Strategisch informatiebeveiligingsbeleid

Gemeente Aa en Hunze

2023-2025

Colofon

Naam document
Strategisch informatiebeveiligingsbeleid gemeente Aa en Hunze 2023-2025.docx

Versienummer
4.0

Classificatie
Bedrijfsvertrouwelijk

Versiedatum
11-10-2023

Versiebeheer
Het beheer van dit document berust bij de CISO van de gemeente Aa en Hunze.

Versie	Wijziging	Datum wijziging	Auteur
1.0	Creatie, kopie van IBD	december 2013	A. Bijvoet
1.1	Diverse kleine wijzigingen inhoud; incl. versiebeheer	februari 2014	A. Bijvoet
1.11	Figuur 1 aangepast aan rollen	maart 2014	A. Bijvoet
1.12	Tekstuele aanpassingen	april 2014	E. Muntinga
1.13	Invulling geven aan de beveiliging voor de gemeente Aa en Hunze	januari 2015	E. Muntinga
1.14	Beleid afstemmen met Assen en Tynaarlo	maart 2015	E. Muntinga
2.0	Geplande herziening van het strategisch Informatiebeveiligingsbeleid	september 2018	A. Bijvoet
2.1	Verwerken opmerkingen Edwin Muntinga (snelle versie DigiD)	september 2018	A. Bijvoet
2.2	Verwerken opmerkingen Marcel en Aaldert (snelle versie DigiD)	september 2018	A. Bijvoet
2.3	Concept voor College (snelle versie DigiD)	oktober 2018	A. Bijvoet
2.4.1	Verwerken opmerkingen Aaldert, Edwin en Bert, Wouter	november 2018	A. Bijvoet
2.4.2	Aanpassingen n.a.v. overleg directie team	december 2018	A. Bonder
2.5	Tekstuele wijzigingen consistentiecheck	december 2018	E. Muntinga
3.0	Regulier update, aanpassingen aan de BIO	september 2020	A. Bijvoet
3.1	N.a.v. eerste ronde feedback collega's; rond gestuurd	november 2020	A. Bijvoet
3.2.2	N.a.v. terugkoppeling Tonnie Vos	december 2020	A. Bijvoet
3.3.1	N.a.v. terugkoppeling DT / Riëtte de Nekker	februari 2021	A. Bijvoet
3.3.2	Vaststelling door gemeentesecretaris	18 februari 2021	A. Bijvoet
3.7	Geplande herziening van het strategisch informatiebeveiligingsbeleid	juli 2023	M. Bloeming
3.8	Verwerken opmerkingen Lianne Smit	augustus 2023	M. Bloeming
3.9	Rollen toegevoegd en bestaande rollen verder uitgewerkt	september 2023	M. Bloeming
4.0	Strategisch informatiebeveiligingsbeleid 2023-2025	oktober 2023	M. Bloeming

Inhoudsopgave

1. Inleiding

Met dit 'strategisch informatiebeveiligingsbeleid 2023-2025' zet de gemeente Aa en Hunze een volgende stap om de beveiliging van haar informatievoorziening[1] te continueren. Het beleid wordt ten minste één keer in de drie jaar geëvalueerd en indien nodig herzien. Indien er nog geen nieuw beleid is vastgesteld, blijft het vastgestelde beleid van kracht. De gemeentesecretaris stelt het beleid vast, waarna het beleid in werking treedt en het eerder vastgestelde strategisch informatiebeveiligingsbeleid vervangt. Daar waar aanvullend beleid ontbreekt, wordt de Baseline Informatiebeveiliging Overheid (BIO) gevolgd.

Binnen de gemeente Aa en Hunze werken we met veel informatie van inwoners, ondernemers, medewerkers en (keten)partners. Deze gebruiken we voor het goed uitvoeren van de gemeentelijke taken. Men moet er op kunnen vertrouwen dat medewerkers van de gemeente Aa en Hunze zorgvuldig en veilig met informatie omgaan en dat er sprake is van een betrouwbare informatievoorziening die steunt op betrouwbare informatiesystemen[2].

Risico's. Technologische ontwikkelingen, een complexere samenleving en bijkomende bedreigingen van buitenaf, stellen doorlopend eisen aan de bescherming van informatie van de gemeente Aa en Hunze. Het dreigingsbeeld van informatiebeveiliging voor Nederlandse gemeenten 2023-2024[3], die trends in beveiligingsdreigingen geeft, onderstreept dit.

De BIO. Aan de basis van dit informatiebeveiligingsbeleid ligt de Baseline Informatiebeveiliging Overheid (BIO) die per januari 2020 in werking is getreden. De werkwijze van de BIO is gericht op eigenaarschap, risicomanagement en het ontwikkelen van vaardigheden. De verwachte nieuwe versie van de BIO is uitgesteld naar eind 2024.

Beleidsonderdelen. Dit informatiebeveiligingsbeleid bevat de beleidsuitgangspunten, rollen en verantwoordelijkheden, eigenaarschap, risicomanagement en bewustwording voor de gemeente Aa en Hunze.

[1] **Informatievoorziening** is het geheel aan activiteiten dat voor een organisatie moet worden uitgevoerd om iedereen de informatie te verstrekken die nodig is om toegewezen functies te vervullen. Binnen de informatievoorziening bevinden zich informatiesystemen.
[2] **Informatiesysteem**: een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie. Informatie op papier kan ook deel uitmaken van een informatiesysteem.
[3] https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2023-2024/

2. Belang van informatiebeveiliging voor Aa en Hunze

Informatie is één van de voornaamste bedrijfsmiddelen van de gemeente Aa en Hunze. De continuïteit van bedrijfsvoering en kwaliteit van data is van groot belang. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering maar ook leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor inwoners, bedrijven, partners en de eigen organisatie met waarschijnlijk ook politieke consequenties. Informatieveiligheid is daarom van groot belang.

Visie

Een betrouwbare[4] en flexibele informatievoorziening is noodzakelijk voor het trefzeker meebewegen van de organisatie van de gemeente Aa en Hunze in het steeds complexere speelveld waarin de gemeente acteert. Medewerkers krijgen hierbij de ruimte en het vertrouwen om te doen wat nodig is om resultaten te bereiken. Hierbij zijn 21e-eeuwse vaardigheden en het bewust en veilig omgaan met informatie essentieel. Hierbij steunen we op de AVG[5] en de BIO[6] en borgen deze risicogericht in de organisatie. Informatiebeveiliging is een kerntaak van de gemeente Aa en Hunze waarbij we er continu voor zorgen dat 'de basis op orde' is en blijft. We zijn zo een digitaal weerbare organisatie voor onszelf, blijven een betrouwbare ketenpartner en inwoners en ondernemers kunnen zo op ons rekenen. De komende jaren zet de gemeente Aa en Hunze zich daarom verder in om informatieveiligheid verder te borgen.

Het proces van informatiebeveiliging is primair gericht op de bescherming van gemeentelijke informatie, zowel intern, binnen samenwerkingsverbanden[7] als in de cloud, met digitale ketenpartners.

Door vooraan bij nieuwe ontwikkelingen betrokken te zijn, worden privacy en informatieveiligheid een logisch onderdeel van deze nieuwe ontwikkelingen zodat er weinig extra lasten zijn. Als bijvoorbeeld bij onderhandelingen over clouddiensten de juiste afspraken worden gemaakt en vastgelegd over informatieveiligheid en privacy, kan de regie op deze clouddienst goed worden uitgevoerd.

De focus bij informatiebeveiliging ligt op veilig omgaan met informatie (uitwisseling) in alle verschijningsvormen, zoals elektronisch, op papier en mondeling. Het gaat niet alleen over bescherming van persoonsgegevens, maar ook over bescherming van vitale maatschappelijke functies die worden ondersteund met informatie (verkeer, vervoer, openbare orde en veiligheid, etc.). Het gaat bij informatieveiligheid zeker niet alleen over ICT. Het gaat ook over verantwoordelijkheid, actuele kennis, houding en gedrag van medewerkers ten aanzien van het gebruik van informatie(systemen).[8]

Als laatste genoemd, maar niet de minste, gaat informatieveiligheid over het proces van de continuïteit van de bedrijfsvoering (dienstverlening).

[4] Met betrouwbaar wordt bedoeld: beschikbaarheid (continuïteit van de bedrijfsvoering), integriteit (juistheid, volledigheid) en vertrouwelijkheid (geautoriseerd gebruik) van gegevens en informatie.
[5] AVG: Algemene Verordening Gegevensbescherming. Europese verordening die de bescherming van persoonsgegevens in alle Europese landen regelt.
[6] BIO: baseline informatiebeveiliging overheid. De basis voor informatiebeveiliging die elke overheidsorganisatie moet invoeren.
[7] SDA, Stichting Attenta, WPDA, RUD, VRD …
[8] Medewerker = (1) ambtenaar in de zin van het Ambtenarenreglement of (2) degene die op arbeidsovereenkomst of anderszins betaalde of niet-betaalde werkzaamheden voor de gemeente Aa en Hunze verricht.

3. Doel en scope informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid richt zich op de aspecten techniek, organisatie en mens. Dit houdt in dat dit beleid alle gemeentelijke processen, onderliggende informatiesystemen, procesautomatisering, 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 omvat. Dit beleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de AVG, UAVG, Wpg, BRP, PNIK/PUN, DigiD 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) en DigiD met norm B.01 eisen. Deze worden in aanvullende onderliggende beleidsdocumenten geformuleerd.

Doelstelling. De strategische doelen van dit informatiebeveiligingsbeleid zijn:

- Het management van de gemeente Aa en Hunze sturing te geven op informatiebeveiliging
- Aan wet- en regelgeving te voldoen
- Risicobeheersing voor informatiebeveiliging te borgen
- De verantwoordelijkheden voor informatiebeveiliging te beleggen
- Adequate bescherming van bedrijfsmiddelen en persoonsgegevens
- Risico's van menselijk gedrag te minimaliseren
- Ongeautoriseerde toegang te voorkomen
- Correcte en veilige informatievoorzieningen te garanderen
- Toegang tot informatiesystemen te beheersen
- Veilige informatiesystemen te waarborgen
- Adequaat te reageren op incidenten
- (Kritieke) bedrijfsprocessen te beschermen
- Een basis te bieden voor doorontwikkeling van de organisatie
- Naleving van dit beleid te waarborgen

Techniek. Ten aanzien van het aspect techniek heeft dit informatiebeveiligingsbeleid betrekking op alle technische middelen waarmee toegang tot informatie kan worden verschaft. Ook de informatiesystemen waar wij als gemeente gebruik van maken vallen hieronder. Daarnaast geeft techniek ons de middelen in handen om de beschikbaarheid, integriteit en vertrouwelijkheid van deze informatie goed te regelen.

Organisatie. Op het vlak van de organisatie gaat informatiebeveiliging over de processen, procedures en afspraken om mens en techniek met elkaar te verbinden, zowel binnen de gemeente, als tussen de gemeente en inwoners, ondernemers en ketenpartners. Hierbij is het van belang dat informatiebeveiliging en privacy aan de voorkant wordt meegewogen.

Mens. Menselijk gedrag is één van de belangrijkste aspecten op het gebied van informatiebeveiliging. Wanneer technische maatregelen zijn getroffen, is het aan de mensen die werken met de technische middelen om hier op een verantwoorde manier mee om te gaan. Op het gebied van 'de mens' zijn verschillende groepen van belang: inwoners, medewerkers en ketenpartners.

Inwoners maken gebruik van de systemen van de gemeente bij de afname van dienstverlening. Voor hen willen we als gemeente veilig omgaan met informatie. We werken mee aan een weerbare digitale samenleving en ondersteunen onze inwoners hierin. Van medewerkers wordt verwacht dat zij 21^{e}-eeuwse vaardigheden beheersen, zich bewust zijn van de mogelijke risico's en op een veilige manier omgaan met informatie. Medewerkers krijgen de ruimte en het vertrouwen om hierin te doen wat nodig is. Waar nodig kunnen zij op ondersteuning rekenen van het management. Met ketenpartners is het van belang dat de juiste afspraken worden gemaakt, vastgelegd en getoetst.

4. Beleidsuitgangspunten

Bepaalde beleidsuitgangspunten zijn van belang voor informatiebeveiliging bij de gemeente Aa en Hunze. De belangrijkste staan hieronder beschreven.

Informatiebeleidsplan 2023 – 2026[9]

Hierin staat beschreven hoe we samen werken aan een flexibele, veilige en beheersbare informatiehuishouding. De gemeente werkt hieraan volgens 5 sporen: Persoonlijk & Toegankelijk, Open & Transparant, Datagedreven, Flexibel & Wendbaar, Veilig & Verantwoord. Dit zijn dan ook de onderwerpen waar informatiebeveiliging zich de komende jaren op richt.

Agenda Digitale Veiligheid 2022-2026

Vanuit het programmaplan Agenda Digitale Veiligheid 2022-2026 ligt de focus op de volgende trends: 'eigen huis op orde', de voorbereiding op digitale ontwrichting, incidenten en crises, het versterken van de weerbaarheid van inwoners en ondernemers, leiderschap: het aangaan van bestuurlijke gesprekken en professionalisering en digitale veiligheid in Europa.

Dreigingsbeeld 2023-2024

Voor het opstellen van plannen voor informatiebeveiliging, is het van belang een actueel beeld te hebben van de risico's en dreigingen. Het dreigingsbeeld van informatiebeveiliging voor Nederlandse gemeenten[10] is hier een belangrijke bron voor.

De grootste risico's voor gemeenten op basis van dit dreigingsbeeld zijn:

- Uitval van dienstverlening en bedrijfsvoering
- Vertrouwelijke informatie in verkeerde handen
- Fouten in de dienstverlening

Het actuele dreigingsbeeld schetst 3 soorten dreigingen die de huidige trend zijn:

- Meer ransomware met destructievere gevolgen
- Steeds meer en ernstiger kwetsbaarheden in software
- Gevaren in ketens uit het zicht

Denk bijvoorbeeld aan de kwetsbaarheid Log4J, die wereldwijd bij bijna elke organisatie aanwezig was en zeer snel misbruikt kon worden. Door aanwezigheid van deze kwetsbaarheid ook bij cloud-leveranciers kwam inzicht in impact veelal langzaam op gang.

Risicogericht werken op basis van de BIO

De Baseline Informatiebeveiliging Overheid (BIO) is het normenkader voor de gehele overheid en is gericht op risicomanagement. Het beveiligen van informatie is een structureel proces waarbij steeds de Plan-Do-Check-Act (PDCA) cyclus wordt doorlopen. De eerste stap in het proces is het maken van een inschatting van mogelijke schade (**impact**) als informatiesystemen (tijdelijk) niet beschikbaar zijn, de informatie niet integer is en/of deze informatie in verkeerde handen valt. De schaal voor impact is klein, midden en groot. Ook wordt een inschatting gemaakt van de **kans** dat dreigingen zich voordoen, waartegen de gemeente beschermd moet worden. De schaalindeling hiervoor is laag, midden en hoog. Kans X Impact resulteert in een inschaling van het **risico**. Langs deze lat worden risico's geprioriteerd en op volgorde van prioriteit behandeld.

De inschatting van mogelijke schade en dreigingen leidt tot beveiligingseisen per informatiesysteem om het risico te beperken. Zonder expliciete analyse is altijd basisbeveiligingsniveau 2 (BBN2) van toepassing voor de beveiliging van informatie(systemen). De BIO geeft maatregelen die gebruikt kunnen worden. Om eisen

[9] https://aaenhunze.bestuurlijkeinformatie.nl/Document/View/7719aa97-348f-4214-9139-e9beaaa0403b

[10] https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2023-2024/

af te dekken, te beginnen met de grootste risico's, wordt aan de verantwoordelijke teamleider – en eventueel gedelegeerde – een advies gegeven om bepaalde maatregelen te (laten) treffen. Ook kan het (rest)risico worden geaccepteerd door de verantwoordelijke teamleider binnen zijn/haar mandaat. Voor hoge restrisico's wordt daarvoor gebruik gemaakt van een risicoacceptatie overeenkomst (RAO). Alle risico's worden geregistreerd in het risicoregister.

Tenslotte moet verantwoording worden afgelegd over de risicoafweging en over de effectieve invulling van de maatregelen zoals beschreven in het risicoregister. Deze verantwoording is onderdeel van de bestuurlijke verantwoording over de beveiliging van informatiesystemen. De wijze en mate van detail van de verantwoording hangt af van het risico. Des te hoger het risico, des te meer detail nodig is in verband met de hogere potentiële impact. Het risicoregister worden periodiek besproken met de teamleider Facilitaire Zaken en de concerncontroller; ook als lid van het directieteam (DT). Met het management (MT) worden de grootste risico's periodiek besproken via de kwartaalrapportages. Hierbij zijn zowel de verantwoordelijke teamleiders, als het DT aanwezig. Indien nodig wordt een risico separaat geagendeerd bij het MT.

De risicogerichte benadering uit de BIO zorgt ervoor dat de beveiliging van informatie(systemen) bij de gemeente bevorderd wordt op de plekken waar dat het meest belangrijk is. Zo kan men erop vertrouwen dat gegevens van de gemeente, in lijn met wet- en regelgeving, passend beveiligd zijn.

Handelingsperspectief voor management

Om deze risico's voor de gemeente Aa en Hunze tot een acceptabel niveau terug te brengen, is het van belang vooraf bij de Privacy & Security Officer (PSO) en Chief Information Security Officer (CISO) advies in te winnen. En voor wat privacy betreft natuurlijk ook van de Functionaris Gegevensbescherming (FG). In het advies staan de bij het proces betrokken medewerkers en teamleiders centraal. De verantwoordelijke teamleider besluit vervolgens over de risicobehandeling.

Een open en veilige cultuur staan voorop en zijn doorslaggevend in deze risicobehandeling. Door naar de beveiligingsrisico's van interne processen te kijken kunnen fouten het best worden voorkomen. Beloning van veilig werken is een sleutel tot succes. Bij het veilig werken door medewerkers verwacht je bewustzijn, het hebben van voldoende kennis en deze kennis ook toepassen. Hierbij geven management en bestuur het goede voorbeeld. Ze reiken daarbij de juiste middelen aan en zorgen ervoor dat de basis op orde is.

Daarnaast zorgt een teamleider - als dit vanwege wet- of regelgeving nodig is - voor het vaststellen van aanvullend beleid of informatiebeveiligingsprocedures voor zijn team. De aanwezigheid van dit beleid is dan verplicht en wordt uitgevraagd bij IT-audits en beveiligingsonderzoeken. De invulling van de maatregelen komt uit de BIO. Daar waar geen aanvullend beleid is vastgesteld, wordt de BIO gevolgd en geldt basisbeveiligingsniveau (BBN) 2.

De 10 principes voor informatiebeveiliging[11]. De 10 principes 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 behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

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 bestuurstafel.

Procedure voor het afhandelen van kwetsbaarheden, datalekken en beveiligingsincidenten

Een informatiebeveiligingsincident vindt plaats wanneer de beschikbaarheid, vertrouwelijkheid of integriteit van informatie wordt verstoord. Denk aan inbrekers, (stroom-)storingen, het ontbreken van een back-up en het achterlaten van een document bij een printer. Als bij dit soort incidenten persoonsgegevens betrokken zijn, dan is er mogelijk sprake van een datalek[12]. Voor de afhandeling hiervan is een separate procedure opgesteld. Deze wordt regelmatig geëvalueerd en zo nodig aangepast. De procedure voor het afhandelen van kwetsbaarheden, datalekken en beveiligingsincidenten (procedure KDB) van de gemeente Aa en Hunze is vastgelegd in een aanvullend document. Incidenten uit het verleden worden geëvalueerd en gebruikt als input voor het actualiseren van het beleid.

De gemeente Aa en Hunze is aangesloten bij de Informatiebeveiligingsdienst (IBD) en heeft hiervoor een ACIB[13] en een VCIB[14] aangesteld. De IBD informeert de ACIB en de VCIB over kwetsbaarheden, dreigingen en beveiligingsincidenten (ook specifiek voor Aa en Hunze). Bepaalde beveiligingsincidenten van Aa en Hunze worden gedeeld met de IBD. Ook informeert het NCSC[15] de gemeente Aa en Hunze regelmatig en in geval van incidenten over informatiebeveiliging.

[11] https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf
[12] Bij een **datalek** gaat het om ongeoorloofde of onbedoelde toegang tot persoonsgegevens. Maar ook om het ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgegevens. Ook hierdoor kunnen de betrokken personen namelijk schade leiden.
[13] ACIB: algemeen contactpersoon informatiebeveiliging. Ontvangt informatie over algemene meldingen, kwetsbaarheden, dreigingen en incidenten.
[14] VCIB: vertrouwd contactpersoon informatiebeveiliging. Ontvangt informatie over algemene en vertrouwelijke meldingen, kwetsbaarheden, dreigingen en incidenten.
[15] NCSC: Nationaal cybersecurity center.

5. Rollen en verantwoordelijkheden

Alle medewerkers hebben in het dagelijks werk te maken met risico's op het vlak van informatiebeveiliging. De medewerker gedraagt zich daarbij verantwoordelijk en wordt hierbij gecoacht door de teamleider. De uitvoering van informatiebeveiliging is een verantwoordelijkheid van de teamleiders (het lijnmanagement). Alle informatiebronnen- en systemen die in de werkprocessen gebruikt worden door de gemeente Aa en Hunze hebben een interne eigenaar die vertrouwelijkheid, privacyeisen en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid van informatie ligt dan ook bij de eigenaar van de informatie: de teamleider. De eindverantwoordelijkheid ligt bij de gemeentesecretaris.

Three Lines Model. Om de naleving van het beleid verder te verbeteren is de organisatie van informatiebeveiliging ingericht op basis van het zogenaamde 'Three Lines Model' (eerder bekend als 'Three Lines of Defence'). In dit model is het lijnmanagement (teamleiders) verantwoordelijk voor het realiseren van informatiebeveiliging en privacy binnen de eigen processen (1e lijn). Zij geven hier – samen met de medewerkers in hun team – uitvoering aan. De Privacy & Security Officer (2e lijn) helpt en adviseert waar nodig de teamleiders en medewerkers met het implementeren van dit beleid (tactisch/operationeel niveau). De CISO (3e lijn) controleert of de gemeente Aa en Hunze aan het informatiebeveiligingsbeleid voldoet en adviseert het management (strategisch/tactisch niveau) . Hierbij geeft de CISO een oordeel met mogelijkheden tot verbetering. De uitwerking van de rollen is in de volgende paragrafen opgenomen.

Medewerker

Het is de verantwoordelijkheid van elke medewerker van de gemeente Aa en Hunze (zowel vast als tijdelijk, intern of extern) om van het informatiebeveiligingsbeleid, procedures, standaarden en de diverse maatregelen omtrent informatiebeveiliging op de hoogte te zijn en deze na te leven. Dit houdt ook het op tijd melden van datalekken en beveiligingsincidenten in. Zie hiervoor ook de Gedragscode van de Gemeente Aa en Hunze. Medewerkers nemen kennis van de bewustwordingsmaatregelen en/of trainingen over informatiebeveiliging. Ze gaan veilig om met informatie van de gemeente Aa en Hunze als onderdeel van hun 21e-eeuwse vaardigheden. Waar nodig spreken we elkaar aan op onveilig gedrag. De teamleider coacht en ondersteunt de medewerkers hierbij.

Functioneel beheer (FB)

Functioneel beheerders spelen een belangrijke rol binnen informatiebeveiliging, voornamelijk op organisatorisch vlak en in het volgen van het informatiebeveiligingsbeleid. Zij hebben diverse cruciale taken waaronder: het functioneel inrichten en onderhouden van informatiesystemen, het uitdelen van autorisaties en het uitvoeren van controles op informatiesystemen. Daarnaast is een functioneel beheerder aanspreekpunt voor de gebruikers van het informatiesysteem en bijbehorende leverancier en automatisering. De functioneel beheerder is niet eindverantwoordelijk voor het informatiesysteem en bijbehorende processen. Het proces- en systeemeigenaarschap is belegd bij de teamleider.

Automatisering (AUT)

Automatisering (AUT) heeft een belangrijke rol binnen informatiebeveiliging, voornamelijk op technisch vlak en in het volgen van het informatiebeveiligingsbeleid. Zij hebben verschillende cruciale taken waaronder: het technisch inrichten van informatiesystemen, het technisch beheren van interne informatiesystemen en het uitvoeren van technische maatregelen om risico's te beperken. Daarnaast is automatisering aanspreekpunt op technisch vlak voor de informatiesystemen die intern bij de gemeente draaien. Automatisering is hiervoor echter niet eindverantwoordelijk. Het proces- en systeemeigenaarschap is belegd bij de teamleider.

Teamleider (TL)

De verantwoordelijkheid voor het voldoen aan het gemeentelijke informatiebeveiligingsbeleid en alle onderliggende informatiebeveiligingsvereisten op operationeel niveau ligt – in de eerste lijn – bij de teamleiders. Teamleiders zijn daarbij eigenaar van het proces en de bijbehorende risico's. De teamleiders

rapporteren aan het directieteam over de uitvoering en borging van de informatiebeveiligingsvereisten. Teamleiders maken met hun betrokken medewerkers een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente hebben en welke risico's er zijn. Op basis van deze inschatting stelt het directieteam vast welke risico's de gemeente loopt en voor welke risico's aanvullende maatregelen worden getroffen. Deze acties worden opgenomen in het risicoregister. Het is de rol van de teamleiders om het informatiebeveiligingsbeleid uit te dragen in de organisatie, de medewerkers hierin te ondersteunen en de naleving ervan te bewaken. Taken die hierbij horen zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures
- Het voldoen aan wet- en regelgeving die op hun processen van toepassing is en invulling geven aan de rollen die binnen die wet- en regelgeving bedacht is
- Het binnen de eigen afdeling uitdragen van het informatiebeveiligingsbeleid en de daaraan gerelateerde procedures
- Het vroegtijdig betrekken van de PSO, CISO en/of FG bij nieuwe of gewijzigde processen
- Het (laten) uitvoeren van risicoanalyses voor de processen waar zij verantwoordelijk voor zijn
- Bespreking van rapportages over beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen

Concerncontroller

De concerncontroller overziet de hele bedrijfsvoering, bijbehorende risico's en is lid van het DT. De CISO en de FG hebben zes-wekelijks een overleg met de concerncontroller en teamleider Facilitaire Zaken over het risicoregister. Tijdens dit overleg worden risico's voor informatieveiligheid (risicoregister), strategische trends en ontwikkelingen op het vlak van informatiebeveiliging en de voortgang van het jaarplan informatiebeveiliging besproken. Indien nodig bespreekt de concerncontroller deze risico's met het DT.

Gemeentesecretaris (GS)

De gemeentesecretaris, de algemeen directeur, stuurt op informatiebeveiliging en is hiervoor ambtelijk eindverantwoordelijk. De gemeentesecretaris is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan het college van B&W. Bij grote informatiebeveiligingsincidenten en datalekken speelt de gemeentesecretaris ook een rol. Het afhandelen hiervan, en rollen, is opgenomen in onderliggende procedures.

Portefeuillehouder (PH)

De burgemeester is portefeuillehouder voor informatiebeveiliging en is hiervoor bestuurlijk eindverantwoordelijk. Het college van B&W legt jaarlijks verantwoording af over informatiebeveiliging aan de gemeenteraad.

Chief Information Security Officer (CISO)

De Chief Information Security Officer (CISO) houdt vanuit een onafhankelijke positie toezicht op de naleving van informatiebeveiliging uitgaande van de BIO en dit beleid. De CISO heeft een interne rol en adviseert management en medewerkers gevraagd en ongevraagd over bijzonderheden, trends en ontwikkelingen rondom informatiebeveiliging. De CISO houdt zich dan ook bezig met organisatorische maatregelen en ontwikkelingen. De CISO is aanspreekpunt voor de interne en externe organisatie m.b.t. informatiebeveiliging en werkt op strategisch en tactisch niveau (3^{e} lijn). Hierbij focust de CISO zich op (de complexere) advisering rondom informatiebeveiliging. Bewustwording in de organisatie is een belangrijk onderdeel hiervan. De CISO adviseert bij projecten, het beheersen van risico's en het opstellen van rapportages. Verder beoordeelt en controleert de CISO onafhankelijk in welke mate de gemeente voldoet aan het informatiebeveiligingsbeleid (o.a. via de ENSIA). Dit wordt gerapporteerd aan de gemeentesecretaris. In periodieke overleggen met de GS en PH wordt de informatiebeveiliging van gemeente Aa en Hunze besproken.

Privacy & Security Officer (PSO)

De Privacy & Security Officer (PSO) heeft een interne rol en adviseert met name op de uitvoering. Bijvoorbeeld bij het nemen van beveiligingsmaatregelen. De PSO is aanspreekpunt voor de interne organisatie m.b.t. informatiebeveiliging en privacy en werkt op tactisch en operationeel niveau (2e lijn). Hierbij ligt de focus op advisering en bewustwording rondom informatiebeveiliging en privacy. De PSO houdt de registers in het ISMS bij, voert analyses uit en stelt procedures en verwerkersovereenkomsten op. Daarmee ondersteunt de PSO de implementatie van de BIO en bijbehorend beleid in de organisatie. De PSO signaleert risico's en brengt deze onder de aandacht bij de eigenaar. Daarbij werkt de PSO nauw samen met de CISO en FG. Ook organiseert de PSO het wekelijkse privacy & security overleg.

6. Vaststelling strategisch informatiebeveiligingsbeleid

Dit strategisch informatiebeveiligingsbeleid treedt in werking na vaststelling door het college van B&W.