gemeente Midden-Groningen

GEMEENTEBLAD

Officiële uitgave van de gemeente Midden-Groningen

Nr. 158528

23 juli

2018

Informatiebeveiligingsbeleid 2018-2021

Het college van burgemeester en wethouders Midden-Groningen;
Gelet op artikel 4:81 Algemene wet bestuursrecht;
Besluit vast te stellen met informatiebeveiligingsbeleid 2018-2021.

1 Inleiding

Onze gemeentelijke organisatie valt of staat met informatie. Of we nu onze rol als dienstverlener, handhaver, beheerder, control, management/ondersteuning, facilitair, ontwikkelaar of politiek orgaan vervullen, we kunnen niets zonder informatie en informatiesystemen.
Daarom is het van belang dat wij onze informatie beveiligen tegen ongewenste toegang, ongewenste wijziging, ongewenste aantasting en de beschikbaarheid garanderen. Onze inwoners kunnen geen andere overheid kiezen en vertrouwen erop dat we hun vertrouwelijke gegevens afdoende beveiligen. Daarom werken we continue aan de informatieveiligheid binnen onze gemeente.

Het gehele gemeentelijk bestuur, zowel de politieke en ambtelijke bestuurders als ook de leidinggevenden, geeft een duidelijke richting aan informatiebeveiliging. Dit doet het bestuur door het tonen van betrokkenheid, het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele gemeente. Dit beleid is van toepassing op alle processen, organisatieonderdelen, objecten (zoals ook gebouwen, gemalen en bruggen), informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid Midden-Groningen (IBB) is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

1.1 Reden voor een actueel Informatiebeveiligingsbeleid

Een aantal landelijke en gemeentelijke ontwikkelingen maken het noodzakelijk, om het Informatiebeveiligingsbeleid te actualiseren en opnieuw vast te stellen:

1. De start van de nieuwe gemeente Midden-Groningen, voortkomende uit de herindeling. Een geldig IB beleid is voor een nieuwe gemeente vereist.
2. Informatiebeveiliging is geen vrijblijvendheid meer, gezien de toenemende cybercrime, waarbij hacks op zowel landelijk- als regionaal niveau vrijwel dagelijks voorkomen. Vanuit het Rijk, de landelijke en Europese politiek wordt daarom veel ingezet om de gemeente op dit gebied te professionaliseren. Zie de verplichtingen vanuit de in november 2013 door de gemeenten aanvaarde VNG-resolutie ‘Informatieveiligheid, als randvoorwaarde voor de professionele gemeente’, zoals het:
    - Aansluiten op de IBD (Informatiebeveiligingsdienst);
    - Implementeren van en expliciet voldoen aan de ‘Baseline voor Informatiebeveiliging Nederlandse Gemeenten’ (BIG) en het;
    - Doorvoeren van ENSIA, als horizontale en verticale verantwoordingsstelsel voor de informatiebeveiliging gebaseerd op de BIG. De verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet) is samengevoegd en gestroomlijnd. Uitgangspunt van ENSIA is de single information audit. Dit betekent dat maar één keer per jaar de zelfevaluatielijst ingevuld dient te worden en de informatie hieruit wordt gebruikt voor de horizontale verantwoording richting gemeenteraad en de diverse verticale verantwoordingslijnen richting departementen. De horizontale verantwoording bestaat uit de zelfevaluatie, een IT-audit, een verklaring van het College van B&W en een passage over informatieveiligheid in het jaarverslag.

3. De opkomst van ‘moderne’ technologieën’, zoals de doorontwikkeling van de digitale (internet)dienstverlening (conform ons ‘Kompas’) en cloudoplossingen, die echter ook weer bedreigingen voor de informatieveiligheid met zich meebrengen (de zogenaamde, inmiddels beruchte cybercriminaliteit). Denk tevens aan de toenemende inzet van mobiele apparaten zoals smartphones en tablets. Zo bieden dergelijke apparaten onze organisatie kansen op het gebied van bereikbaarheid, flexibiliteit en inzet op locatie. Echter, het is zaak om adequaat te handelen in geval bijvoorbeeld

een I-phone ergens ‘vergeten’ of wellicht ontvreemd is. Een goede beveiliging van de mobiele apparaten en de daarop aanwezige gegevens is van een niet te onderschatten wezenlijk belang.

4. De overheveling van rijkstaken naar de gemeenten, zoals de in 2015 in werking getreden decentralisaties. Het gaat hier niet alleen meer om de lokale gemeentelijke informatieveiligheid. De mogelijke bedreigingen en risico’s strekken verder dan het eigen gemeentelijk grondgebied. Deze schaalvergroting en het gebruik van uiterst privacygevoelige gegevens binnen het sociaal domein (denk aan de jeugdzorg), vereist een professionele, integrale aanpak en sturing.

5. Het hebben van een vastgesteld, actueel Informatiebeveiligingsbeleid is een wettelijke (audit)verplichting, voortvloeiende vanuit onder andere de BIG en de wetgeving voor respectievelijk BRP, Digid en Suwi.

1.2 Doel van het document

Dit IBB document beschrijft de beleidsuitgangspunten voor onze gemeente op het gebied van informatiebeveiliging en is afgeleid van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Betreffende Baseline is bedoeld om:

- Gemeenten een gemeenschappelijk, uniform normenkader te bieden om aan alle eisen op het gebied van informatiebeveiliging te kunnen voldoen;
- De auditlast op gemeenten te verminderen;
- Gemeenten een aantoonbaar betrouwbare partner te laten zijn.

Aan de hand van het realiseren en houden aan genoemde beleidsuitgangspunten, bestaande uit beleidsregels en een beschrijving van bijhorende deelbeleidsgebieden, zorgen we ervoor dat de informatieveiligheid in de basis op orde is. Daar staan we voor.

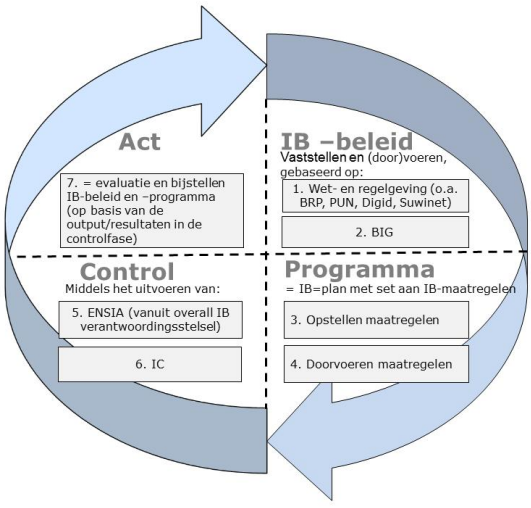
1.3 Uitwerking van het beleid

Dit document dient als kapstok voor verdere uitwerking en inbedding van het informatiebeveiligingsbeleid, de standaarden, de procedures en de processen.

Het Informatiebeveiligingsbeleid is organisatie breed en team overstijgend. Indien noodzakelijk, zullen afzonderlijke taakgebied specifieke IB-maatregelen gehanteerd worden, zoals een afzonderlijke autorisatieplan voor Suwi.

Inbedding zal plaatsvinden door het opstellen en uitvoeren van het Informatiebeveiligingsprogramma Midden-Groningen 2018-2021 met daarin zowel de al genomen (door de drie afzonderlijke gemeenten HSSM) als de nog te nemen concrete maatregelen. Deze maatregelen zullen aan de hand van diverse, zo BIG conform mogelijke analyses (risico-, GAP- en impactanalyse) inzichtelijk gemaakt worden.

Het volgende schema geeft in hoofdlijnen de samenhang en volgordelijkheid tussen het IBB, het op te stellen en uit te voeren programma en toetsing & naleving weer. Gebaseerd op het gangbare model van de PDCA-cyclus (Plan, Do, Check en Act):



2 De beleidsregels informatieveiligheid

Voor het veilig met informatie omgaan, worden voor onze gemeentelijke organisatie de volgende beleidsregels gehanteerd. Deze regels gelden voor alle in- en externe medewerkers van de gemeente, inclusief de politieke en ambtelijke bestuurders:

1. Wachtwoorden zijn strikt persoonlijk

Je wachtwoorden zijn strikt persoonlijk en dienen uitsluitend door jou gebruikt te worden om toegang te krijgen tot de betreffende systemen. Geef je wachtwoord dus niet aan derden of een collega en bewaar ze op een veilige (digitale) plek, dus niet in je agenda of op een geel briefje!

2. Melden van beveiligingsincidenten

Meldt beveiligingsincidenten zo snel als mogelijk via Topdesk. Zie hiertoe het proces melden van beveiligingsincidenten. Denk bij beveiligingsincidenten niet alleen een digitale inbraak door een hacker, maar ook aan een kwijtgeraakte USB-stick (met persoonsgegevens), een verloren of gestolen laptop of als persoonsgegevens naar een verkeerd e-mailadres gestuurd worden. Indien vervolgens blijkt dat het om een datalek gaat (persoonsgegevens in handen gekomen van derden die geen toegang tot die gegevens zouden mogen hebben), dan zijn we verplicht om dit binnen 72 uur bij de Autoriteit Persoonsgegevens te melden, conform de wet meldplicht datalekken.

3. Geheimhoudingsplicht

Binnen diverse teams wordt veelal met persoonsgegevens gewerkt. Voor het werken en de omgang met persoonsgegevens zijn vanuit de overheid diverse regels opgesteld, die zijn verwoord in de Wet bescherming persoonsgegevens (WBP) cq de Europese Privacywetgeving (AVG). Kern van het privacyverhaal is, dat je persoonsgegevens niet verder bekend mag maken dan voor de uitoefening van je functie noodzakelijk is. Dit betreft persoonsgegevens die jou uit hoofde van je functie bekend worden, alsmede overige informatie waarvan je weet of redelijkerwijze kunt vermoeden dat geheimhouding verplicht is. Zie hiertoe ons afzonderlijk privacybeleid- en protocol.

4. Gedragscode Internet- en e-mail-gebruik

De gedragscode Internet- en e-mailgebruik geeft aan hoe de medewerkers behoren om te gaan met Internet en e-mail op de werkplek. Tevens bevat de code regels over de wijze waarop controle op het gebruik van Internet- en e-mail kan plaatsvinden.

Maak gebruik van je eigen gemeentelijke e-mailaccount en stuur geen vertrouwelijke gemeentelijke gegevens door naar een privé e-mailadres.

Wees alert op de zogenaamde phishing e-mails. Open geen e-mails die je niet vertrouwd, dubieus zijn, een bijlage of een link bevatten. Zie hiertoe de met enige regelmaat op het Intranet geplaatste berichtgeving.

NB toegang op het netwerk tot privé e-mail, via de web-mail (zoals gmail.com of outlook.com) is afgeschermd.

5. Kennisnemen van het informatiebeveiligingsbeleid

Het binnen onze organisatie geldende informatiebeveiligingsbeleid en de bijbehorende richtlijnen, instructies en protocollen zijn op iedereen van toepassing. Denk hierbij aan het in- en uitdiensttredingsproces en hoe hiertoe te handelen. Vraag de teamleider voor meer informatie hierover.

6. Beperk het gebruik van mobiele gegevensdragers zoals USB-sticks en externe harddisks

Maak geen gebruik van mobiele gegevensdragers zoals USB-sticks en externe harddisks voor het bewaren of overzetten van vertrouwelijke gegevens. Mocht het toch noodzakelijk zijn, zorg voor versleuteling van deze gegevens en neem dan hiertoe met Automatisering contact op (voor het éénmalig vrijgeven van een USB-poort. De USB-poorten op ons netwerk zijn namelijk standaard uitgeschakeld.

7. Clear desk / clear screen policy

De vertrouwelijke omgang met persoonsgegevens houdt o.a. in dat elke werkplek zodanig is ingericht, dat onbevoegden niet in jou afwezigheid aan deze gegevens kunnen komen. Dat betekent dat jij je thinclientsessie bewust dient te vergrendelen met behulp van de schermvergrendeling (Windows- + L toets tegelijk indrukken), wanneer jij je werkplek verlaat. Ook mogen geen vertrouwelijke gegevens, zoals dossiers of verslagen, onbeheerd op je bureau of bij de printer blijven liggen.

8. Geen vertrouwelijke gegevens in de prullenbak

De correcte omgang met vertrouwelijke gegevens – waaronder persoonsgegevens – is erg belangrijk binnen de gemeente. Ook het vernietigen van deze gegevens moet op een veilige manier plaats vinden.

Daarom zijn er special gekenmerkte papiercontainers aanwezig. Maak hiervan gebruik en stop vertrouwelijke gegevens nooit in de prullenbak of in een bak op je kamer die bestemd is voor oud-papier.

9. Wissel gegevens veilig uit
Wanneer het nodig is om vertrouwelijke informatie naar buiten onze organisatie te sturen, naar bijvoorbeeld een leverancier of zorgpartij, doe dit dan alleen via een beveiligde transfer- of e-mailverbinding tussen onze organisatie en de derde partij. Automatisering kan je hierin faciliteren.

10. Zorg voor een veilig gebruik van je mobiele telefoon
We hebben voor onze bereikbaarheid een mobiele telefoon in bruikleen. Draag ook hier zorg voor een veilig gebruik van de telefoon. Zie hiertoe de richtlijnen telefonie.

11. Veilig thuiswerken
Zorg ook in de thuiswerksituatie voor een veilig gebruik en volg de richtlijnen voor het telewerken. Om veilig vanuit huis op ons gemeentelijk netwerk te kunnen inloggen, maken we gebruik van een tweefactor authenticatie middels een softwaretoken.

12. Aanspreken van onbekende personen
Ben je al een keer in de situatie geweest, dat je iemand binnen het gebouw tegenkwam, waar officieel geen publiek zonder begeleiding mag komen en je niet wist wie deze persoon was en wat zij daar te doen had? Spreek deze persoon aan, stel jezelf voor en vraag, wat hij of zij hier komt doen. Nieuwe collega's, uitzendkrachten of ander ingehuurd personeel stellen het op prijs om aangesproken te worden en op deze manier contacten te kunnen leggen. Echter, personen die niet bevoegd zijn om zich op deze plek te bevinden worden hierdoor op deze overtreding gewezen. Wijs hun beleeft, maar duidelijk, de weg naar het publieke gedeelte van het gebouw en – belangrijk – begeleidt ze daar naartoe.

13. Haast, stress, werkdrukte versus informatiebeveiliging
Informatiebeveiliging krijg je niet gratis – het kost je energie en werkt vaak tegen je als je haast hebt en de werkdrukte hoog is. Echter, informatiebeveiliging is uitermate belangrijk voor je werk en hoort bij de professionele en bekwame uitvoering van het werk. Neem het daarom zeer serieus – onze inwoners vertrouwen erop!

3 Toelichting IB-Beleid

3.1 Wat is Informatiebeveiliging?
Informatiebeveiliging is de verzamelnaam voor de processen en maatregelen, 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 / continuïteit:* het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;

- *exclusiviteit / vertrouwelijkheid:* het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;

- *integriteit / betrouwbaarheid:* het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

Door beleid hierop te voeren, biedt het ons bestuur en management sturing op en ondersteuning voor onze informatiebeveiliging.

3.2 Beleidsdeelgebieden
Ons IBB bevat de volgende deelgebieden, die conform de (strategische variant van de) BIG zijn:
1. Beveiligingsbeleid;
2. Organisatie van informatiebeveiliging;
3. Beheer van bedrijfsmiddelen;
4. Beveiliging van personeel;
5. Fysieke beveiliging en beveiliging van de omgeving;
6. Beheer van communicatie- en bedieningsprocessen;

7. Toegangsbeveiliging (fysiek en logisch);
8. Verwerving, ontwikkeling en onderhoud van informatiesystemen;
9. Beheer van informatiebeveiligingsincidenten;
10. Bedrijfscontinuïteitsbeheer;
11. Naleving.

Het IB-programma wordt conform deze deelgebieden opgesteld.

3.3 Waarom informatiebeveiliging?
Informatie is het belangrijkste bedrijfsmiddel van een gemeente. Toegankelijke en betrouwbare overheidsinformatie is essentieel voor een gemeente, die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt aan burgers en raadsleden en die met minimale middelen maximale resultaten behaalt. De bescherming van waardevolle informatie is hetgeen waar het uiteindelijk om gaat.

3.4 Randvoorwaarden
- Het College, de directie en de teamleiders dragen het beveiligingsbeleid op passende wijze uit aan alle medewerkers.

- De gemeenteraad (op voorstel vanuit het College) zal, met afweging van de kosten, risico's en baten, voldoende middelen beschikbaar stellen om informatiebeveiliging binnen de gehele organisatie te implementeren en de diverse initiatieven uit het IB-programma uit te laten voeren.

- De directie en de teamleiders zullen met de nodige voortvarendheid een herstelactie in gang (laten) zetten wanneer naar aanleiding van een beveiligingsincident of audit blijkt dat het beveiligingsniveau onvoldoende is. Dit om te borgen dat de risicoblootstelling adequaat naar een acceptabel niveau terug wordt gebracht en doen dit in samenspraak met Automatisering en de adviseur Informatiebeveiliging/CISO.

- Een nauwe samenwerking en korte lijnen tussen Automatisering, Informatiemanagement cq CISO is essentieel om adequaat om te kunnen gaan met (aanpassingen in) het beleid en beleidsuitvoering.

- Adequate informatiebeveiliging vereist de betrokkenheid en ondersteuning van het gehele personeel, inclusief externe en tijdelijke medewerkers. Daarom worden jaarlijks de verantwoordelijkheden op het gebied van informatiebeveiliging met alle medewerkers besproken. En daar waar nodig worden medewerkers geïnformeerd en zo nodig opgeleid.

- Om de informatiebeveiliging af te stemmen op interne en externe ontwikkelingen wordt tweejaarlijks een risicoanalyse uitgevoerd. Of zodra wijzigingen in de omgeving, technische wijzigingen of dreigingsveranderingen hier aanleiding voor geven.

- Om ervoor te zorgen dat onze informatiebeveiliging "in control" is en blijft, zal informatiebeveiliging worden opgenomen in de planning en control cyclus en sluit daarbij aan op de in ENSIA gehanteerde verantwoordingssystematiek en bijbehorende termijnen. Concerncontrol toetst in samenspraak met de adviseur Informatiebeveiliging in dat kader of de vastgestelde beveiligingsmaatregelen worden nageleefd.

3.5 Reikwijdte en afbakening informatiebeveiliging
Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, beeldscherm et cetera) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook mensen en processen. Studies laten zien dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral door menselijk handelen en een tekort schietende organisatie. Voorbeelden van informatiebeveiligingsmaatregelen zijn: clear desk- en screenbeleid, wachtwoordenbeleid, beveiligingsincidentenbeheer, beleid ten aanzien in- en uitdiensttreding en maatregelen in het kader van de diverse domeinverplichtingen (zoals vanuit de wet BRP, BAG, Suwi en Digid),en hoe om te gaan met mobiele apparaten en aanwijzingen voor telewerken.

gemeente Midden-Groningen

3.6 Goedkeuring en geldigheid

Dit IBB wordt goedgekeurd door het bestuur (College van B&W) en is geldig tot 1 januari 2021. Indien nodig zal het informatiebeveiligingsbeleid eerder worden herzien.

3.7 Verantwoordelijkheden en taken informatiebeveiliging

- Het College is verantwoordelijk voor de vaststelling en wijziging van het informatiebeveiligingsbeleid en de naleving hiervan.
- De directie is verantwoordelijk voor de vaststelling en wijziging van ons integrale IB-programma en de uitvoering hiervan.
- Ieder team zorgt voor het treffen en naleven van beveiligingsmaatregelen, daar waar nodig en van toepassing binnen het team.
- Alle medewerkers zijn verantwoordelijk voor hun eigen handelen.
- De adviseur informatiebeveiliging/CISO:

- Adviseert de organisatie op tactisch niveau over het informatiebeveiligings- en privacybeleid.
- Draagt zorg voor het opstellen, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid en de daaruit voortvloeiende informatiebeveiligings-plannen en controleert de werking en naleving van het informatiebeveiligingsbeleid en daaruit voortvloeiende maatregelen.
- Draagt zorg voor een samenhangend pakket van maatregelen ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen de gemeenten en de eigen organisatie en initieert periodieke beveiligingsaudits, risico-, afhankelijkheids- en kwetsbaarheidsanalyses.
- Bevordert (o.a. doormiddel van voorlichting) de informatiebeveiliging van de organisatie.
- Signaleert risico's en doet verbetervoorstellen.
    - In ons integrale IB-programma worden specifieke verantwoordelijkheden en taken vastgelegd onder deelbeleidsgebied “Organisatie van informatiebeveiliging”.

3.8 Uitgangspunten IB-beleid

Onze gemeenten hanteren bij het opstellen, uitvoeren en managen van het IBB, de volgende uitgangspunten (ontleend aan de Code voor Informatiebeveiliging (NEN/ISO 27002:2007) en de BIG):

1. De verantwoordelijkheden voor de bescherming van informatie en informatiesystemen en het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn)management (directie en teamleiders), met **het College van B&W als eindverantwoordelijke**.

2. Door **periodieke controle, organisatie brede planning én coördinatie** wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het IB-programma (=plan met uitgewerkte maatregelen) het fundament onder een betrouwbare informatievoorziening. In het IB-programma wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het programma wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.

3. Informatiebeveiliging is een **continu verbeterproces**. ‘Plan, do, check en act’ vormen samen het **management systeem** van informatiebeveiliging.

4. De **adviseur informatiebeveiliging/CISO**, ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de informatieveiligheid en rapporteert hierover.

5. De gemeente stelt de benodigde **mensen en middelen beschikbaar** om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.

6. **Regels en verantwoordelijkheden** voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld. Alle medewerkers van de gemeente worden over het gebruik van beveiligingsprocedures geïnformeerd.

7. 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.

3.9 Doelgroep
Het gemeentelijk IB-beleid is bedoeld voor **alle** in- en externe **medewerkers** van de gemeente inclusief de politieke en ambtelijke bestuurders en tevens voor alle **leveranciers** en (sociale) **ketenpartners**.

3.9.1 Cloud- en externe partijen
- IB-beleid, landelijke normen en wet en regelgeving gelden ook voor externe partijen (leveranciers, ketenpartners) waarmee de gemeente samenwerkt en informatie mee uitwisselt.
- Bij contractuele overeenkomsten gelden in beginsel altijd de gemeentelijke Inkoopvoorwaarden bij IT (GIBIT), waarin onder meer geheimhouding en aansprakelijkheid is geregeld. Afwijkingen op de inkoopvoorwaarden dienen te worden getoetst aan IB-beleid. Vereiste beveiligingsmaatregelen worden aanvullend vastgelegd in contracten en/of bewerkersovereenkomsten. Daarin is onder meer geborgd dat beveiligingsincidenten/datalekken onmiddellijk worden gerapporteerd en dat de gemeente het recht heeft afspraken te (laten) controleren.
- Voor externe hosting van data en/of services gelden naast generiek IB-beleid de landelijke beleidsaandachtspunten vanuit NCSC voor cloud computing verwoord in het document ‘Cloud computing’ door de IBD/VNG. De gemeente is gehouden aan:
  - regels omtrent grensoverschrijdend dataverkeer;
  - toezicht op naleving van regels door de externe partij(en);
  - hoogste beveiligingseisen voor bijzondere categorieën gegevens;
  - melding bij de Autoriteit Persoonsgegevens (AP) bij doorgifte van persoonsgegevens naar derde landen (buiten de EU).

4 Toelichting IB-deelgebieden

4.1 Beveiligingsbeleid

Het belang van informatie(veiligheid)
Informatie is één van de voornaamste bedrijfsmiddelen van onze gemeente. 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 burgers, 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
De komende jaren zet onze gemeente in op het verhogen van informatieveiligheid en verdere professionalisering van de IB-functie in de organisatie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken

Doelstelling
Dit informatiebeveiligingsbeleid (IB-beleid) is het kader voor passende technische, organisatorische en intermenselijke maatregelen om gemeentelijke informatie te beschermen en te waarborgen, dat de gemeente voldoet aan relevante wet en regelgeving. We streven er naar om ‘in control’ te zijn en daarover op professionele wijze verantwoording af te leggen. In control 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 en als laatste dat dit geheel verankerd is in de PDCA-cyclus.

Uitgangspunten
- Het informatiebeveiligingsbeleid van onze gemeente is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

- Het beleid is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002) en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

- Het IB-beleid wordt vastgesteld door het college van B&W. De directie herijkt periodiek het IB-programma aan maatregelen.

- Het uitvoeren van de VNG resolutie 'informatieveiligheid'. Van deze resolutie zijn de belangrijkste punten:
  1. Informatieveiligheid wordt onderdeel van de collegeambities 2018-2021 en wordt opgenomen in de portefeuille van één van de leden van het college van B&W;
  2. Gemeenten zorgen voor verankering van informatieveiligheid op de gemeentelijke agenda, waarbij het college de gemeenteraad informeert;
  3. Bestuurlijke en organisatorische borging van informatieveiligheid, door aansluiting in de planning- en controlcyclus;
  4. De gemeenten maken de lokale invulling rondom het thema van informatieveiligheid transparant voor burgers, bedrijven en (keten)partners; Dit betekent onder andere een jaarlijkse verantwoording richting College en Raad en het invullen van de IB-monitor op 'waarstaatjegemeente'.

Risico, indien niet op orde
Het College en de directie kunnen niet overeenkomstig de bedrijfsmatige- en wettelijke verplichtingen op IBB sturen. Zo wordt er vanuit de BRP-wetgeving (voorheen GBA), Digid-audit, Suwi-audit en vanuit de VNG resolutie, een vastgesteld IBB vereist.
Indien we geen vastgesteld, actueel IB-beleid hebben, voldoen we niet aan onze wettelijke verplichtingen en bestaat het risico dat de gemeente hierop aangesproken wordt en dat een landelijke koppeling (zoals Digid of Suwi) dreigt te worden afgesloten.

4.2 Organisatie van de informatiebeveiliging

Doelstelling
- Beheren van de informatiebeveiliging (IB) binnen de organisatie.

- Er is een beheerkader vastgesteld om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen.

- Goedkeuring door de directie van het informatiebeveiligingsbeleid, de toewijzing van de rollen en de coördinatie en beoordeling van de implementatie van het beleid binnen de organisatie.

Risico, indien niet op orde
Zonder beheerorganisatie kun je geen invulling geven aan je informatiebeveiligingsbeleid.
Vanuit onder andere BRP-wetgeving, Digid-audit, Suwi-audit en vanuit de VNG resolutie, wordt een aantoonbare organisatie van de informatiebeveiliging vereist.
Indien we hiertoe geen beheersorganisatie hebben, voldoen we niet aan onze wettelijke verplichtingen en bestaat het risico dat de gemeente hierop aangesproken wordt en leidt het mogelijk tot afsluiting van een landelijke voorziening (zoals Digid of Suwi). Zo dient er voor Suwi-net een specifieke security officer Suwi-net aangewezen te worden.

Voor Midden-Groningen zal een beveiligingsorganisatie neergezet worden. Onder verantwoordelijkheid van de directie zijn de werkgroepleden Informatiebeveiliging (en Privacy) verantwoordelijk voor de implementatie van de maatregelen. In deze werkgroep zijn in ieder geval vertegenwoordigers vanuit Personeelsbeleid, Automatisering, Gebouwenbeheer, Informatiemanagement, BRP, Rijbewijzen en Reisdocumenten, Suwi (daar waar nodig op ad-hoc basis) vertegenwoordigd. Betreffende werkgroep wordt voorgezeten door de Adviseur Informatiebeveiliging/CISO.

4.3 Beheer van bedrijfsmiddelen

Doelstelling

Het handhaven van een adequate bescherming van bedrijfsmiddelen (NB gaat om ALLE bedrijfsmiddelen.

EN

Informatie heeft een geschikt niveau van beveiliging.

Risico, indien niet op orde

- Bedrijfsmiddelen en informatie zijn blootgesteld aan risico's zoals diefstal, beschadiging of onoordeelkundig gebruik, waarbij niet voor alle ICT-configuratie items is vastgelegd wie de eigenaar/hoofdgebruiker is.

- Wanneer de bedrijfsmiddelen niet zijn toegewezen aan een eigenaar bestaat het risico dat ook niemand verantwoordelijkheid neemt voor de benodigde beveiligingsmaatregelen.

4.4 Beveiliging van personeel

Doelstelling

- Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.

- De verantwoordelijkheden ten aanzien van beveiliging is vóór het dienstverband vastgelegd in passende functiebeschrijvingen en in de arbeidsvoorwaarden.

- Alle kandidaten voor een aanstelling, ingehuurd personeel en externe gebruikers worden gescreend, in het bijzonder voor vertrouwensfuncties.

- Werknemers, ingehuurd personeel en externe gebruikers, die ICT-voorzieningen gebruiken tekenen een overeenkomst over hun beveiligingsrollen en –verantwoordelijkheden.

Risico, indien niet op orde

Het aannemen of inhuren van nieuw personeel en het laten verrichten van werkzaamheden door externe medewerkers verdient extra aandacht, omdat menselijk falen en bedreigingen van menselijke aard significante invloed kunnen hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.

4.5 Fysieke beveiliging en beveiliging van de omgeving

Doelstelling

- Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie, bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.

- ICT-voorzieningen, die kritieke of gevoelige bedrijfsactiviteiten ondersteunen, behoren fysiek te worden ondergebracht in beveiligde ruimten, beschermd door afgegrensde beveiligde gebieden, in een gecontroleerde omgeving, beveiligd met geschikte beveiligingsbarrières en toegangsbeveiliging. Ze behoren fysiek te worden beschermd tegen toegang door onbevoegden, schade en storingen.

- Het voorkomen van verlies, schade of diefstal van apparatuur en bescherming tegen fysieke bedreigingen en gevaren van buitenaf.

Risico, indien niet op orde

- Onbevoegde toegang tot kritieke systemen of waardevolle informatie. Bij het ontbreken van registratie zijn incidenten bovendien niet herleidbaar tot individuen.

- Door bijvoorbeeld de inzet van externen, de toeloop van leveranciers en andere niet-medewerkers of het feit dat de medewerkers op meerdere locaties op geruime afstand van elkaar gevestigd zijn, is het betrekkelijk eenvoudig voor niet-medewerkers om toegang tot de panden te krijgen door tegelijk met een geautoriseerde medewerker naar binnen te gaan.

- Als informatie zichtbaar op bureaus ligt, is er een verhoogd risico m.b.t. de vertrouwelijkheid.

- Geen procedures voor het veilig verwijderen of hergebruiken van ICT-apparatuur.

- Bescherming van apparatuur, waaronder apparatuur die buiten de locatie wordt gebruikt en het verwijderen van bedrijfseigendommen, is noodzakelijk om het risico van toegang door onbevoegden tot informatie te verminderen en om de apparatuur en informatie te beschermen tegen verlies of schade.

4.6 Beheer van communicatie- en bedieningsprocessen
(Beveiliging van apparatuur en informatie)

Doelstelling
- Waarborgen van een correcte en veilige bediening van ICT-voorzieningen.

- Vastgestelde verantwoordelijkheden en procedures voor beheer en bediening van alle ICT-voorzieningen. Dit omvat tevens de ontwikkeling van geschikte bedieningsinstructies.

- Toepassing, waar nodig, van functiescheiding om het risico van nalatigheid of opzettelijk misbruik te verminderen.

Risico, indien niet op orde
- Het ontbreken van documentatie kan leiden tot fouten, niet-uniforme wijze van gegevensinvoer, of in geval de beheerder/bediener uitvalt, tot problemen rondom de continuïteit.

- Onjuiste autorisaties kunnen leiden tot foutieve handelingen, fraude en verduistering.

- Het niet uitvoeren en vastleggen van technische en functionele applicatietesten en/of de resultaten hiervan, kan in bepaalde omstandigheden (tijdsdruk, vakantieperiodes, etc.) leiden tot een verhoogd risico van uitval of gegevens verlies.

- De gemeente gaat steeds meer samenwerken en informatie uitwisselen in ketens en besteedt meer taken uit. Bij beheer van systemen en gegevens door een derde partij, kan ook informatie van de gemeente op straat komen te liggen. De gemeente blijft verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten, waarbij het beheer bij een andere partij ligt.

- Programmatuur en ICT-voorzieningen zijn kwetsbaar voor virussen.

- Het ontbreken van een regeling voor antivirus bescherming bij medewerkers thuis leidt tot hogere beveiligingsrisico's.

4.7 (Logische) Toegangsbeveiliging

Doelstelling
Voorkomen onbevoegde toegang tot het centrale ICT-domein van de organisatie

Risico, indien niet op orde

- Wanneer toegangsbeheersing niet expliciet gebaseerd is op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en/of een aanvullende risicoanalyse, is niet duidelijk of het juiste niveau van beveiliging wordt gehanteerd.

- Verstoringen door onjuist cq niet geautoriseerd gebruik van ICT-ruimtes of ICT-componenten (m.n. waar ook niet ICT-teams toegang hebben).

De identiteit van een gebruiker die toegang krijgt tot gemeentelijke informatie dient te worden vastgesteld. Logische toegang is gebaseerd op de classificatie van de informatie.

4.8 Verwerving, ontwikkeling en onderhoud van informatiesystemen

Doelstelling
Beveiliging bij ontwikkel en ondersteuningsprocessen.

Risico, indien niet op orde
- Verstoring in de continuïteit en beschikbaarheid van de informatiesystemen.

- Incorrecte verwerking, verlies, onbevoegde modificatie en ongeautoriseerd gebruik van informatie.

4.9 Beheer van informatiebeveiligingsincidenten

Doelstelling
- Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden, die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.

- Formele procedures voor rapportage van gebeurtenissen en escalatie. Alle werknemers, ingehuurd personeel en externe gebruikers zijn op de hoogte van deze procedures voor het rapporteren van de verschillende soorten gebeurtenissen en zwakke plekken die invloed kunnen hebben op de beveiliging van de bedrijfsmiddelen.

- Er is een verplichte meldingssystematiek in werking om alle informatiebeveiligingsgebeurtenissen en zwakke plekken zo snel mogelijk te rapporteren aan de aangewezen contactpersoon.

Risico, indien niet op orde
Als incidenten niet geregistreerd worden, is niet duidelijk waar en wanneer er zich incidenten voor doen of voor hebben gedaan. Op deze wijze kan er geen lering worden getrokken uit deze incidenten om deze in de toekomst te voorkomen of om preventief betere maatregelen te implementeren.

4.10 Bedrijfscontinuïteitsbeheer

Doelstelling
- Onderbreken van bedrijfsactiviteiten tegengaan en kritische bedrijfsprocessen beschermen

- tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.

- Een adequaat beheerproces van bedrijfscontinuïteit om de uitwerking op de organisatie, veroorzaakt door het verlies van informatie en het herstellen daarvan tot een aanvaardbaar niveau te beperken.

- Informatiebeveiliging is een integraal onderdeel van het totale bedrijfscontinuïteitsproces en andere beheerprocessen binnen de organisatie.

Risico, indien niet op orde

Onderbreking van bedrijfsactiviteiten en kritische bedrijfsprocessen als gevolg van omvangrijke storingen in informatiesystemen of rampen.

4.11 Naleving

Doelstelling
- Voorkomen schending wet- en regelgeving of contractuele verplichtingen.
- Beoordeling naleving van het beveiligingsbeleid.

- Richtlijnen bij audits informatie systemen

Risico, indien niet op orde
De kans op genoemde risico's vanuit de IB-deelgebieden neemt toe als er niet wordt nageleefd.

Te nemen tegenmaatregelen
Voorbeelden van de te hiertoe te nemen, nader in het Informatiebeveiligingsprogramma te benoemen en uit te werken tegenmaatregelen zijn:
- Inrichten verantwoordingsproces richting Bestuur (Directie, College en Raad)
- Verticale verantwoording vanuit ENSIA (naar de diverse Rijksoverheidsorganen in relatie met de diverse zelfevaluaties en audits centraal georganiseerd vanuit ENSIA).

Dit IB-beleid treedt in werking na vaststelling door college van B&W
Aldus vastgesteld door:
Burgemeester en wethouders van gemeente Midden-Groningen op 29 mei 2018.