gemeente
SCHIERMONNIKOOG

Gemeenteraad Schiermonnikoog

Zaaknummer::	466909
Datum:	8 april 2025
Bijlagen:	1
Onderwerp:	Informatiebeveiligingsplan
Verzenddatum:	15 april 2025

Geachte leden van de Raad,

Voor u ligt het informatiebeveiligingsbeleid 2025-2029 van de Friese eilanden, vastgesteld door het College van burgemeester en wethouders van Schiermonnikoog. Dit beleid vervangt het in 2020 vastgestelde 'Informatiebeveiligingsbeleid Friese Waddeneilanden'.
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. In dit document zijn deze beleidsuitgangspunten nader uitgewerkt en zijn beveiligingseisen en- maatregelen opgenomen die voor alle medewerkers, processen en systemen van Gemeente Schiermonnikoog gelden. Daarnaast zijn de verantwoordelijkheden voor informatiebeveiliging beschreven.

Wat is informatiebeveiliging
Informatiebeveiliging is het samenhangend stelsel van beheersingsmaatregelen dat de beschikbaarheid, de betrouwbaarheid en vertrouwelijkheid en controleerbaarheid van informatie garandeert. Informatiebeveiliging is geen doel op zich maar moet de primaire bedrijfsprocessen ondersteunen en de veilige en verantwoorde uitvoering daarvan mogelijk maken.
Een overheid die informatiebeveiliging niet omarmt, verliest het vertrouwen van burgers, bedrijven en toezichthouders en daarmee dus haar legitimiteit. Daar waar gesproken wordt over informatie geldt dit ook voor de onderliggende gegevens.

Het begrip informatiebeveiliging heeft aldus betrekking op:

- Beschikbaarheid/ continuïteit: het zorgdragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- Vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.
- Controleerbaarheid: Controleerbaarheid is de mogelijkheid om (achteraf) vast te stellen of ingevoerde beheersmaatregelen werken.

bezoekadres . Nieuwestreek 5 . Schiermonnikoog . postadres . Postbus 20 . 9166 ZP . Schiermonnikoog telefoon (0519) 53 50 50 . e-mail .postbus20@schiermonnikoog.nl . www.schiermonnikoog.nl

Baseline Informatiebeveiliging Overheid (BIO)
Gemeente Schiermonnikoog stemt haar bedrijfsvoering over informatiebeveiliging af op de norm NEN-ENISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). De BIO vormt met ingang van 01-01-2020 één gezamenlijk normenkader voor Overheid, Rijk, Waterschappen en Provincies. De BIO vervangt daarmee de Baseline Informatiebeveiliging Gemeenten (BIG). De BIO is een doorontwikkeling van de BIG en is gebaseerd op de ISO 27002. De BIO legt meer nadruk op risicomanagement en minder nadruk op maatregelen. Een groot verschil met de BIG is dat alle BIO-maatregelen verplichte maatregelen zijn, er is geen sprake meer van 'pas toe of leg uit' principe.

In de BIO zijn de rollen van de bestuurder, lijnmanager, systeemeigenaar en proceseigenaar ten aanzien van risicomanagement explicieter beschreven. Zo hebben alle belangrijke processen een proceseigenaar en belangrijke informatiesystemen een systeemeigenaar. Een nadere uiteenzetting van de BIO is terug te vinden als bijlage 2 van dit beleidsdocument.

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 stel 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 II
- 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)

Scope van het strategische informatiebeveiligingsbeleid
Dit beleid is van toepassing op de gehele organisatie, alle gemeentelijke processen, informatie, informatiesystemen en gegevens(verzamelingen) van de gemeente en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur. Het heeft betrekking op het politiek bestuur, alle medewerkers, inwoners, gasten, bezoekers en externe relaties. Het borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen.
Het gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitbrengen en handhaven van een informatiebeveiligingsbeleid van en voor de hele gemeente.

Financiën
Het vaststellen van dit strategisch Informatiebeveiligingsbeleid past binnen de bestaande begroting en kost geen extra geld. Aan de implementatie van eventuele maatregelen uit dit beleid kunnen wel kosten vastzitten. Voor de komende jaren is hiermee in de begroting rekening mee gehouden.

Met vriendelijke groet,

Ineke van Gent
Burgemeester

Bijlage: Informatiebeveiligingsbeleid 2025-2029