1STROOM DUIVEN & WESTERVOORT

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 346

20 april 2021

Officiële uitgave van de gemeenschappelijke regeling 1Stroom

Besluit van het dagelijks bestuur van het openbaar lichaam 1Stroom houdende regels omtrent de manier hoe 1Stroom zich voorziet in adequate informatiebeveiliging

Informatiebeveiliging gaat over het beschermen van informatie om uiteindelijk de continuïteit van de bedrijfsvoering en dienstverlening te kunnen garanderen.

Samenvatting

Het succes van onze organisatie hangt steeds meer af van informatie, nieuwe technologieën en computersystemen. Die informatie moet goed worden beveiligd, zeker als er persoonsgegevens worden opgeslagen. In dit document is verwoord op welke manier onze organisatie voorziet in adequate informatiebeveiliging en daarmee voldoet aan de relevante wet- en regelgeving. Recente praktijkvoorbeelden zoals de 'Hack van Lochem', de aanval met ransomware bij de Universiteit van Maastricht en de cyberaanval op de gemeente Hof van Twente benadrukken nogmaals het belang van dit onderwerp.
Met het strategisch informatiebeveiligingsbeleid wil de gemeente ook bijdragen aan een betere kwaliteit van de informatievoorziening en zorgen voor een juiste balans tussen functionaliteit, veiligheid en privacy.

Beschreven wordt op wie, op welke onderdelen van onze organisatie en op welke apparaten en applicaties het beleid van toepassing is. Informatiebeveiliging werkt door in alle lagen van de organisatie. Naast de reikwijdte van het beleid worden de taken en verantwoordelijkheden van de betrokken functionarissen beschreven. Het lijnmanagement is verantwoordelijk voor haar eigen processen, de directie zorgt ervoor dat beveiligingsmaatregelen daadwerkelijk worden geïmplementeerd. De eindverantwoordelijkheid van het informatiebeveiligingsbeleid ligt bij het dagelijks bestuur van de Gemeenschappelijke Regeling 1Stroom.

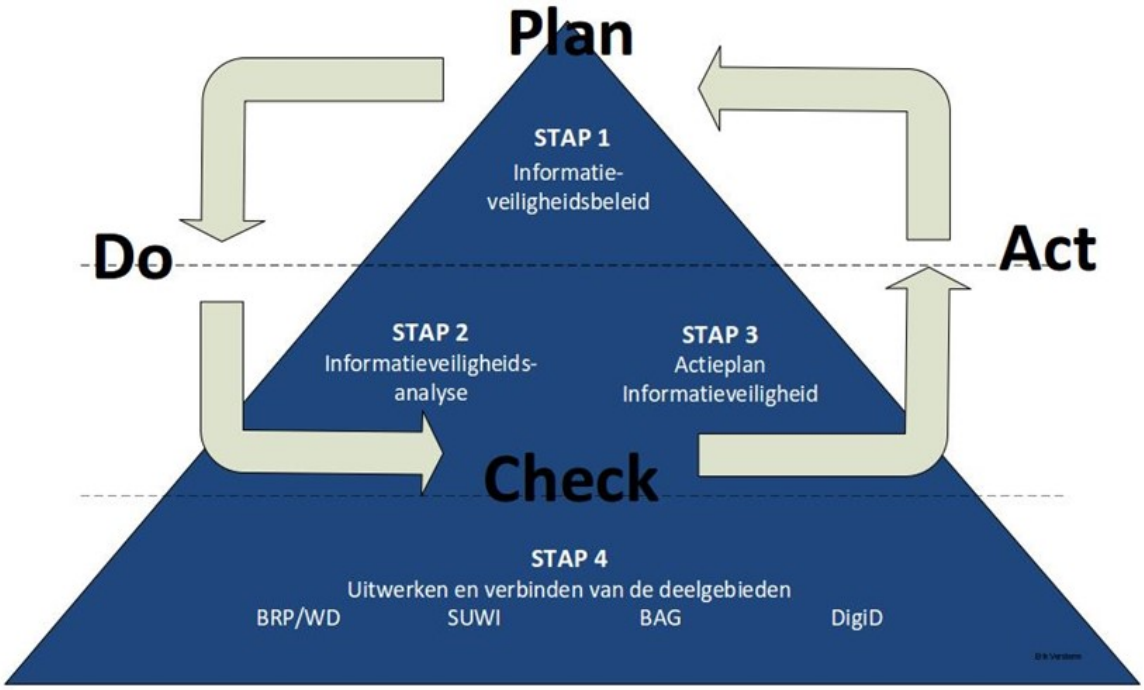
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. De mens zelf creëert de grootste risico's. Daarom is het ook belangrijk en noodzakelijk dat we voortdurend werken aan het vergroten van het beveiligingsbewustzijn van onze medewerkers om de kennis van risico's te verhogen en veilig en verantwoord gedrag aan te moedigen.

Informatiebeveiliging is een continu proces, waarbij we steeds kijken naar mogelijke verbeteringen. Dit gebeurt onder andere door jaarplannen, controles en bijsturing.

In dit plan wordt al vooruitlopend op de doorontwikkeling van onze organisatie gebruik gemaakt van de term afdelingsmanagers.

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2021 tot en met 2023 en vervangt het in 2017 vastgestelde 'Gemeentelijk Informatiebeveiligingsbeleid 2017' van de twee afzonderlijke gemeenten Duiven en Westervoort.
Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau (stap 3) en werkinstructies op operationeel niveau (stap 4).



Figuur 1 Het Strategisch Informatiebeveiligingsbeleid in de PDCA-cyclus

Met dit 'Strategisch Gemeentelijk Informatiebeveiligingsbeleid 2021-2023' zet de GR 1Stroom de volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de organisatie te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO) zie bijlage B. De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG, zie bijlage A.

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatiebeveiligingsbeleid voor de jaren 2021 tot 2023. Het strategisch beleid wordt gebruikt om de basis te leggen voor het tactische beleid en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. Het is het bestuurlijk kader om de beschikbaarheid, integriteit en vertrouwelijkheid van de (persoons)gegevens en andere informatie(systemen) te waarborgen, zodat onze organisatie voldoet aan relevante wet- en regelgeving. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen Informatiebeveiligingsplan (IBP).

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen gemeentelijk Informatiebeveiligingsplan (vastgesteld door de directie) worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de afdelingsmanagers, de CISO, het dreigingsbeeld van de IBD en de uitkomsten van ENSIA. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

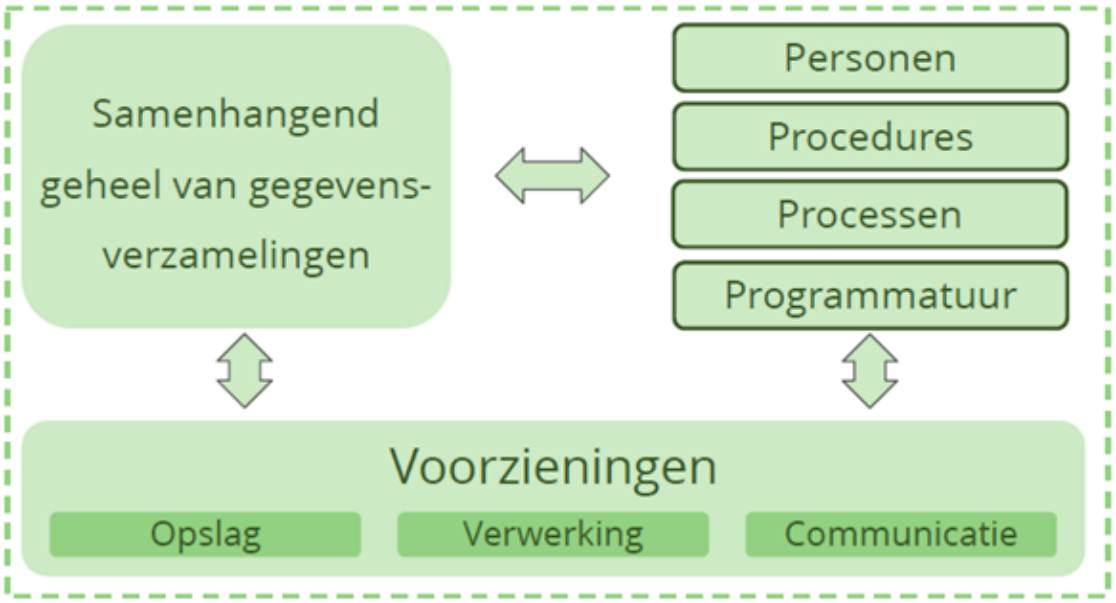
1.2 Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen.

Informatiebeveiliging heeft de volgende doelen:

- Het waarborgen van de beschikbaarheid van informatie van de gemeente.
- Het waarborgen dat informatie juist, volledig en actueel is (integriteit) en alleen toegankelijk is voor personen die vanuit hun rol/functie daar toegang tot mogen hebben (beschikbaarheid, integriteit en vertrouwelijkheid).
- Het voorkomen van beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan verminderen.

Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van de informatiesystemen[1], ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.



Figuur 2 Informatiesysteem

Het beperkt zich niet alleen tot een technisch vraagstuk dat de ICT-afdeling maar moet oplossen. Informatiebeveiliging is een bedrijfsbreed kwaliteitsvraagstuk en heeft betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

1.3 Ambitie en visie van de gemeente in relatie tot informatieveiligheid

De colleges van Duiven en Westervoort, maar ook de Gemeenschappelijke Regeling 1Stroom hebben in de coalitieakkoorden en de Missie & Visie een groot aantal beleidsuitgangspunten en doelen geformuleerd. De ambitie van de beide organen is ook bepalend voor de informatievoorziening en hiermee ook bepalend voor de informatieveiligheid. Om de ambities waar te kunnen maken is een solide inrichting van het informatiebeheer en de informatiebeveiliging noodzakelijk. Daarnaast is de inrichting van de informatiebeveiliging ook zeker bepalend voor de continuïteit van de bedrijfsvoering en de dienstverlening aan onze inwoners en bedrijven.

1.4 Volwassenheidsniveau informatiebeveiliging

Het volwassenheidsmodel informatiebeveiliging biedt ons een handreiking om na te gaan waar wij staan met onze informatiebeveiliging. Het maakt ook duidelijk wat er allemaal nog moet gebeuren om de kroonjuwelen van onze geautomatiseerde gegevensverwerking in onze organisatie en de organisaties waarmee wij samenwerken op orde te krijgen. Daarnaast worden wij ook geconfronteerd met een toenemende druk van wet- en regelgeving ten aanzien van informatiebeveiliging en de bescherming van persoonsgegevens.
Een solide inrichting van informatiebeveiliging aan de voorkant voorkomt gedoe achteraf. Om deze solide inrichting te bereiken, is het noodzakelijk om op het gebied van informatieveiligheid te professi-

1) Informatiesystemen: Een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur. Alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.

onaliseren. Het huidige volwassenheidsniveau van informatiebeveiliging van GR 1Stroom ligt tussen niveau 2 en niveau 3. De realistische ambitie is om in 2023 volwassenheidsniveau 4 te bereiken. Zodra dat niveau bereikt is, heeft de organisatie informatieveiligheid geborgd binnen haar processen. Zij voldoet aan wet- en regelgeving én heeft voldoende kennis om proactief op ontwikkelingen te anticiperen. Zij weet haar risico's te verkleinen tot een acceptabel niveau in lijn met de ambities uit de strategische agenda's van de colleges, de gemeenteraden en 1Stroom.

Niveau 5 – continu verbeterend • De beheersmaatregelen zijn verankerd in het integrale risicomanagementraamwerk, waarbij continu gezocht wordt naar verbetering.
Niveau 4 – beheerst en meetbaar • De effectiviteit van de beheersmaatregelen wordt periodiek geëvalueerd.
Niveau 3 - gedefinieerd • De beheersingsmaatregelen zijn gedocumenteerd en worden op een gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.
Niveau 2 – herhaalbaar • De beheersingsmaatregelen zijn aanwezig en worden op een consistente en gestructureerde, maar informele wijze uitgevoerd.
Niveau 1 – initieel • De beheersingsmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.

Tabel 1 Volwassenheidsniveau 's informatiebeveiliging

Noodzakelijke randvoorwaarde om deze groei te bereiken, is de beschikbaarheid van kwalitatieve en kwantitatieve resources op de afdelingen en bij onze ICT-partner, de RID De Liemers. Dit strategische informatiebeveiligingsbeleid 2021-2023 is het kader om informatie in onze organisatie te beschermen en draagt bij aan een verdere professionalisering van informatiebeveiliging.

1.5 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid zijn de volgende:

1.5.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is veel meer gericht op risicomanagement dan de oude norm, de BIG. Dat wil zeggen dat de afdelingsmanagers nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of de informatie in de bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

1.5.2 De 10 principes voor informatiebeveiliging (zie bijlage A)

De 10 principes voor informatiebeveiliging[2] zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

2) Deze principes zijn gelijk met de BIO in werking getreden, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG).

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

1.5.3 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten[3] geeft jaarlijks een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus en prioritering aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

1.5.4 Informatie uit incidenten en inbreuken op de beveiliging

De gemeente kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.
Daarnaast worden ook steeds meer de 'lesson learned' van incidenten bij andere overheidsorganisaties en semi-overheidsorganisatie gedeeld[4]. Indien van belang en toepassing worden de aanbevelingen en maatregelen ook opgenomen in de activiteitenplanning.

1.6 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen.
Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatie-beveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[5] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. Ook zullen praktische operationele handreikingen worden uitgebracht, zoals een handleiding voor het uitvoeren van een risicoanalyse voor het opstellen van een beveiligingsplan.
De inhoud en structuur van dit document zijn afgestemd op die van de ISO en de BIO. Ook het Informatiebeveiligingsplan zal deze structuur volgen.

1.7 Plaats van het strategisch beleid

Deze nota beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven 'Informatiebeveiligingsplan GR 1Stroom'.

1.8 Scope informatiebeveiliging

De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen (bijvoorbeeld politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.
Dit strategisch Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende algemene beveiligingseisen uit wetgeving af zoals voor de BRP, PNIK (reisdocumenten) en SUWINET. Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI, DigiD en de gemeentelijke basisregistraties). Deze eisen worden in aanvullende documenten geformuleerd.
Bewust wordt in het strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

1.9 Uitgangspunten

Het bestuur, de directie en het afdelingsmanagement spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang, die de verschillende delen van de informatievoorziening voor onze organisatie heeft, de risico's die de organisatie hiermee loopt en welke van deze risico's onacceptabel hoog zijn[6]. Op basis hiervan zet het

3) Laatstverschenen Dreigingsbeeld Informatiebeveiliging 2020/2021 / Cybersecuritybeeld Nederland 2020 NCSC
4) Bijvoorbeeld Leren van Lochem en de Cyberaanval Universiteit Maastricht
5) De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.
6) Zie de bijlage: Informatiebeveiliging en de lijnmanager – Wat is uw rol?

management dit beleid voor informatiebeveiliging op, draagt dit uit naar de medewerkers en de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de organisatie en de relevante landelijke en Europese wet- en regelgeving.

1.9.1 Strategische doelen
De strategische doelen van het informatiebeveiligingsbeleid zijn:
- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewer-kers.
- Het waarborgen van de naleving van dit beleid.

Een groot aantal van de hierboven genoemde punten zijn a.h.w. een invulling van de eisen zoals ook omschreven in artikel 32 van de AVG: passende technische en organisatorische maatregelen om een adequaat beveiligingsniveau te waarborgen voor de verwerking van persoonsgegevens.

1.9.2 Belangrijkste uitgangspunten
De belangrijkste uitgangspunten van het beleid zijn:
- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang.
- Het dagelijks bestuur van 1Stroom is eindverantwoordelijke voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de GR 1Stroom hebben een interne (proces)eigenaar, die de vertrouwelijkheid en/of waarde bepaalt van de informatie die de informatiebronnen en -systemen bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen, volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- 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.

1.9.3 Invulling van de uitgangspunten
Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:
- Het dagelijks bestuur van 1Stroom stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- De directie stelt jaarlijks het informatiebeveiligingsplan vast.
- De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp spe-cifieke tactische beleidsregels, die aanvullend zijn op dit strategisch beleid.
- De directie is verantwoordelijk voor het vragen om informatie bij het management en ziet erop toe dat het management adequate maatregelen genomen heeft voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.

- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatie-voorziening en rapporteert hierover rechtstreeks aan de directie.
- Tijdens P&C-cyclus dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rappor-tage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten tevens wor-den opgenomen in de auditplannen.
- Het management is verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, BAG, BGT) en toekomstige ba-sisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de organisatie en het behalen van de doelen die zijn gesteld.
- Alle medewerkers van onze organisatie worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informa-tie.
- Het management dient erop toe te zien dat de controle op het verwerken van persoonsge-gevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Het ma-nagement en/of de proceseigenaar voert quickscans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

1.9.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een informatiebeveiligingsplan opgesteld onder leiding van de CISO, geba-seerd op:
  - de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (EN-SIA);
  - het dreigingsbeeld gemeenten van de IBD en het Nationaal Cyber Security Centrum (NCSC);
  - De door het management ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

2. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn (CISO, security officers) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

2.1 Aansturing: directieteam

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van het management. De directie zorgt dat het ma-nagement zich verantwoordt over de beveiliging van de informatie die onder hen berust. De directie zorgt dat de verantwoordelijk portefeuillehouder binnen het college (de burgemees-ter) gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van 1Stroom. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in onze organisatie gezien als een integraal onderdeel van het risicomanagement.

2.2 Uitvoering: afdelingsmanagers

Informatiebeveiliging valt onder de verantwoordelijkheden van alle afdelingsmanagers. Om deze verantwoordelijkheid waar te maken, dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat

alle processen, systemen, data, applicaties[7] altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. De afdelingsmanagers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de teams over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in het structurele overleg tussen de directie en de afdelingsmanagers.

Taken van de afdelingsmanagers in het kader van informatiebeveiliging zijn:
- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid, de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

De voorbereiding en coördinatie van het overleg ligt bij de CISO.

2.3 Controle en verantwoording
Dit Strategisch Beleid is een verantwoordelijkheid van het dagelijks bestuur van de Gemeenschappelijke Regeling 1Stroom. De bestuurders en directie van de GR 1Stroom zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.
De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informa-tiebeveiliging aan de portefeuillehouder. De directie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van de tactische (deel) beleidsonder-werpen, die aanvullend zijn op dit strategische beleid.

2.3.1 ENSIA
De gemeente verantwoordt zich over informatiebeveiliging via de ENSIA-systematiek. Dat betekent dat jaarlijks een ENSIA-coördinator wordt aangewezen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke proceseigenaar. De proceseigenaar levert in overleg met de ENSIA-coördinator alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college van B en W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging. Ook worden de eventuele verbetermaatregelen ver-meld die de gemeente gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de raad.

Middels deze verantwoording wordt het bestuur van de GR 1Stroom geïnformeerd over de stand van zaken en de voortgang. De twee colleges en gemeenteraden worden door middel van een kennisgeving geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de GR 1Stroom informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

Vastgesteld op 31 maart 2021 door het dagelijks bestuur van de Gemeenschappelijke Regeling 1Stroom.

mr. H.B. Hieltjes
voorzitter

M. van der Jagt
Secretaris

7) In de vakliteratuur als geheel vaak ook informatiecluster genoemd.