Informatiebeveiligingsbeleid
2025 - 2029

gemeente SCHIERMONNIKOOG

Gemeente Ameland

gemeente Terschelling

gemeente Vlieland

Inhoudsopgave

1. Inleiding

1.1. Aanleiding

Door de steeds verdergaande samenwerking en professionalisering van de Friese Waddeneilanden nemen de digitalisering van de interne en externe informatievoorziening en de digitale dienstverlening verder toe. Daarvoor worden informatiesystemen intern en extern met (een toenemend aantal) ketenpartners gekoppeld. Door deze koppelingen ontstaat een steeds complexere infrastructuur van informatiesystemen die de basis vormt voor de totale informatievoorziening. Daarmee zijn de Friese Waddeneilanden afhankelijker geworden van de goede en veilige werking van deze informatievoorziening. Hoe waardevoller de informatie is, hoe belangrijker het is dat de juiste maatregelen getroffen worden om de operationele risico's te beheersen.

Veel informatiesystemen zijn echter niet primair ontworpen met het oog op de veiligheid van informatie. Daarnaast is het veiligheidsniveau dat met alleen fysieke en technische middelen kan worden bereikt beperkt. Het dient daarom te worden ondersteund met passende beheerprocessen en procedures. De menselijke factor (het menselijk gedrag) vormt daarbij een belangrijke en doorslaggevende rol in het daadwerkelijk realiseren van de veiligheid van informatie in de praktijk. Kennis, houding en gedrag van medewerkers zijn hierbij cruciaal. Eén van de belangrijkste uitgangspunten van het beleid die betrekking heeft op de menselijke factor luidt dan ook:

‘Iedere medewerker, zowel vast als tijdelijk, intern of extern is verplicht informatie en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.’

1.2. Doel van het beleid

Dit document geeft algemene beleidsuitgangspunten over informatiebeveiliging. In dit document zijn deze beleidsuitgangspunten nader uitgewerkt en zijn beveiligingseisen en maatregelen opgenomen die voor alle medewerkers, processen en systemen van De Friese Waddeneilanden gelden. Daarnaast zijn de verantwoordelijkheden voor informatiebeveiliging beschreven. Het doel van dit beleid is het beheersen van risico's rond de ontwikkeling, het beheer en het gebruik van de ICT-infrastructuur, de informatiesystemen en ICT-bedrijfsmiddelen, de informatie-uitwisseling, de informatie zelf, en de gebruikers van die informatie. Dit informatiebeveiligingsbeleid is het kader voor passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en de beschikbaarheid ervan te waarborgen, waarbij de gemeente voldoet aan relevante wet- en regelgeving.

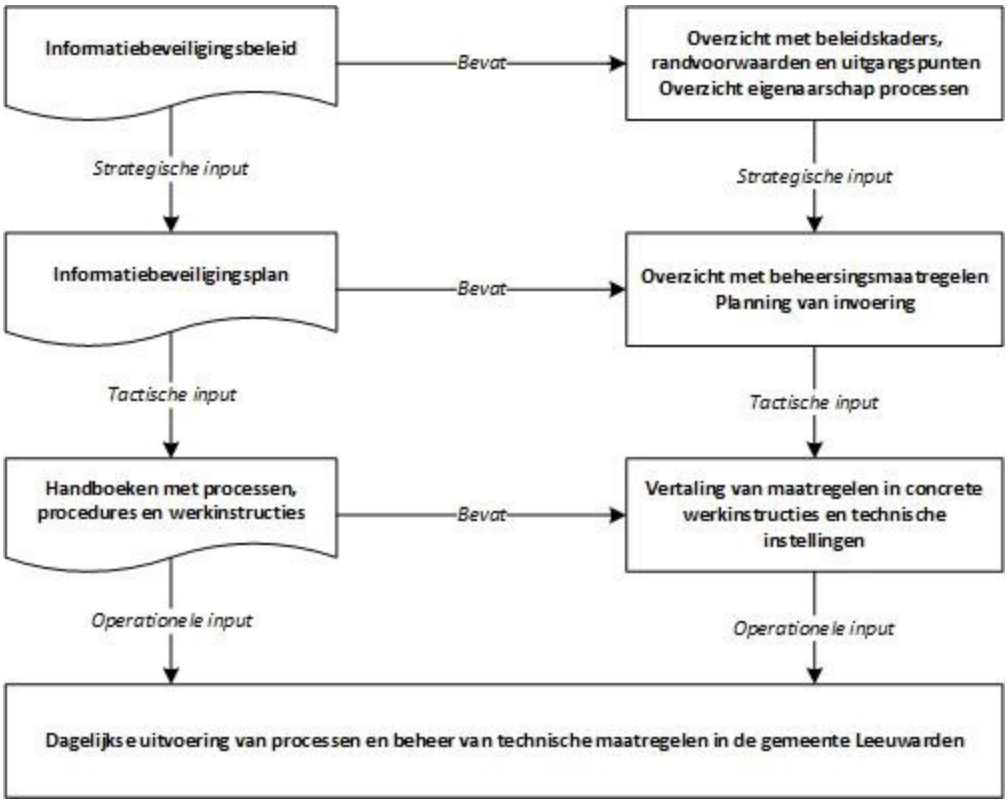
De Friese Waddeneilanden streven ernaar om aantoonbaar ‘in control’ te zijn en daarover op professionele wijze verantwoording af te leggen. In control zijn betekent weten welke maatregelen genomen zijn en of ze werken. De basis voor het afwegen van nog te nemen maatregelen is risicoafweging.

Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is. Bijstelling en vaststelling van het informatiebeveiligingsbeleid vindt plaats om de drie jaar of eerder als zich belangrijke wijzigingen voordoen.

1.3. Werkingssfeer

Het informatiebeveiligingsbeleid bevat de formele uitgangspunten en verwijzing naar de relevante gebieden waarop maatregelen getroffen dienen te worden om informatiebeveiligingsrisico's te kunnen mitigeren (verkleinen) en de maatregelen goed te kunnen invoeren en borgen binnen de Friese Waddeneilanden. Het beleid is van toepassing op alle informatie, informatieverwerkingsprocessen en systemen (hardware en software, zowel binnen de ICT-infrastructuur als daarbuiten) die wordt gebruikt door alle interne en externe medewerkers van de Friese Waddeneilanden. Daarmee vallen zowel de primaire operationele dienstverlenings-/ productieprocessen, als alle processen voor bestuurlijke en technische ondersteuning binnen de Friese Waddeneilanden binnen het bereik van dit beleid.

Het doel van het beleid is het beheersen van risico’s rond de ontwikkeling, het beheer en de het gebruik van de ICT-infrastructuur, de informatiesystemen en ICT-bedrijfsmiddelen, de informatie-uitwisseling, de informatie zelf, en de gebruikers van die informatie. In het informatiebeveiligingsplan worden de beleidsuitgangspunten nader uitgewerkt. Op basis van risicoanalyses wordt gekozen welke concrete technische en organisatorische maatregelen noodzakelijk zijn om de informatiebeveiligingsdoelstellingen uit dit beleid te bereiken. Deze vertaling is weergegeven in onderstaand figuur 1.



Figuur 1 – Vertaling beleidsuitgangspunten naar concrete werkinstructies en instellingen

1.4. Doelgroep

Dit beleid is bedoeld voor alle interne en externe medewerkers binnen de Friese Waddeneilanden. Het is vooral gericht op diegenen die betrokken zijn bij de ontwikkeling, uitvoering, sturing en naleving van het informatiebeveiligingsbeleid. De bestuurders en het management spelen een belangrijke rol bij de besluitvorming over dit onderwerp en de sturing ervan binnen de planning- & control-cyclus. Zie onderstaande tabel voor een korte toelichting van de verantwoordelijkheid per doelgroep.

Doelgroep	**Verantwoordelijkheid voor**
Gemeenteraad	Toezichthouden
College van B&W	Integraal bestuurlijk verantwoordelijk (kaderstelling)
Gemeentesecretaris	Ambtelijk eindverantwoordelijk
Directie	Ambtelijk sturing op het beleid
Lijnmanagement/proceseigenaren	Sturing op informatieveiligheid en controle op naleving
Medewerkers	Gedrag en naleving
Gegevenseigenaren	Classificatie: bepalen van beschermingseisen van informatie
Auditors en controller	Onafhankelijk toetsing naleving
Beleidsmakers	Opstellen beleid en toetsing procedures en uitvoering aan het informatiebeveiligingsbeleid
Beveiligingsfunctionarissen	Dagelijkse coördinatie op uitvoering en naleving van het informatiebeveiligingsbeleid
Communicatie	Vrijgave van (publieke) informatie
Personeel, Organisatie en Ontwikkeling (PO&O)	Arbeidsvoorwaarden, integriteit personeel, procedures voor instroom, doorstroom en uitstroom van medewerkers
Facilitair Beheer	Fysieke beveiliging en toegang
Informatie- en Communicatie-Technologie (ICT)	Technische beveiliging
Informatiemanagement	Informatiebeveiliging binnen vakgebied en -toepassing
Inkoop	Inkoopvoorwaarden, toetsing in contractbeheer

Doelgroep	Verantwoordelijkheid voor
Financien en Administratie	Begroting en verantwoording integriteit van financiële informatie
Leveranciers en ketenpartners	Ondersteunen gemeente Leeuwaren om compliant te worden en te blijven aan de Baseline Informatiebeveiliging Overheid (BIO)

1.5. Leeswijzer

Het beleid is zodanig opgezet dat het een naslagwerk vormt voor alle bestuurders en medewerkers die in het kader van hun reguliere werkzaamheden, in een project of ad hoc moeten weten aan welke kwaliteitsaspecten ten aanzien van informatieveilig werken aandacht moet worden besteed.

Hoofstuk 1 bevat de aanleiding en wordt het doel en de werkingssfeer van informatiebeveiligingsbeleid beschreven. Het bevat daarnaast ook een korte samenvatting en de ambitie en de visie van de Friese Waddeneilanden op informatieveiligheid. In de tabel in paragraaf 1.4 is per doelgroep aangegeven voor wie het beleid bedoeld is.

Vervolgens wordt in hoofdstuk 2 de kern van informatiebeveiliging, de context en de primaire uitgangspunten en principes uiteengezet. Het bevat uitleg over het, voor de overheid verplichte, normenkader de Baseline Informatiebeveiliging Overheid (BIO) en de manier invulling wordt gegeven aan risicomanagement en de borging van informatiebeveiliging. Dit hoofdstuk bevat tevens de visie van de Friese Waddeneilanden op informatiebeveiliging en de samenhang tussen dit beleid, het ICT-beleid en de wettelijke grondslagen die van toepassing zijn.

Hoofdstuk 3 bevat het horizontale en verticale verantwoordingsmechanisme voor informatiebeveiliging en tenslotte wordt in hoofdstuk 4 beschreven hoe informatiebeveiliging wordt georganiseerd en hoe de rollen, taken en verantwoordelijkheden belegd zijn.

Voor de leesbaarheid van het beleid is ervoor gekozen om alle begrippen niet in een aparte bijlage op te nemen maar in de tekst zelf te verklaren, de afkortingen worden alleen bij het eerste gebruik voluit geschreven.

1.6. Samenvatting

De Friese Waddeneilanden zijn, evenals iedere verbonden organisatie, zelf bestuurlijk (wettelijk) eindverantwoordelijk voor informatiebeveiliging binnen haar eigen organisatie. Dit informatiebeveiligingsbeleid is de basis voor de werkprocessen om de beveiliging van alle informatie binnen de Friese Waddeneilanden (en de keten) als één geheel te kunnen waarborgen. Het is van toepassing op alle interne en externe medewerkers binnen de Friese Waddeneilanden en is in lijn met de relevante Nederlandse en Europese wet- en regelgeving.

Het basisuitgangspunt is dat er door de Friese Waddeneilanden minimaal wordt voldaan aan het gemeentelijke normenkader: de Baseline Informatiebeveiliging Overheid (BIO), waarbij het 'pas toe of leg *expliciet* uit'-principe altijd geldt indien daaraan (nog) niet wordt of kan worden voldaan. Het informatiebeveiligingsbeleid geeft alle uitgangspunten weer voor de organisatorische en technische maatregelen in het informatiebeveiligingsplan. Alle bestaande en nieuwe processen, procedures, medewerkers en technische instellingen moeten (gaan) voldoen aan dit beleid. Tevens geeft het beleid weer op welke wijze zal worden toegezien op de naleving van het beleid binnen de Friese Waddeneilanden.

De belangrijkste uitgangspunten van het beleid zijn:

1. Het **informatiebeveiligingsbeleid** vormt samen met het **informatiebeveiligingsplan** één van de fundamenten onder een betrouwbare informatievoorziening. Hierin wordt de betrouwbaarheid van de informatievoorziening én de Friese Waddeneilanden breed benaderd. Zij worden periodiek (het beleid minimaal eens per vier jaar) bijgesteld op basis van de nieuwe interne en externe ontwikkelingen, de incidentenregistraties en de (bestaande) procesrisicoanalyses.

2. Het **bestuurlijk niveau** is **eindverantwoordelijk** voor informatiebeveiliging en draagt deze verantwoordelijkheid en het beleid actief uit.

3. Alle **taken, bevoegdheden en verantwoordelijkheden** voor de bescherming van informatie en voor het uitvoeren van beveiligingsprocedures zijn binnen iedere organisatie **expliciet vastgelegd**.

4. Door een **brede planning van de Friese Waddeneilanden, coördinatie én periodieke controle** op informatiebeveiliging wordt de kwaliteit van de informatievoorziening verankerd binnen de Friese Waddeneilanden.

5. Informatie en informatiesystemen zijn van kritiek en vitaal belang voor de Friese Waddeneilanden en zijn **geclassificeerd** om maatregelen gericht in te kunnen zetten.

6. Informatiebeveiliging is een **continu verbeterproces**, dat is ingericht conform het 'Plan, do, check en act'-principe.

7. Informatiebeveiliging is **integraal** opgenomen in de reguliere **planning- & controlcyclus** (als **informatiebeveiligingsmanagementsysteem**) van alle Friese Waddeneilanden en vormt een integraal aspect van gegevensmanagement.

8. De **informatiebeveiligingsfunctionaris**, de Chief Information Security Officer (CISO) ondersteunt vanuit zijn **onafhankelijke** positie de informatiebeveiligingsfunctionarissen binnen de Friese Waddeneilanden en binnen de verbonden organisaties. Zij bewaken en verhogen de betrouwbaarheid van de eigen informatievoorziening. De CISO coördineert de initiatieven binnen de Friese Waddeneilanden en rapporteert over de voortgang.

9. De Friese Waddeneilanden stellen de benodigde **mensen en middelen** beschikbaar conform de bestaande afspraken om haar informatie en de informatievoorziening te kunnen beveiligen volgens de wijze gesteld in dit beleid.

10. **Procedures en regels** die voortvloeien uit het informatiebeveiligingsbeleid dienen te worden vastgelegd, vastgesteld (op het juiste niveau), **uitgevoerd** en periodiek **geëvalueerd**. Alle medewerkers van de Friese Waddeneilanden worden verplicht getraind in het gebruik van de noodzakelijke beveiligingsprocedures.

11. Iedere medewerker, zowel vast als tijdelijk, intern of extern is **verplicht informatie en informatiesystemen te beschermen** tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

1.7. Ontwikkelingen op het gebied van informatieveiligheid

Digitale weerbaarheid en bewustwording medewerkers

Bewustwording van onze medewerkers is bij het verwerken van deze informatie een cruciaal onderwerp als het gaat om informatieveiligheid. Onze informatiebeveiliging kan technisch wel in orde zijn, maar wanneer medewerkers hier niet bewust naar handelen liggen beveiligingsincidenten, zoals datalekken, nog steeds op de loer. Medewerkers zijn zich vaak onvoldoende bewust van de gevolgen van kleine menselijke fouten. Het is verleidelijk om met technologie te proberen gebruikersgerelateerde beveiligingsincidenten te vermijden of terug te dringen. Cybercriminelen maken daarnaast steeds vaker gebruik van e-mail phishing technieken (hengelen) omdat het veel eenvoudiger is om iemand op een link te laten klikken of een besmette bijlage te laten openen, dan digitaal in computersysteem in te breken. Alleen technologie inzetten is geen oplossing; informatiebeveiliging begint bij een bewuste medewerker.

De meest incidenten worden nog steeds veroorzaakt door menselijke handelen. Dit blijkt ook uit het interne datalekken-register van de Gemeente Leeuwarden. Over het jaar 2020 zijn in totaal 61 (2019: 35) datalekken gemeld bij de Functionaris voor de Gegevensbescherming (FG), waarvan 12 (2019: 19) zijn gemeld bij de Autoriteit Persoonsgegevens (AP). Een forse stijging van het aantal intern gemelde datalekken terwijl er minder incidenten gemeld moesten worden aan de Autoriteit Persoonsgegevens. Dit wijst erop dat medewerkers vaker herkennen wat een datalek is, terwijl de ernst van de datalekken minder was in 2020. Uit analyse is gebleken dat in bijna alle gevallen deze datalekken zijn veroorzaakt door onbedoeld en onbewust handelen van medewerkers.

Uit de gepubliceerde cijfers van de Autoriteit Persoonsgegevens (AP) over het jaar 2018 blijkt dat er 20.881 datalekken gemeld zijn door organisaties en bedrijven die persoonsgegevens verwerken. Net als in 2017 was het meest voorkomende type datalek het versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger, goed voor 63% van de meldingen. Dit kan bijvoorbeeld een brief met gevoelige gegevens zijn die bij de verkeerde persoon terecht is gekomen (en is geopend) of een foutief geadresseerde mail met vertrouwelijke gegevens. Het kwijtraken of de diefstal van een gegevensdrager zoals een laptop of usb-stick (14%) is daarna het meest voorkomende type datalek. De soorten gegevens die het meest vrijkomen bij een datalek zijn NAW-gegevens, het BSN, medische en andere privacygevoelige gegevens.

In 2019 ontving de Autoriteit Persoonsgegevens (AP) bijna 27.000 datalekmeldingen. Dat is een stijging van 29% ten opzichte van 2018. De AP ontving dit jaar een kwart meer meldingen naar aanleiding van hacking, phishing of malware-incidenten dan in het jaar daarvoor. Vooral grotere organisaties, die persoonsgegevens van veel mensen verwerken, lijken hier doelwit van.

Uit de vele datalekken die gemeld zijn bij de Autoriteit Persoonsgegevens (AP) is af te leiden dat medewerkers vaak, al dan niet onbedoeld en onbewust, een rol spelen bij het veroorzaken hiervan. Uiteindelijk is de informatiebeveiliging zo sterk als de zwakste schakel, in dit geval onze medewerkers. Er dient gebouwd te worden aan een sterke informatieveilige omgeving, zowel op het vlak van techniek als op het vlak van de mens. Een bewuste medewerker is een zeer belangrijk fundament voor informatiebeveiliging.

Voor de periode 2025-2029 gaan wij op een aantal manieren uitvoering geven aan het vergroten van de digitale weerbaarheid en bewustzijn. Dit doen wij door:

- gerichte voorlichting te geven op afdelings-overleggen;
- aandacht te vragen voor security en privacy gerelateerde activiteiten en onderwerpen in de vorm van nieuwsberichten, e-mailberichten en narrowcasting;
- het aanbieden van training in de vorm van e-learning en security-awareness-games;
- het voeren van gerichte campagnes om de weerbaarheid te toetsen;
- het verhogen van het kennisniveau van technisch- en functioneel beheerders;
- het beschikbaar stellen van tools voor het wachtwoordbeheer en het beveiligd uitwisselen van e-mail en bestanden.

2. Informatiebeveiliging

2.1. Begrippenkader

De Friese Waddeneilanden hanteren de Baseline Informatiebeveiliging Overheid (BIO) definitie van informatiebeveiliging:

*"Het proces van vaststellen van de vereiste **betrouwbaarheid** van informatieverwerking in termen van **beschikbaarheid, integriteit en vertrouwelijkheid (BIV)** alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen."*

Het begrip informatiebeveiliging heeft aldus betrekking op volgende vier kwaliteitsaspecten:

- **Beschikbaarheid (continuïteit)**: het zorgdragen voor het zonder belemmeringen beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers, overeenkomstig de daarover gemaakte afspraken en wettelijke voorschriften. Beschikbaarheid wordt gedefinieerd als de ongestoorde voortgang van een informatieverwerking zonder verlies van informatie;
- **Integriteit (betrouwbaarheid)**: het waarborgen van de correctheid, authenticiteit, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking. Informatie die wordt weergegeven moet in overeenstemming zijn met de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen. Hiervoor dient informatie beschermd te worden tegen mutaties door onbevoegden en tegen onbevoegde mutaties;
- **Vertrouwelijkheid (exclusiviteit)**: het beschermen van informatie tegen kennisname door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn. Uitsluitend bevoegde personen hebben (vooraf) goedgekeurde toegang tot informatie en kunnen gebruik maken van informatie;
- **Controleerbaarheid**: de mogelijkheid om en de wijze waarop (achteraf) vast te stellen is hoe de informatievoorziening en haar componenten zijn gestructureerd. Controleerbaarheid is een randvoorwaardelijk kwaliteitsaspect om aantoonbaar te kunnen sturen op de eerste drie primaire kwaliteitsaspecten. Een regelmatige controle op uitvoering van de beheersmaatregelen is noodzakelijk om vast te stellen of deze goed werken of hebben gewerkt. Daarom is een audittrail (het spoor van een audit of controle) van groot belang.

2.2. Belang van informatiebeveiliging

Informatie is één van de voornaamste bedrijfsmiddelen van de Friese Waddeneilanden. Het verlies van informatie, uitval van ICT, of het door onbevoegden kennisnemen of (bewust) manipuleren van informatie kan ernstige gevolgen hebben voor de bedrijfsvoering. Het kan direct of indirect ook leiden tot politieke consequenties doordat maatschappelijke en/of financiële schade kan ontstaan en de Friese Waddeneilanden daarmee imagoschade oplopen. Incidenten hebben namelijk mogelijk ernstig negatieve gevolgen voor burgers, bedrijven, partners en/of de eigen organisatie met waarschijnlijk ook politieke consequenties. Informatieveiligheid is daarom van groot belang en informatiebeveiliging is het proces dat daaraan invulling geeft. Informatiebeveiliging is geen doel op zich maar moet de primaire bedrijfsprocessen ondersteunen en de veilige en verantwoorde uitvoering daarvan mogelijk maken. Het proces van informatiebeveiliging is primair gericht op bescherming van informatie binnen de Friese Waddeneilanden.

2.3. Uitgangspunten van informatiebeveiliging

De Friese Waddeneilanden hanteren met betrekking tot informatiebeveiliging de volgende uitgangspunten:

1. Burgers, bedrijven en organisaties moeten erop kunnen vertrouwen dat gegevens in goede handen zijn bij de Friese Waddeneilanden.

2. Een betrouwbare informatievoorziening vormt een essentiële succesfactor voor een efficiënte en effectieve bedrijfsvoering. Omdat de Friese Waddeneilanden onderdeel uitmaken van de totale overheid en ook verbonden is met andere ketenpartijen, heeft een onveilige situatie bij de Friese Waddeneilanden direct gevolgen voor de veiligheid van andere overheden of partijen.

3. Informatiebeveiliging is noodzakelijk om de betrouwbaarheid, integriteit, beschikbaarheid (continuïteit) en controleerbaarheid van de informatievoorziening te kunnen borgen.

4. De informatiebeveiligingstaken worden als integraal onderdeel van de dagelijkse bedrijfsvoering in de organisatie belegd.

5. Informatiebeveiliging is niet vanzelfsprekend en moet georganiseerd worden. Het vergroten van het bewustzijn en acceptatie van medewerkers over informatiebeveiliging vraagt continu aandacht van het management.

6. Het realiseren van een 100% veiligheid is een onmogelijkheid. Daarom worden alle specifieke veiligheidsvraagstukken ‘risk-based’ benaderd. Dat wil zeggen: beveiligingsmaatregelen worden getroffen op basis van een inschatting van mogelijke risico’s.

7. Het bestuur en het management handelt conform de tien bestuurlijke principes informatieveiligheid die zijn opgesteld door de VNG (zie bijlage 1).

8. Periodiek onafhankelijke controle door de Chief Information Security Officer (CISO) is nodig om vast te stellen of de informatiebeveiliging voldoet aan het informatiebeveiligingsbeleid, respectievelijk of de uitgevoerde maatregelen voldoende zijn om het gewenste niveau van informatiebeveiliging te bewerkstelligen.

9. Informatiebeveiliging moet informatiebeveiligingsincidenten voorkomen, respectievelijk de effecten van het optreden van incidenten beperken.

10. Informatiebeveiligingsmaatregelen mogen niet ten koste gaan van de veiligheid van eigen personeel en van derden.

11. Het gewenste informatiebeveiligingsniveau wordt vastgelegd in de vorm van minimumeisen. Op basis van wet- en regelgeving, overeenkomsten met andere overheden en derden, of bij bijzonder kwetsbare en vitale componenten van de informatievoorziening, kan op onderdelen een hoger niveau van informatiebeveiliging gelden.

12. Medewerkers, zowel vast als tijdelijk, intern of extern, hebben een eigen verantwoordelijkheid voor hun gedrag binnen de gestelde normen en eisen en spreken elkaar aan op onveilig gedrag. Ook signaleren zij mogelijke zwakke plekken in de beveiliging en melden deze direct aan de leidinggevenden.

13. Medewerkers, zowel vast als tijdelijk, intern of extern hebben een geheimhoudingsverklaring en-/of integriteitsverklaring getekend. Medewerkers moeten bekwaam zijn in het uitvoeren van de functietaken en in dat kader de benodigde opleidingen gevolgd hebben.

14. Medewerkers krijgen niet meer autorisaties dan nodig voor het uitvoeren van hun taak. Autorisaties worden verstrekt volgens de principes 'need to know' en 'need to do'. Waar noodzakelijk wordt functiescheiding toegepast bij het toekennen van autorisaties.

15. Informatiesystemen hebben een toegewezen systeemeigenaar en processen hebben een toegewezen proceseigenaar.

16. Voor bestaande en nieuwe informatiesystemen is een Basis-Beveiligings-Niveau (BBN-) toets op basis van de BIO uitgevoerd om vast te stellen welke maatregelen op grond de BIO verplicht gelden ten aanzien van deze systemen.

17. Informatiesystemen, en de output van deze systemen, zijn geclassificeerd volgens de richtlijn dataclassificatie (2019) en minimaal beveiligd volgens het bepaalde classificatieniveau. Aanvullend wordt voor de informatiesystemen met classificatie vertrouwelijk en hoger een risicoanalyse uitgevoerd.

18. Bij de uitvoering van de informatiebeveiliging wordt gebruik gemaakt van een Plan-Do-Check-Act cyclus. Met deze PDCA-cyclus sluit de gemeente aan bij de Eenduidige Normatiek Single Information Audit (ENSIA) die sinds 2017 door alle gemeenten wordt gehanteerd. De resultaten daaruit zijn richtinggevend voor de jaarplanning.

19. Met samenwerkingspartners en leveranciers waar informatiebeveiliging een rol speelt worden op voorhand afspraken gemaakt over het vereiste niveau van informatiebeveiliging. Deze afspraken worden vastgelegd in standaard inkoopvoorwaarden en/of (verwerkers)overeenkomsten.

2.4. Visie op informatiebeveiliging

De ambitie van de Friese Waddeneilanden is om de komende jaren de informatieveiligheid te verhogen en de totale informatiebeveiligingsfunctie binnen alle heel de organisatie verder te professionaliseren. Daarmee bereiken de Friese Waddeneilanden onder andere dat:

De basis voor een betrouwbare informatievoorziening wordt gegarandeerd die noodzakelijk is voor het goed functioneren van de Friese Waddeneilanden en de verbonden organisaties en die de basis vormt voor de bescherming van rechten en plichten van burgers en bedrijven (binnen en buiten de Friese Waddeneilanden waarvoor taken worden uitgevoerd door de Friese Waddeneilanden.

Informatiebeveiliging wordt binnen de Friese Waddeneilanden en verbonden organisaties gezamenlijk en integraal, op basis van risicomanagement, gericht opgepakt zodat een eenduidig geheel (raamwerk) aan beheersingsmaatregelen ontstaat dat de gehele keten versterkt.

Het onderwerp wordt breed gedragen binnen alle bestuurlijke en ambtelijke lagen van de Friese Waddeneilanden en verbonden organisaties als onderdeel van zowel goed werkgeverschap, opdrachtnemerschap en opdrachtgeverschap. Informatiebeveiliging is de basis voor de dienstverlening en nieuwe innovatieve manieren van werken, die op verantwoorde wijze blijvend mogelijk worden gemaakt.

2.5. Baseline Informatiebeveiliging Overheid (BIO)

Als leidraad voor de informatiebeveiliging hanteren de Friese Waddeneilanden vanaf 01-01-2020 de Baseline Informatiebeveiliging Overheid (BIO). De BIO vormt één gezamenlijk normenkader voor Overheid, Rijk, Waterschappen en Provincies. Had voorheen iedere overheidslaag zijn eigen baseline, nu is er met gezamenlijke inspanning één BIO voor de gehele overheid. De BIO vervangt daarmee de Baseline Informatiebeveiliging Gemeenten (BIG).

Het gebruik van één normenkader voor de gehele overheid biedt een aantal voordelen:

- Het versterken van de informatieveiligheid door betere afstemming binnen ketens van overheden en andere partijen;
- Administratieve lastenverlichting bij overheid en bedrijven, zowel afnemers als leveranciers, door uniforme beveiligingsnormen bij de overheid;
- Aansluiting bij internationale regelgeving en standaarden;
- Vermindering van onderhoudskosten.

De BIO is een doorontwikkeling van de BIG en is gebaseerd op de ISO 27002. De ISO 27002 is de formele benaming van de ‘Code voor Informatiebeveiliging’ en een internationale erkende norm waarmee informatie procesmatig kan worden beveiligd, met als doel de vertrouwelijkheid, beschikbaarheid en integriteit van informatie binnen de organisatie zeker te stellen. Deze norm bevat richtlijnen en principes voor het initiëren, implementeren, onderhouden en verbeteren van

informatiebeveiliging binnen een organisatie. De ISO bestaat uit 114 controls; de term ‘control’ wordt in de ISO vertaald als een beheersmaatregel. De BIO volgt de opbouw van de ISO 27002 en zijn controls.

Een deel van de controls is uitgewerkt in verplichte maatregelen, omdat zij:

- voortvloeien uit wet- en regelgeving). Het niet treffen van een dergelijke maatregel is dan in strijd met deze externe wet- en regelgeving;

- zo basaal zijn dat zij het fundament vormen van een betrouwbare c.q. professionele informatievoorziening;

- dienstbaar zijn aan de beveiliging in een procesketen of netwerk; niet-naleving door een enkele organisatie is per saldo ineffectief voor de gehele keten. Het vormt een risico voor alle andere partijen in de keten en leidt bij hen tot extra maatregelen en kosten. Voor de keten als geheel is dit inefficiënt. Voor een generieke dienst geldt een afweging die analoog is aan het ketenvraagstuk.

De BIO legt meer nadruk op risicomanagement en minder nadruk op maatregelen. Een groot verschil met de Baseline Informatiebeveiliging Gemeenten (BIG) is dat alle BIO-maatregelen verplichte maatregelen zijn, er is geen sprake meer van ‘pas toe of leg uit’ principe. De BIO noemt deze verplichte maatregelen ‘overheidsmaatregelen’. De overheidsmaatregelen dekken niet de gehele beveiligingsdoelstellingen van de control af. Net als bij de controls geldt hier een hardheidsbepaling: in het geval een maatregel voor een specifiek geval niet van toepassing kan zijn, vervalt de verplichting.

In de BIO zijn de rollen van de bestuurder, lijnmanager, systeemeigenaar en proceseigenaar ten aanzien van risicomanagement explicieter beschreven (zie hoofdstuk 4). Zo hebben alle belangrijke processen een proceseigenaar en belangrijke informatiesystemen een systeemeigenaar.

2.5.1. Tactische uitgangspunten Baseline Informatiebeveiliging Overheid

De tactische uitgangspunten van het informatieveiligheidsbeleid gaan in op de beheerdoelstellingen per onderdeel van de BIO. De BIO kent naast het Information Security Management System (ISMS – zie paragraaf 2.11 borging van informatiebeveiliging) een aantal inhoudelijke onderwerpen. Deze onderwerpen staan veelal niet op zich daar de onderwerpen vaak samen zorgen voor een niveau van veiligheid. Zo is er samenhang tussen de HRM-processen instroom, doorstroom en uitstroom en het beheer van autorisaties. Op het gebied van communicatie op het internet is er samenhang met het beheer van encryptiesleutels. Wanneer een organisatie excelleert op één gebied kan een ander gebied weer voor onveiligheid zorgen. We zeggen dan ook wel dat de beveiliging zo goed is als de zwakste schakel in de keten.

Per onderwerp zullen we op tactisch niveau aangeven wat het doel is van dit beheeraspect.

Veilig personeel

Doelstelling

Medewerkers dienen geschikt te zijn en geschikt te blijven voor hun functie. De belangrijkste waarborg is het aantrekken van betrouwbaar en geschikt personeel en de zorg dat de medewerkers geschikt blijven voor hun functie, zodat ze op een goede wijze met de informatie van de organisatie om kunnen gaan tijdens en na afloop van hun contract.

Toelichting

Informatieveiligheid valt en staat met de kennis, houding en gedrag van de medewerkers. Om de juiste medewerkers in de organisatie te krijgen, deze gedurende hun loopbaan te trainen en te coachen zodat zij over de kennis en vaardigheden beschikken die nodig zijn om hun functie naar behoren uit te voeren.

Beheer van bedrijfsmiddelen*

Doelstelling

De organisatie gebruikt een groot aantal systemen (apparatuur, devices en software) om de informatievoorziening te faciliteren. Het doel van dit beheer aspect is het identificeren van alle hard- en software zodat deze op een adequate wijze beheerd en beveiligd kunnen worden.

Toelichting

Om informatie adequaat te kunnen beheren is het van belang om inzicht te hebben in diverse ICT-componenten die gebruikt worden om informatie te verwerken. Er kan pas adequaat beheer gevoerd worden wanneer je in het zicht hebt wat je moet beheren. De administratie waarin de ICT-componenten worden beschreven, ook wel Configuratie Management Database (CMDB) genoemd, dient als basis van diverse beheerprocessen zoals patchmanagement, incidentmanagement evenals het informatieclassificatiesysteem waarmee de behoefte, de prioriteit en de mate van beveiliging door de verantwoordelijk manager kan worden bepaald.

Toegangsbeveiliging*

Doelstelling

Toegang tot informatie en informatie op een passende wijze beveiligen zodat onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie wordt voorkomen.

Toelichting

Om effectieve toegangscontrole tot vertrouwelijke en privacygevoelige informatie te kunnen invoeren en onderhouden wordt er een toegangsrichtlijn opgesteld. Naast deze toegangsrichtlijn heeft ieder informatiesysteem nog een specifiek gedefinieerde uitwerking omtrent toegang, dat is afgestemd op het beveiligingsniveau van de informatie.

Cryptografie*

Doelstelling

Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

Toelichting
Een effectieve manier om informatie te beveiligen tegen onbevoegde inzage is het versleutelen van deze informatie. Dit gebeurt bij voorkeur zowel bij de opslag als het transport. Belangrijk beheeraspect is dat versleuteling wordt toegepast met behulp van sleutels die veilig genoeg zijn conform de actuele standaarden. Om verlies van data te voorkomen is het van belang dat er ten aanzien van het beheer van de sleutels goede maatregelen zijn getroffen.

Fysieke beveiliging en de beveiliging van de omgeving
Doelstelling
Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatie verwerkende faciliteiten van de organisatie voorkomen.

Toelichting
Een belangrijk aspect van informatieveiligheid is het voorkomen dat onbevoegden fysiek toegang hebben tot informatie. Ondanks de snelle ontwikkeling van digitale informatieverwerking is veel informatie ook nog analoog beschikbaar. Daarnaast dienen de informatie verwerkende computers en devices beschermd te worden tegen onbevoegde toegang.

Fysieke beveiliging wordt ingezet om onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatie verwerkende faciliteiten van de organisatie voorkomen.

Beveiliging bedrijfsvoering*
Doelstelling
Correcte en veilige bediening van informatie verwerkende faciliteiten ter voorkoming van ongewenste aanpassingen, verlies en diefstal van gegevens

Toelichting
Informatie wordt door de gehele organisatie heen gebruikt en daarnaast wordt informatie ook gedeeld met andere organisaties. Doordat informatie wordt hergebruikt is het van belang dat informatie goed wordt beheerd. Uitgangspunt hierbij is dat ieder brok aan informatie wordt beheerd vanuit een aangewezen organisatieonderdeel die daarvoor eenduidige processen en controlemaatregelen heeft ingericht om de kwaliteit van de informatie te kunnen waarborgen.

Communicatiebeveiliging*
Doelstelling
Informatie van de organisatie die via het interne netwerk intern dan wel extern wordt getransporteerd dient afdoende te worden beveiligd om onderschepping en/of ongewenste aanpassing van informatie te voorkomen.

Toelichting
Bij het beheer van netwerken moet onderscheid worden gemaakt tussen het eigen netwerk en netwerken die de grens van de organisatie overschrijden. Voor transport van vertrouwelijke en privacygevoelige gegevens via netwerken dienen extra maatregelen ter waarborging van de veiligheid te worden getroffen om te zorgen dat de data-integriteit en de vertrouwelijkheid bij transport is gewaarborgd. Zeker nu we steeds meer met externe partijen samenwerking is het van groot belang te kunnen vertrouwen op de communicatiekanalen.

Aankoop, ontwikkeling en onderhoud van informatiesystemen

Doelstelling

Waarborgen dat informatieveiligheid integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus en bij het testen van systemen. Dit zowel bij interne systemen als bij gebruik van een cloud-leverancier.

Toelichting

Bij de ontwikkeling van (informatie)systemen moeten beveiliging en privacy vanaf aanvang in het ontwerpproces of in het pakket aan eisen worden meegenomen. Bij standaardprogrammatuur moet voor aanschaf worden vastgesteld of geautomatiseerde beveiligingsmaatregelen zijn ingebouwd en aan de eisen vanuit de AVG wordt voldaan. Bij het onderhoud van (informatie)systemen moet informatieveiligheid een vast aandachtspunt zijn.

Leveranciersrelaties

Doelstelling

Er dienen met leveranciers overeenkomsten te worden gesloten die ervoor zorgen dat de dienstverlening in overeenstemming is met het informatieveiligheidsbeleid en de wettelijke bepalingen.

Toelichting

Organisaties zijn ten aanzien van de verwerking van informatie sterk afhankelijk van diverse leveranciers. Dit niet alleen vanwege de aanschaf en de primaire werking maar vanwege de dienstverlening die verbonden is aan de primaire dienstverlening. Het is van belang om met de leveranciers goede afspraken te maken over de aard van de dienstverlening. Daarnaast dient te worden gecontroleerd of ook aan de eisen wordt voldaan.

Beheer van informatie-beveiligingsincidenten

Doelstelling

Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatieveiligheid incidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging

Toelichting

Het beheer van incidenten kent twee gezichtspunten. Ten eerste dienen incidenten snel en adequaat te worden afgehandeld maar daarnaast zijn incidenten ook een signaal dat bestaande maatregelen wellicht niet voldoen. Het is dus van belang dat een incident zowel goed en snel wordt afgehandeld en dat daarnaast een analyse plaatsvindt zodat duidelijk is wat de oorzaak is geweest en hoe we er structureel voor kunnen zorgen dat een dergelijk voorval niet meer plaats kan vinden.

Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Doelstelling

Beschikbaarheid van informatie verwerkende faciliteiten bewerkstelligen.

Toelichting

Continuïteitsbeheer heeft als doel om ervoor te zorgen dat de dienstverlening intern en extern ongestoord kan plaatsvinden. Om de dienstverlening ongestoord doorgang te laten vinden dienen we zowel te kijken naar de systemen die nodig zijn als naar de facilitaire voorzieningen.

Naleving

Doelstelling

Verzekeren dat informatieveiligheid wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie ter voorkoming van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatieveiligheid en beveiligingseisen.

Toelichting

Het uitdragen van beleid en het opstellen van procedures moeten een waarborg bieden voor de kwaliteit. Het controleren van het beleid en de naleving van de procedures zijn erop gericht om te beoordelen of beleid en procedures ook werkbaar zijn in de praktijk. Daarnaast kunnen controles ook gebruikt worden om verdere sturing te geven aan de organisatie en zijn daarmee een essentieel onderdeel van de governance.

*valt onder de verantwoordelijkheid en beheer van het Shared Service Center (SSC)

2.5.2. Risicobenadering

De Friese Waddeneilanden volgen een aanpak van informatiebeveiliging op basis van risicobeheersing. Met een aanpak gebaseerd op risicobeheersing zijn de Friese Waddeneilanden in staat om een evenwichtige set van beveiligingsmaatregelen te implementeren en in staat om daarbij een goede afweging tussen kosten en noodzaak te maken. Risicobeheersing omvat de processen voor de identificatie van risico's en het selecteren, implementeren en bewaken van maatregelen om deze te reduceren tot een acceptabel niveau. Het risico is de kans op beveiligingsincidenten en de impact daarvan op het werkproces en wordt bepaald door de proceseigenaar.

Het risico van beveiligingsincidenten is de kans op beveiligingsincidenten maal de impact daarvan op het proces: risico = kans x impact.

Voor het bepalen van - te mitigeren - risico's kijken de Friese Waddeneilanden expliciet naar:

- Kans: hoe groot is de kans dat een bedreiging zich binnen een proces en-/of informatiesysteem kan voordoen
- Impact: wat is het gevolg van een bedreiging, als deze zich heeft voorgedaan, voor de gemeente in termen als financieel, imago, bestuurlijk en/of haar omgeving

Ook wordt een inschatting gemaakt van de dreigingen waartegen beschermd moet worden. De inschatting van mogelijke schade en dreigingen leidt tot beveiligingseisen om risico's te beperken. Om deze eisen af te dekken worden passende maatregelen getroffen of wordt het (rest)risico geaccepteerd.

Vanuit de theorie kan men op vijf verschillende manieren een risico benaderen:

1. **Beperken**: expliciet benoemen en analyseren van het risico en vervolgens de benodigde maatregelen treffen om de kans en de impact te beperken.
2. **Vermijden**: pas het object of activiteit aan zodat het risico niet langer optreedt.
3. **Verplaatsen**: pas het object of activiteit aan zodat het risico naar een ander object wordt verplaatst.
4. **Overdragen**: beleggen van het geheel of een gedeelte van het risico bij een andere partij door het (proces) uit te besteden aan bijvoorbeeld een leverancier of door het te verzekeren.
5. **Accepteren**: expliciet accepteren, door het hoogste bevoegde gezag, van de eventuele schade van het opgetreden risico.

Het startpunt voor een gestructureerde opbouw is het uitvoeren van een nulmeting, een zogenaamde GAP-analyse, op basis van de BIO. Deze analyse is bedoeld om inzicht te krijgen in het zogenaamde 'gat' tussen datgene wat nodig is en wat ontbreekt. Op basis van dat inzicht vindt een impactanalyse plaats waardoor de gemeente in staat is om prioritering te geven aan verbeterpunten voor de korte (het zogenaamde laaghangend fruit) en maatregelen voor de lange termijn.

Ook voert de organisatie periodiek risicoanalyses uit ten aanzien van haar informatiesystemen en bedrijfsprocessen. Door specifiek te kijken naar mogelijke bedreigingen en risico`s, en bijpassende maatregelen om risico`s te beperken, zijn de Friese Waddeneilanden in staat om haar systemen en bedrijfsprocessen adequaat en doelgericht te beschermen.

2.5.3. Basisbeveiligingsniveaus en maatregelen

Om risicomanagement hanteerbaar en efficiënt te houden, kiest de Baseline Informatiebeveiliging Overheid (BIO) voor risicomanagement dat is gebaseerd op te beschermen belangen en relevante dreigingen. Eén van de vernieuwingen van de BIO is dat er onderscheid is naar drie Basisbeveiligingsniveaus (BBN).

De beschreven belangen en dreigingen worden uitgedrukt in basis-beveiligings-niveaus: (BBN), namelijk:

BBN1 : informatiesystemen op BBN1 zijn systemen waarvoor BBN2 als te zwaar wordt gezien. Voor BBN1 ligt de nadruk op '*wat mag minimaal verwacht worden?*' Het kan voorkomen dat er nog wel hogere beschikbaarheids- en integriteitseisen nodig zijn. BBN1 is waar alle overheidssystemen als minimum aan moeten voldoen.

BBN2 : Voor informatiesystemen binnen de overheid vormt BBN2 het uitgangspunt. Voor BBN2 en BBN2+ ligt de nadruk op de bescherming van de meest voorkomende categorieëninformatie volgens het principe '*valt de maatregel onder goed huisvaderschap en toont deze beveiliging de betrouwbare overheid?*'

BBN2 is van toepassing indien:

- er vertrouwelijke informatie wordt verwerkt;
- mogelijke incidenten leiden tot bestuurlijke commotie;
- de veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem.

BBN2+ : het komt voor dat een proces of systeem een hoger beschermingsniveau nodig heeft dan BBN2, maar dat weerstand tegen statelijke actoren niet per se noodzakelijk is. Voor die situaties is het niveau BBN2+ van toepassing.

BBN3 : BBN3 richt zich op de bescherming van als Departementaal Vertrouwelijk en vergelijkbaar vertrouwelijk bij andere overheidslagen gerubriceerde informatie, waarbij weerstand geboden moet worden tegen de dreiging, zoals Advanced Persistant Threats (APT's), die uitgaat van statelijke actoren en beroepscriminelen. BBN3 is van toepassing indien hoog niveau van beveiliging. Er zijn maar 3 vragen die gesteld moeten worden om op het niveau van BBN3 uit te komen:

1. Is er weerstand vereist tegen statelijke actoren?
2. Heeft de informatie die ontvangen is een bepaalde classificatie (boven BBN2) meegekregen van de (externe) bronhouder?
3. Is er weerstand nodig tegen georganiseerde misdaad en zware criminaliteit?

Als één van deze vragen met JA kan worden beantwoord, dan is BBN3 van toepassing.

Het bepalen van de basisbeveiligingsniveaus moet gezien worden in relatie tot de implementatie van de baseline. Het uitgangspunt van de BIO is dat een organisatie die de baseline volledig heeft geïmplementeerd de generieke beveiliging op orde heeft. Daarom hoeft de organisatie weinig aanvullende maatregelen te treffen voor de systemen van BBN2 (en 1) maar mogelijkerwijs wel voor de systemen op BBN3.

Daarnaast geldt dat het bepalen van de beveiligingsniveaus een project is dat in drie jaar wordt uitgevoerd en telkens per onderzocht systeem inzicht oplevert of en welke aanvullende maatregelen nodig zijn. De uitvoering van die maatregelen kan dus vrijwel meteen beginnen mits gelijktijdig aan de implementatie van de BIO wordt gewerkt.

Het behoort tot de rol van het management, proceseigenaar en/of systeemeigenaar van de Friese Waddeneilanden om door middel van een risicoanalyse per systeem vast te stellen welk beveiligingsniveau nodig is. Dat geldt voor bestaande en nieuwe informatiesystemen. Het aanpassen van bestaande systemen is echter arbeidsintensief en kostbaar. Vooraf maatregelen treffen is namelijk veel effectiever en goedkoper dan achteraf repareren.

De taakstelling voor deze planperiode is daarom vierledig:

1. toepassing van de volledige BIO op de gemeentelijke ICT-infrastructuur;
2. op elk IV/ ICT-project wordt het principe van 'security by design' toegepast;

3. uiterlijk aan het eind van de planperiode is voor elk gemeentelijke informatiesysteem bepaald welke Basisbeveiligingsniveau van toepassing is en welke eventuele extra beveiligingsmaatregelen nodig zijn;
4. door opsplitsing in deelprojecten worden maatregelen gaandeweg in gang gezet.

2.6. Reikwijdte

De reikwijdte van informatiebeveiliging omvat de opslag en uitwisseling van informatie in alle verschijningsvormen binnen alle interne processen met onderliggende informatiesystemen. Dit beleid omvat derhalve niet alleen de beveiliging van **digitale** informatie binnen de ICT-infrastructuur van de Friese Waddeneilanden (de technische infrastructuur van hardware en applicaties / informatiesystemen), maar omvat ook alle informatie daarbuiten zoals digitale informatie (in cloudapplicaties en op digitale gegevensdragers), **analoge** informatie (op fysieke gegevensdragers zoals papier) en zelfs **impliciete** / 'mondelinge' informatie (kennis en ervaring van mensen die kan worden geuit).

Het omvat het gebruik van deze informatie door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht de locatie, het tijdstip en het gebruikte proces, software of apparatuur. Het gaat bij informatiebeveiliging dus niet alleen over ICT: verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid. Informatiebeveiliging is uitdrukkelijk niet gelijk aan de bescherming van privacy. Privacy heeft als primaire doelstelling vertrouwelijkheid van persoonsgegevens te waarborgen.

Informatiebeveiliging is de belangrijkste randvoorwaarde / een zeer belangrijk middel om privacy aantoonbaar te kunnen garanderen. Informatiebeveiliging gaat dus breder dan privacy, omdat het ook randvoorwaardelijk is voor de bescherming van de vitale maatschappelijke functies, die worden ondersteund / gereguleerd met informatie (verkeer/vervoer, openbare orde en veiligheid, waterstanden, et cetera).

Dit beleid omvat de algemene basis voor de gehele informatiebeveiliging binnen de Friese Waddeneilanden. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke beveiligingseisen, zoals bijvoorbeeld in het sociale domein voor Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI) en de gemeentelijke basisregistraties (BAG, BGT, BRO, BRP, WOZ).

2.7. De 10 bestuurlijke principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op de BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De BIO positioneert de bestuurder en het management sterker in de rol waarin hij of zij meer risico-gebaseerd stuurt op het gebied van informatieveiligheid. Om nadere invulling te geven aan risicomanagement zijn door de VNG ‘De 10 bestuurlijke principes voor informatiebeveiliging’ ontwikkeld. In bijlage 1 van dit beleidsstuk staat een uitvoerige beschrijving van deze bestuurlijke principes. Hieronder staat een kort overzicht van de 10 bestuurlijke principes die het college overneemt:

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

2.8. Relatie tussen informatiebeveiliging en privacy

Informatiebeveiliging en privacy zijn termen die soms door elkaar worden gebruikt. Informatiebeveiliging en privacy zijn echter twee verschillende begrippen. Ze hebben wel een gemeenschappelijk raakvlak. Informatiebeveiliging heeft een bredere scope dan de bescherming van enkel persoonsgegevens. Informatiebeveiliging draait om de bescherming van alle gevoelige informatie tegen aantasting van integriteit, vertrouwelijkheid en beschikbaarheid. Bijvoorbeeld ook de beveiliging van politiek gevoelige of financiële gegevens. Een informatiebeveiligingsincident hoeft daarom niet altijd een datalek te betreffen. Dat is enkel het geval wanneer er persoonsgegevens betrokken zijn.

Een adequate informatiebeveiliging (van persoonsgegevens) is wettelijk verplicht voor gemeenten om te kunnen voldoen aan de Algemene Verordening Gegevensbescherming (AVG), de Europese privacywet. Artikel 32 van de AVG schrijft voor dat:

“Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen”.

De bescherming van persoonsgegevens maakt daarmee onderdeel uit van informatiebeveiliging. De AVG laat de inschatting van risico’s en het bepalen van de benodigde maatregelen over aan de verwerkingsverantwoordelijke (de gemeente). Normenkaders als de BIO helpen de gemeente om de risico’s goed in te schatten en de benodigde maatregelen te treffen. Hoe de Friese Waddeneilanden omgaan met privacy en de AVG is beschreven in de ‘*Beleidsnotitie gegevensbescherming Gemeente Leeuwarden’*.

Door informatiebeveiliging te organiseren en door het nemen van passende maatregelen worden persoonsgegevens beschermd om beveiligingsincidenten en datalekken te voorkomen. De organisatie beschikt over een Functionaris Gegevensbescherming (FG), die onafhankelijk toezicht houdt op de naleving van de AVG. Het toezicht strekt zich daarbij ook uit tot het nemen van voldoende technische- en organisatorische maatregelen om (persoons)gegevens te beschermen.

2.9. Relatie met informatiebeleid en ICT-beleid

Het informatiebeveiligingsbeleid heeft een sterke relatie met het informatiebeleid en het ICT-beleid. Ambities uit het IT-jaarplan en aanpassingen in het ICT-landschap worden vertaald naar projecten in de organisatie. Per project of nieuw informatiesysteem wordt in samenspraak met de Chief

Information Security Officer (CISO), op grond van risico, beoordeeld of er voldoende beheersingsmaatregelen zijn getroffen om de informatieveiligheid te kunnen waarborgen.

Ook is er een sterke samenhang tussen informatiebeveiliging en ICT. Het ICT-beleid vormt de kaders en uitgangspunten waarmee de ICT-omgeving en het beheer van de omgeving is ingericht. Uitgangspunten voor netwerkbeveiliging, systeem-hardening, patching, logging en monitoring uit het ICT-beleid dienen in lijn te zijn met het informatiebeveiligingsbeleid.

Omdat belangen bij het gebruik van informatie, het inrichten van het ICT-landschap en de beveiliging van informatie kunnen verschillen, is informatieveiligheid 'buiten de lijn' ingericht. Zo is de functie van CISO niet ondergebracht bij ICT om zijn gezags- en autoriteitspositie te kunnen uitoefenen en behouden. Het Informatiebeveiligingsbeleid biedt daarmee de noodzakelijke waarborgen voor vertrouwelijkheid, beschikbaarheid, integriteit en controleerbaarheid van informatie. De Information Security Officer (ISO) heeft zitting in het wijzigingsoverleg (Change Advisory Board – CAB) om te waarborgen dat informatieveiligheid wordt meegewogen bij het doorvoeren van wijzigingen in het informatie- en ICT-landschap.

2.10. Grondslagen

De juridische grondslag voor informatiebeveiliging is terug te vinden in wet- en regelgeving, zoals onder meer in de Algemene Verordening Gegevensbescherming (AVG). Informatiebeveiliging en bescherming van persoonsgegevens zijn onlosmakelijk met elkaar verbonden. De AVG stelt dat organisaties passende technische en organisatorische maatregelen moeten treffen in het kader van informatiebeveiliging om op een adequate manier persoonsgegevens te beschermen. Deze maatregelen maken deel uit van het informatiebeveiligingsbeleid van een gemeente. De gemeente dient zich aan diverse wetten en regelgeving te houden, waaruit maatregelen ontstaan op het gebied van informatiebeveiliging. Wetten en regelingen die van toepassing zijn (niet limitatief):

- De Algemene Verordening Gegevensbescherming (AVG)
- De Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)
- De Wet politiegegevens (Wpg)
- De Wet Computercriminaliteit III
- Burgerlijk Wetboek, de Telecommunicatiewet, de Auteurswet, de Wet op de Jaarrekening, de Archiefwet en het Wetboek van Strafvordering, etc. Deze bevatten in het algemeen een resultaatverplichting tot een passend niveau van informatiebeveiliging.
- Wet algemene bepalingen Burgerservicenummer
- Archiefwet
- Participatiewet, Wmo en Jeugdwet
- De BIO is een afgeleide van de Code voor Informatiebeveiliging (NEN/ISO 27002)

Het gemeentebrede informatiebeveiligingsbeleid is een algemene basis. Voor bepaalde (kern)taken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen of normenkaders. Dit zijn:

- BRP (Basisregistratie persoonsgegevens)
- BAG (Basisregistraties Adressen en Gebouwen)
- WOZ (Basisregistratie Waardering Onroerende Zaken)
- BGT (Basisregistratie Grootschalige Topografie)
- BOR (Beheer openbare ruimte)
- BRO (basisregistratie ondergrond)
- SUWI (wet Structuur Uitvoering Werk en Inkomen)
- DigiD (Digitale Identiteit bij de overheid)
- PUN (Paspoort Uitvoeringsregeling Nederland)

2.11. Borging van de informatiebeveiliging

De Friese Waddeneilanden kopen informatiebeveiliging in via het SSC. Het SSC maakt voor de borging van informatiebeveiliging gebruik van een Information Security Management System (ISMS). Een ISMS is een procesgerichte benadering voor informatiebeveiliging en bestaat uit een Plan-Do-Check-Act cyclus (PDCA-cyclus) om aantoonbaar grip te blijven houden op de diverse voorbereidende, uitvoerende, beherende en controlerende activiteiten die periodiek nodig zijn om informatieveiligheid naar een hoger niveau te tillen. Het helpt onder andere om risico's te beheersen, passende beveiligingsmaatregelen te treffen, lering te trekken uit incidenten en daarmee de betrouwbaarheid en de kwaliteit van de informatievoorziening en bedrijfscontinuïteit te waarborgen.

Om verder borging en controle van het informatiebeveiligingsbeleid en de daarvan afgeleide plannen te realiseren, vinden periodiek risicoanalyses plaats. Daarnaast wordt gewerkt met de BIO als normenkader om gericht te werken aan het verhogen van de informatieveiligheid.

De stand van de informatiebeveiliging wordt jaarlijks beschreven in een beveiligingsplan. Maatregelen worden vastgelegd in een uitvoeringsplan dat in co-creatie met de teamleiders en het management tot stand komt. Het uitvoeringsplan wordt daarbij opgesteld vanuit registraties in het ISMS.

Het beveiligingsplan en het uitvoeringsplan worden jaarlijks afgestemd met directieteam en vastgesteld door het College.

2.12. Samenwerking met gemeenten, ketenpartners, leveranciers en instanties

Shared Service Centrum

Binnen deze samenwerking is de rol van het Shared Service Centrum (SSC) vastgelegd en als ambtelijke organisatie geplaatst bij de Friese Waddeneilanden. Het SSC levert diensten op het gebied van Financiën, Communicatie, Facilitair Beheer, PO&O, Informatiemanagement en ICT. Voor ICT houdt dit in dat het SSC Leeuwarden opereert als centrumgemeente voor de levering, dan wel uitbesteding, van ICT-faciliteiten (infra-omgeving, werkplekken, telefonie e.d.). Deze faciliteiten worden door SSC-ICT ingekocht en uitgerold ten behoeve van de samenwerkende organisaties. De organisaties leveren daarbij regulier wensen aan met betrekking tot deze voorzieningen. Deze samenwerkingsvorm kan als klant-leverancier-model worden gezien.

De samenwerking is contractueel vastgelegd in een aantal overeenkomsten:

- Centrumregeling: dit is een juridische vorm van een Gemeenschappelijke Regeling (GR) waarin de centrumgemeente taken en functies uitvoert voor andere gemeenten;
- Service Level Agreement (SLA): document waarin de kwaliteit van de geleverde diensten staat beschreven;
- Productendienstencatalogus (PDC): in deze catalogus staan alle producten en diensten die geleverd (kunnen) worden;
- Dossier Afspraken en Procedures (DAP): dit dossier bevat specifieke operationele uitvoeringsafspraken die gemaakt zijn met de afnemer.

Naast deze formeel vastgelegde vormen van samenwerking, worden er specifieke afspraken gemaakt over de samenwerking. Dit kan per gremium, type dienstverlening en project/programma verschillen. Hoe de samenwerking wordt ingericht hangt af van de behoefte en kan verlopen van klant-leverancier-relatie tot een relatie van gelijkwaardige partners.

Informatiebeveiliging: Centrale (SSC) en lokale verantwoordelijkheden in de regionale samenwerking

Het SSC faciliteert een (veilige) werkplekomgeving met kantoorautomatisering en biedt technische platform-hosting aan voor bedrijfsapplicaties van de afnemer. Om te voorkomen dat individuele uitgangspunten of afspraken zwakheden veroorzaken, gelden de ICT-beveiligingsmaatregelen van de Gemeente Leeuwarden als uitgangspunt. Denk hierbij aan virusscanning, firewall-instellingen, wachtwoordbeleid, e-mailfiltering en andere maatregelen die worden genomen op de informatiebeveiliging te borgen.

Het SSC is niet verantwoordelijk voor het functioneel beheren van de intern gehoste bedrijfs-applicaties van de afnemer tenzij hier, bijvoorbeeld voor het gebruik van generieke systemen, afspraken over zijn gemaakt om het (volledige) technische en functioneel beheer centraal bij het SSC uit te laten voeren. De afnemer is zelf verantwoordelijk voor het veilig beheren van de gemeentelijke bedrijfsapplicaties. Denk hierbij aan het veilig inrichten van bedrijfsapplicaties en het uitvoeren van privacy- en security risicoanalyses om daarmee passende technische en organisatorische maatregelen vast te stellen die zijn gebaseerd op te beschermen belangen en relevante dreigingen van de informatievoorzieningen. Dit kunnen maatregelen zijn in de vorm van logische toegangsbeveiliging, autorisaties, het wijzigingsbeheer (applicatie-updates, wijzigingen functionele inrichting etc.), het patch-management van applicaties (het proces voor het repareren ‘patchen’ van bekende (beveiligings-)problemen in software) en het leveranciersmanagement (contracten en verwerkersovereenkomsten waarin afspraken worden vastgelegd over de verwerking van persoonsgegevens). In onderstaande tabel zijn bovenstaande taakverantwoordelijkheden uitgewerkt.

Taak/Verantwoordelijkheid	Shared Service Centrum (SSC)	Lokale organisatie
Technisch beheer ICT-omgeving	•	
Netwerkbeheer	•	
Technisch applicatiebeheer bedrijfsapplicaties	•	
Werkplek inclusief kantoorautomatisering	•	
Functioneel beheer bedrijfsapplicaties	Alleen voor bepaalde generieke (basis-)applicaties	•
Wijzigingsbeheer en patch-management applicaties	Procesondersteuning via het SSC	•
Leveranciersmanagement	Centraal voor Centric-applicaties ten behoeve van de samenwerking	•

Taak/Verantwoordelijkheid	Shared Service Centrum (SSC)	Lokale organisatie
Autorisaties en logische toegangsbeveiliging bedrijfs-applicaties		•
Privacy- en security-risicoanalyses		•
Bewustwordingsprogramma privacy en informatiebeveiliging		•

• = Taakverantwoordelijke

De gemeentelijke samenwerkingspartner en het Shared Service Centrum (SSC) zijn verplicht om aan de Baseline Informatiebeveiliging Overheid (BIO) te voldoen. Gezien de onderlinge afhankelijkheden die ontstaan door de samenwerking via het SSC streven alle afnemers zo veel mogelijk naar een gelijkluidend informatiebeveiligingsbeleid, gebaseerd op wet- en regelgeving en landelijke normen zoals de Algemene verordening gegevensbescherming (AVG), de Baseline Informatiebeveiliging Overheid (BIO) en 'best practices', uitgewerkt in regels voor onder informatiegebruik, bedrijfscontinuïteit en naleving.

Security Incident Response Team (SIRT)

De afnemers hebben de plicht het Security Incident Response Team (SIRT) van de Gemeente Leeuwarden (bestaande uit het hoofd ICT, de ICT-architect, de Operational Security Officer ICT, de Information Security officer (ISO) en de CISO) direct op de hoogte brengen bij beveiligingsincidenten die zich binnen deelnemende organisaties voordoen die gevolgen kunnen hebben voor de samenwerking. De melding heeft als doel dat het SIRT kan afwegen of een incident bij één organisatie ook gevolgen heeft of maatregelen vraagt voor andere deelnemende gemeenten en organisaties. Het Shared Service Centrum heeft de plicht de afnemers te informeren over beveiligingsincidenten die voor de samenwerking gevolgen kunnen hebben. De Chief Information Security Officer (CISO) van de Friese Waddeneilanden zal hierover de security officer of de directie van de afnemer informeren.

Samenwerking met leveranciers, ketenpartners en instanties

De Gemeente Leeuwarden betrekt ook veel diensten van verschillende leveranciers en ketenpartners, bijvoorbeeld voor haar ICT-infrastructuur en informatiesystemen. Door de steeds verdergaande samenwerking en professionalisering van de Gemeente Leeuwarden nemen de digitalisering van de interne en externe informatievoorziening en de digitale dienstverlening verder toe. Daarvoor worden (informatie-)systemen intern en extern met een toenemend aantal ketenpartners gekoppeld. Door deze koppelingen ontstaat een steeds complexere infrastructuur van informatiesystemen die de basis vormt voor de totale informatievoorziening. Daarmee zijn de Friese

Waddeneilanden afhankelijker geworden van de goede en veilige werking van deze (informatie-)voorzieningen.

Het is van belang om met de leveranciers goede afspraken te maken over de aard van de dienstverlening. Met deze leveranciers en ketenpartners, waar informatiebeveiliging een rol speelt, worden op voorhand afspraken gemaakt over het vereiste niveau van informatiebeveiliging dat de Gemeente Leeuwarden stelt. Afspraken worden vastgelegd in overeenkomsten. De Gemeente Leeuwarden hanteert hiervoor standaard-overeenkomsten, die landelijk beschikbaar gesteld worden zoals de GIBIT-inkoopvoorwaarden en de standaard verwerkersovereenkomsten, die afgeleid is van de VNG-standaard, waarin afspraken worden vastgelegd dat een derde partij zorgvuldig met persoonsgegevens om springt en zich houdt aan de gemaakte afspraken.

Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Deze controles worden uitgevoerd aan de hand van het periodiek opvragen en beoordelen van certificaten en onafhankelijke verklaringen die laten zien dat een leverancier voldoet aan alle eisen rondom informatiebeveiliging en uitgevoerde security-assessment (penetratietesten) en (geautomatiseerde) kwetsbaarheidsanalyses waarmee inzicht wordt verkregen of de leverancier voldoet aan de geschiktheidseisen die gesteld zijn tijdens de aanbesteding.

3. Verantwoording informatiebeveiligingsbeleid

Het is van belang dat een gemeentelijke organisatie verantwoording aflegt over het door haar gevoerde beleid. In 2017 is het landelijke project ENSIA (Eenduidige Normatiek Single Information Audit) gestart om zorg te dragen voor een voor de overheid uniforme wijze van verantwoording over informatiebeveiliging. ENSIA helpt gemeenten in één keer slim verantwoording af te leggen over informatieveiligheid gebaseerd op de BIO (Baseline Informatiebeveiliging Overheid). De verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).

ENSIA maakt daarbij onderscheid tussen de horizontale en de verticale verantwoording, waarbij de horizontale verantwoording als basis dient voor de verticale verantwoording. Uitgangspunt is het horizontale verantwoordingsproces aan de gemeenteraad. Dit vormt de basis voor het verticale verantwoordingsproces aan nationale partijen die een rol hebben in het toezicht op informatieveiligheid. Bij het afleggen van verantwoording wordt het principe van single information single audit toegepast; alle informatie die noodzakelijk is voor verticale verantwoording is ook onderdeel van het horizontale verantwoordingsproces.

3.1. Horizontale verantwoording

De Baseline Informatiebeveiliging Overheid (BIO) vormt met ingang van 01-01-2020 de kern van de verantwoording over informatieveiligheid aan de gemeenteraad. De ‘horizontale verantwoording’ bestaat uit een zelfevaluatie, een IT-audit, een Collegeverklaring ENSIA inzake DigiD en Suwinet en een passage over informatieveiligheid in het jaarverslag.

3.2. Verticale verantwoording

Over informatiebeveiliging en in het bijzonder de BRP, PUN, Suwinet, BRO, BAG, BGT en DigiD moeten gemeenten ook verantwoording afleggen richting toezicht- en stelselhouders, ook wel ‘verticale verantwoording'. De horizontale verantwoording, waaronder de zelfevaluatie, een IT-audit, en een verklaring van het College van B&W vormt de basis voor deze verticale verantwoording.

3.3. Informatiebeveiligingsplan

Het informatiebeveiligingsplan vormt samen met dit beleidsstuk de fundering van de informatiebeveiliging van de Friese Waddeneilanden. De kernelementen in dit informatiebeveiligingsplan zijn:

- Beschrijving van het huidige niveau van informatiebeveiliging, waarbij de huidige situatie van de informatiebeveiliging wordt afgezet tegenover de maatregelen beschreven in normenkaders, waaronder de Baseline Informatiebeveiliging Overheid (BIO);
- Recente ontwikkelingen op het gebied van informatiebeveiliging, zoals het in productie nemen van nieuwe informatiesystemen, gewijzigde wet- en regelgeving, dreigingen, of beveiligingsincidenten;
- Risicoafweging, waarbij duidelijk is beschreven welke risico`s de organisatie loopt, welke risico`s worden beheerst, en welke risico`s de organisatie (tijdelijk) accepteert;
- Een overzicht van de aanwezige (informatie)systemen waarbij is aangegeven welke systemen bedrijfs-kritisch zijn op basis van classificatie en risicoanalyse. Het overzicht wordt als bijlage aan het informatiebeveiligingsplan toegevoegd.

Het informatiebeveiligingsplan wordt jaarlijks geactualiseerd en besproken met de portefeuillehouder, de gemeentesecretaris, het directieteam (DT), de concerncontroller, de Chief Information Officer (CIO) en het Bedrijfsvoeringsplatform (BVP). Het informatiebeveiligingsplan wordt vervolgens vastgesteld door het college van burgemeester en wethouders.

3.4. Uitvoeringsplan Informatiebeveiliging

Het uitvoeringsplan informatiebeveiliging is onderdeel van het informatiebeveiligingsplan. In het uitvoeringsplan staan concrete acties beschreven om nieuwe (BIO-)maatregelen te implementeren, en-/of bestaande maatregelen te verbeteren. De maatregelen vloeien voort uit wet- en regelgeving, normenkaders zoals de BIO, BBN-toetsen, ENSIA, interne wijzigingsprocessen (change) of dataclassificatie en aanvullende risicoanalyse.

Het uitvoeringsplan komt in co-creatie met de betrokken teams tot stand. In het uitvoeringsplan staan maatregelen helder omschreven, geprioriteerd o.b.v. risico en zijn verantwoordelijkheden benoemd. De maatregelen zijn, waar mogelijk, aangevuld met een kostenaanduiding en voorzien van een realistisch tijdspad.

Het uitvoeringsplan, en de voortgang van geplande maatregelen, wordt eens per jaar besproken met de portefeuillehouder, het Directieteam (DT), de concerncontroller, de Chief Information Officer (CIO) en het Bedrijfsvoeringsplatform (BVP). In het overleg wordt de voortgang van implementatie van maatregelen besproken en vindt waar nodig bijstelling plaats van het uitvoeringsplan.

Naast het implementeren van de BIO, past de organisatie dataclassificatie en risicoanalyse toe ten aanzien van belangrijke processen, informatieverzamelingen en informatiesystemen. Samen met de proceseigenaar en/of systeemeigenaar, applicatiebeheerder, systeembeheerder en andere betrokkenen worden dreigingen en kwetsbaarheden in kaart gebracht die kunnen leiden tot een beveiligingsincident. Mitigerende maatregelen worden afhankelijk van risico geprioriteerd en opgenomen in het kwaliteitsbeheersysteem Information Security Management System (ISMS) en toegevoegd aan het uitvoeringsplan informatiebeveiliging.

4. Organisatie van de informatiebeveiliging

De wijze waarop het informatiebeveiligingsbeleid binnen de gemeente is verankerd, vormt het fundament van de borging van informatiebeveiliging. Het bestuur, de directie en het teammanagement spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Om informatiebeveiliging te beheren en blijvend te borgen in de gemeentelijke organisatie zijn duidelijke afspraken nodig over verantwoordelijkheden, taken en rollen. Het gaat hier over de governance rond informatiebeveiliging waarbij onderlinge samenwerking bepalend is voor het succes. In dit hoofdstuk zijn de verantwoordlijkheden voor de interne organisatie en voor de gemeenteraad, als toezichthouder, nader uitgewerkt.

4.1. De gemeenteraad

De gemeenteraden van de Friese Waddeneilanden dragen specifieke bevoegdheden voor de controle en de toetsing op de werking van beleid binnen de gemeenten, zo ook voor informatieveiligheid. Door de geplande invoering van de Eenduidige Normatiek Single Information Audit (ENSIA) legt het College in het jaarverslag direct verantwoording af aan de gemeenteraad over het onderwerp informatiebeveiliging.

4.2. Interne organisatie

In relatie tot informatiebeveiliging onderscheiden we voor de interne organisatie van de Friese Waddeneilanden de volgende verantwoordelijkheden.

4.2.1. College B&W

Het college van B&W is bestuurlijk verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeente en stelt kaders op voor informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders. Het college van B&W stelt formeel het informatiebeveiligingsbeleid vast, delegeert de uitvoering hiervan aan het directieteam en informeert de gemeenteraad over dit thema.

Binnen het college van B&W valt informatiebeveiliging onder de portefeuille van een van de portefeuillehouders. Het directieteam adviseert het college van B&W formeel over het vast te stellen beleid. Het college van Burgemeester en Wethouders handelt volgens, in overeenstemming met de 10 bestuurlijke principes informatieveiligheid (zie paragraaf 2.5)

4.2.2. Directie

De gemandateerde verantwoordelijkheid voor informatieveiligheid ligt bij de directie. De directie stelt het gewenste niveau van informatieveiligheid vast voor de gemeente.

De directie is ambtelijk verantwoordelijk voor de beveiliging van informatie en de daarbij behorende algemene sturing.

Het directieteam:

- stuurt de organisatie aan op beveiligingsrisico's;
- stelt jaarlijks het informatiebeveiligingsplan en uitvoeringsplan vast in een directieoverleg;
- ziet erop toe dat de teamleiders adequate maatregelen genomen hebben voor de bescherming van de informatie, gegevensverzamelingen en informatiesystemen, die onder hun verantwoordelijkheid vallen;
- controleert of de getroffen maatregelen overeenstemmen met de beveiligingseisen en of deze voldoende bescherming bieden;
- evalueert periodiek beleidskaders en stelt waar nodig bij;
- handelt conform de 10 bestuurlijke principes informatieveiligheid (zie paragraaf 2.5).

4.2.3. Concerncontroller

De concerncontroller toetst in samenspraak met de CISO of de vastgestelde beveiligingsmaatregelen worden nageleefd. De concerncontroller staat buiten het primaire proces en is onafhankelijk. De concerncontroller heeft een onafhankelijke positie en kan het bestuur gevraagd en ongevraagd adviseren.

4.2.4. Chief Information Officer (CIO)

De Chief Information Officer (CIO) van de Gemeente Leeuwarden is ook verantwoordelijk voor het strategische informatiebeleid en informatiemanagement van de Friese Waddeneilanden. De CIO zorgt ervoor dat onze informatievoorziening goed aansluit op de doelstellingen van de organisatie. ICT, de bedrijfsstrategie en de organisatie zijn daarbij belangrijke aandachtsgebieden voor de CIO. In de samenleving neemt informatievoorziening en ICT – denk daarbij aan grote thema's als bijvoorbeeld cloud computing, het nieuwe werken en de slimme samenleving – een steeds belangrijke positie in. De CIO speelt een sleutelrol in de innovatieve samenwerking met Leeuwarden, gericht op slimme oplossingen voor de opgaven binnen de snelgroeiende stad.

4.2.5. Teamleiders/Coördinatoren

Teamleiders/Coördinatoren zijn operationeel eindverantwoordelijk voor de integrale beveiliging binnen hun organisatieonderdelen, bedrijfsprocessen, gegevensverzamelingen en informatiesystemen. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal 1 eigenaar hebben, er moet dus altijd iemand verantwoordelijk zijn.

De manager en teamleiders:

- voeren maatregelen uit, die op grond van de BIO op het team van toepassing zijn, en die zijn opgenomen in het uitvoeringsplan informatiebeveiliging;
- voeren maatregelen uit, als uitkomst van dataclassificatie en/ of risicoanalyse, van een informatiesysteem waarvan zij systeemeigenaar zijn ;

- voeren maatregelen uit, als uitkomst van dataclassificatie en/ of risicoanalyse, van een proces waarvan zij proceseigenaar zijn ;
- stellen op basis van een expliciete risicoafweging beveiligingseisen vast voor informatiesystemen en processen en zijn verantwoordelijk voor het uitdragen van de maatregelen die voortvloeien uit deze eisen;
- houden zich strikt aan de procedures voor indiensttreding, doorstroom en uitdiensttreding waarbij autorisaties, toegangsmiddelen en bedrijfsmiddelen tijdig worden aangevraagd en tijdig worden beëindigd en/of ingenomen;;
- dragen er zorg voor dat aanvragen voor (systeem)autorisaties, toegangsmiddelen, en bedrijfsmiddelen in overeenstemming zijn met de uit te voeren werkzaamheden van medewerkers;
- controleren periodiek of aan medewerkers toegekende autorisaties en bedrijfsmiddelen nog benodigd zijn voor het uitoefenen van de functie
- sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en bewustzijn);
- melden incidenten en datalekken en rapporteert in hoeverre hun organisatieonderdeel voldoet aan het informatiebeveiligingsbeleid van de gemeente;
- houden zich aan het wijzigingsmanagement bij nieuw te implementeren ICT oplossingen.

4.2.6. Personeel, Organisatie en Ontwikkeling (PO&O)

Het team is verantwoordelijk voor:

- het actueel houden en uitdragen van procedures voor in- en uitdiensttreding en wijziging van functie;
- screening van nieuwe medewerkers;
- het in ontvangst nemen en beoordelen van Verklaringen Omtrent het Gedrag (VOG).

4.2.7. Informatie & Communicatie Technologie (ICT)

Informatie & Communicatie Technologie (ICT) van het Shared Service Centrum is (mede)verantwoordelijk voor:

- het verzorgen van de beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen die voortvloeien uit de beveiligingseisen en bijbehorende risicoanalyse;
- het beheren van werkplekken, telefonie, serverplatformen, lokale netwerken, WIFI, externe netwerkverbindingen zoals VPN-verbindingen, GEMnet, Digikoppeling, Enterprise Service Bus, en verzorgt het technische (wijzigings-)beheer van databases, bedrijfsapplicaties en kantoorautomatiseringshulpmiddelen;
- alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen;

- alle beheeraspecten van informatiebeveiliging die betrekking hebben op ICT-aangelegenheden zoals incident- en probleemmanagement, configuratie- en wijzigingsbeheer, hardening, patching, logging van activiteiten, back-up & recovery en uitwijk;
- het actief acteren op acute dreigingen die een gevaar vormen voor de informatievoorziening.

4.2.8. Chief Information Security Officer (CISO)

De CISO heeft een adviserende, faciliterende en coördinerende rol en zorgt ervoor dat taken belegd zijn op het gebied van informatiebeveiliging. De CISO is verantwoordelijk voor:

- het actueel houden van het informatiebeveiligingsbeleid en het informatiebeveiligingsplan;
- het inrichten van de informatiebeveiligingsorganisatie;
- de voorbereiding op toekomstige informatiebeveiligingsrisico's en ICT-beveiligingsrisico's o.b.v. het dreigingsbeeld Nederlandse Gemeenten;
- het gevraagd en ongevraagd adviseren van het college, het directieteam, managers, teamleiders en de concerncontroller;
- het opstellen van het beveiligingsplan en uitvoeringsplan op en het verzorgen van de actualisatie van deze plannen;
- het toezien op de voortgang van de realisatie van beveiligingsmaatregelen zoals vastgelegd in beveiligingsplannen waaronder ook de specifieke beveiligingsplannen voor de BRP, reisdocumenten en rijbewijzen en Suwinet;
- het coördineren van de uitvoering van informatieveiligheidsmaatregelen uit het uitvoeringsplan;
- het twee maal per jaar rapporteren aan het Privacy en Security Overleg (PSO) over de stand van de informatiebeveiliging en de voortgang. Aan het Privacy en Security Overleg (PSO) wordt deelgenomen voor de Chief Information Officer (CIO), de Concerncontroller, de Functionaris Gegevensbescherming (FG) en de CISO;
- het adviseren van de ontwikkelteams van de Leeuwarden Digitale Agenda op het gebied van security en privacy en voor de aspecten 'Security By Design' en 'Privacy By Design';
- het onderhouden van een intern en extern netwerk rond informatiebeveiliging;
- het aanjagen van bewustwording rond het onderwerp informatiebeveiliging;
- het ondersteunen van projecten die de informatieveiligheid vergroten, waarbij de primaire verantwoordelijkheid voor deze projecten bij het lijnmanagement ligt;
- de afhandeling en evaluatie van incidenten en het bijhouden van een registratie van informatiebeveiligingsincidenten.

4.2.9. Information Security Officer (ISO)

De Information Security Officer (ISO) van de Gemeente Leeuwarden speelt naast de CISO een belangrijke rol in het opstellen van en vertalen van het informatiebeveiligingsbeleid naar (technische) beveiligingsmaatregelen. De ISO draagt zorg de dagelijkse aansturing van

informatiebeveiligingsactiviteiten binnen de gemeente. De ISO ondersteunt het management bij het uitvoeren van risk-assessments en het opstellen van de technische en organisatorische beveiligingseisen op basis van de Baseline Informatiebeveiliging Overheid (BIO). De ISO zorgt in het kader van informatiebeveiliging voor een beveiligingsplan en de daarbij behorende -standaarden, -procedures van de inrichting, kwaliteit en borging, risicoanalyse, risicomonitoring, incidentenregistratie, trainingen en evaluaties.

4.2.10. Operational Security Officer (OSO)

De Operational Security Officer (OSO) van de Gemeente Leeuwarden is verantwoordelijk voor het actief handhaven van het informatiebeveiligingsbeleid. Waar de Chief Information Security Officer (CISO) verantwoordelijk is voor het beleid, de coördinatie en de samenhang van beveiliging, is de Operational Security Officer (OSO) verantwoordelijk voor de uitvoering van de verschillende technische beveiligingsonderwerpen.
De Operational Security Officer zorgt, samen met de CISO, voor een samenhangend pakket van maatregelen ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie

4.2.11. Functionaris Gegevensbescherming (FG)

De Functionaris Gegevensbescherming (FG) van de Gemeente Leeuwarden is de interne toezichthouder voor de Friese Waddeneilanden als het gaat om privacy, naleving van de AVG, en de bescherming van persoonsgegevens. Onder de Europese privacy-verordening (AVG), die sinds mei 2018 van kracht is, zijn alle overheidsorganisaties verplicht een FG aan te stellen. De FG is verantwoordelijk voor het toezicht houden op de naleving van de privacywetten en –regels, het inventariseren en bijhouden van gegevensverwerkingen en het afhandelen van vragen en klachten van mensen binnen en buiten de organisatie. De FG houdt daarbij toezicht op de uitvoering van de technische- en organisatorische maatregelen om persoonsgegevens te beschermen tegen verlies, beschadiging of vernietiging, zoals beschreven in de AVG.

4.2.12. Privacy Officer (PO)

Waar de CISO verantwoordelijk is voor het informatiebeveiligingsbeleid is de Privacy Officer van de Gemeente Leeuwarden (ook wel juridisch adviseur privacy), verantwoordelijk voor het vormgeven en bewaken van het privacybeleid binnen de gemeente. Daarnaast ondersteunt de Privacy Officer (PO) de proces- en systeemeigenaar bij de uitvoering van een PIA. De PO speelt ook een belangrijke rol op de werkvloer, zo heeft zij net als de CISO een adviserende rol richting de vak-afdelingen en kan hij of zij vragen beantwoorden zoals: hoe moeten we deze gegevens delen? Aan welke regels dienen we ons te houden? Welke maatregelen moeten we de externe partij opleggen?

4.2.13. De beveiligingsbeheerder

Voor de volgende specifieke gegevensverzamelingen is een beveiligingsbeheerder aangewezen: BRP, PUN (Beveiligingsfunctionaris), BAG, BGT, SUWI (Security Officer Suwinet) en DigiD. De beveiligings-beheerder is verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid van specifieke gegevensverzamelingen.

4.2.14. Security Officer Suwinet

De Security Officer beheert beveiligingsprocedures en -maatregelen in het kader van Suwinet-Inkijk, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen en normenkaders is geïmplementeerd. De Security Officer Suwinet bevordert en adviseert over de beveiliging van Suwinet, verzorgt rapportages over de status, controleert of maatregelen worden nageleefd, evalueert, adviseert en doet voorstellen voor verbetering van de beveiliging van Suwinet.

De Security Officer Suwinet heeft formeel wat betreft rapportages een bijzondere rol. Deze rapporteert namelijk rechtstreeks aan de bestuurlijk verantwoordelijke en is tevens gemandateerd om specifieke gebruikersrapportage op te vragen wanneer op basis van eigen waarneming een vermoeden bestaat van misbruik of oneigenlijk gebruik van gegevens vanuit Suwinet-Inkijk.