse verbreed naar de organisatie en vanuit het informatiebeveiligingsbeleid opgesteld door de CISO.

Onderstaande bronnen kunnen invloed hebben op het wijzigen van het IB-beleid:

- Wetgeving
- Gemeentelijk beleid
- Resultaten van een Baselinetoets gevolgd door een risicoanalyse
- Resultaten risicoanalyse
- Input van de IBD
- Uitkomsten van Audits
- Opgetreden incidenten
- Uitvoerbaarheid van beveiligingsprocessen

3.6. Bescherming van informatie, classificatie

Het beschermingsniveau van informatie wordt uitgedrukt in classificatieniveaus voor beschikbaarheid, integriteit en vertrouwelijkheid van informatie:

* **Beschikbaarheid:** hoeveel en wanneer data toegankelijk is en gebruikt kan worden. De onderscheiden niveaus zijn: niet nodig; noodzakelijk; belangrijk en essentieel.

* **Integriteit:** het in overeenstemming zijn van informatie met de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen (juistheid, volledigheid en tijdigheid). De onderscheiden niveaus zijn: niet zeker; beschermd; hoog en absoluut.

* **Vertrouwelijkheid:** de bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie voor een gedefinieerde groep van gerechtigden. De onderscheiden niveaus zijn: openbaar; bedrijfsvertrouwelijk, vertrouwelijk en geheim.

Niveau	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Geen	Niet nodig gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn (bv: ondersteunende tools als routeplanner)	Niet zeker informatie mag worden veranderd (bv: templates en sjablonen)	Openbaar informatie mag door iedereen worden ingezien (bv: algemene informatie op de externe website van de gemeente)
Laag	Belangrijk informatie mag incidenteel niet beschikbaar zijn (bv: administratieve gegevens)	Beschermd het bedrijfsproces staat enkele (integriteits-) fouten toe (bv: rapportages)	Bedrijfsvertrouwelijk informatie is toegankelijk voor alle medewerkers van de organisatie (bv: informatie op het intranet)
Midden	Noodzakelijk informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk (bv: primaire proces informatie)	Hoog het bedrijfsproces staat zeer weinig fouten toe (bv: bedrijfsvoeringinformatie en primaire procesinformatie zoals vergunningen)	Vertrouwelijk informatie is alleen toegankelijk voor een beperkte groep gebruikers (bv: persoonsgegevens, financiële gegevens)
Hoog	Essentieel informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten (bv: basisregistraties)	Absoluut het bedrijfsproces staat geen fouten toe (bv: gemeentelijke informatie op de website)	Geheim informatie is alleen toegankelijk voor direct geadresseerde(n) (bv: zorggegevens en strafrechtelijke informatie)

Tabel 3.1: Classificatie van informatie

Hoe geven we concreet uitvoering aan het toekennen van classificatieniveaus?

Het toekennen van classificatieniveaus aan data en/of informatiesystemen is van groot belang, omdat daarmee het (vereiste) beschermingsniveau kenbaar gemaakt wordt. Aan de hand hiervan kan worden bepaald welke beveiligingseisen gelden en welke maatregelen moeten worden genomen. Dit is bijvoorbeeld relevant voor beheerders die lang niet altijd bekend zijn met de inhoud en dus de waarde van data, maar wel worden geacht adequate beschermingsmaatregelen te treffen. De volgende factoren oefenen invloed uit op de adequate beveiligingsmaatregelen: beleidsuitgangspunten, architectuurprincipes, beveiligingseisen (en hoe deze te interpreteren).

Classificatieniveaus zijn afgeleid van de waarde van data en het belang van het bedrijfsproces waarin deze data een rol spelen. Stel daarom vast wat het belang is van de bedrijfsvoeringsprocessen voor de organisatie en hoe deze processen worden ondersteund door de ICT voorzieningen. Er zijn drie beschermingsniveaus van laag naar hoog. Daarnaast is er nog een niveau 'geen'. Dit niveau geeft aan dat er geen beschermingseisen worden gesteld, bijvoorbeeld omdat informatie openbaar is.

Classificatie vindt plaats door de kritieke processen van de gemeentelijke organisatie te inventariseren aan de hand van: verstoring of uitval van het proces, systeem, eigenaar, gegevens, hardware. Hierbij wordt een link gelegd met de toegepaste informatiemiddelen en informatiesystemen per proces.

4. Aanpak van informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen.

Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek¹⁶ in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. De inhoud en structuur van dit beleid zijn afgestemd op die van de ISO en de BIO. Ook het Informatiebeveiligingsplan en het ISMS zullen deze structuur volgen.

Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. Dit informatiebeveiligingsbeleid beschrijft op strategisch niveau de informatiebeveiliging. Het zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt en geconcretiseerd in het jaarlijks 'Gemeentelijk Informatiebeveiligingsplan' (vastgesteld door het managementteam). Dit wordt gedaan op basis van input van de afdelingsmanagers, de FG, de CISO, het dreigingsbeeld van de IBD en de uitkomsten van ENSIA. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist.

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. Dit strategisch gemeentelijke Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de BRP, PUN en Suwi. Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld Suwi en gemeentelijke basisregistraties). Deze worden in aanvullende documenten geformuleerd. Bewust wordt in het strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

In dit hoofdstuk is de aanpak beschreven van de veertien beveiligingsaspecten uit de BIO zoals die door gemeente Drimmelen worden gebruikt. Daarnaast worden deze beveiligingsaspecten gedetailleerd uitgewerkt in aanvullende beleidsstukken.

4.1. Risicobeoordeling en risico-afweging

Risicobewustzijn van alle medewerkers van gemeente Drimmelen is de sleutel tot een effectieve informatiebeveiliging. Risicobewustzijn wordt volledig ondersteund door het management en zal gestimuleerd worden door middel van bewustwordingssessies en publicaties via onder meer het intranet. Het risicobewustzijn wordt ook ondersteund door het opstellen en naleven van gedragscodes en gebruikersovereenkomsten en zal aandacht krijgen in functiebeschrijvingen en arbeidscontracten of op de algemene inkoopvoorwaarden gebaseerde overeenkomsten met derden.

Via de baselinetoets en risicoanalyse conform de opzet van de IBD, worden mogelijke dreigingen en informatiebeveiligingsrisico's geïdentificeerd en geïndexeerd. Het management zal de resultaten die hier

¹⁶ De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.

uit voortkomen beoordelen en voor 'rendabele' maatregelen bijdragen leveren aan het implementatieplan ter vermindering van het risico tot een acceptabel niveau.

4.2. Organiseren van informatiebeveiliging

Het organiseren van de informatiebeveiliging is beschreven in paragraaf 3.2 van dit beleidsdocument. Het toewijzen van rollen en verantwoordelijkheden is een managementverantwoordelijkheid en wordt verder uitgewerkt in het IB-plan.

Organisatorisch is het zo geregeld dat er een scheiding is van beheertaken en overige gebruikerstaken.

- ✓ In beginsel mag niemand autorisaties hebben om een gehele cyclus van handelingen in een informatiesysteem te beheersen, zodanig dat beschikbaarheid, integriteit of vertrouwelijkheid kan worden gecompromitteerd.
- ✓ In beginsel is er een scheiding tussen beheertaken en overige gebruikstaken. Hierbij worden beheerwerkzaamheden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.

Mobiele apparatuur en telewerken

Beveiligingsmaatregelen die worden getroffen, hebben betrekking op zowel door de gemeente verstrekte middelen als privé-apparatuur die voor zakelijk gebruik worden ingezet ('bring your own device' (BYOD)). Mobiele apparatuur wordt waar mogelijk beheerd en beveiligd via een Mobile Device Management (MDM) oplossing. Op privé-apparatuur waarmee verbinding wordt gemaakt met het gemeentelijke netwerk is de gemeente bevoegd om beveiligingsinstellingen af te dwingen, als de situatie hierom vraagt. Richtlijn is dat privé-apparatuur alleen verbonden mag worden met het gemeentenetwerk via de telewerkvoorzieningen met een twee factor authenticatie op het publieke netwerk.

4.3. Veilig personeel

Bij het aannemen of inhuren van nieuw personeel en het laten verrichten van werkzaamheden door externe medewerkers wordt bewerkstelligd dat zij hun verantwoordelijkheden begrijpen ten aanzien van informatieveiligheid. Deze verantwoordelijkheden zijn vóór het dienstverband vastgelegd in een passende functiebeschrijving/opdracht en in de arbeidsvoorwaarden/inhuurovereenkomst. Alle medewerkers behoren een passende bewustzijnsopleiding en -training ten aanzien van informatiebeveiliging te krijgen. Bij indiensttreding overleggen alle medewerkers (intern en extern) een specifiek voor de functie verstrekte Verklaring Omtrent het Gedrag (VOG). Voor het gebruik van gemeentelijke informatie gelden de rechten en plichten zoals vastgelegd in de diverse documenten, zoals het CAR-UWO, huisregels, integriteits- en geheimhoudingsverklaring. Het plegen van inbreuk op de informatiebeveiliging kan disciplinaire maatregelen tot gevolg hebben.

4.4. Beheer van bedrijfsmiddelen

Bedrijfsmiddelen die aan medewerkers van gemeente Drimmelen beschikbaar worden gesteld, dienen voor zakelijke doeleinden toegepast te worden en conform de beveiligings- en gedragsregels te worden gebruikt. Opgeslagen en verwerkte informatie van of voor gemeente Drimmelen op systemen van de gemeente blijft te allen tijde eigendom van gemeente Drimmelen. De internationale en lokale privacywetgeving zal gehandhaafd worden wanneer een beroep wordt gedaan op eigendomsrechten. Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging. In hoofdstuk 3.4 wordt de classificatie van informatie beschreven. De bedrijfsmiddelen worden beheert in overeenstemming met het

classificatieschema. De wijze waarop vertrouwelijk of hoger geclassificeerde informatie is opgeslagen, voldoet aan de eisen van het Nationaal Bureau voor Verbindingsbeveiliging (NBV). Informatie op bedrijfsmiddelen wordt op een veilige manier verwijderd.

De bedrijfsmiddelen van gemeente Drimmelen zijn geïnventariseerd en blijven eigendom van de gemeente Drimmelen. De verantwoordelijkheid voor de levenscyclus van een bedrijfsmiddel wordt door een goedkeurende directie aan een medewerker overgedragen.

4.5. Toegangsbeveiliging

Toegang tot informatie en IT-faciliteiten zal op basis van 'need to know' worden beperkt zodat gebruikers toegang krijgen tot datgene wat noodzakelijk is voor het uitvoeren van de functie. De toegang wordt verstrekt aan de hand van het mandaat register. Toegang tot informatiesystemen wordt geïnitieerd door de afdelingsmanager van de medewerker op basis van het toekennen van een autorisatieprofiel die hoort bij de medewerkersrol. Na het accorderen door de informatie- of informatiesysteemeigenaar zullen de autorisaties worden toegekend en geregistreerd. Het ontzeggen van toegang tot informatiesystemen wordt eveneens geïnitieerd door de afdelingsmanager.

Na het afmelden van medewerkers, stagiaires of inhuurkrachten die uit dienst zijn of waarvan de opdracht is gestopt, worden door de informatie- of informatiesysteemeigenaar (functioneel beheerder) de autorisaties ingetrokken.

De functioneel beheerder van informatiesystemen zoals het Document Management-, Financieel- en HRM-systeem krijgen via het wijzigingssysteem een toekenning op een verzoek tot toegang tot een autorisatieprofiel door. Op basis van deze toekenning (goedgekeurd door het betreffende afdelingsmanager) verwerkt elke functioneel beheerder de autorisatie in zijn/haar systeem. Sommige informatiesystemen werken op basis van singel-sign-on¹⁷ via dezelfde gebruikersnaam en wachtwoord om op het netwerk in te loggen. Andere informatiesystemen maken gebruik van tweefactor authenticatie.¹⁸ De wachtwoorden moeten voldoen aan bepaalde vereisten.

4.6. Cryptografie

Gemeente Drimmelen zorgt voor het correct en doeltreffend gebruik van cryptografie¹⁹ om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

Digitale documenten van de gemeente waar burgers en bedrijven rechten aan kunnen ontleen, maken gebruik van Public Key Infrastructure (PKI) Overheid certificaten voor tekenen en/of encryptie. Hiervoor wordt een richtlijn PKI en certificaten opgesteld. De gemeente kent diverse PKI's. Voorbeeld: om veilig de digitale formulieren van de Inspectie SZW te kunnen gebruiken, is er op de achtergrond een certificaat geplaatst dat er voor zorgt dat de gegevens die daar worden ingevuld, beveiligd worden verzonden aan de Inspectie SZW. Om die veiligheid optimaal te garanderen is, conform de voorschriften van de overheid, het nieuwste type certificaat geïnstalleerd.

¹⁷ Single-sign-on-software (afgekort SSO) stelt eindgebruikers in staat om eenmalig in te loggen waarna automatisch toegang wordt verschaft tot meerdere applicaties en resources in het netwerk.

¹⁸ Iets dat hij is (een biometrisch gegeven/gebruikersnaam), iets dat hij weet (een wachtwoord of een pincode) en iets dat hij heeft (een telefoon of een zogenaamde token)

¹⁹ Versleutelen van informatie

Het gebruik van informatiesystemen, alsmede uitzonderingen en informatiebeveiligingsincidenten, worden vastgelegd in logbestanden op een manier die in overeenstemming is met het risico, en zodanig dat tenminste wordt voldaan aan alle relevante wettelijke eisen.

4.7. Fysieke beveiliging en beveiliging van de omgeving

Gemeente Drimmelen heeft ICT-voorzieningen geïmplementeerd voor de eigen bedrijfsprocessen en voor locaties die onderlinge interne communicatie en samenwerking met partners, inwoners van de gemeente Drimmelen en medewerkers op afstand mogelijk maakt. Deze ICT-voorzieningen zijn deels in beheer en eigendom van gemeente Drimmelen en deels uitbesteed.

ICT-voorzieningen, die kritieke of gevoelige bedrijfsactiviteiten ondersteunen, dienen fysiek te worden ondergebracht in beveiligde ruimten, beschermd door afgegrensde beveiligde gebieden, in een gecontroleerde omgeving, beveiligd met geschikte beveiligingsbarrières en toegangsbeveiliging. Ze zijn fysiek beschermd tegen toegang door onbevoegden, schade en storingen. Onbeheerde apparatuur wordt beveiligd achter gelaten. Voor de werkplek geldt clear screen en clear desk²⁰.

Voor bepaalde diensten wordt gebruik gemaakt van externe publieke netwerken zoals het internet. Hiervoor zijn diverse beveiligingsmaatregelen en beheersmaatregelen geïmplementeerd om de beschikbaarheid, integriteit en vertrouwelijkheid te waarborgen.

4.8. Beveiliging bedrijfsvoering

Bedieningsprocedures worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben. Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst in de vorm van wijzigingsbeheer. Informatie en informatieverwerkende faciliteiten moeten worden beschermd tegen malware²¹ en technische kwetsbaarheden moeten worden beheerd. Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest om geen gegevens te verliezen. Op deze manier kan de continuïteit van de gegevensverwerkingen worden gegarandeerd. Gebeurtenissen worden d.m.v. logbestanden vastgelegd, bewijs verzameld en beoordeeld.

4.9. Communicatiebeveiliging

Om informatie te beschermen behoren netwerken te worden beheerd en beheerst. Netwerken dienen te worden gescheiden (groepen van informatiediensten, -gebruikers en -systemen). Het transporteren van informatie naar een externe partij moet beveiligd plaatsvinden. Berichten worden beschermd tegen onbevoegde toegang, wijziging of weigering van dienstverlening in overeenstemming met het classificatieschema. Er moet toestemming worden verkregen voorafgaand aan het gebruiken van externe openbare diensten zoals instant messaging, sociale netwerken of delen van bestanden.

Voor het gebruik van gemeentelijke informatie gelden de rechten en plichten zoals vastgelegd in de diverse documenten, zoals het CAR-UWO, huisregels, integriteits- en geheimhoudingsverklaring. De gemeente Drimmelen onderschrijft daarbij artikel 2:5 (2.1.5) uit de Awb.

²⁰ Vergrendeling van de pc en leeg bureau aan het eind van de dag

²¹ Software die computersystemen verstoren (toegang krijgen tot gevoelige informatie en/of een computersysteem)

In de Awb staat de geheimhouding geregeld in art 2:5 (2.1.5)

Een ieder die is betrokken bij de uitvoering van de taak van een bestuursorgaan en daarbij de beschikking krijgt over gegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden, en voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift ter zake van die gegevens een geheimhoudingsplicht geldt, is verplicht tot geheimhouding van die gegevens, behoudens voor zover enig wettelijk voorschrift hem tot mededeling verplicht of uit zijn taak de noodzaak tot mededeling voortvloeit.

Voor de omgang met vertrouwelijke en/of geheime informatie hanteert gemeente Drimmelen :

- ✓ Openbaarheid van bestuur is de regel.
- ✓ Vertrouwelijkheid kan, maar dan zo kort mogelijk; heeft geen juridische status.

Geheimhouding is de uitzondering, maar mag alleen worden opgelegd als dat volstrekt noodzakelijk is (zoals bij een WOB-verzoek) en daarbij moeten procedures correct worden doorlopen.

4.10. Acquisitie, ontwikkeling en onderhoud van informatiesystemen

Informatiebeveiliging maakt integraal deel uit van informatiesystemen in de gehele levenscyclus. De eisen die verband houden met informatiebeveiliging worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen. Gedetailleerde risicobeoordelingen en een juiste keuze van beheersmaatregelen zijn onmisbaar. Beveiligd ontwikkelen is een eis voor het opbouwen van een beveiligde dienstverlening, architectuur, software en een beveiligd systeem.

4.11. Leveranciersrelaties

Gemeenten maken gebruik van leveranciers voor het leveren van producten en diensten waarbij informatiebeveiliging een rol speelt. Hiervoor bestaat het GIBIT als gemeenschappelijke inkoopvoorwaarden bij IT. Gemeente Drimmelen maakt gebruik van bedrijfsmiddelen die toegankelijk zijn voor of uitbesteed zijn aan leveranciers. Voor de beveiliging hiervan moet met de leverancier een verwerkersovereenkomst worden overlegd waarin de leverancier aantoont dat hij voldoet aan alle hoogste informatiebeveiligingseisen. Indien het een nieuwe leverancier betreft dan dient dit meegenomen te worden in het inkooptraject, waarbij tevens een risicoafweging wordt gemaakt. Het beveiligingsbeleid van de leverancier moet dezelfde garanties geven als het beveiligingsbeleid van de gemeente en/of dat past bij het product of dienst. Ook aan de verbinding naar de Cloud worden hoge eisen gesteld die getoetst moeten worden.

4.12. Beheer van beveiligingsincidenten

De medewerker dient geconstateerde of vermoede data-/beveiligingslekken en beveiligingsincidenten *direct* te melden bij de CISO van de gemeente. Beveiligingsincidenten worden gemeld bij de CISO, worden als zodanig geregistreerd en voorgelegd aan het securityoverleg. Voor afhandeling geldt de rapportage en escalatielijn volgens het informatiebeveiligingsplan.

Voorbeelden van data-/beveiligingslekken en beveiligingsincidenten zullen via voorlichting en communicatie in het kader van de bewustwording duidelijk gemaakt moeten worden. Daarnaast kan er van incidenten geleerd worden om de kans van optreden in de toekomst te verminderen.

Er is sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident kan gedacht worden aan bijvoorbeeld het kwijtraken van een USB-stick, een verkeerd verstuurd email, de diefstal van een laptop of aan een inbraak door een hacker. Een beveiligingslek is een zwakke plek als gevolg van een menselijke fout of een zwakke plek in het systeem (hard- of software), die functies toelaat die niet toegestaan zijn, of onbevoegden toegang tot gegevens of functies verschaft. Beveiligingslekken kunnen berusten op programmeerfouten, ontwerpfouten of verkeerde configuraties. Hierbij heeft ICT een rol maar ook de functioneel beheerder die de toegang tot systemen/data autoriseren en kunnen monitoren. Bijvoorbeeld een data-/beveiligingslek wordt vaak als eerste door ICT geconstateerd. Dit kan zijn infectie door virus, zoek zijn van gegevensdragers, etc..

4.13. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Er zijn voor de belangrijkste processen en systemen continuïteits-/uitwijkplannen die door middel van een beheerst proces van informatiebeveiliging tot stand komen. Er worden minimaal jaarlijks oefeningen of testen gehouden om de continuïteitsplannen te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold. Daarnaast behoren er passende contacten met relevante overheidsinstanties te worden onderhouden.

4.14. Naleving

Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van alle gemeentelijke processen waarin wordt gewerkt met gevoelige informatie. Informatieveiligheid is een kwaliteitskenmerk van het primaire proces, waarop de manager van elke afdeling stuurt. De kwaliteit wordt gemeten aan:

- de mate waarin een volledige set aan maatregelen is geïmplementeerd, gebaseerd op vastgesteld beleid;
- efficiency en effectiviteit van de geïmplementeerde maatregelen;
- de mate waarin de informatiebeveiliging het bereiken van de strategische doelstellingen ondersteunt.

Voor elk type registratie wordt de bewaartermijn, het opslagmedium en eventuele vernietiging bepaald in overeenstemming met wet, regelgeving, contractuele verplichtingen en bedrijfsmatige eisen. Bij de keuze van het opslagmedium wordt rekening gehouden met de bewaartermijn, de achteruitgang van de kwaliteit van het medium in de loop van de tijd en de voortdurende beschikbaarheid van hulpmiddelen (zoals hard- en software) om de gegevens te raadplegen en te bewerken.

Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of pentesten. In de P&C cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging.

Gegevens op papier worden beschermd door een deugdelijke opslag en een regeling voor de toegang tot archiefruimten. Documenten, opslagmedia, in- en uitvoergegevens en systeemdokumentatie worden beschermd tegen onbevoegde openbaarmaking, wijziging, verwijdering en vernietiging.

Het gebruik van informatiesystemen, alsmede uitzonderingen en informatiebeveiligingsincidenten, worden vastgelegd in logbestanden op een manier die in overeenstemming is met het risico, en zodanig dat tenminste wordt voldaan aan alle relevante wettelijke eisen.

5. Kwaliteitsbewaking

In dit hoofdstuk staat de bewaking van de kwaliteit van het IB-beleid uitgelegd op het vlak van: communiceren over het IB-beleid, borgen van processen e.d., actueel houden van het IB-beleid en het toezien op naleving van het IB-beleid.

5.1. Communicatie

In de communicatie van dit beleid staat de bewustwording centraal van de medewerkers (en ingehuurd derden) en de naleving van de regels en richtlijnen. Om dit te bewerkstelligen zullen er gedragsregels opgesteld en gecommuniceerd worden zodat medewerkers weten wat er van hun verwacht wordt, welke risico's er zijn en welke rechten en plichten ze hebben. Veranderingen en aanpassingen in het managementsysteem worden door het management beoordeeld en intern gecommuniceerd, indien nodig ook naar relevante externe partijen.

Het management bevordert naleving en bewustwording en bepaalt:

- wat gecommuniceerd wordt;
- wanneer gecommuniceerd wordt;
- met wie gecommuniceerd wordt;
- wie de communicatie uitvoert en;
- welke processen door de communicatie beïnvloed worden.

Dit vertaalt zich in beveiligingsrichtlijnen en aandacht voor dit thema in de nieuwsvoorziening. Afspraken worden vastgelegd. Naast bespreking in bijeenkomsten zijn het documentmanagementsysteem (DMS), het algemene communicatiekanaal intranet en 'Drimmelding' de voornaamste bronnen van informatie.

5.2. Borging

Borging vindt plaats door middel van vastlegging van de overeengekomen werkwijze. Dit kan via een of meer van de volgende vormen van vastlegging: procesbeschrijvingen, richtlijnen, gedragscode, procedures, werkinstructies of tooling²². Wat er ook wordt vastgelegd, deze informatie dient voor alle medewerkers toegankelijk te zijn en zal via het intranet verspreid worden, zodat in het geval van incidenten en calamiteiten deze snel en eenduidig toegankelijk is. Het gaat hier voor een groot deel om zaken die al bestaan maar die nog niet gebundeld zijn en die geactualiseerd moeten worden.

5.3. Geldigheid en evaluatie

Het College van gemeente Drimmelen is eigenaar van dit beleidsdocument. Het beheer, opstellen en actueel houden van het beleidsdocument is de verantwoordelijkheid van de CISO namens het management.

²² Een tool is een term die gebruikt wordt voor hulpprogramma's die bepaalde handelingen voor een gebruiker makkelijker maken of helemaal overnemen. Het is een hulpmiddel, een gereedschap.

Dit beleid is vier jaar geldig en wordt minimaal één keer per jaar geëvalueerd samen met het IB-plan. Dit met het oog op:

- Gemeentelijk beleid
- Veranderende wet- en regelgeving of organisatie
- Resultaten van een Baselinetoets gevolgd door een risicoanalyse
- Resultaten risicoanalyse
- Input van de IBD
- Uitkomsten van Audits
- Opgetreden incidenten
- De stand van de techniek (beveiliging en bedreiging)
- Voortschrijdend inzicht
- Uitvoerbaarheid van beveiligingsprocessen
- De toereikende, de tactische en de operationele uitvoering ervan

Op grond van een jaarlijkse toetsing van de informatiebeveiliging via audits en zelfevaluatie, veranderende wet- en regelgeving of door andere omstandigheden, kan dit beleid tussentijds worden bijgesteld.

5.4. Naleving

Naleving van het beleid wordt gecontroleerd. Niet naleving van het beleid kan disciplinaire maatregelen tot gevolg hebben, conform lokale regel- en wetgeving. Periodiek zijn er diverse audits, zelfevaluaties, bewustwordingssessies, en risicoanalyses. Deze acties zorgen ervoor dat het beleid wordt gecontroleerd op zijn toepasbaarheid, volledigheid en werking.

6. Informatiebeveiligingsbeleid gemeente Drimmelen

In dit afsluitende hoofdstuk zijn alle beleidsregels uit het beleidsdocument samengebracht en samengevat tot de feitelijke beleidsregels voor informatiebeveiliging, die de gemeente Drimmelen heeft vastgesteld bij college besluit.

Het doel van dit hoofdstuk is dat de strategische uitgangspunten van de gemeente Drimmelen vaststaan. Waarmee het college richting geeft aan de wijze waarop zij invulling wil geven aan de BIO. Deze strategische uitgangspunten vormen het kader voor de tactische vertaling hiervan door het management.

6.1. Algemeen

Het bestuur en management spelen een cruciale rol bij het uitvoeren van dit IB-beleid. Zo maakt het management een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente hebben, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Het management legt deze inschatting van het belang en de risico's voor aan het college. Het college bepaalt vervolgens de kaders en maakt de afwegingen rondom de maatregelen voor informatieveiligheid die het management voorstelt. Op basis van het collegebesluit zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat het informatiebeveiligingsbeleid ondersteunt en zich hierbij betrokken voelt, door het uitbrengen en handhaven van een IB-beleid van en voor de hele organisatie. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verwerkingen). Het IB-beleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving. Dit strategische beleid is nader uitgewerkt op tactisch niveau met nadere concrete aanwijzingen in het informatiebeveiligingsplan.

De gemeente is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van het beleid. Hierbij geldt:

- ✓ Er is wetgeving waaraan altijd moet worden voldaan, zoals niet uitputtend: AVG, Suwi, BAG, BGT, BRO en PUN, maar ook de archiefwet.
- ✓ Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Overheid (BIO).
- ✓ Het college stelt dit normenkader vast, waarbij er ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

6.2. IB-beleid gemeente Drimmelen 2020 – 2023

Bij het vaststellen van het IB-beleid worden de volgende besluiten genomen:

- Instemmen met het Informatiebeleid gemeente Drimmelen met ingangsdatum 1 januari 2020.
- Opnemen in het jaarverslag een vast onderdeel 'informatiebeveiliging'.
- Instemmen met de uitvoering van dit beleid.
- Instemmen met de uitwerking van dit beleid in het informatiebeveiligingsplan.
- Instemmen met de kwaliteitsbewakingsvoorstellen voor communicatie, borging van de PDCA-cyclus via het Information Security Management System (ISMS), jaarlijkse evaluatie en controle op naleving.
- Beoordelen van het IB-beleid (jaarlijks) en van het ISMS op basis van een evaluatierapport en een rapportage met incidenten en restrisico's.

De volgende uitgangspunten zijn ontleend aan de Code voor Informatiebeveiliging (ISO 27002) en de Baseline Informatiebeveiliging Overheid:

✓	Alle informatie en informatiesystemen vallen onder dit beleidskader van informatiebeveiliging. De verantwoordelijkheid voor informatiebeveiliging ligt bij het management, met het College van B&W als eindverantwoordelijke. De verantwoordelijkheden voor de bescherming en privacy van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd. De gemeente blijft verantwoordelijk voor haar eigen informatievoorziening, ongeacht of document- of informatiesystemen zich intern of extern bevinden.
✓	Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving, zoals de basisregistraties, Suwi, Paspoorten en ID-bewijzen, maar ook de archiefwet en de Algemene Verordening Gegevensbescherming.
✓	De gemeente kiest voor een optimale beveiliging van de haar toevertrouwde informatievoorziening en passende maatregelen. Een optimale veiligheid ontstaat door het zorgvuldig afwegen van afhankelijkheid en kwetsbaarheid van gemeente processen en risico's versus kosten/consequenties van beveiligingsmaatregelen. Hierbij wordt een balans gezocht tussen risico's en kosten/consequenties van de benodigde beveiligingsmaatregelen.
✓	Specifieke regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld door het managementteam. Alle medewerkers van de gemeente worden bewust gemaakt van en getraind in het gebruik van beveiligingsprocedures.
✓	Iedere medewerker, zowel vast als tijdelijk, intern/ extern is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.
✓	Informatiebeveiliging is een continu verbeterproces. In tegenstelling tot het beleid stelt de gemeente minimaal tweejaarlijks een informatiebeveiligingsplan op, waarin de beschikbaarheid, de integriteit en de vertrouwelijkheid van de informatievoorziening organisatie breed wordt benaderd.
✓	'Plan, Do, Check en Act' vormen samen het managementsysteem van informatiebeveiliging en wordt ondergebracht in de bestaande P&C cyclus.
✓	De CISO ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover zo nodig rechtstreeks aan het college.
✓	De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.

Bijlage 1: Wet- en regelgeving

Om de BIO praktisch uitvoerbaar te maken, zijn in veel overheidsmaatregelen verwijzingen opgenomen naar bestaande wet- en regelgeving. Deze verwijzingen hebben als voordeel dat degene die met de BIO aan de slag gaat er concreet op gewezen wordt dat er reeds bestaande wet- en regelgeving is waarin (beveiligings)eisen zijn vastgelegd. Bovendien zijn deze verwijzingen zo ook in de ISO 27002-indeling gepositioneerd. Er is bewust gekozen voor het maken van verwijzingen en niet voor het herformuleren om misinterpretatie te voorkomen. Voor de genoemde wet- en regelgeving geldt dat de BIO alleen bepaalde beveiligingsaspecten heeft meegenomen. Het is niet de intentie dat de BIO de genoemde wet- en regelgeving volledig afdekt.

In de overheidsmaatregelen zijn verwijzingen opgenomen naar de volgende wet- en regelgeving:

- Ades baseline profile standard (geavanceerde en gekwalificeerde digitale handtekeningen)
- Algemeen Rijksambtenarenreglement (ARAR)
- Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT 2016)
- Archiefwet
- AVG (in de plaats getreden van de WBP en is sinds 25 mei 2018 van kracht);
- Beveiligingsvoorschrift 2013 (BVR 2013), Stcrt. 2013, 15496
- CM(2002)49 (Security within The North Atlantic Treaty Organization)
- Gedragsregeling voor de digitale werkomgeving (1 juli 2016; SGO besluit)
- Het NKBR (Normenkader beveiliging Rijkskantoren) 2015
- Interne klokkenluidersregeling
- ITIL, ASL of BSL framework
- Kader Rijkstoegangsbeleid
- NCSC classificatie
- 'Pas toe of leg uit'-lijst van het Forum Standaardisatie.
- Programma van Eisen PKI Overheid (beheer van digitale certificaten)
- Responsible disclosure procedure (melden van kwetsbaarheden in ICT)
- Telecommunication Infrastructure Standard for Data Centers (TIA-942)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR2007), Stcrt. 2007, 122/11
- Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIR-BI 2013)
- Wet basisregistratie personen (Wet BRP)
- Wet structuur uitvoeringsorganisatie werk en inkomen (Wet Suwi)
- Wet veiligheidsonderzoeken (WVO)

De BIO treedt niet in de plaats van een Data Protection Impact Assessment (DPIA). Een DPIA gaat namelijk over veel meer dan alleen de beveiliging van persoonsgegevens, zoals het vraagstuk van rechtmatigheid van verwerking.