

Informatiebeveiligingsbeleid

Gemeente Aa en Hunze

2020-2022

Colofon

Naam document

Strategisch informatiebeveiligingsbeleid gemeente Aa en Hunze 2020-2022-
v3.3.2.docx

Versienummer

3.3.2

Classificatie

Bedrijfsvertrouwelijk

Versiedatum

18 februari 2021

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 nav. 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

Inhoud

Inhoud	3
1. Inleiding	4
2. Belang van informatiebeveiliging voor Aa en Hunze.....	5
3. Doel en scope informatiebeveiligingsbeleid	7
4. Beleidsuitgangspunten	8
5. Rollen en verantwoordelijkheden	12
6. Sturing en verantwoording	13
7. Omgang met aanvullend beleid en procedures	15
8. Evaluatie en wijziging van het beleid	15
9. Vaststelling informatiebeveiligingsbeleid	16
Bijlage A: Toelichting aanvullend beleid en procedures	17

1. Inleiding

Met dit 'informatiebeveiligingsbeleid 2020-2022' zet de gemeente Aa en Hunze een volgende stap om de beveiliging van haar informatievoorziening¹ te continueren.

Binnen de gemeente Aa en Hunze werken we met veel informatie van inwoners, ondernemers, medewerkers en (keten)partners. Deze gebruiken we voornamelijk 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 er sprake is van een betrouwbare informatievoorziening die steunt op betrouwbare informatiesystemen².

Risico's. Technologische ontwikkelingen, een grotere digitale overheid, een complexere samenleving en bijkomende bedreigingen van buitenaf, stellen andere eisen aan de bescherming van informatie van de gemeente Aa en Hunze om de informatieveiligheid te borgen. Het dreigingsbeeld van informatiebeveiliging voor Nederlandse gemeenten 2021-2022³, die trends in beveiligingsdreigingen geeft, onderstreept dit. Het dreigingsbeeld schetst beveiligingsrisico's voor de ambtelijke organisatie, het openbaar bestuur, de politiek, de inwoners en ondernemers van de gemeente Aa en Hunze. Dit informatiebeveiligingsbeleid draagt bij aan het verminderen van deze risico's en stelt daarvoor kaders en geeft hiervoor aanwijzingen.

De BIO. Een belangrijke andere ontwikkeling die aan de basis ligt van dit informatiebeveiligingsbeleid is 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.

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-2021-2022/>

2. Belang van informatiebeveiliging voor Aa en Hunze

Informatie is één van de voornaamste bedrijfsmiddelen van de gemeente Aa en Hunze. 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. Informatiebeveiliging (IB) is het proces dat dit belang dient.

Visie

Een betrouwbare⁴ 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, dingen in het werk anders te doen, waarbij elke medewerker zich bewust is van het veilig omgaan met informatie en dit in het werk laat zien. Hierbij steunen we op de AVG⁵ en de BIO⁶ 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 we een betrouwbare ketenpartner en kunnen inwoners en ondernemers op ons rekenen. De komende jaren zet de gemeente Aa en Hunze daarom verder in om de informatieveiligheid te borgen. Om de doorontwikkeling van informatieveiligheid te borgen en beter te sturen op resultaten, wordt aangesloten bij de P&C cyclus en maken we gebruik van een ISMS.

Het proces van informatiebeveiliging is primair gericht op de bescherming van gemeentelijke informatie, zowel intern, binnen samenwerkingsverbanden⁷ 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 er bijvoorbeeld bij de onderhandelingen over cloud diensten 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 ook zeker niet alleen over ICT. Maar ook over verantwoordelijkheid, actuele kennis, houding en gedrag van medewerkers ten aanzien van het gebruik van informatie(systemen).⁸

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, BSDA, Attenta, RUD, ...

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.

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

3. Doel en scope informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid van de gemeente Aa en Hunze heeft de volgende doelstelling en kaders.

Doelstelling van dit informatiebeveiligingsbeleid is om:

- Het DT van de gemeente Aa en Hunze sturing te geven op informatiebeveiliging
- Te voldoen aan wet- en regelgeving
- Risicobeheersing voor informatiebeveiliging te borgen
- De verantwoordelijkheden voor informatiebeveiliging te beleggen
- Een basis te bieden voor doorontwikkeling van de organisatie

Deze doelen worden verder in dit document uitgewerkt in de beleidsonderwerpen.

Het informatiebeveiligingsbeleid richt zich op de aspecten techniek, organisatie en mens.

Techniek. Ten aanzien van het aspect techniek (IT) heeft dit informatiebeveiligingsbeleid betrekking op alle technische middelen waarmee toegang tot informatie kan worden verschaft. Daarnaast geeft techniek ons de middelen in handen om de vertrouwelijkheid, betrouwbaarheid en integriteit van deze informatie goed te regelen.

Organisatie. Ten aanzien van het aspect organisatie gaat de 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 en ondernemers.

Bewustzijn. Medewerkers staan centraal en werken steeds meer flexibel digitaal. Ze zijn zich hierbij bewust van informatiebeveiliging en laten dit zien in het werk en de resultaten. Als de techniek en de organisatie flexibel ingericht zijn, maar medewerkers laten gevoelig informatie in de digitale omgeving 'rondslingeren' of melden geen datalekken, dan staan alle technische maatregelen en procedures buiten spel. Het gedrag van mensen en daarmee het bewustzijn van de medewerkers is de zwakste schakel in de beveiligingsketen. Ten aanzien van het aspect mens heeft dit informatiebeveiligingsbeleid betrekking op alle medewerkers van de gemeente Aa en Hunze, maar ook op de inwoners en bezoekers die gebruik maken van een informatiesysteem van de gemeente.

4. Beleidsuitgangspunten

De onderstaande beleidsuitgangspunten zijn van belang voor informatiebeveiliging bij de gemeente Aa en Hunze.

Strategische toekomstvisie 2025, Collegeprogramma 'Samen Doen 2018-2022'

Het College geeft vorm aan bestuur en 'Samen Doen' door een creatief en innovatief klimaat te stimuleren waarbinnen inwoners de ruimte krijgen om ideeën te ontwikkelen en uit te voeren die bijdragen aan een prettige en toekomstbestendige leefomgeving. De basis hiervoor is vertrouwen, maatwerk, ruimte, integraliteit en samenwerking.

Inwoners, ondernemers, dorpsbelangen en andere organisaties kennen hun eigen omgeving, weten wat er past en nemen daarom zelf steeds vaker het voortouw. Hierdoor komen veel nieuwe vormen van samenwerking tot stand waarbij ook wordt geëxperimenteerd met andere manieren van samenwerken.

Bij het kiezen en opzetten van de samenwerkingsvorm, denken we ook al na over de informatiebeveiliging en nemen we daarin verantwoordelijkheid in de gekozen samenwerkingsvorm.

Organisatieontwikkeling 'Aa en Hunze stroomt'

In onze organisatie ontwikkeling werken we eraan om de effectief en efficiënt werkende organisatie te worden die in staat is om te voldoen aan de behoefte en wensen van inwoners, bedrijven en politiek.

De maatschappij verandert en inwoners en bedrijven verwachten niet altijd meer een strak regulerende en regisserende gemeente Aa en Hunze, maar allerlei vormen van participatie. We gaan anders werken. Van buiten naar binnen denken, doen en communicatie met inwoners en bedrijven is steeds meer digitaal.

Dit kan alleen succesvol zijn als ook de informatieveiligheid geborgd is. Medewerkers staan hierin centraal en nemen de verantwoordelijkheid om veilig om te gaan met informatie van de gemeente Aa en Hunze. Digitale vaardig zijn van medewerkers van de gemeente Aa en Hunze blijft een kerncompetentie waar doorlopend aan gewerkt moet worden om 'de basis op orde' te houden.

Dreigingsbeeld 2021-2022

Voor het opstellen van plannen voor informatiebeveiliging, is het van belang een goed beeld te hebben van de risico's. Het dreigingsbeeld van informatiebeveiliging voor Nederlandse gemeenten is een bron hiervoor.

Het dreigingsbeeld van informatiebeveiliging voor Nederlandse gemeenten 2021-2022 van de Informatiebeveiligingsdienst, de IBD⁹ onderdeel VNG, laat zien dat er een aantal soorten dreigingen naar voren komen zowel van binnen als van buiten de gemeente. Dit geldt ook voor de gemeente Aa en Hunze. Deze dreigingen geven diverse risico's voor de ambtelijke organisatie, het openbaar bestuur, de politiek, de inwoners en ondernemers van gemeenten.

⁹ [Het handelingsperspectief](#) van het dreigingsbeeld 2021-2022 is te vinden op pagina's 16 t/m 18.

Risico's voor de ambtelijke organisatie

Bij het dagelijks werken met informatie(systemen) komen de grootste informatie-beveiligingsrisico's naar voren. Hierdoor wordt het borgen van integriteit en vertrouwelijkheid steeds groter. Het betreft hier bijvoorbeeld fraude en onbedoelde mailing. Het belang van plannen voor bedrijfscontinuïteit wordt vanwege het toenemende ICT gebruik groter. Zie ook de Citrix kwetsbaarheid¹⁰ die bij gemeenten grote verstoring van de bedrijfsvoering met zich meebracht. Maar ook de impact van Covid-19 die ervoor heeft gezorgd dat digitaal thuiswerken meer regel dan uitzondering is geworden. De Cyberaanval bij 't Hof van Twente begin december 2020 zorgt *(op moment van schrijven nog steeds)* voor een maandenlange verstoring van de dienstverlening, hoge herstelkosten en imagoschade.

Risico's voor het bestuur en de politiek

Bestuurders krijgen in hun werk veel gevoelige informatie onder ogen. Voor informatieveiligheid is het belangrijk dat naast de medewerkers van de gemeente Aa en Hunze, ook de bestuurders zorgvuldig omgaan met deze informatie. De risico's zijn hier met name kans op imagoschade, financiële schade en schade aan de democratische processen.

Risico's voor de inwoners en de ondernemers

Inwoners en ondernemers van de gemeente Aa en Hunze zijn voor veel zaken afhankelijk van de overheid, zorg, werk, voorzieningen, inkomen, jeugdzorg, ed. Uitlekken van betrokken informatie levert veel schade op. Uitval van ICT systemen kan voor inwoners en ondernemingen serieuze gevolgen hebben. Beïnvloeding door een lek in de beveiliging van procesautomatisering voor bruggen, gebouwen en verkeerslichten kan tot ontwrichting leiden.

Voor deze risico's is een handelingsperspectief opgenomen in het dreigingsbeeld 2021-2022 van de IBD.'

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 Functionaris informatiebeveiliging (FIB) en CISO advies in te winnen. Hierin staan 'de medewerkers en teamleiders centraal bij het nemen van besluiten over risico's. Door naar de beveiligingsrisico's van de interne processen te kijken kunnen fouten het best worden voorkomen.

Een open en veilige cultuur staan voorop en zijn doorslaggevend in de risicobehandeling. Beloning van veilig werken is een sleutel tot succes. Bij het veilig werken door medewerkers verwacht je bewust zijn, voldoende kennis hebben en kunnen toepassen er wordt verwacht dat management en bestuur het goede voorbeeld geven. Ze reiken daarbij de juiste middelen aan en zorgen er voor dat de ICT basis op orde is. Daarbij wordt uitgegaan van de onderstaande risicogerichte benadering van de gemeente Aa en Hunze.

¹⁰ <https://www.ncsc.nl/actueel/nieuws/2020/januari/13/vele-nederlandse-citrix-servers-kwetsbaar-voor-aanvallen>

Risicogerichte benadering

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 teamleider, die eindverantwoordelijk is voor de werkprocessen.

Het beveiligen van informatie is een structureel proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen. Het doorlopen van dit proces is een verantwoordelijkheid van het lijnmanagement waar de CISO en de FIB uitvoering aan geven. De CISO meer aan de strategische-/tactische kant en de FIB meer tactisch-/ operationeel.

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 hiervoor 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 afgehandeld.

De inschatting van mogelijke schade en dreigingen leidt tot beveiligingseisen per informatiesysteem om het risico te beperken. Het uitgangspunt is daarbij basisbeveiligingsniveau 2 (BBN 2). Of dit niveau passend is kan getoetst worden met de BBN-toets. De BIO schrijft voor welke maatregelen per geval van toepassing zijn op het informatiesysteem. Om deze eisen af te dekken, te beginnen met de grootste risico's, wordt aan de eindverantwoordelijke teamleider –en eventueel gedelegeerde- een advies gegeven om bepaalde maatregelen te (laten) treffen. Ook kan het (rest)risico worden geaccepteerd door de verantwoordelijk teamleider binnen zijn mandaat. Voor hoge restrisico's wordt daarvoor gebruik gemaakt van een risicoacceptatie overeenkomst (RAO). Alle risico's worden geregistreerd in het risicoregister. Het risicoregister wordt regelmatig met DT besproken.

Ten slotte moet verantwoording worden afgelegd over de risicoafweging en over de effectieve invulling van de maatregelen. 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. Van de grootste risico's wordt de teamleider middelen periodiek geïnformeerd, zodat deze indien nodig geagendeerd kunnen worden bij het management.

Deze risicogerichte benadering uit de BIO zorgt er voor dat de beveiliging van informatie(systemen) bij de gemeente bevorderd wordt op de plekken waar dat het meest belangrijk is. Deze teams kunnen erop vertrouwen dat gegevens van de gemeente, in lijn met wet- en regelgeving, passend beveiligd zijn.

Informatiebeveiligingsmaatregelen

De overheid (incl. gemeenten) heeft ISO 27002¹¹ omarmd als framework voor informatiebeveiligingsmaatregelen. De BIO is de vertaling van ISO 27002 vanuit overheidsperspectief. Om te voorkomen dat in gelijke situaties maatregelen worden geselecteerd uit verschillende normenkaders, is het van belang om deze in eerste instantie te selecteren uit de BIO. Dit is dan ook herkenbaar voor ketenpartners van de gemeente Aa en Hunze. Als er uiteindelijk geen passende maatregelen uit de BIO geselecteerd kunnen worden, dan kunnen er andere maatregelen gekozen worden.

Beveiligingsincidenten en datalekken

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 datalek¹². Voor de afhandeling hiervan is een separate procedure opgesteld. Deze wordt regelmatig geëvalueerd en zo nodig aangepast. De procedure voor het afhandelen van beveiligingsincidenten en datalekken van de gemeente Aa en Hunze is vastgelegd in een aanvullend document.

De gemeente Aa en Hunze is aangesloten bij de IBD en heeft hiervoor een ACIB¹³ en een VCIB¹⁴ 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 NCSC¹⁵ de gemeente Aa en Hunze regelmatig en in geval van incidenten over informatiebeveiliging.

Eenduidige Normatiek Single Information Audit (ENSIA)

De gemeente Aa en Hunze verantwoordt zich vanaf 2017 jaarlijks over informatiebeveiliging middels de ENSIA systematiek. Dit gebeurt aan de rijksdiensten over het veilig gebruik van DigiD en SUWInet door een IT-audit. Maar ook aan het college van burgemeester en wethouders (college van B&W) en aan de gemeenteraad op basis van een zelfevaluatie BIO, de gemeentelijke jaarstukken en de 'Collegeverklaring' ENSIA.

¹¹ De ISO 27002 'Code voor Informatiebeveiliging' geeft richtlijnen en principes voor het initiëren, het implementeren, het onderhouden en het verbeteren van informatiebeveiliging binnen een organisatie. Deze standaard is een best practice om informatie- beveiligingsrisico's aan te pakken met betrekking tot vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening. De standaard kan gezien worden als een nadere specificatie van de ISO 27001-standaard.

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 de verantwoordelijkheid om digitaal vaardig te zijn en veilig om te gaan met informatie van de gemeente Aa en Hunze. Ook spreken we elkaar aan op onveilig gedrag. De teamleider coacht en ondersteunt de medewerkers hierbij.

Het management van Aa en Hunze bestaat uit het directie team en de teamleiders. Het bestuur en management van de gemeente Aa en Hunze speelt een cruciale rol bij het uitvoeren van dit strategisch informatiebeveiligingsbeleid.

Betreffende medewerkers met de teamleiders maakt 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 directie team vast welke risico's de gemeente loopt en voor welke risico's aanvullende maatregelen worden getroffen. Deze acties worden opgenomen in een jaarplan/jarenplanning informatiebeveiliging. Op deze manier geeft het management een duidelijke richting aan informatiebeveiliging. Het is de rol van de teamleiders om dit beleid uit te dragen in de organisatie, de medewerkers hierin te ondersteunen en de naleving ervan te bewaken.

Three lines of defence

Om de naleving van het beleid verder te verbeteren is de organisatie van informatiebeveiliging ingericht op basis van het zgn. 'Three lines of defence' model (3LoD). De functionaris informatiebeveiliging (2^e lijn) helpt waar nodig de teamleiders en medewerkers (1^e lijn) met het implementeren van dit beleid. De CISO (3^e lijn) controleert of de gemeente Aa en Hunze aan het informatiebeveiligingsbeleid voldoet. De uitwerking van de rollen is in de volgende paragrafen opgenomen.

Ambtelijke rollen en verantwoordelijkheden

Medewerker

Het is de verantwoordelijkheid van elke medewerker van de gemeente Aa en Hunze om het informatiebeveiligingsbeleid, procedures, standaarden en de diverse maatregelen omtrent informatiebeveiliging op de hoogte te zijn en na te leven. Van medewerkers wordt tevens verwacht dat ze kennis nemen van de bewustwordingsmaatregelen en/of trainingen omtrent informatiebeveiliging.

Teamleider

De verantwoordelijkheid voor het voldoen aan het gemeentelijke informatiebeveiligingsbeleid en alle onderliggende informatiebeveiligingsvereisten op operationeel niveau ligt –in de eerste lijn– bij de teamleiders. De teamleiders rapporteren aan het directieteam over de uitvoering en borging van de informatiebeveiligingsvereisten.

De gemeentesecretaris

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 een aparte procedure.

Directie team (DT)

Een lid van het DT, in de praktijk de concern controller, stemt periodiek af met de CISO over de risico's voor de informatieveiligheid (risicoregister), strategische trends en ontwikkelingen op het vlak van informatiebeveiliging en de voortgang van het jaarplan informatiebeveiliging.

Chief Information Security Officer (CISO)

De chief information security officer (CISO) houdt vanuit een onafhankelijke positie toezicht op de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening, op basis van het informatiebeveiligingsbeleid. De CISO rapporteert hier gevraagd en ongevraagd over aan de gemeentesecretaris. Daarnaast adviseert de CISO over het informatiebeveiligingsbeleid. Verder beoordeelt en controleert de CISO onafhankelijk in welke mate de gemeente voldoet aan het gemeentelijke informatiebeveiligingsbeleid.

Functionaris informatiebeveiliging (FIB)

De FIB is het eerste aanspreekpunt -in de 2^e lijn- voor informatiebeveiliging binnen de organisatie en adviseur voor het management. De FIB adviseert in beginsel over informatiebeveiligingsvraagstukken en helpt bij het opstellen van beleid. Waar nodig schakelt de FIB met de CISO. Daarnaast ondersteunt de FIB de lijn met het uitvoeren van risicoanalyses, het implementeren van beveiligingsmaatregelen en het afleggen van verantwoording over informatiebeveiliging. Verder is de FIB de beheerder van het ISMS, de organisator van het wekelijkse operationeel beveiligingsoverleg en degene die zorgt voor afstemming over bewustwordingscampagnes op het gebied van privacy en informatiebeveiliging.

Bestuurlijke rollen en verantwoordelijkheden

Het college van B&W legt jaarlijks verantwoording af over informatiebeveiliging aan de gemeenteraad conform de ENSIA en laat zich regelmatig informeren over informatiebeveiliging

6. Sturing en verantwoording

Sturing

Dit informatiebeveiligingsbeleid wordt door de directeur van de gemeente Aa en Hunze vastgesteld en is van toepassing op alle bestuursorganen en de ambtelijke organisatie van de gemeente Aa en Hunze. DT kan het College naar behoeven informeren over informatiebeveiliging.

Het college van B&W, de gemeentesecretaris en de teamleiders (c.q. proceseigenaren) sturen op informatiebeveiliging op basis van de volgende uitgangspunten:

1. De gemeentesecretaris stelt het informatiebeveiligingsbeleid vast;
2. De gemeentesecretaris informeert de portefeuillehouder in het college van B&W over het informatiebeveiligingsbeleid;
3. Het college van B&W informeert de raad over informatiebeveiliging;
4. De gemeentesecretaris en de teamleiders voorziet in de noodzakelijke middelen voor de uitvoering van het informatieveiligheidsbeleid;
5. Het informatiebeveiligingsbeleid vormt samen met het Privacybeleid het fundament onder een betrouwbare informatievoorziening.

Borging informatiebeveiligingsbeleid

Om het vastgestelde informatiebeveiligingsbeleid bekendheid en betekenis te geven in de organisatie, worden de teamleiders en de functioneel beheerders daarover geïnformeerd.

Daarnaast wordt het beleid op een voor iedereen in de organisatie goed vindbare plek opgeslagen.

Overlegstructuur informatiebeveiliging en privacy

Vanaf 2019 is er een wekelijks operationeel werkoverleg over privacy en informatiebeveiliging opgezet. De vaste bezetting bestaat uit de informatiemanager, de coördinator van automatisering, de FIB, de FG en de CISO.

Dit overleg kent een agenda en notulen. Vaste agenda punten zijn:

- Incidenten- en datalekken, aantallen en soorten
- Risico's: laag, midden en hoog
- Wijzigingen verwerkingsregister
- Actualiteiten

Naast dit overleg is er een standaard 6 wekelijks overleg met de concerncontroller, ook als lid van DT. In dit gesprek worden risico's uit het risicoregister, bijzonderheden uit het operationeel overleg en strategische ontwikkelingen besproken. Mocht er aanleiding zijn, wordt een onderwerp door de concerncontroller meegenomen voor de verdere bespreking in het DT.

Risico's in het kader van informatiebeveiliging en privacy hebben de teamleider als eigenaar. Deze worden regelmatig besproken met de teamleider en DT.

Aansluiting bij planning en control

Informatiebeveiliging is een continu verbeterproces. Om meer integraal te sturen wordt er aansluiting gezocht bij de planning en control cyclus. Als er aanvullende middelen nodig zijn voor het nemen van beveiligingsmaatregelen, dan dient dit tijdig vastgesteld te zijn zodat dit aan kan sluiten bij de begroting.

In het continu verbeteren wordt ook een ISMS ingezet binnen de gemeente Aa en Hunze.

7. Omgang met aanvullend beleid en procedures

In aanvulling op het informatiebeveiligingsbeleid van de gemeente Aa en Hunze dient er voor diverse specifieke onderwerpen/thema's aanvullend beleid worden opgesteld. Deze onderwerpen/thema's komen uit de BIO. In bijlage A zijn de op te stellen aanvullende beleidsstukken en procedures nader toegelicht.

Daarnaast zorgt een teamleider als dit door wet- of regelgeving nodig is voor het vaststellen van aanvullend beleid of informatiebeveiligingsprocedures voor zijn team. De aanwezigheid van dit beleid is verplicht en wordt uitgevraagd bij IT-audits en beveiligingsonderzoeken. In bijlage A is een lijst opgenomen van aanvullend informatiebeveiligingsbeleid en is dit beleid toegelicht.

Het opstellen van de aanvullende stukken die nog niet aanwezig zijn vereist afstemming vooraf, borging in de organisatie en evaluatie. Dit vereist de nodige aandacht en planning. Deze planning wordt jaarlijks vastgelegd in het jaarplan privacy en informatiebeveiliging.

8. Evaluatie en wijziging van het beleid

Afwijken van het beleid is in beginsel niet toegestaan, wanneer op onderdelen toch wordt afgeweken moet dit gemotiveerd gebeuren. Dit informatiebeveiligingsbeleid treedt in werking na vaststelling door de gemeentesecretaris. Het beleid wordt ten minste één keer in de drie jaar geëvalueerd en indien nodig herzien. Hierbij wordt onder andere gekeken naar de doelmatigheid en doeltreffendheid van het beleid binnen de gemeente Aa en Hunze.

9. Vaststelling informatiebeveiligingsbeleid

Dit Informatiebeveiligingsbeleid treedt in werking na vaststelling door de gemeentesecretaris.
Aldus vastgesteld door de gemeentesecretaris van de gemeente Aa en Hunze:

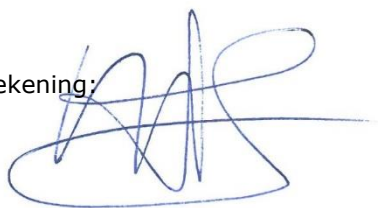
Ondertekening:

Naam: M. Tent

Functie: Gemeentesecretaris

Datum: 19 februari 2021

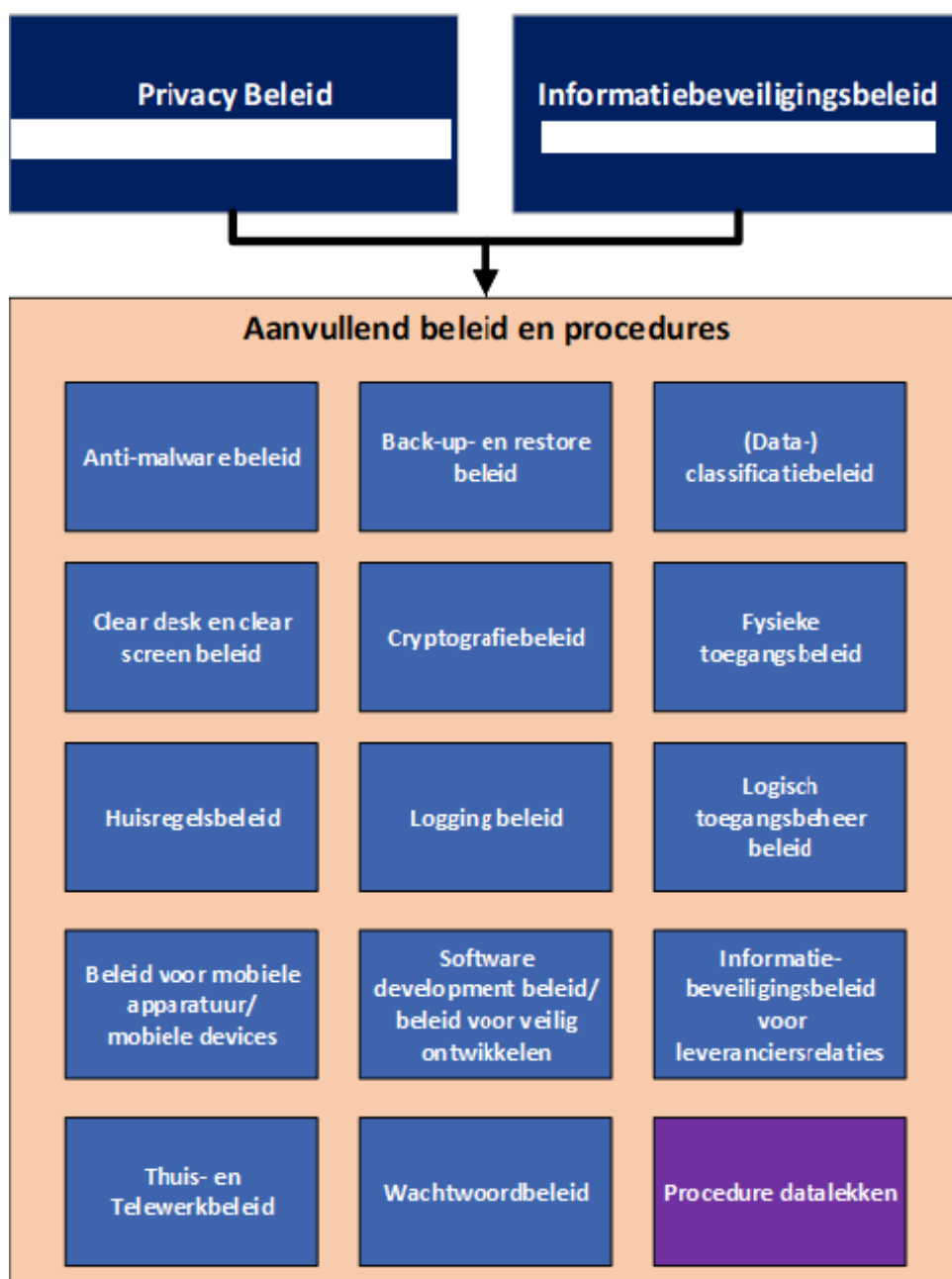
Handtekening:

A handwritten signature in blue ink, consisting of several loops and a long horizontal stroke extending to the right.

Bijlage A: Toelichting aanvullend beleid en procedures

In aanvulling op dit overkoepelend informatiebeveiligingsbeleid van de gemeente Aa en Hunze wordt er beleid opgesteld voor specifieke informatiebeveiligingsonderwerpen, zogenaamd aanvullend themabeleid. De operationele kennisproducten uit de BIO (BIO-OP) worden als handreiking gebruikt voor het opstellen van deze aanvullende beleidsstukken. Op basis van risicoanalyse en/of behoeftebepaling vanuit de gemeentelijke organisatie wordt er een prioritering gemaakt in het opstellen van de diverse aanvullende beleidsstukken. Volgens een planning wordt dit ingevoerd.

Onderstaand het overzicht van de aanvullende informatiebeveiligingsbeleidstukken die worden genoemd in de BIO. Het gaat hierbij om de huidige BIO onderwerpen. Dit is –onder andere door nieuwe ontwikkelingen op het gebied van privacy en informatiebeveiliging– onderhevig aan verandering.



De in bovenstaand overzicht weergegeven aanvullende beleidsstukken worden hieronder kort toegelicht.

Aanvullend beleid	Toelichting
1. Anti-malware beleid	Het anti-malware beleid van de gemeente geeft richting aan de wijze waarop de gemeente maatregelen wenst te treffen voor een adequate detectie, preventie en herstel van verstoringen als gevolg van malware. Malware is een verzamelnaam voor kwaadaardige en/of schadelijke software. De meeste mensen gebruiken het woord virus, maar in feite is virus een soort malware. Malware kan ernstige schade toebrengen aan gemeentelijke systemen en het kan de informatievoorziening verstoren in termen van beschikbaarheid, exclusiviteit en integriteit.
2. Back-up- en restore beleid	Het doel van dit beleid is te voorkomen dat in geval van gedeeltelijk of geheel verlies of beschadiging van data en/of programmatuur de dienstverlening van de gemeente hinder ondervindt. Back-up en restore is een belangrijke beschikbaarheidsmaatregel die ervoor zorgt dat corrupte, verloren of vernietigde bedrijfsinformatie hersteld kan worden.
3. (Data-)classificatiebeleid	Het (data-)classificatiebeleid van de gemeente geeft aanvullende beleidskaders voor het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Hierbij wordt de relatie gelegd naar het BBN niveau van de Baseline informatiebeveiliging overheid (BIO). Classificatie is het toekennen van een beveiligingsniveau aan data met als doel passende maatregelen te treffen.
4. Clear desk en clear screen beleid	Een beleid waarmee ervoor gezorgd wordt dat gevoelige informatie, zowel in fysieke als digitale vorm, niet onbeschermd wordt achtergelaten in persoonlijke en publieke werkruimten zodra iemand de werkplek verlaat. Een Clear Desk Policy betekent simpel gezegd dat er zo min mogelijk op je bureau ligt. Een Clear Screen Policy betekent onder andere dat je als werknemer verplicht bent om je computerscherm te vergrendelen zodra je de werkplek verlaat.
5. Cryptografiebeleid	Versleuteling (encryptie) is een manier om gegevens te beveiligen door ze onleesbaar te maken voor onbevoegden. Dit doe je als informatie niet voor iedereen bestemd is. Ten behoeve van encryptie dienen er binnen de gemeente regels te zijn, die gehanteerd moeten worden als encryptie wordt geïntroduceerd.
6. Huisregels/ huisregelbeleid	Huisregels maken duidelijk aan de klant welke regels er gehanteerd worden binnen het stadhuis. Ze maken ook meteen duidelijk dat afwijkend gedrag niet wordt getolereerd en dat er eventueel stappen kunnen worden ondernomen. Ook voor de medewerkers zijn huisregels van belang. Vastgestelde huisregels bieden houvast en geven duidelijkheid over wat wel en niet getolereerd wordt in de gemeentelijke gebouwen betreffende gedrag e.d..
7. Logging beleid	Ten behoeve van de beveiliging van informatie is er een logging-beleid voor alle gemeentelijke ICT-voorzieningen. Het doel van dit beleid is duidelijke regels neer te leggen die in relatie tot logging genomen moeten worden binnen de gemeente. Informatiesystemen en ICT-infrastructuur genereren loginformatie voor veel activiteiten, soms als normale statusmelding, soms als resultaat van een activiteit van een gebruiker of beheerder maar ook informatie als resultaat van onvoorziene omstandigheden of fouten. Een log beschrijft wat er gebeurt binnen systemen. Tegenwoordig zijn de beschrijvingen van systemen soms zo gedetailleerd dat ze beschrijven waarom een gebeurtenis heeft plaatsgevonden.
8. Fysieke toegangsbeleid	Het doel van dit beleid is te voorkomen dat onbevoegden toegang krijgen tot ruimtes met informatie waar zij geen kennis van behoren te nemen, dan wel dat informatie kan worden aangepast. Het toegangsbeleid spitst

	zich daarnaast toe op de fysieke beveiliging van kantoren, ruimten en faciliteiten.
9. Thuis- en Telewerkbeleid	Ten behoeve van de beveiliging van gemeentelijke systemen en de informatie binnen deze gemeentelijke systemen is dit beleid er op gericht hoe met telewerken omgegaan moet worden. De volgende definitie voor telewerken wordt hierbij gehanteerd: 'onafhankelijk van tijd en plaats werken met behulp van informatie- en communicatietechnologie (ICT), buiten de vaste werkomgeving' van de gemeente.
10. Logisch toegangsbeheer beleid	Ten behoeve van de beveiliging van gemeentelijke informatiesystemen en de informatie binnen deze gemeentelijke informatiesystemen is dit beleid er op gericht hoe met logische toegangsbeveiliging omgegaan moet worden. Logische toegangsbeveiliging is het geheel aan maatregelen welke tot doel hebben, de toegang tot gegevens en informatiesystemen te beheersen zodat gegevens, informatiesystemen en resources worden beschermd tegen ongeautoriseerde acties'. Onder acties wordt onder andere verstaan: raadplegen, verwijderen, wijzigen en gebruik.
11. Software development beleid/ beleid voor veilig ontwikkelen	Er dienen gemeentelijke beleidsregels met betrekking tot goedkeuringsprocedures voor ICT-voorzieningen te zijn.
12. Informatiebeveiligingsbeleid voor leveranciersrelaties	Het inkoopproces is een belangrijk proces binnen gemeenten. Gemeenten zijn namelijk in grote mate afhankelijk van leveranciers. Via contractmanagement moeten de belangen van gemeenten geborgd zijn. Hierbij is het belangrijk dat er goede afspraken worden gemaakt met leveranciers, waaronder over de informatiebeveiliging. Wanneer gemeenten IT-gerelateerde inkopen doen, wordt aanbevolen om gebruik te maken van de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT).
13. Beleid voor mobiele apparatuur/ mobiele devices	Mobiele apparaten zoals smartphones, tablets en laptops worden veelal gebruikt om gemeentelijke informatie in te zien of te verwerken. Dit heeft enerzijds te maken met de informatiesamenleving en het feit dat gemeenten steeds meer digitaal gaan werken en anderzijds verandert het concept van werken waarbij er steeds meer tijd- en plaats onafhankelijk wordt gewerkt. Doordat data op deze mobiele apparaten wordt verwerkt is het belangrijk om beleid te hebben waarin is bepaald hoe hiermee moet worden omgegaan.
14. Wachtwoordbeleid	In de BIO worden wachtwoordeisen benoemd die het nodig maken dat de gemeente in aanvulling op het informatiebeveiligingsbeleid nadere regels stelt ten aanzien van het gebruik van wachtwoorden.

Aanvullende procedures	Toelichting
1. Procedure datalekken	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. Een datalek moet zo snel mogelijk na ontdekking, zo mogelijk binnen 72 uur, worden gemeld bij de Autoriteit Persoonsgegevens. Deze meldingsplicht geldt niet als er geen risico's voor (natuurlijke) personen uit voortkomen. Vanuit de AVG is het verplicht om datalekken intern vast te leggen en te documenteren. Het datalek, de gevolgen van het datalek en de genomen maatregelen moeten worden beschreven.

Toelichting aanvullend beleid op basis van regels

In aanvulling op dit overkoepelend informatiebeveiligingsbeleid en naast het hiervoor genoemde themabeleid gebaseerd op de BIO, is er aanvullend beleid nodig om te voldoen aan wet- en regelgeving.

Onderstaand is een lijst opgenomen met dit aanvullend beleid met toelichting. Deze lijst is –onder andere door nieuwe wettelijke ontwikkelingen of verplichtingen - onderhevig aan verandering. Er wordt hier geen lijst met procedures weergegeven omdat deze nogal omvangrijk kunnen zijn en aan verandering onderhevig.

Aanvullend beleid	Grondslag	Toelichting
1. BRP	artikelen 1.9 t/m 1.13, 4.1 t/m 4.3 Wet BRP, AVG	De Basisregistratie Personen (BRP) bevat persoonsgegevens van (ex)inwoners van Nederland. Alleen organisaties met een publieke of maatschappelijke taak kunnen gegevens uit de BRP. De gemeente houdt persoonsgegevens van inwoners bij in de BRP. Om gegevens in de BRP te mogen gebruiken of bekijken, gelden regels van de Algemene verordening gegevensbescherming (AVG) en de Wet basisregistratie personen (Wet BRP). Regels voor de inrichting, de werking en de beveiliging van de gemeentelijke BRP voorziening zijn opgenomen in de artikelen 1.9 t/m 1.13 van de Wet basisregistratie personen. De artikelen 4.1 t/m 4.3 daaruit stellen regels omtrent het toezicht, onderzoek en informatieverstrekking. Ingevolge -ten minste- de bovenstaande artikelen van de Wet basisregistratie personen dient er aanvullend informatiebeveiligingsbeleid, procedures en werkinstructies te zijn.
2. PUN	PUN, artikelen 90-95	De wetgever stelt eisen aan de opslag, uitgifte en administratie van reisdocumenten. Deze eisen zijn neergelegd in de Paspoortuitvoeringsregeling Nederland 2001, kortweg 'PUN' genoemd. Hoofdstuk XII van deze regeling bevat regels over de beveiliging voor de uitvoering voor de PUN. Ingevolge deze wet dient er aanvullend informatiebeveiligingsbeleid, procedures en werkinstructies te zijn.
3. Suwinet	Specifiek Suwinet-normenkader Afnemers 2017	Voor het uitvoeren van de Wet structuur uitvoeringsorganisatie werk en inkomen, wordt er gebruik gemaakt van de Gezamenlijke elektronische Voorziening Suwinet (GeVS). Bij dit gebruik is het normenkader Afnemers Suwinet van kracht. Dit normenkader vereist een aanvullend beleids(plan).
4. DigiD		Alle organisaties die DigiD gebruiken moeten voldoen aan een beveiligingsnorm. Om de normen te borgen dient er aanvullend operationeel beleid te zijn geformuleerd conform de ICT-beveiligingsrichtlijnen (NCSC, 2015).