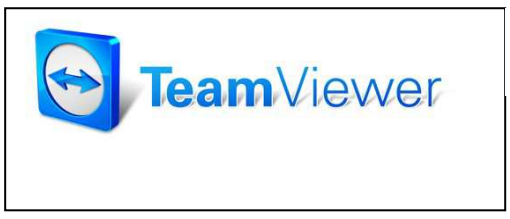
GEMEENTE REIMERSWAAL



Versie : **1.0**

Datum : **9 augustus 2017**

Poststuknummer : **17.014110**

Versie Informatie

Versie	Auteur	Datum	Omschrijving verandering
0.9	L. Addink	6 juli 2017	Versie bespreking werkgroep Informatieveiligheid Reimerswaal
1.0	L. Addink	9 augustus 2017	Versie advies college (17.014030)

Inhoud:

Inleiding

De Gemeente Reimerswaal is een informatie-intensieve organisatie, primair gefocust op dienstverlening. De medewerkers van de gemeente moeten kunnen beschikken over betrouwbare informatie om de klanten zo optimaal mogelijk te kunnen helpen en adviseren. Burgers en bedrijven moeten erop kunnen vertrouwen dat hun gegevens bij de gemeente in goede handen zijn.

De gemeente is steeds afhankelijker van goed werkende informatievoorziening en -systemen. De veiligheid die met de technische middelen kan worden bereikt is begrensd. De menselijke factor (het menselijk gedrag) speelt in de praktijk een steeds grotere, veelal zelfs een doorslaggevende, rol in het daadwerkelijk realiseren van informatieveiligheid in de praktijk.

Naast informatiebeveiliging is bescherming van privacy een belangrijk aspect. Hoewel dit gezien kan worden als een afzonderlijke onderwerp met andere regelgeving, zijn beiden in de praktijk onlosmakelijk verbonden. Om die reden is er gekozen voor een gecombineerde benadering onder de noemer informatieveiligheid. Informatieveiligheid is veel meer dan ICT, het gaat in veel gevallen om de mens in de organisatie en de manier waarop deze met risico's omgaat. Is de medewerker zich bewust van die risico's? Zijn bestuurders zich bewust van de risico's van en voor de organisatie?

Om te voorkomen dat binnen elk van de werkgebieden van de gemeente separaat beleid ontwikkeld en geïmplementeerd moet worden, is de keuze gemaakt om een organisatiebreed informatieveiligheidsbeleid op te stellen. Hierbij worden organisatiebrede, overkoepelende onderwerpen geïntegreerd en in algemeen beleid en algemene procedures vastgelegd. Specifieke zaken worden per werkgebied in aparte, aanvullende, onderdelen opgenomen.

Doel van dit document is om ondersteuning te bieden aan het bestuur, het management en de organisatie bij de sturing op en het beheer van informatieveiligheid. Er wordt op strategisch niveau beschreven, welke uitgangspunten organisatiebreed ten aanzien van de informatiebeveiliging en bescherming van privacy voor de Gemeente Reimerswaal gelden. Dit document zal samen met de tactische- , technische beveiligingsmaatregelen en procedures een adequaat niveau van veiligheid voor de organisatie moeten opleveren waardoor de kwaliteitskenmerken van informatie, te weten: beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van de informatie, binnen de organisatie zijn gewaarborgd.

1. Uitgangspunten

1.1 Wettelijke basis

De wettelijke basis van informatiebeveiliging en de bescherming van privacy valt af te leiden uit Europese richtlijnen en landelijke wet- en regelgeving, zoals (niet uitputtend):

- De Grondwet.
- De Auteurswet.
- De Telecommunicatiewet.
- De Ambtenarenwet.
- De Wet computercriminaliteit.
- De Wet bescherming persoonsgegevens (Wbp).
- De Archiefwet / Archiefregeling.
- De Databankenwet.
- De Wet elektronisch bestuurlijk verkeer.
- De Wet elektronische handtekeningen.
- De Wet algemene bepalingen burgerservicenummer.
- De Paspoortwet.
- De Wet basisregistratie personen (BRP).
- De Wet openbaarheid van bestuur (Wob).
- De Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI).
- De Wet basisregistratie adressen en gebouwen (BAG).
- De Wet kenbaarheid publiekrechtelijke beperkingen (WKPB).
- De nieuwe Wet ruimtelijke ordeningen (nWRO).
- De Wet meldplicht datalekken
- De Algemene Verordening Gegevensbescherming (AVG) - m.i.v. 25 mei 2018

Op grond van bovenstaande wet- en regelgeving worden eisen gesteld aan het niveau van informatieveiligheid, de beheersmaatregelen en de controle (interne controle (ic)/interne audit) daarop.

1.2 Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

Het informatiebeveiligingsbeleid is volledig gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING). Deze is afgeleid van (inter)nationale informatiebeveiligingsnormen, waarbij in de Baseline Informatiebeveiliging Nederlandse Gemeenten de methodiek en de terminologie specifiek is aangepast, om aan te sluiten op de geldende situatie binnen gemeenten. Zowel voor de gemeente zelf als voor externe partijen (leveranciers, ketenpartners) waarmee de gemeente samenwerkt (en informatie mee uitwisselt) geldt hierbij het “pas toe of leg uit” beginsel.

1.3 Algemene oriëntatie en positionering

Informatieveiligheid maakt een onlosmakelijk deel uit van de bedrijfsvoering en de primaire processen van de organisatie en haar omgeving. In de uitwerking vormt het een samenhangend geheel van maatregelen van procedurele, organisatorische, fysieke, technische, personele en juridische aard.

Raakvlakken:

- Algemeen beveiligingsbeleid (bijv. deuren, kluizen, toegangscontrole, alarmering).
- Personeelsbeleid (bijv. screening, opleiding en functietypering).
- Organisatiebeleid (bijv. functiescheiding).
- Informatiseringsbeleid (bijv. standaardisatie, internet en cloud computing).
- Privacybeleid (bijv. correct gebruik van persoonsgegevens).
- Juridisch beleid (bijv. afbreukrisico’s bij privacyschendingen, clausulering in overeenkomsten met derden, third party mededelingen).
- Dienstverleningsconcepten (bijv. website, het Nieuwe Werken, DigiD).

Het doel van informatiebeveiliging is het behoud van:

- beschikbaarheid/continuïteit (voorkomen van uitval van systemen);
- integriteit/betrouwbaarheid (gegevens zijn juist, actueel en volledig);
- vertrouwelijkheid/exclusiviteit (onbevoegden kunnen geen kennis nemen van gegevens die niet voor hen bestemd zijn);
- controleerbaarheid.

2. Vormgeving van de Informatieveiligheid

2.1 Verantwoordelijkheid en bevoegdheid informatieveiligheidsbeleid

De verantwoordelijkheid voor informatieveiligheidsbeleid ligt op bestuurlijk niveau bij het college van burgemeester en wethouders en op ambtelijk niveau bij de gemeentesecretaris.

De gemeenteraad heeft een specifieke bevoegdheid om de werking van beleid binnen de gemeente te controleren, inclusief het informatiebeveiligingsbeleid.

2.2 Scope van het informatieveiligheidsbeleid

Dit beleid omvat alle gemeentelijke informatieprocessen. Hieronder vallen zowel de ambtelijke als bestuurlijke informatieprocessen. Het beleid heeft niet alleen betrekking op de verwerking, uitwisseling en opslag van digitale informatie, maar ook op de informatie in fysieke c.q. analoge vorm, ongeacht de locatie, het tijdstip of de gebruikte apparatuur.

2.3 Ambitie van de organisatie

De gemeente Reimerswaal hanteert een ambitieniveau waarbij wordt voldaan aan voorgeschreven wet- en regelgeving en conformeert zich daarbij aan landelijke regelgeving.

2.4 (beveiligings)maatregelen

- De gemeente Reimerswaal volgt en geeft uitvoering aan de (beveiligings)maatregelen zoals die opgenomen zijn in de meest actuele versie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG - VNG/KING).
- Het college van burgemeester en wethouders kan besluiten om bepaalde (beveiligings)maatregelen uit de BIG niet in te vullen en het risico dat daar uit voortvloeit als ‘geaccepteerd risico’ te beschouwen. Een dergelijk besluit wordt met de redenen toegelicht en jaarlijks geëvalueerd.

2.5 Procedures en afspraken

- Het college van burgemeester en wethouders of de gemeentesecretaris stellen zo nodig aanvullende maatregelen en/of procedures op om de (beveiligings)maatregelen uit de BIG, of andere wet- en/of regelgeving te kunnen realiseren en/of de uitvoering daarvan te kunnen aantonen.
- De maatregelen en/of procedures worden vastgelegd in een dossier afspraken en procedures (DAP) informatieveiligheid.

2.6 Borging van het informatieveiligheidsbeleid

Om borging van de (beveiligings)maatregelen, procedures en afspraken te realiseren wordt gebruik gemaakt van een Information Security Management System (ISMS). Voor het actualiseren hiervan wordt een Plan Do Check Act cyclus (PDCA cyclus) doorlopen. Hiervoor wordt zoveel als mogelijk aangesloten op de reguliere Planning & Control- cyclus en de mondelinge managementrapportages.

Voor de beoordeling van de actualiteit van het informatieveiligheidsbeleid wordt minimaal het volgende gehanteerd:

- Het Informatieveiligheidsbeleid wordt 1x per 3 tot 4 jaar beoordeeld op actualiteit.
- De status van de implementatie van de (beveiligings)maatregelen uit de BIG, of andere wet- en/of regelgeving wordt minimaal één keer per jaar voorgelegd aan het college van burgemeester en wethouders.
- Mede op basis van de status van de implementatie (beveiligings)maatregelen en de prioriteiten die er aan toegekend worden, wordt een informatiebeveiligingsplan opgesteld voor een periode van 1 tot 2 jaar. Dit plan wordt vastgesteld door het college van burgemeester en wethouders.
- De door het college van burgemeester en wethouders vastgestelde geaccepteerde risico's worden 1x per jaar geëvalueerd.

Los van het bovenstaande kunnen documenten indien nodig tussentijds worden bijgesteld.

2.7 Relatie met andere documenten

Dit document vormt de basis voor het geleidelijk verder uitwerken, herstructureren en sturen van informatieveiligheid binnen onze organisatie. In de loop van de jaren zijn er om verschillende redenen en vanuit andere vakgebieden besluiten genomen die mogelijk raakvlakken of overlap hebben met dit document en /of nieuwe zaken waartoe besloten wordt. Het één op één (geheel of gedeeltelijk) intrekken van dergelijke besluiten is vanwege een gefaseerde aanpak niet altijd mogelijk. In die gevallen is het meest recent genomen besluit van toepassing in combinatie met 'niet geraakte delen' van de het vorige besluit.

3. Organisatie van de informatieveiligheid

3.1 Algemeen

De vaststelling en implementatie van de informatieveiligheidsstructuur en de gemeentebrede beleidsnormen vormen de verantwoordelijkheid van het college van burgemeester en wethouders van de Gemeente Reimerswaal. Voor het nemen van operationele maatregelen is de gemeentesecretaris gemandateerd. Dit geldt ook in geval van ketenafhankelijkheid en bij afdeling overstijgende (informatie)systemen.

3.2 Verantwoordelijkheidsniveaus binnen de organisatie

Binnen de Gemeente Reimerswaal worden de volgende verantwoordelijkheidsniveaus met betrekking tot informatieveiligheid onderscheiden:

Functie/Rol	**Verantwoordelijkheid op hoofdlijnen**
College van B en W	Vaststellen duidelijk te volgen informatieveiligheids- en privacybeschermingsbeleid.
Gemeentesecretaris	Implementeren van de beveiliging en privacybescherming binnen de bedrijfsprocessen en de interne en externe (informatie)systemen.
Leidinggevenden	Zorgdragen voor een goede informatiebeveiliging en privacybescherming binnen de werkprocessen van hun afdeling / eenheid, de uitvoering en handhaving ervan.
Medewerk(st)ers	Actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie.
Chief Information en Security Officer (CISO)	Actueel houden van het informatieveiligheidsbeleid, het adviseren bij projecten en het managen van risico's evenals het opstellen van rapportages
Security Officer SUWInet burgerzaken	beheer, coördinatie en advies ten aanzien van de informatieveiligheid van SUWInet voor het onderdeel burgerzaken.
Beveiligingsbeheerder specifieke gegevensverzameling (BRP, PUN, etc.)	beheer, de coördinatie en het advies ten aanzien van de informatieveiligheid van specifieke gegevensverzamelingen.
Functionaris gegevensbescherming	Toezicht houden op de toepassing en naleving van de Algemene Verordening Gegevensbescherming (AVG) en andere wet- en/of regelgeving op het werkgebied.
Coördinator ENSIA	Organiseren van de noodzakelijke samenwerking voor ENSIA en zorgdragen voor het (laten) invullen van de zelfevaluatie.
Vertrouwd Contactpersoon Informatie Beveiliging (VCIB)	Contact met de Informatie beveiligingsdienst over landelijke incidentmeldingen of waarschuwingen waarvan de inhoud een vertrouwelijk karakter heeft en de eventuele interne opvolging daarvan.
Werkgroep Informatieveiligheid Reimerswaal	implementeren van de BIG, ENSIA en AVG en het bewerkstelligen van bewustwording eigen organisatie.

De taken en verantwoordelijkheden op het gebied van beleid, uitvoering en naleving van informatieveiligheid, alsmede de toewijzing hiervan aan personen, organisatieonderdelen of externe partijen, worden door het college van burgemeester en wethouders of de gemeentesecretaris per functie, rol, of taak(gebied) vastgesteld. Een overzicht hiervan wordt opgenomen in een dossier afspraken en procedures (DAP) informatieveiligheid.

3.3 Verantwoordelijkheidsniveaus belegd buiten de eigen organisatie

De gemeente Reimerswaal is sinds 21 mei 2013 deelnemer aan de Gemeenschappelijke Regeling samenwerking De Bevelanden (GR De Bevelanden). Deze organisatie is een openbaar lichaam en rechtspersoon.

De uitvoering van de werkzaamheden door GR De Bevelanden vindt deels plaats op basis van delegatie en deels op basis van mandaat. In het geval van delegatie wordt de verantwoordelijkheid voor de betreffende taken overgedragen. In het geval van mandaat worden de taken namens de aangesloten partijen uitgevoerd en blijven deze zelf verantwoordelijk.

De taakvelden waarop binnen die organisatie samengewerkt wordt zijn:

a. ICT (mandaat)
b. Informatievoorziening (mandaat)
c. P & O en salarisadministratie (mandaat)
d. Werk, Inkomen en ZORG (delegatie)

Op basis van de samenwerkingsovereenkomst en de samenhang in techniek en bedrijfsvoering is de gemeente Reimerswaal voor de implementatie en/of uitvoering van een aantal (beveiligings)maatregelen en procedures (mede) afhankelijk van GR De Bevelanden en/ of dient de implementatie en/of uitvoering door deze organisatie in overleg met, of samen met de Gemeente Reimerswaal en andere deelnemers plaats te vinden en de op basis van wet- en/of regelgeving vereiste aanvullende overeenkomsten afgesloten te worden. De afspraken, maatregelen en/of procedures worden vastgelegd in een dossier afspraken en procedures (DAP) informatieveiligheid.

Door de Gemeente Reimerswaal heeft de volgende functies/rollen met betrekking tot informatieveiligheid (mede) toegewezen aan medewerk(st)ers van GR De Bevelanden:

Functie/Rol	**Verantwoordelijkheid op hoofdlijnen**
Security Officer SUWInet Werk, Inkomen en Zorg (WIZ)	het beheer, de coördinatie en het advies ten aanzien van de informatieveiligheid van SUWInet. Voor het onderdeel WIZ.
Vertrouwd contactpersoon Informatie Beveiliging (VCIB)	Contact met de Informatie beveiligingsdienst over landelijke incidentmeldingen of waarschuwingen waarvan de inhoud een vertrouwelijk karakter heeft en de eventuele interne opvolging daarvan.

3.4 Verantwoording

Vanaf 2017 moet de gemeente jaarlijks verantwoording afleggen over de kwaliteit van de informatieveiligheid van diverse informatiesystemen op basis van ENSIA (Eenduidige Normatiek Single Information Audit). ENSIA vervangt de aparte verantwoordingsprocedures voor de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).
Met ENSIA verantwoordt de gemeente zich vanaf 2017 ook horizontaal aan de gemeenteraad. ENSIA sluit aan op de gemeentelijke planning en control-cyclus. Het gemeentebestuur krijgt hierdoor meer overzicht over de informatieveiligheid van de gemeente.

De wettelijke verantwoordingsplicht is niet in alle gevallen ook direct van toepassing voor organisaties die activiteiten voor, of namens de gemeente uitvoeren. Indirect mag de gemeente echter wel verlangen dat er door deze organisaties op dezelfde basis met informatieveiligheid en privacy omgegaan wordt als binnen de eigen organisatie. Hierover zullen deze organisaties afspraken worden gemaakt.

3.5 Relatie met andere documenten

Vastgesteld ……..