gemeente Dalfsen

Strategisch informatiebeveiligingsbeleid gemeente Dalfsen 2021-2024

Datum: juli 2021

Documentbeheer

Beheersinformatie	
Document of registratie	Strategisch beleid informatiebeveiliging gemeente Dalfsen 2021-2024
Bewaartermijn	-
Classificatie	-

Versiebeheer			
Versie	Datum	Auteur	Opmerkingen
0.1	24 januari 2020	J.H.B. van Maanen	Eerste concept (intern BMC)
0.2	7 maart 2020	J.H.B. van Maanen	Tweede concept (intern BMC)
0.3	27 maart 2020	L.I. van Deenen	Derde concept (intern BMC)
0.4	2 april 2020	L.I. van Deenen	Finale concept (extern distribueerbaar)
0.5	9 juni 2020	L.I. van Deenen	Geredacteerd concept (extern distribueerbaar)
0.6	29 januari 2021	L.I. van Deenen	Geredacteerd concept (extern distribueerbaar)
0.7	12 maart 2021	M. Stam	Eerste concept (intern BMC)
1.0	7 juli 2021	M. Stam	Definitief document

Distributielijst		
Versie	Datum	Verspreid aan
0.1	24 januari 2020	I. van Deenen, L. Knol
0.2	7 maart 2020	I. van Deenen, L. Knol
0.3	27 maart 2020	L.Knol, J.H.B. van Maanen
0.4	2 april 2020	M. Stam, L. Knol, J.H.B. van Maanen
0.5	9 juni 2020	M. Stam, L. Knol, J.H.B. van Maanen
0.6	29 januari 2021	M. Stam, L. Knol

Eigenaar			
Versie	Datum	Eigenaar	Herziening
0.4	2 april 2020	CISO Dalfsen	M. Stam; L. Knol; T. de Roo
0.5	9 juni 2020	CISO Dalfsen	J. Leegwater
0.6	29 januari 2021	CISO Dalfsen	M. de Man
0.7	12 maart 2021	CISO Dalfsen	M. Stam
1.0	7 juli 2021	CISO Dalfsen	P. Everloo, M. Stam

Inhoud

1. Inleiding

1.1 Voorwoord

De gemeente Dalfsen is een informatie-intensieve organisatie met een primaire focus op dienstverlening. Het belang van informatie is exponentieel toegenomen en hiermee significant voor de gemeentelijke organisatie. Informatie is namelijk één van de voornaamste bedrijfsmiddelen voor het realiseren van doelstellingen, zoals:

- optimale dienstverlening en bereikbaarheid;
- resultaatgericht werken;
- klantgericht werken;
- zaak- en procesgericht werken;
- data gedreven werken;
- digitaal werken, plaats- en tijdonafhankelijk;
- efficiënte en gecontroleerde interne- en ketensamenwerking;
- uitvoering van wettelijke kaders.

Deze organisatiekenmerken vragen om een betrouwbare en veilige informatievoorziening. De medewerkers van de gemeente moeten kunnen beschikken over betrouwbare informatie om de betrokken burgers, bedrijven en organisaties optimaal te kunnen helpen en adviseren. De burgers, bedrijven en organisaties moeten op hun beurt erop kunnen vertrouwen dat hun gegevens bij de gemeente in goede handen zijn.

Toegankelijke en betrouwbare overheidsinformatie is essentieel voor een gemeente die zich verantwoordelijk gedraagt en die aanspreekbaar en servicegericht is. Daarnaast is deze toegankelijke en betrouwbare informatie ook essentieel voor het transparant en proactief afleggen van verantwoording aan burgers en gemeenteraad en voor het behalen van maximale resultaten met minimale middelen. De bescherming van waardevolle informatie is hetgeen waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe meer maatregelen getroffen moeten worden.

Voor u ligt het strategisch informatiebeveiligingsbeleid van de gemeente Dalfsen voor de jaren 2021 tot en met 2024. In dit beleid wordt de visie voor informatiebeveiliging, vanuit het belang van informatie, geformuleerd. Dit strategische beleid is richtinggevend en kaderstellend. Het beleid wordt uitgewerkt met gerelateerde beleidsdocumenten voor informatiebeveiliging op tactisch niveau en met werkinstructies op operationeel niveau.

De basis van dit informatiebeveiligingsbeleid wordt gevormd door de Baseline Informatiebeveiliging Overheid (BIO - VNG/IBD). De BIO is afgeleid van de internationale informatiebeveiligingsnormen NEN-ISO/IEC 27001:2017 en 27002:2017. Deze standaarden zijn respectievelijk een norm voor de implementatie en planmatige borging van informatiebeveiliging binnen organisaties en een verzameling van beveiligingsmaatregelen voor een praktische en concrete aanpak binnen de organisatie.

1.2 Leeswijzer

Dit document bevat strategische beleidsuitgangspunten op het gebied van informatiebeveiliging. Hierin staat het volgende beschreven: de uitgangspunten, het sturings- en verantwoordings-mechanisme en de rollen en verantwoordelijkheden aangaande informatiebeveiliging. Daarnaast is rekening gehouden met de wettelijke kaders die aan informatieverwerking binnen specifieke onderdelen worden gesteld. Om te voorkomen dat binnen elk van die gebieden separaat beleid ontwikkeld en geïmplementeerd wordt, is de keuze gemaakt dit gemeentebrede informatie-beveiligingsbeleid op te stellen voor alle organisatieonderdelen.

Dit beleid brengt niet de huidige situatie in beeld, maar beschrijft het ambitieniveau aangaande gemeentebrede informatiebeveiliging. Het beleid heeft een looptijd van drie jaar, waarna evaluatie en bijstelling zal plaatsvinden.

Dit document bevat relevante verwijzingen naar bepalingen in de BIO (aangeduid met haken [ ]). Echter, dit betekent niet dat in alle gevallen de volledige maatregel door de implementatie van dit beleid wordt afgedekt.

1.3 Algemene oriëntatie en positionering

Informatiebeveiliging maakt deel uit van de bedrijfsvoering en de primaire processen van de organisatie en haar omgeving. In de uitwerking vormt het een samenhangend geheel van maatregelen van procedurele, organisatorische, fysieke, technische, personele en juridische aard.

Informatiebeveiliging is de verzamelnaam voor de processen die ingericht worden om de betrouwbaarheid van gemeentelijke processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk onheil. Het begrip 'informatiebeveiliging' heeft betrekking op:

- Beschikbaarheid: het zorgdragen voor het beschikbaar zijn van informatie en informatie-verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers.
  Gegevens en functionaliteit dienen voor gebruikers zodanig beschikbaar te zijn dat zij hun taken optimaal kunnen uitvoeren.
- Integriteit: het waarborgen van de correctheid, volledigheid en tijdigheid van informatie en informatieverwerking.
  De juistheid en actualiteit van gegevens en functionaliteit dient te voldoen aan de daarvoor gestelde normen en wet- en regelgeving.
- Vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden.
  Toegang tot (persoons)gegevens en functionaliteit is beperkt tot degenen die daartoe door de eigenaar hiervan zijn vastgesteld.
- Controleerbaarheid: de mate waarin de juistheid en volledigheid van informatie en gegevensverwerking kan worden gecontroleerd.
  Zijn verwerkingen, handelingen en besluiten aantoonbaar en daardoor controleerbaar en te auditen. Ook: werken de getroffen maatregelen zoals deze bedoeld zijn.

1.4 Context en ontwikkelingen

De hieronder toegelichte context en ontwikkelingen in en rond het taakveld informatiebeveiliging, dan wel de gemeentelijke organisatie, zijn meegenomen in de formulering en uitgangspunten van dit beleidsstuk.

1.4.1 Wettelijke basis en controle beveiligingsnormen

De wettelijke basis van informatiebeveiliging valt af te leiden uit Europese richtlijnen en landelijke wet- en regelgeving. In bijlage 1 staat hiervan een - niet uitputtend - overzicht weergegeven. Op grond van deze wet- en regelgeving worden er eisen gesteld aan het niveau van informatie-beveiliging, de beheersmaatregelen en de controle (interne controle (ic)/interne audit) daarop.

1.4.2 Baseline Informatiebeveiliging Overheid

Alle Nederlandse gemeenten hanteren vanaf 1 januari 2020 samen met de rijksoverheid, de waterschappen en de provincies één uniform normenkader voor informatiebeveiliging: de Baseline Informatiebeveiliging Overheid (BIO). Deze vervangt voor gemeenten de Baseline Informatie-beveiliging Gemeenten (BIG). De BIO is gebaseerd op de internationale ISO27001/2-standaard en biedt een baseline met verschillende niveaus van beveiliging. Risicomanagement vormt zowel de basis van de BIO als een leidend uitgangspunt bij de implementatie en het gebruik ervan.

Daar waar dit vereist is of nodig wordt geacht op basis van risicomanagement, worden door de gemeente aanvullende tactische beleidsdocumenten opgesteld.

1.4.3 Algemene Verordening Gegevensbescherming

De invoering van de Algemene Verordening Gegevensbescherming (AVG) heeft gezorgd voor toenemende aandacht voor de bescherming van persoonsgegevens. Het belang van privacy neemt voor zowel de betrokkene als voor de gemeente steeds meer toe, evenals de impact van privacy schendingen.

In de AVG is de eis opgenomen om "passende" organisatorische- en technische maatregelen te nemen tegen "ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging". Het begrip "passend" geeft niet alleen aan dat er een proportionaliteit tussen de beveiligingsmaatregelen en de aard van de te beschermen gegevens moet zijn, maar ook dat beveiliging niet statisch kan zijn, maar mee moet bewegen met dreigingen en de stand der techniek.

De relatief nieuwe gemeentelijke publieke processen in het sociaal domein kennen hier een extra gevoeligheid en afbreukrisico.

1.4.4 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het door de IBD/VNG periodiek opgestelde Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee zeer geschikt om focus aan te brengen in het actualiseren van beleid. De volgende thema's worden voor de periode 2021-2022 geprioriteerd:

- Blijf aandacht besteden aan interne bewustwording (interne onbedoelde en bedoelde incidenten);
- Onderhoudt – dan wel intensiveer – de ICT-security inrichting (externe ongerichte en gerichte incidenten);
- Borg de continuïteit van de bedrijfsvoering (beschikbaarheid bij calamiteiten);
- Versterk de integriteit van gegevens (de invoer en controle van/op juiste gegevens in informatiesystemen);
- Voorkom ongeautoriseerde toegang tot vertrouwelijke informatie (menselijke en technische fouten);
- Voer de regie over risicomanagement (procesgerichte risico's analyseren en mitigeren);
- Cultiveer een veilige en open organisatie (biedt functionele en veilige oplossingen, beloon veilig gedrag en zorg voor een open meld- en leercultuur).

1.4.5 Forum Standaardisatie

De gemeente Dalfsen is als overheidsorganisatie verplicht te voldoen aan de standaarden uit de 'pas toe of leg uit'-lijst[1] met verplichte standaarden voor de publieke sector van het Forum Standaardisatie. Hiertoe horen onder meer de normen NEN-ISO/IEC 27001:2013 en NEN-ISO/IEC 27002:2013 waarop de BIO is gebaseerd. Bij de aanbesteding van nieuwe producten en/of diensten of het verlengen van bestaande producten en/of diensten worden de relevante open standaarden uit de lijst van het Forum Standaardisatie uitgevraagd.

1.4.6 De informatiemaatschappij, digitalisering en innovatie

We leven in toenemende mate in een informatiemaatschappij waarbij digitalisering de standaard is. Bij de dagelijkse taakuitoefening wordt dan ook steeds meer gebruik gemaakt van applicaties, digitale middelen, mobile devices en gekoppelde databases waarbij informatiesystemen steeds meer in open verbinding staan met de buitenwereld. Ook door schaalvergroting en samenwerking in ketenautomatisering neemt de kans op, en de impact van, incidenten toe. Eenzelfde risico ligt in het integreren of koppelen van systemen die niet van oorsprong zijn ontworpen met veiligheid in gedachte.

Initiatieven zoals 'Common Ground' (een beweging waarin gemeenten werken aan een stapsgewijze modernisering van de ICT-infrastructuur met snelle en open uitwisseling van gegevens), innovaties zoals 'the Internet of Things' (het 'slim' maken van statische objecten door die te voorzien van technische innovaties) en 'Artificial Intelligence' (kunstmatige intelligentie, welke een computer zelfstandig kan laten nadenken en beslissen) ontstaan tevens binnen deze maatschappelijke verandering. Deze hebben ook degelijk een impact op hoe omgegaan moet worden met informatiebeveiliging binnen gemeenten. De toename van de hoeveelheid gegevens en het sneller en gemakkelijker uitwisselen hiervan, vraagt aandacht voor informatiebeveiliging. Innovatieve manieren van werken, leggen hiernaast druk op informatiebeveiliging doordat er ook risico's en kwetsbaarheden ontstaan. Hoewel het de informatiebeveiliging kan bevorderen door innovaties toe te passen, kan het een gevaar vormen voor de bedrijfsvoering doordat er bijvoorbeeld te weinig beveiligingsmaatregelen getroffen worden of beschikbaar zijn.

1.4.7 De gemeente als regie-organisatie

Doordat (de uitvoering van) veel taken – betreffende primaire processen als ook ondersteunende processen – door ketenpartners of toeleveranciers worden uitgevoerd, worden hoge eisen gesteld aan opdrachtgeverschap en regievoering.

[1] Dit betekent dat de overheid deze normen toepast, tenzij er expliciet geformuleerde redenen zijn om dat niet te doen.

1.5 Scope

De scope van dit beleid omvat de volgende onderdelen:

- Alle gemeentelijke informatieprocessen, zowel ambtelijke als bestuurlijke;
- De onderliggende informatiesystemen, informatie en gegevens van de gemeente en betrokken externe partijen;
- Het gebruik van deze onderliggende informatiesystemen door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Organisatorisch zijn de uitgangspunten van dit beleid van toepassing op zowel de ambtelijke organisatie als op (de leden van) het college en alle hieronder ressorterende bestuursorganen. Hetzelfde geldt ook voor de gemeenteraad en de griffie en de daaraan gelieerde organisatieonderdelen (zoals de rekenkamer).

Het informatiebeveiligingsbeleid is bedoeld voor alle in- en externe medewerkers en ketenpartners van de gemeente Dalfsen. Een overzicht van de doelgroepen van dit beleid en de bijbehorende rol bij informatiebeveiliging zijn hieronder weergegeven. De specifieke taken en verantwoordelijkheden van beveiligingsrollen zijn nader uitgewerkt in hoofdstuk 4.

Doelgroep	Rol bij informatiebeveiliging
Gemeenteraad	Controle, toetsing en conformatie aan dit beleid
College van B&W	Integrale verantwoordelijkheid
MT	Kaderstelling en implementatie
Griffie	Conformerend aan dit beleid
Griffie	Sturing op risico's en controle op naleving
Beleidsmakers	Plan- en beleidsvorming binnen kaders
Eenheidsmanagers en proceseigenaren	Via classificatie bepalen van beschermingseisen
Eenheidsmanagers en proceseigenaren	Sturing op risico's en controle op naleving
ICT	Technische, systeem- en applicatiebeveiliging
Facilitaire zaken	Fysieke beveiliging en fysieke toegangsbeveiliging
HR	Arbeidsvoorwaardelijke zaken
Communicatie	Bevorderen bewustwording
Medewerkers	Gedrag en naleving
CISO	Dagelijkse coördinatie van informatiebeveiliging
FG	Toezicht op naleving AVG
Control	Toetsing
Auditors	Onafhankelijke toetsing
Leveranciers en ketenpartners	Compliance met eisen en richtlijnen
Burgers, klanten	Informatief

2. Informatiebeveiligingsbeleid

Doelstelling
Het bieden van ondersteuning aan het bestuur, het managementteam en de organisatie bij de sturing op en het beheer van informatiebeveiliging.

Resultaat
Beleid waarin de taken, bevoegdheden en verantwoordelijkheden voor informatiebeveiliging alsmede het vereiste beveiligingsniveau zijn vastgelegd.

2.1 Strategisch uitgangspunten voor informatiebeveiliging

Dit beleidsdocument geldt als kader voor alle zaken binnen de gemeente Dalfsen omtrent informatiebeveiliging. Tezamen met het Bedrijfsinformatieplan, welke leidend is voor alle zaken omtrent informatievoorziening, dekken deze beleidsstukken de uitgangspunten af die gehanteerd worden binnen de gemeente in het kader van het informatiedomein.

Het informatiebeveiligingsbeleid heeft als doel het waarborgen van de continuïteit van de informatievoorziening – en daarmee van de bedrijfsvoering – en het minimaliseren van de schade door het voorkomen van beveiligingsincidenten en het beperken van eventuele gevolgen ervan. Dit strategische kader is richtinggevend en kaderstellend voor het tactische informatiebeveiligingsbeleid en voor passende organisatorische en technische maatregelen. Deze hebben ten doel gemeentelijke informatie te beschermen en te waarborgen dat de gemeente haar bedrijfsdoelstellingen met digitalisering kan realiseren en dat zij daarmee voldoet aan relevante wet- en regelgeving.

De gemeente streeft ernaar om ‘in control’ te zijn en daarover op professionele wijze verantwoording af te leggen. Om in control te zijn op informatiebeveiliging is het van belang dat wordt aangesloten bij de bestaande P&C-cyclus, ten behoeve van de benodigde financiële middelen en de verantwoording daarover. Ten tweede betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn en dat er een SMART-planning is van de maatregelen die nog niet genomen zijn. Dit geheel dient verankerd te zijn in de PDCA-cyclus.

Informatiebeveiliging is geen doel op zich. Dit informatiebeveiligingsbeleid moet dan ook in samenhang gezien worden met onder meer de informatievisie, de organisatievisie en de dienstverleningsvisie en passen binnen wet- en regelgeving. De materie van informatie en data is complex; het is één samenhangend geheel voor de hele organisatie en hierbij is samenwerking tussen alle gebruikers vereist. Governance is nodig om dit te sturen en gericht door te ontwikkelen. Daarbij is de Governance er ook op gericht om de basis solide te houden. Ditzelfde geldt onverminderd voor informatiebeveiliging. Governance houdt in ieder geval in:

- sturing door onder meer integratie in de P&C-cyclus (zie hoofdstuk 3);
- helderheid in rollen, taken en verantwoordelijkheden (zie hoofdstuk 4);
- samenhang bewaken en prioriteiten stellen in implementatie en ontwikkeling.

Het college behoort dit gemeentebrede strategische beleidsdocument voor informatiebeveiliging goed te keuren en kenbaar te maken aan alle medewerkers, alsmede hiernaar te handelen [5.1.1.1].

2.2 De vertaling naar tactisch beleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor het tactische beleid en daarmee richting te geven aan de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. De BIO is hiervoor een zwaarwegend kader met een gedeeltelijk verplicht karakter. De BIO bevat namelijk normen op alle te onderscheiden gebieden van informatiebeveiliging van de gemeente. De BIO stelt normen voor de volgende onderwerpen:

- Informatiebeveiligingsbeleid;
- 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 informatiebeveiligingsincidenten;
- IB-aspecten van bedrijfscontinuïteitsbeheer;
- Naleving.

De processen worden binnen de organisatie tegen het licht gehouden ten behoeve van het lokaliseren van risico's, welke onder deze onderwerpen geschaard kunnen worden. De BIO schrijft vervolgens op basis van de classificatie van deze risico's een set met verplichte maatregelen voor. Hiermee worden het tactische beleid en actieplan geformuleerd. Dit staat verder uitgewerkt in hoofdstuk 3. De vertaling naar operationeel niveau zal hiermee bestaan uit talrijke maatregelen, richtlijnen, procedures en andere operationele documentatie. Deze zullen de praktische uitwerking vormen van het tactische beleid. De op te stellen en te implementeren werkzaamheden worden uitgewerkt in een twee jaarlijks te schrijven gemeentelijk actieplan.

2.3 Visie op informatiebeveiliging: uitgangspunten

De gemeente Dalfsen draagt er zorg voor dat de informatiebeveiliging goed georganiseerd wordt en blijft. De volgende uitgangspunten en leidende principes worden hierbij gehanteerd:

- Het college is eindverantwoordelijke voor de informatiebeveiliging, daarmee in het bijzonder de portefeuillehouder voor informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement.
- Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Dalfsen hebben een proceseigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de proceseigenaar van de informatie.
- Alle informatie en informatiesystemen zijn van belang voor de gemeente; bepaalde informatie is van vitaal en kritiek belang. Dit wordt geclassificeerd door middel van een dataclassificatie (zie hoofdstuk 3).
- Informatiebeveiliging vraagt een onafhankelijke regie en soms ingrijpen in bestaande structuren. Daarmee vraagt informatiebeveiliging om centrale en onafhankelijke beveiligingsfunctionarissen.
- De gemeente voldoet aan de wet- en regelgeving op het gebied van informatiebeveiliging en privacy.
- Het tactisch informatiebeveiligingsbeleid van de gemeente Dalfsen wordt gevormd door de BIO, uit te breiden met onderwerp specifieke beleidsdocumenten waar dat in de BIO vereist wordt. De gemeente conformeert zich tevens aan toekomstige wijzigingen in de BIO.
- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging. Er wordt aansluiting gevonden bij de bestaande P&C-systematiek.
- De registratie en analyse van beveiligingsincidenten geven waardevolle informatie om van te leren en dus worden incidenten uit het verleden ook nadrukkelijk in het verbeterproces van informatiebeveiliging gebruikt.
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Iedere medewerker, zowel vast als tijdelijk, intern of 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.
- Externe partijen moeten aan het beveiligingsniveau hanteren zoals opgenomen in dit beleid; zij moeten tevens aan kunnen tonen dat zij voldoen aan dit niveau van beveiliging.
- Bij de inkoop van nieuwe applicaties of diensten worden informatiebeveiligingseisen in een Programma van Eisen opgenomen, op basis van een risicoanalyse dan wel dataclassificatie. Hieraan moet voldaan worden door de leverancier, waarbij de proces- of applicatie-eigenaar verantwoordelijk is voor de controle op de naleving hiervan.
- Specifieke informatie op het gebied van informatiebeveiliging van relevante expertise-groepen, leveranciers van hardware, software en diensten en de IBD wordt gebruikt om de informatiebeveiliging te verbeteren [12.6.1].
- De gemeente heeft uitgewerkt met welke instanties contact wordt onderhouden en door wie [6.1.3.1]. Dit overzicht wordt minimaal jaarlijks bijgewerkt [6.1.3.2].

3. Borging van het informatiebeveiligingsbeleid

Doelstelling
Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.

Resultaat
Een beheerst proces voor ontwikkeling, uitvoering, controle en bijsturing van informatiebeveiliging binnen de organisatie.

Om de borging van het informatiebeveiligingsbeleid en de daarvan afgeleide plannen te realiseren, wordt naast een toebedeling van rollen (zie hoofdstuk 4), onderstaande Plan, Do, Check, Act (PDCA) cyclus doorlopen. Onderstaande uitgangspunten worden gehanteerd bij het doorlopen van de PDCA-cyclus. Het doorlopen van deze cyclus resulteert in een Information Security Management System (ISMS) (zie figuur 1) [18.2.1.1]. Gedurende het doorlopen van de cyclus kunnen betrokken documenten worden gewijzigd.

3.1 Informatiebeveiligingsbeleid

De start ligt bij de visie op informatiebeveiliging en het informatiebeveiligingsbeleid. Dit is een organisatiebreed beleid dat de uitgangspunten, de normen en de kaders biedt voor de beveiliging van alle onderliggende gemeentelijke informatieprocessen. Uitzonderingen hierop zijn toegestaan, maar dan wel duidelijk gemotiveerd én verifieerbaar; dit wordt ook wel het ‘pas toe of leg uit’-principe genoemd.

Bijstelling van het (strategische) informatiebeveiligingsbeleid vindt plaats rond een cyclus van drie jaar. Indien zich grote wijzigingen voordoen, vindt actualisatie eerder plaats [5.1.2.1]. De raad stelt het strategisch informatiebeveiligingsbeleid vast, waarmee het ook op de gemeenteraad van toepassing is.

3.2 Informatiebeveiligingsanalyse

Stap twee is gericht op het implementatietraject. De implementatiefase begint met het uitvoeren van een informatiebeveiligingsanalyse. Tijdens deze informatiebeveiligingsanalyse wordt allereerst een overzicht opgesteld van de gegevensverzamelingen/applicaties in de gemeentelijke organisatie. Deze worden toegewezen aan een eigenaar en geclassificeerd op de risicoklassen beschikbaarheid, integriteit en betrouwbaarheid van de informatie (ook wel dataclassificatie genoemd). Het gehanteerde classificatiemodel voor de dataclassificatie staat weergegeven in bijlage 2. Hierbij wordt het Basis Beveiligingsniveau (BBN) per informatiesysteem vastgesteld. De uitleg van de verschillende BBN’s staat weergegeven in bijlage 3. Hiermee kunnen de corresponderende maatregelen vanuit de BIO geselecteerd worden. Daarnaast kan middels de BBN’s bepaald worden om een diepgaande risicoanalyse uit te voeren. Vervolgens wordt de praktijksituatie in de gemeente getoetst aan het gemeentebrede informatiebeveiligingsbeleid en aan de beveiligingsmaatregelen u1it de BIO door middel van het uitvoeren van een risico-inventarisatie en -evaluatie (RI&E), een GAP-analyse, een scan van de fysieke beveiliging (rondgang gebouw) en een evaluatie van het vorige actieplan. Bijstelling van de informatiebeveiligingsanalyse vindt om het jaar plaats.

In de informatiebeveiligingsanalyse worden niet alleen de ‘harde aspecten’ onderzocht; dat wil zeggen de techniek, de regels en de procedures. Daarnaast worden ook de ‘zachte aspecten’ meegenomen in de analyse. Deze richten zich op het menselijk handelen, de cultuuraspecten en de sociale en fysieke inrichting van de organisatie.

3.3 Actieplan

Op basis van de informatiebeveiligingsanalyse wordt in stap drie een actieplan opgesteld. De in de analyse geconstateerde risico’s worden gewogen en waar nodig van maatregelen voorzien. Het invoeren van maatregelen gebeurt vanuit een risicobenadering. De effecten van de maatregelen moeten in verhouding staan tot de noodzakelijke beveiliging. Hierbij wordt ook gebruik gemaakt van beveiligingsclassificaties (dataclassificatie). Prioritering van de acties wordt gedaan op basis van de risico’s die vanuit de RI&E zijn geconstateerd, de beschikbare tijd en de beschikbare middelen. Hierdoor ontstaat een compact actieplan waarmee de gemeente vaststelt welke verbeteracties gedurende een periode van twee jaar worden uitgevoerd. Dit actieplan vormt een praktische leidraad voor de verbetering en borging van informatiebeveiliging in de organisatie. Het directieteam stelt het actieplan vast. De informatiebeveiligingsorganisatie komt bij elkaar om de implementatie van het

actieplan informatiebeveiliging te evalueren, te bewaken en waar nodig bij te stellen. Dit vindt conform de bespreking in het informatiebeveiligingsoverleg (zie paragraaf 4.2) minimaal tweemaal per jaar plaats.

Jaarlijks wordt het actieplan opgesteld onder leiding van de CISO, o.a. gebaseerd op:

- De uitkomsten van de uitgevoerde informatiebeveiligingsanalyse;
- De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
- Het dreigingsbeeld gemeenten van de IBD;
- De door de eenheidsmanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn;
- Registraties uit het incidentenregister;
- Bedrijfsinformatieplan.

3.4 Technische en organisatorische maatregelen

Stap vier bestaat uit het opleveren van een complete set aan technische en organisatorische maatregelen die gericht is op de specifieke eisen van een onderdeel. Het kan gaan om maatregelen uit de BIO, maar ook om specifieke maatregelen voor applicaties zoals de BRP, SUWI, de BAG, het financiële systeem of om de primaire processen van de organisatie, ICT-beheerprocessen of de inrichting van de ICT-platformen. Dit betreft met name het opstellen van procedures en werkinstructies.

3.5 Audits en naleving

Het directieteam beoordeelt regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen inzake beveiliging [18.2.2]. Daarin wordt in lijn met de P&C-cyclus en ondersteunt door een in control verklaring (ICV) gerapporteerd over het doorlopen van de beschreven cyclus met betrekking tot informatiebeveiliging. In deze rapportage worden ook andere voor informatiebeveiliging en privacy relevante onderwerpen – zoals auditresultaten en de uitkomsten van interne controles – behandeld [18.1.4.2; 18.2.2.1].

Figuur 1: De informatiebeveiligingspiramide met PDCA-cirkel

Om te beoordelen of de gemeente haar informatiebeveiligingsbeleid- en doelstellingen heeft behaald, worden periodieke onafhankelijke controles en audits uitgevoerd - waarbij een onafhankelijke deskundige partij een toets uitvoert op de opzet, bestaan en werking van beheersmaatregelen. Hiertoe kan een externe (erkende) partij worden ingeschakeld of de eigen afdeling concern control/auditafdeling. De uitgevoerde dataclassificatie ten behoeve van de informatiebeveiligingsanalyse wordt tevens getoetst. Hierbij wordt bekeken in hoeverre de classificatie van beveiligingsniveau in de praktijk doorstroomt naar gepaste beveiligingsmaatregelen en de opvolging hiervan.

Jaarlijks wordt een auditplan (intern controleplan) opgesteld waarin wordt vastgelegd welke interne controles en audits in het komende jaar plaatsvinden en op welke informatiesystemen deze betrekking hebben [18.2.1.2]. In dit plan wordt tevens een beschrijving van de uit te voeren controles opgenomen en worden deze door de uitvoerders en verantwoordelijken (lijnniveau) te verrichten controles gekoppeld aan een tijdsplanning. Ook de jaarlijkse controle op de technische naleving van beveiligingsnormen bij informatiesystemen, zoals penetratietesten, zijn onderdeel van dit plan [18.2.3.1]. Over de resultaten van de uitgevoerde audits wordt door de lijnverantwoordelijken gerapporteerd aan de concerncontroller / controller informatiebeveiliging.[2] De concern controller / controller informatiebeveiliging rapporteert over de voortgang van het interne controleplan aan de CISO en het bestuur.

[2] Deze twee functies kunnen door een of door twee personen worden uitgeoefend.

4. Organisatie van de informatiebeveiliging

Doelstelling
Het benoemen van het eigenaarschap van de bedrijfsprocessen met bijbehorende informatieprocessen en/of (informatie)systemen en het verankeren van de hieraan verbonden verantwoordelijkheden [8.1.2].

Resultaat
Verankering in de gemeentelijke organisatie van verantwoordelijkheden, taakomschrijvingen en coördinatie- en rapportagemechanismen met betrekking tot informatiebeveiliging.

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model is het lijnmanagement – de eerste lijn – verantwoordelijk voor de eigen processen, waaronder ook voor informatiebeveiliging. De tweede lijn (CISO, security officers) ondersteunt, adviseert, coördineert en bewaakt of het managementteam zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering (VIC, verbijzonderde interne controle). Hier is op onderdelen nog een vierde lijn aan toe te voegen in de vorm van een (op onderdelen verplichte) externe audit.

4.1 Verantwoordelijkheidsniveaus binnen de gemeente Dalfsen

Binnen de gemeente Dalfsen worden – waar relevant in lijn met geldende wet- en regelgeving – de hierna te noemen verantwoordelijkheids- en takenniveaus met betrekking tot informatiebeveiliging onderscheiden [6.1.1.2].

4.1.1 Controle en toetsing door de gemeenteraad

De gemeenteraad draagt een specifieke bevoegdheid voor de controle en de toetsing op de werking van beleid binnen de gemeente Dalfsen, zo ook voor informatiebeveiliging. De gemeenteraad stelt het informatiebeveiligingsbeleid vast. Het college legt vervolgens in lijn met de P&C-cyclus jaarlijks verantwoording af aan de gemeenteraad over de stand van zaken van informatiebeveiliging ten opzichte van het in dit beleid vastgestelde kader. Dit doet het college middels een collegeverklaring (ICV) – waarop door een auditor Assurance wordt afgegeven – en in het jaarverslag met een passage over informatiebeveiliging in de paragraaf bedrijfsvoering [18.2.2.1].

4.1.2 Conformering van de griffie aan dit beleid

De griffie is als apart orgaan binnen de ambtelijke organisatie verantwoordelijk voor de eigen processen, systemen en gegevens die zich hierin bevinden en verwerkt worden. Daarmee is de griffie ook verantwoordelijk voor de staat van informatiebeveiliging binnen de eigen processen. De griffie conformeert zich aan dit informatiebeveiligingsbeleid en hanteert daarmee hetzelfde kader voor informatiebeveiliging als de ambtelijke organisatie.

4.1.3 Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden op organisatieniveau

Het college draagt als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen de eindverantwoordelijkheid voor een passend niveau van informatiebeveiliging. Hierbij neemt zij de tien bestuurlijke principes voor informatiebeveiliging in acht die door de Nederlandse Vereniging van Gemeenten (2019) zijn geformuleerd (zie bijlage 5). Verder stelt ze met het voorliggende beleidsdocument de kaders ten aanzien van informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving vast. Het college informeert de gemeenteraad over de informatiebeveiliging van de gemeente door dit op te nemen in de jaarrekening van de gemeente. Hierin wordt de gemeenteraad op de hoogte gebracht van de stand van zaken, de uitgevoerde plannen van het afgelopen jaar, de tijdsplanning en de plannen voor het volgende jaar. Daarnaast worden de Chief Information Security Officer (CISO) en de concerncontroller / controller informatiebeveiliging op basis van een vastgesteld functieprofiel aangesteld door het college [6.1.1.2; 6.1.1.3; 6.1.1.4].

4.1.4 Verantwoordelijkheden en taken op organisatieniveau

De CISO voert namens het college activiteiten uit voor informatiebeveiliging. Deze stelt in overleg met het directieteam – waaronder de gemeentesecretaris – en het managementteam het gewenste niveau van informatiebeveiliging vast voor de gemeente. De beveiligingseisen worden per

bedrijfsproces vastgesteld. De CISO is daarnaast verantwoordelijk voor de juiste implementatie van de beveiliging in de bedrijfsprocessen en in de in- en externe (informatie)systemen. De gemeentesecretaris/algemeen directeur stelt voor ieder (informatie)systeem een procesverantwoordelijke of systeemeigenaar aan. De procesverantwoordelijke of systeemeigenaar is verantwoordelijk voor het stellen van eisen aan een systeem en de inrichting van de controle hierop, zodat voldaan wordt aan het informatiebeveiligingsbeleid en de relevante wettelijke eisen [8.1.2]. Bij afwezigheid van de gemeentesecretaris/algemeen directeur zijn de verantwoordelijkheden in het kader van informatieveiligheid belegd bij de adjunct gemeentesecretaris/algemeen directeur. De gemeentesecretaris/algemeen directeur heeft de rol van CIO binnen de gemeente Dalfsen en is daarmee verantwoordelijk voor de algehele informatievoorziening.

De gemeentesecretaris/algemeen directeur heeft in ieder geval de volgende verantwoordelijkheden:

- Het stellen van operationele kaders en het geven van sturing ten aanzien van informatiebeveiliging;
- Het sturen op risico's omtrent informatiebeveiliging;
- Het periodiek evalueren van beleidskaders en deze bijstellen waar nodig;
- Het (laten) controleren of de getroffen beveiligingsmaatregelen overeenstemmen met de betrouwbaarheidseisen en of deze beveiligingsmaatregelen voldoende bescherming bieden;
- Het beleggen van de verantwoordelijkheid voor informatiebeveiligingscomponenten en -systemen;
- Het inrichten van functiescheiding tussen uitvoerende, controlerende en beleidsbepalende taken met betrekking tot informatiebeveiliging om fraude en/of fouten te voorkomen.

4.1.5 Verantwoordelijkheden en taken op eenheidsniveau

De eenheidsmanagers en de griffier (proceseigenaren) zijn eigenaar van en integraal verantwoordelijk voor de (informatie)beveiliging van de informatieprocessen en -systemen binnen hun organisatieonderdeel.

De eenheidsmanagers en griffier hebben in ieder geval de volgende verantwoordelijkheden:

- Het classificeren van opgeslagen data in applicaties en gegevensverzamelingen;
- Het opstellen van betrouwbaarheidseisen voor de afdelingsinformatiesystemen;
- De keuze voor en de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- Het uitvoeren van risicoscans informatiebeveiliging om risicoafwegingen te kunnen maken;
- Verantwoordelijkheid nemen voor het realiseren van de informatiebeveiliging binnen de processen waar zij verantwoordelijk voor zijn. Dit geldt ook voor onderdelen die uitbesteed zijn of worden uitgevoerd bij samenwerkingsverbanden, ketenpartners en leveranciers;
- Medewerkers attenderen op hun verantwoordelijkheid ten aanzien van informatiebeveiliging in hun dagelijkse werkprocessen;
- Het sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en op naleving van regels en richtlijnen;
- Het oplossen van beveiligingsincidenten (voorval dat de betrouwbaarheid, beschikbaarheid of vertrouwelijkheid van de informatievoorziening verstoort, en daarmee de informatiebeveiliging kan aantasten) [16.1.2.5];
- Het expliciet vaststellen van relevante wettelijke, statutaire, regelgevende, en/of contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen voor elk informatiesysteem (een samenhangende, gegevensverwerkende functionaliteit voor de besturing of ondersteuning van één of meer bedrijfsprocessen) en de organisatie [18.1.1];
- Het waarborgen van privacy en bescherming van persoonsgegevens conform relevante wet- en regelgeving [18.1.4];
- Erop toezien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben;
- Opdracht geven voor en toezien op het uitvoeren van periodieke beveiligingsaudits;
- Het rapporteren, via de CISO, over compliance (voldoen) aan wet- en regelgeving en algemeen beleid van de gemeente in de P&C-rapportages.

4.1.6 Chief Information Security Officer (CISO)

Deze rol is op organisatieniveau verantwoordelijk voor het actueel houden van het informatiebeveiligingsbeleid, het coördineren van de uitvoering van het beleid, het adviseren bij projecten, het beheersen van risico's en het opstellen van rapportages.

De CISO heeft in ieder geval de volgende verantwoordelijkheden:

- Rapporteert rechtstreeks aan de gemeentesecretaris/algemeen directeur en de portefeuillehouder;
- Coördineert het formuleren van informatiebeveiligingsbeleid;
- Coördineert de uitvoering van de informatiebeveiligingsanalyse en zorgt voor de actualisatie hiervan;
- Coördineert de prioritering van informatiebeveiligingsmaatregelen uit de informatiebeveiligingsanalyse en de uitvoering van het actieplan informatiebeveiliging;
- Bewaakt de uitvoering van het actieplan informatiebeveiliging en de naleving van het beleid;
- Stelt een plan op voor overleg en rapportage met betrekking tot informatiebeveiliging;
- Ondersteunt de gemeentesecretaris/algemeen directeur, de adjunct gemeentesecretaris/directeur en het managementteam met kennis over informatiebeveiliging, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen;
- Is het aanspreekpunt voor medewerkers van de gemeente Dalfsen over het onderwerp informatiebeveiliging;
- Volgt de externe invloeden die van invloed zijn op het informatiebeveiligingsbeleid en de informatiebeveiligingsanalyse;
- Geeft gevraagd én ongevraagd advies over informatiebeveiliging aan de gehele organisatie;
- Bevordert het beveiligingsbewustzijn in de organisatie;
- Houdt de registratie van informatiebeveiligingsincidenten bij in een incidentenregister en is verantwoordelijk voor de juiste afhandeling en evaluatie van informatiebeveiligings-incidenten;
- Ondersteunt het college bij het maken van de rapportage over de informatiebeveiliging van de gemeente in het jaarverslag;
- Onderhoudt contact met relevante overheidsinstanties;
- Ondersteunt vanuit een onafhankelijke centrale positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan het directieteam, voorafgaand aan de P&C-gesprekken;
- Rapporteert over de informatiebeveiliging van de gemeente in de P&C-managementrapportages en levert een In Control Statement. Hierbij bundelt de CISO de deelbijdragen van het managementteam.

4.1.7 De concerncontroller – controller informatiebeveiliging

Deze rol is op organisatieniveau verantwoordelijk voor het verbijzonderde toezicht op de naleving van het informatiebeveiligingsbeleid, de realisatie van voorgenomen beveiligingsmaatregelen en de escalatie van beveiligingsincidenten.

De concerncontroller / controller informatiebeveiliging[3] is in ieder geval verantwoordelijk voor:

- De periodieke toetsing op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van informatiebeveiliging; dit gebeurt in samenwerking met de beveiligingsbeheerders;
- De controle op de voortgang van het uitvoeren van de maatregelen uit de informatiebeveiligingsanalyse en het actieplan informatiebeveiliging;
- De controle op de periodieke actualisatie van het informatiebeveiligingsbeleid en de informatiebeveiligingsanalyse;
- De bewaking van het niveau van informatiebeveiliging;
- De toetsing van evaluatieproces van beveiligingsincidenten;
- De rapportage van bevindingen aan het directieteam en het college.

De rol van concerncontroller / controller informatiebeveiliging heeft op twee specifieke deelgebieden een voorgeschreven benaming. Dit betreft het gebied van reisdocumenten en rijbewijzen. Het betreft de volgende benamingen:

- Beveiligingsfunctionaris reisdocumenten: verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures reisdocumenten.
- Beveiligingsfunctionaris rijbewijzen: verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures rijbewijzen.

[3] Deze twee functies kunnen door een of twee personen worden uitgeoefend.

4.1.8 De beveiligingsbeheerder

Deze rol is verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatiebeveiliging binnen een specifiek deelgebied. In wetgeving worden verschillende benamingen aan rollen gegeven voor veelal dezelfde taken en verantwoordelijkheden ten aanzien van specifieke gegevensverzamelingen. Om eenduidigheid in naamgeving te verkrijgen, wordt in dit beleidsdocument de beveiligingsverantwoordelijkheid ten aanzien van een specifieke gegevensverzameling toegewezen aan de zogenoemde beveiligingsbeheerder. Hierbij volgen de deelgebieden waarbij een beveiligingsbeheerder is aangewezen met vermelding van eventuele officiële rolbenaming: DigiD, BRP, Waardedocumenten (officieel autorisatiebevoegde Reisdocumenten/Aanvraagstations en Autorisatiebevoegde Rijbewijzen), SUWI (officieel Security Officer SUWI) en de BAG, BGT en BRO. Daarnaast worden er (indien mogelijk) beveiligingsbeheerders aangewezen op verschillende aspecten van de gemeentelijke bedrijfsvoering (zoals facilitaire zaken, ICT (Demand Manager) DIV (archivering) en personeelszaken) en de primaire processen (bijvoorbeeld sociaal domein, financiën, beveiliging, handhaving, publieksdiensten (eventueel gecombineerd met BRP en waarde documenten), ruimte/omgeving).

Specifiek verplichte beveiligingsbeheerdersrollen:

- Autorisatiebevoegde Reisdocumenten/Aanvraagstations: verantwoordelijk voor het beheer van de autorisaties (het toekennen van rechten in informatiesystemen aan personen of groepen) voor de reisdocumentenmodules (RAAS en aanvraagstations).
- Autorisatiebevoegde Rijbewijzen: verantwoordelijk voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW.
- Security Officer SUWI: verantwoordelijk voor het beheer van beveiligingsprocedures en maatregelen in het kader van Suwinet. De Security Officer verzorgt minimaal tweemaal per jaar een rapportage met betrekking tot de beveiligingsstatus van Suwinet aan het college en vraagt daarnaast meerdere keren per jaar een rapportage op bij het BKWI over het gebruik van Suwinet door de gemeente.

De beveiligingsbeheerder is voor het toegewezen deelgebied verantwoordelijk voor het geheel van activiteiten gericht op de toepassing en naleving van de maatregelen en procedures die voortkomen uit het informatiebeveiligingsbeleid, inclusief de maatregelen die betrekking hebben op de audit en zelfevaluatie.

4.1.9 Applicatiebeheer

Het beheer van applicaties, technisch dan wel functioneel, is een belangrijk aspect in de beveiliging van de gemeentelijke informatie. Het gebruik van applicaties blijft toenemen. In de loop van de tijd is binnen de gemeente een wildgroei aan vak- en back-officeapplicaties ontstaan. De configuratie, beveiliging (updates/patches), toegang en het beheer hiervan zijn enkele aspecten die bij gestructureerde uitvoering de risico’s kunnen mitigeren.

4.1.9.1 Technisch beheer

De gemeente Dalfsen heeft in 2020 de ICT-organisatie uitbesteed aan het Shared Service Centrum ONS (SSC-ONS). Hiermee is het technische applicatiebeheer ook binnen deze partij komen te liggen. De verantwoordelijkheid voor de uitvoering ligt bij het SSC-ONS, waarbij de functioneel beheerder vanuit de gemeente de directe lijn is naar deze organisatie. De communicatie over de stand van zaken dient tussen het SSC-ONS en de functioneel beheerder plaats te vinden. Configuratiemanagement en beveiligingswerkzaamheden dienen in deze lijn belegd te worden. Bij escalatie neemt de Demand Manager de communicatie over.

4.1.9.2 Functioneel beheer

De functioneel beheerders zijn verantwoordelijk voor het beheer van de applicaties en het bewaken van de functionaliteiten. De functioneel beheerder werkt als schakel tussen verschillende afdelingen en probeert het operationele en tactische niveau dichter bij elkaar te brengen.

De functioneel beheerder focust op vijf aandachtsgebieden:

- De applicatie functioneel inrichten;
- De applicatie functioneel beheren;
- Gebruikers ondersteunen en ontzorgen;
- Functionele documentatie beheren;
- Informeren en rapporteren.

De samenwerking tussen functioneel beheer en technisch beheer is veranderd sinds de uitbesteding van ICT naar SSC ONS in februari 2020. Er vindt overleg plaats met de volgende functies of rollen:

- Contactpersonen leveranciers en partner;
- Strategisch Adviseur Informatievoorziening;
- Adviseur Informatievoorziening;
- Adviseur Informatiebeveiliging (CISO);
- Key users;
- Contactpersonen gebruikersorganisatie;
- Collega functioneel beheerders (ook van andere gemeenten);
- Technisch applicatiebeheerder vanuit SSC ONS;
- Medewerkers Servicedesk ONS;
- Medewerkers behandelaarsgroepen.

4.1.10 Verantwoordelijkheden eenheid overstijgende informatiesystemen

Applicaties vanuit bedrijfsvoering zijn eenheidsoverstijgende (informatie)systemen binnen de gemeente en worden onder de verantwoordelijkheid van de eenheidsmanager bedrijfsvoering gefaciliteerd en onderhouden. Deze systemen, die door meer dan één gemeentelijk organisatieonderdeel worden gebruikt, bevatten gegevens die door meerdere organisatieonderdelen worden vastgelegd. De gemeente Dalfsen heeft ICT uitbesteed aan het SSC-ONS, waarmee de verantwoordelijkheid voor het technisch beheer en de veiligheid van dit systeemtype bij die partij komt te liggen. De procesverantwoordelijke van een bedrijfsvoering applicatie draagt er zorg voor dat bij het gebruik ervan de wettelijke eisen en de gemeentelijke voorschriften worden nageleefd en dat de verantwoordelijkheden voor beveiliging voor alle betrokken partijen duidelijk omschreven zijn.

De gemandateerd eigenaar maakt minimaal de volgende schriftelijk afspraken met het gemeentelijke organisatieonderdeel of de externe organisatie dat van het eenheidsoverstijgend (informatie)systeem gebruik wordt gemaakt:

- Voorwaarden voor het toegestane gebruik van het eenheidsoverstijgend (informatie) systeem;
- De verantwoordelijkheden van de gebruikende partij binnen zijn organisatieonderdeel voor de gegevens uit het eenheidsoverstijgend (informatie)systeem;
- Voorwaarden met betrekking tot de bescherming van het verwerken van persoonsgegevens;
- Voorwaarden die de gebruikende partij verplichten voorzieningen te treffen voor een passend niveau van informatiebeveiliging;
- Procedure(s) betreffende autorisatie van medewerkers;
- Procedure(s) betreffende toezicht op de naleving van afspraken en oplossen van eventuele geschillen;
- Het recht op inzage in de resultaten van de externe audits en zelfevaluaties bij de gebruikende partij waaruit blijkt in welke mate deze aan het gemeentelijk informatiebeveiligingsbeleid voldoet.

4.1.11 Functionaris gegevensbescherming (FG)

De FG is conform de algemene verordening gegevensbescherming (AVG) de interne toezichthouder op de verwerking van persoonsgegevens binnen de gemeente [18.1.4.1]. Het is in die hoedanigheid een functie; geen rol. De FG heeft de volgende wettelijke taken (art. 39 lid 1 AVG), vertaald naar de situatie bij de gemeente:

- Informeren en adviseren van de gemeenteraad, het college, het directieteam, het managementteam en de medewerkers over hun verplichtingen met betrekking tot gegevensbescherming;
- Toezien op naleving van zowel de AVG als andere wetten met betrekking tot gegevensbescherming, als ook het beleid met betrekking tot de bescherming van persoonsgegevens van de verwerkingsverantwoordelijke of de verwerker. Hierbij hoort tevens toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
- Desgevraagd adviseren omtrent gegevensbeschermingseffect beoordeling, ook wel Data Protection Impact Assessment (DPIA) genoemd, en toezien op de uitvoering daarvan;
- Toezichthouden op de registraties en afhandeling van beveiligingsincidenten waarbij persoonsgegevens betrokken zijn en toezichthouden op het melden van een datalek bij de Autoriteit Persoonsgegevens en bij de betrokkenen;
- Samenwerken met en als contactpunt optreden voor de Autoriteit Persoonsgegevens;

- Rekening houden met risico's naar de aard, omvang en context van verwerkingen van persoonsgegevens;
- Contactpersoon binnen de organisatie;
- Rapporteren aan de hoogste leidinggevende van de verwerkingsverantwoordelijke, zijnde in veel gevallen het college of de burgemeester en in sommige gevallen de gemeenteraad.

De FG heeft voor privacy een toezichthoudende taak, vergelijkbaar met de taak van concerncontroller / controller informatiebeveiliging voor informatiebeveiliging. De uitvoering en implementatie van het beleid is belegd bij de Privacy Officer.

4.1.12 De Privacy Officer

Deze rol is gericht op de uitvoering en de naleving van de Algemene verordening gegevensbescherming (AVG). Daarnaast adviseert de medewerker over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.

De Privacy Officer heeft in ieder geval de volgende verantwoordelijkheden:

- Beoordelen van de verwerking van persoonsgegevens tegen de achtergrond van de kaders van privacywetgeving en adviseert het directieteam en het managementteam bij wijzigingen in procesuitvoering, bedrijfsvoering en de toepassing van een gegevensbeschermingseffect beoordeling (DPIA);
- Als adviserend lid deelnemen aan programma's en projecten waarvan het resultaat gevolgen kan hebben voor de wijze van verwerking van persoonsgegevens;
- Uitleggen van de privacyvoorschriften in de AVG en de sectorale wetgeving;
- Coördineren van de privacywerkzaamheden, informeren en het verzorgen van meldingen bij de FG;
- Coördineren, samenvoegen en openbaar maken van de overzichten van gegevensverwerkingen die worden aangeleverd door de organisatieonderdelen van de gemeente;
- Coördineren van verzoeken om inzage, correctie en verzet ten aanzien van persoonsgegevens en adviseren over de afhandeling;
- Rapporteren aan het directieteam;
- Inrichten van procedures voor het afhandelen van datalekken waarbij persoonsgegevens betrokken zijn;
- Beheer en onderhoud van de standaarddocumenten voor verwerkersovereenkomsten, convenanten en reglementen;
- Adviseren en ondersteunen bij het besluitvormingsproces en het afsluiten van verwerkersovereenkomsten en convenanten en de vaststelling van reglementen.

4.1.13 De medewerkers

Alle medewerkers dragen *verantwoordelijkheid* voor de beveiliging van de activiteiten die behoren tot hun eigen functie en taken. Zij betrachten zorgvuldigheid en discipline bij het omgaan met informatie en (informatie)systemen. Zij zijn zich bewust van de eisen ten aanzien van de betrouwbaarheid, de integriteit, de beschikbaarheid en de controleerbaarheid van de informatieprocessen waarbij zij zijn betrokken. In het tactisch informatiebeveiligingsbeleid zijn gedragsregels in het kader van informatiebeveiliging uitgewerkt. Iedere medewerker wordt geacht deze gedragsregels te kennen en uit te dragen bij het uitoefenen van zijn of haar functie.

4.2 Overleg en afstemming

4.2.1 Overleg informatiebeveiliging

Binnen de gemeente Dalfsen wordt minimaal twee maal per jaar een intern overleg informatiebeveiliging georganiseerd. De CISO is voorzitter van het overleg. Bij dit overleg zijn aanwezig:

- De CISO;
- De concerncontroller / controller informatiebeveiliging;
- De adviseur Informatievoorziening;
- Beveiligingsbeheerders t.a.v.: BRP/Waardedocumenten, BAG, BGT, BRO, SUWI en DigiD;
- Beveiligingsbeheerders t.a.v.: FZ, DIV en HR;
- Privacy Officer en FG;
- Applicatie- en functioneel beheerders;
- Demand Manager ICT.

Omdat de ICT is uitbesteed aan het SSC-ONS, vindt ook daar afstemmingsoverleg plaats op het vlak van informatiebeveiliging: het BTO-overleg. Hierbij zijn de CISO's van alle aan het SSC gelieerde organisaties aanwezig, tezamen met de CISO en de TISO vanuit het SSC-ONS.

4.2.2 Overleg informatiebeveiliging en privacy
Maandelijks overleggen de CISO, de FG en de Privacy Officer over tactische en operationele zaken. Ieder kwartaal zal concern controller / controller informatiebeveiliging uitgenodigd worden.

4.2.3 Incidentteam
Het incidentteam heeft tot taak het onderzoeken en afhandelen van mogelijke beveiligingsincidenten, waaronder datalekken. Het komt in actie zodra er een informatiebeveiligingsincident is geconstateerd of aangemeld.

Het team bestaat uit de CISO, de Privacy Officer, concerncontroller / controller informatiebeveiliging en de voor het incident verantwoordelijke proceseigenaar en de beveiligingsbeheerder. De FG neemt deel als adviseur. Indien nodig wordt het team per casus uitgebreid met andere specialisten (Demand Manager ICT, HR, juridisch, communicatie, etc.)

4.2.4 Overleg CISO - I-advies
Maandelijks overleggen de CISO en de adviseur(s) informatiemanagement over ontwikkelingen en tactische en operationele zaken binnen de organisatie, waaronder wijzigingen van en het aanschaffen van nieuwe ICT-voorzieningen.

4.3 Informatiebeveiligings-crisisbeheersing
Voor interne crisisbeheersing dient een kernteam informatiebeveiliging geïnstalleerd te zijn. Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten (gebeurtenis die een zodanige verstoring van informatiesystemen of processen tot gevolg heeft, dat aanzienlijke maatregelen moeten worden genomen om het oorspronkelijke werkingsniveau te herstellen). Het directieteam stelt vast in welke gevallen en door wie contacten met autoriteiten (brandweer, toezichthouders, IBD [12.6.1, 6.1.3.3] enz.) wordt onderhouden [6.1.3]. De criteria voor de handels- en werkwijze tijdens grote incidenten of calamiteiten worden nader in een procedure dan wel Business Continuity Plan uitgewerkt. Het kernteam bestaat in ieder geval uit:

- Gemeentesecretaris/algemeen directeur (voorzitter);
- CISO;
- On-Demand Manager ICT;
- De verantwoordelijke beveiligingsbeheerder (afhankelijk van het incident of de calamiteit);
- Relevante experts (indien nodig);
- Een lid van team Communicatie.

5. Bijlagen

5.1 Bijlage 1: Rollen en namen van de informatiebeveiligingsorganisatie gemeente Dalfsen

Rol	Naam	Vervanger
Ciso	Marcel Stam	-
Concerncontroller Controller Informatieveiligheid	Paula Everloo	-
Beveiligingsbeheerder BRP	Hans van Scheepen	-
Beveiligingsbeheerder WD	Hans van Scheepen	-
Beveiligingsbeheerder BAG	Arnout Boer	-
Beveiligingsbeheerder BGT	Arnout Boer	-
Beveiligingsbeheerder BRO	Arnout Boer	-
Beveiligingsbeheerder DigiD	Gerrit Huisman	-
Security Officer SUWI	Rianne de Kroon	-
Beveiligingsbeheerder Facilitair Beheer	Marcel Heerink	-
Beveiligingsbeheerder ICT / Demand	Marcel Stam	-
Beveiligingsbeheerder DIV	Heleen Karchoud	-
Beveiligingsbeheerder HR	Hetty Krul	Linda IJsseldijk
Privacy Officer	Anne-Lisa Karzijn	Marcel Stam, Maarten de Man
Functionaris Gegevensbescherming	Maarten de Man	-

5.2 Bijlage 2: Overzicht van wet- en regelgeving onderliggend aan informatiebeveiliging (niet uitputtend)

- Auteurswet
- Telecommunicatiewet
- Ambtenarenwet
- Wet computercriminaliteit
- Algemene verordening gegevensbescherming (AVG)
- Archiefwet / Archiefregeling
- Beveiligingsnorm DigiD
- Databankenwet
- Wet elektronisch bestuurlijk verkeer
- Wet elektronische handtekeningen
- Wet algemene bepalingen Burgerservicenummer
- Paspoortwet
- Paspoortuitvoeringsregeling Nederland (PUN)
- Reglement Rijbewijzen
- Wet basisregistratie personen (Wet BRP)
- Wet openbaarheid bestuur (Wob)
- Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI)
- Wet Basisregistratie Adressen en Gebouwen (BAG)
- Wet Basisregistratie grootschalige topografie (BGT)
- Wet Basisregistratie Ondergrond (BRO)
- Wet Kenbaarheid Publiekrechtelijke Beperkingen (WKPB)
- Wet Politiegegevens (Wpg)
- Wet ruimtelijke ordening (Wro)

5.3 Bijlage 3: Classificatietabel dataclassificatie

Classificatietabel			
Niveau	**Vertrouwelijkheid**	**Integriteit**	**Beschikbaarheid**
Geen / 0 **(geen schade)**	**Openbaar** Informatie mag door iedereen worden ingezien *(bijv: algemene informatie op de website, openbaar gemaakte stukken)*	**Niet zeker** Informatie mag worden veranderd, er zijn geen garanties m.b.t. de juistheid of volledigheid van de informatie *(bijv: templates en sjablonen)*	**Niet nodig** Gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn (MTD* meerdere weken) *(bijv: ondersteunende tools als routeplanner)*
Laag / I **(enige schade)**	**Bedrijfsvertrouwelijk** Informatie die door alle medewerkers van de organisatie mag worden ingezien *(bijv: informatie op het intranet, zakelijke contactgegevens van medewerkers)*	**Beschermd** Onjuiste of onvolledige informatie heeft nauwelijks impact op processen, informatie moet hooguit opnieuw worden verzameld *(bijv: interne (management) rapportages, verzamelde publieke informatie)*	**Belangrijk** Informatie mag incidenteel niet beschikbaar zijn (MTD* 2 weken) *(bijv: administratieve gegevens, zoals personeelsadministratie, factuurverwerking)*
Midden / II **(serieuze schade)**	**Vertrouwelijk** Informatie die door een kleine groep medewerkers (zoals een afdeling of een (project)team) mag worden ingezien, voor zover nodig voor hun taken *(bijv: overige persoonsgegevens, BSN, aanbestedings-, handhavings-, en vergunningsinformatie, financiële procesgegevens, integriteitsprocedures, specifieke informatie over beveiliging)*	**Hoog** Onjuiste of onvolledige informatie leidt tot verkeerde beslissingen en heeft impact op processen *(bijv: salarisadministratie, primaire procesinformatie zoals vergunningen, handhavingsinformatie,)*	**Noodzakelijk** Informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk (MTD* 1 week) *(bijv: primaire proces informatie)*
Hoog / III **(zeer grote schade)**	**Geheim** Informatie die alleen door medewerkers met een specifieke rol of functie mag worden ingezien, voor zover nodig voor hun taken en waartoe zij toegang hebben op basis van rol of functie *(bijv: gezondheids-/medische en justitiële gegevens, informatie die beschermd moet worden tegen statelijke actoren)*	**Absoluut** Onjuiste of onvolledige informatie kan grootschalige juridische consequenties hebben of leiden tot een crisissituatie met aanzienlijke financiële schade *(bijv: specifieke gemeentelijke informatie op de website o.a. informatie waaraan rechten zijn te ontlenen, beschikkingen en besluiten)*	**Essentieel** Informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten (MTD* 1 dag) *(bijv: basisregistratie BRP, crisisbeheersing)*

5.4 Bijlage 4: Uitleg Basisbeveiliging niveaus BIO

- Basisbeveiligingsniveau 1 (BBN 1)

Dit is het niveau waaraan alle overheidssystemen minimaal dienen te voldoen. Denk daarbij aan het volgen van wet- en regelgeving, de AVG en algemene beheersmaatregelen. Op dit niveau gaat het over openbare en niet-gevoelige informatie.

- Basisbeveiligingsniveau 2 (BBN 2)

Bij dit niveau ligt de focus op bewuste bescherming van veelgebruikte informatie. Op dit niveau wordt namelijk vertrouwelijke informatie verwerkt en ook is het zo dat incidenten kunnen leiden tot commotie. De veiligheid van andere systemen is op dit niveau bovendien afhankelijk van de veiligheid van het eigen systeem.

- Basisbeveiligingsniveau 3 (BBN 3)

Een BBN-score van 3 is van uitzonderlijk niveau. Op dit niveau vindt actieve bescherming van vertrouwelijke en kritische informatie plaats. Dit betreft zeer gevoelige informatie waarbij verlies ervan zeer grote impact heeft. Volgens de IBD is deze, naast enkele uitzonderingen, doorgaans niet van toepassing op gemeentelijke processen en informatiesystemen. Op het moment dat deze score van toepassing is, zijn er aanvullende maatregelen nodig aanvullend op de BIO-norm welke voortvloeien uit een diepgaande risicoanalyse.

5.5 Bijlage 5: De 10 bestuurlijke principes voor informatiebeveiliging (VNG Realisatie; 2019)

5.5.1 Bestuurders bevorderen een veilige cultuur

Menselijk gedrag en cultuur beïnvloeden op significante wijze alle aspecten van risicomanagement op elk niveau en in elk stadium.
Zonder open cultuur waar iedereen vrij is om te spreken, is het niet goed mogelijk om risico's te identificeren en als de risico's niet bekend zijn, kunt u ze ook niet adresseren. Als u in uw organisatie een cultuur bevordert waarin mensen zich vrij voelen om risico's te melden en maatregelen voor te stellen, dan kunt u adequaat reageren op dreigingen en samenhangende risico's.

5.5.2 Informatiebeveiliging is van iedereen

Passende en tijdige betrokkenheid van belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties in aanmerking worden genomen. Dit resulteert in een verbeterd bewustzijn en goed geïnformeerd risicomanagement.
Iedereen moet betrokken worden bij risicomanagement, in alle lagen van de organisatie. Maak gebruik van de kennis en verantwoordelijkheid van proces- en systeem eigenaren. Gebruik uw Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG) en concerncontroller / controller informatiebeveiliging als onafhankelijke adviseur en laat ze samenwerken in een risicoteam, waar u vanzelfsprekend ook zitting in heeft. Laat uw interne communicatie aandacht besteden aan het verspreiden van de boodschap, het belang en het voordeel van risicomanagement binnen uw organisatie. Goed uitgevoerd risicomanagement creëert waarde voor de organisatie omdat de kwaliteit van besluiten toeneemt en de kans op falen afneemt.

5.5.3 Informatiebeveiliging is risicomanagement

Risicomanagement wordt bewust toegepast bij alle organisatie activiteiten.
Risicomanagement werkt alleen als het geïntegreerd is in alle werkprocessen van de organisatie. Dat kan alleen bereikt worden als risico's regelmatig op de agenda staan en als risico's een plek/paragraaf krijgen in alle bestuurlijke documenten. Maak lijnmanagers verantwoordelijk voor risicomanagement door afspraken met ze te maken over uw risicobereidheid. Lijnmanagers zijn verantwoordelijk voor de maatregelen en rapportage daarover.

5.5.4 Risicomanagement is onderdeel van de besluitvorming

Risicomanagement is onderdeel van alle besluiten en risicomanagement is chefsache.
U kunt als bestuurder alleen de juiste richting aangeven als informatie u bereikt. Door dreigingen en risico's mee te nemen in de vragen die u stelt aan uw managers kunt u er in uw beslissingen ook rekening mee houden. Zo kunt u bijsturen voordat risico's manifest worden en escalatie voorkomen.

5.5.5 Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking

Het risicomanagementproces is aangepast en staat in verhouding tot de externe en interne context van de organisatie die verband houdt met haar doelstellingen.
Het risicomanagementproces moet passen bij de organisatie en ondersteunen aan de organisatiedoelstellingen. De keten is zo sterk als de zwakste schakel. De gemeente dient met ketenpartners en leveranciers regelmatig het gesprek te voeren over risico's en de maatregelen die ervoor zorgen dat de risico's tot een acceptabel niveau worden teruggebracht.

5.5.6 Informatiebeveiliging is een proces

Risico's kunnen ontstaan, veranderen of verdwijnen als de externe en interne context van een organisatie verandert. Risicomanagement detecteert en anticipeert op die veranderingen en gebeurtenissen op een gepaste en tijdige manier.
Risicomanagement moet een cyclisch, iteratief en terugkerend proces zijn, want dreigingen veranderen, doelstellingen veranderen, de omgeving verandert en wetgeving verandert. Indien u in uw risicomanagement geen rekening houdt met een veranderende omgeving, dan zijn uw maatregelen op termijn wellicht niet doeltreffend of doelmatig.

5.5.7 Informatiebeveiliging kost geld

Risico's moeten behandeld worden en er zijn vele manieren om veiligheid te realiseren, maar aan alle zijn kosten verbonden.
Risico's kunt u ontwijken, mitigeren, overdragen of wegnemen door het nemen van preventieve-, repressieveen/of correctieve maatregelen. Welke strategie u ook kiest, ze kosten allemaal middelen in termen van tijd en geld. Voor maatregelen kan derhalve een kosten-batenanalyse worden gemaakt.

5.5.8 Onzekerheid dient te worden ingecalculeerd

De input voor risicomanagement is gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen. Risicomanagement houdt expliciet rekening met eventuele beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn verbonden. Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden.
Zonder goede informatie kunt u geen goede risico-inschattingen en besluiten nemen. Zonder goede en tijdige informatie bent u niet bekend met de risico's die uw organisatie loopt.

5.5.9 Verbetering komt voort uit leren en ervaring

Risicobeheer wordt voortdurend verbeterd door leren en ervaring.
Risicomanagement gedijt het beste in een organisatie die leert van ervaringen en op basis hiervan verbeteringen doorvoert. Hoe goed u uw informatiehuishouding ook beveiligt, incidenten zullen altijd voorkomen. Door te zoeken naar verbeterpunten en de wil om te leren bouwt u doorlopend aan het verhogen van uw digitale weerbaarheid.

5.5.10 Het bestuur controleert en evalueert

Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen.
Controle is belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn in de organisatie. Naast verslagen en managementrapportages zijn incidenten, en dan vooral de manier waarop ze afgewikkeld worden, een goede graadmeter om te zien hoe de organisatie Vereniging van Nederlandse Gemeenten 7 omgaat met het onderwerp. Medewerkers kunnen erop vertrouwen dat besluiten op bestuursniveau genomen worden, wanneer de situatie daar om vraagt.