Drents Overijsselse Delta

uw waterschap

Informatieveiligheidsbeleid

mei 2018

Inhoud

1 Inleiding

1.1 Aanleiding

Organisaties zijn steeds afhankelijker van betrouwbare informatie en systemen waar het deze informatie is opgeslagen. Op basis van informatie worden essentiële beslissingen genomen, processen gestuurd en andere partijen van informatie voorzien.

Binnen de Rijksoverheid is jaren geleden de trend ingezet om informatie op digitale wijze met burgers en andere partijen uit te wisselen door middel van onder meer internetportalen en e-loketten. De betrouwbaarheid van informatie en daarmee de betrouwbaarheid van de organisatie wordt bepaald door de maatregelen die zijn getroffen om deze informatie te beschermen.

Potentiële bedreigingen voor procesmeetgegevens, privé-informatie van burgers en de procesbesturingssystemen zijn helaas gemeengoed geworden. De lekken omtrent DigiD, aanvallen op SCADA systemen en het misbruiken van overheidssystemen om gegevens te stelen zijn hier voorbeelden van.

Aantasting van integriteit van een organisatie moet te allen tijde worden voorkomen.

In 2013 is op landelijk niveau de Baseline Informatiebeveiliging Waterschappen (BIWA) opgesteld. Het informatieveiligheidsbeleid van WDODelta is gebaseerd op de BIWA. Hierbij is ervoor gekozen het beleid op strategisch/tactisch niveau te formuleren. De meer operationele onderdelen van het geformuleerde beleid zullen in informatieveiligheidsplannen worden opgenomen.

1.2 WDODelta en informatieveiligheid

Het waterschap wil ten aanzien van de uitvoering van de kerntaken een betrouwbare partner zijn. Binnen de processen is de afhankelijkheid van gegevens en informatie groot. Een betrouwbare informatievoorziening is van essentieel belang voor de bedrijfsvoering en de continuïteit daarvan.

Betrouwbaarheid en continuïteit zijn ook van belang voor het imago van het waterschap. Om dit te kunnen waarborgen is beveiliging essentieel. Het waterschap dient hiervoor structurele maatregelen te nemen.

2 Kaders

2.1 Scope

Voor WDODelta is een informatie- en automatiseringsstrategie opgesteld. Hierin wordt in hoofdlijnen ingegaan op informatieveiligheid. Voorliggend informatieveiligheidsbeleid is een nadere uitwerking en invulling hiervan.

Dit informatieveiligheidsbeleid is van toepassing op het gehele waterschap en op de informatie-uitwisseling binnen het waterschap en uitwisseling met andere organisaties. Het gaat hier dan ook niet alleen om technische maatregelen, maar ook om maatregelen die het bewustzijn ten aanzien informatieveiligheid vergroten.

Binnen de scope van dit beleid vallen ook de diensten en de dienstverlening die door externe partijen (bijv. leveranciers) worden uitgevoerd namens het waterschap. Voor deze diensten en dienstverlening geldt dat desbetreffende partijen dienen aan te sluiten bij beleid van het waterschap en de hieruit voortkomende beveiligingsmaatregelen.

2.2 Bereik

Het informatieveiligheidsbeleid is niet gebonden aan locaties. Het omvat dus de locatie van het waterschapskantoor, de districts- of regiokantoren, gemalen, rioolwaterzuiveringsinstallaties (RWZI) en alle overige objecten in beheer van het waterschap.
De beveiligingsuitgangspunten en de beveiligingseisen die het waterschap stelt zijn ook van toepassing op momenten wanneer medewerkers van het waterschap zich met informatie van het waterschap buiten deze locaties bevinden. Denk hierbij bijvoorbeeld aan veldwerkzaamheden en thuiswerken, al dan niet ondersteund met mobiele apparatuur[1].

Informatie binnen het waterschap omvat alle gegevens die worden gebruikt. Hieronder vallen onder meer: procesgegevens, persoonsgegevens (van zowel burgers als personeel), gegevens van leveranciers, beleidsdocumenten, aanbestedingsdocumenten, contracten en facturen. Deze informatie kan in allerlei vormen aanwezig zijn. Hierbij valt te denken aan informatie op papier of in digitale vorm, maar ook in mondelinge vorm bijvoorbeeld via telefoon uitgewisselde informatie.

De informatievoorziening binnen het waterschap betreft alle (proces-) domeinen. De beveiliging heeft tot doel om binnen deze domeinen de primaire en ondersteunende processen van betrouwbare informatie te voorzien. Daarbij wordt continu beoordeeld welke informatie adequaat beveiligd is en waar verbetering nodig is.

Het informatieveiligheidsbeleid geldt voor zowel het bestuur als voor alle medewerkers van het waterschap, inclusief tijdelijk personeel en ingehuurd personeel.

2.3 Relatie met andere beleidsterreinen

Het informatieveiligheidsbeleid is afgeleid van de doelstellingen die het waterschap nastreeft ten aanzien van informatievoorziening en ICT.

2.4 Wet en Regelgeving

Het beleid is afgeleid van de wet- en regelgeving die op het waterschap van toepassing is. Voor informatieveiligheid zijn de relevante wetten:
a. Grondwet (m.n. art. 10 en art. 13)
b. Wet Computercriminaliteit (WCC);

[1] In toenemende mate wordt (vertrouwelijke) informatie ontsloten op mobiele apparaten die geen onderdeel zijn van de traditionele IT-voorzieningen en zich veelal buiten de fysieke omgeving van het waterschap bevinden (smartphones, tablets, telewerkplek etc.). Bij het toepassen van deze technologie gelden onverminderd dezelfde veiligheidsuitgangspunten als voor de traditionele voorzieningen. Het belangrijke verschil is de bewustwording van de individuele bestuurder en/of medewerker van de eigen verantwoordelijkheid bij het omgaan met informatie via mobiele apparaten.

c. Algemene Verordening Gegevensbescherming (AVG);
d. Comptabiliteitswet;
e. Telecommunicatiewet;
f. Wet elektronische handtekeningen;
g. Algemene wet bestuursrecht;
h. Wet basisregistratie personen;
i. Archiefwet;
j. Intellectueel eigendomsrecht (bv. tegen illegale software);
k. Waterwet;
l. Wet Elektronisch Bestuurlijk Verkeer;
m. Wet Openbaarheid van Bestuur (WOB).

2.5 Normen

De volgende normen zijn van toepassing op het informatieveiligheidsbeleid:

- Nederlandse Overheids Referentie Architectuur (NORA), Katern Informatiebeveiliging;
- Voorschrift Informatiebeveiliging Rijksdienst (VIR);
- Voorschrift Informatievoorziening Rijksdienst Bijzondere Informatie (VIR-BI);
- Code voor Informatiebeveiliging (NEN-ISO 27001/27002);
- De Baseline voor Informatiebeveiliging Waterschappen (BIWA).

2.6 Landelijke ontwikkelingen

Bij de uitwerking van dit beleid in planvorming zal rekening gehouden worden met:

- De verplichtingen die aan alle organisaties met een vitale maatschappelijke functie, waaronder de waterschappen, zijn gesteld door het ministerie van Veiligheid en Justitie omtrent continuïteitsmanagement en het treffen van voorzieningen tegen uitval van ICT en elektriciteit;
- De verplichtingen die aan alle organisaties die gebruik maken van DigiD/eID, zijn gesteld door het ministerie van Binnenlandse Zaken en Koninkrijkrelaties over het jaarlijks uitvoeren van een onafhankelijke ICT-beveiligingsassessment;
- De richtlijnen die zijn opgesteld door de landelijke Taskforce Bestuur & Informatieveiligheid Dienstverlening (BID).

2.7 Relatie met het privacybeleid (AVG)

Met ingang van 25 mei 2018 treedt de nieuwe privacywetgeving (AVG) in werking. Hiervoor is door WDODelta apart beleid vastgesteld. Het privacybeleid heeft echter een relatie met het informatieveiligheidsbeleid. Onderdelen met een nauwe samenhang tussen privacy en informatieveiligheid zullen in de uitvoering gezamenlijk worden opgepakt.

3 Beleid

3.1 Ambitie

Voor informatieveiligheid streeft het waterschap het volgende na:

- Het waterschap wil in control zijn en blijven van zijn informatiehuishouding waarbij gebruik wordt gemaakt de geldende beveiligingsnormen (ISO/NEN) en wordt voldaan aan de vigerende wet- en regelgeving;
- De bedrijfsprocessen en continuïteit zijn leidend voor informatieveiligheid: informatieveiligheid is een integraal onderdeel van de reguliere werkprocessen;

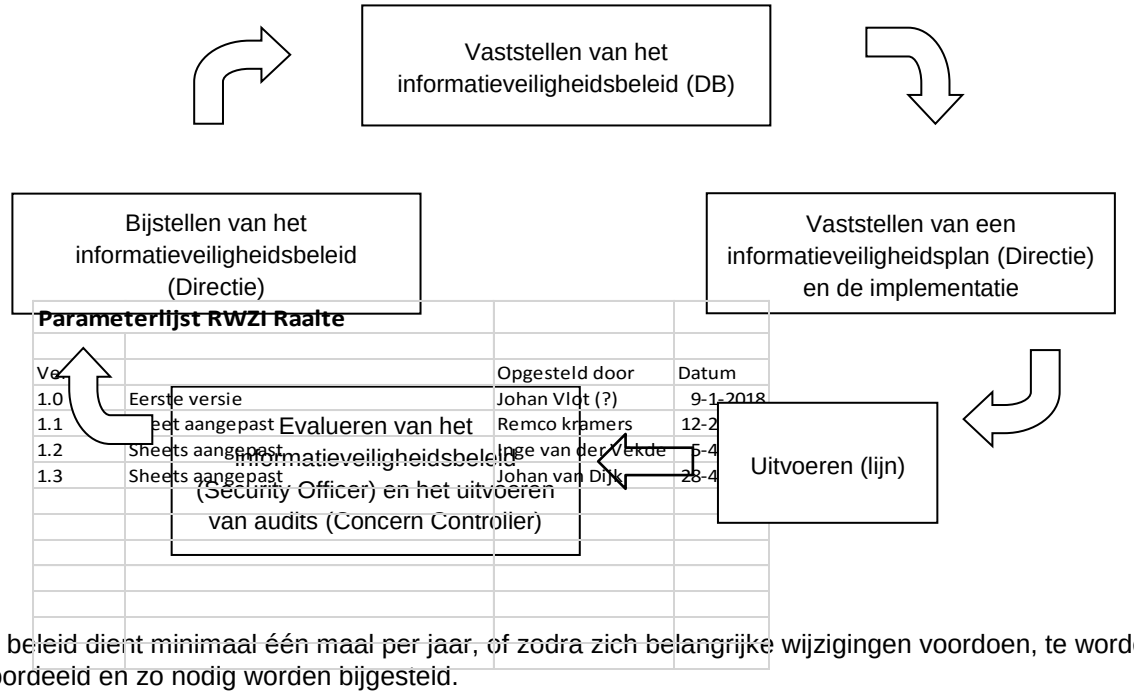
3.2 Doelstellingen informatieveiligheidsbeleid

Met het vastgestelde informatieveiligheidsbeleid wil het waterschap:

- Een consistente richtlijn gebruiken voor het handelen van het bestuur en de ambtelijke organisatie van het waterschap als het gaat over onderwerp informatieveiligheid;
- Richting en kaders geven aan de organisatie van informatieveiligheid binnen het waterschap en de rollen en verantwoordelijkheden die een ieder heeft ten aanzien hiervan;
- De continuïteit van de bedrijfsvoering waarborgen en het risico op schade voor de organisatie als gevolg van inbreuken op de informatieveiligheid op een aanvaardbaar niveau beheersen.

3.3 Sturing

Het proces m.b.t. informatieveiligheidsbeleid is een cyclisch proces (plan-do-check-act (PDCA)). Het proces bestaat uit de volgende stappen:



Het beleid dient minimaal één maal per jaar, of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld en zo nodig worden bijgesteld.

3.4 Basisprincipes informatieveiligheid

Informatieveiligheid is gebaseerd op 3 basisprincipes:

- Beschikbaarheid: informatie en essentiële informatiediensten zijn op de juiste momenten beschikbaar voor gebruikers;
- Integriteit: informatie is juist, volledig en actueel;
- Vertrouwelijkheid: informatie is beschermd tegen onbevoegde kennisname.

3.4.1 Beschikbaarheid

Een belangrijke doelstelling van informatieveiligheid is het garanderen van de benodigde beschikbaarheid van informatiesystemen. Beschikbaarheid is de eerste eis die gesteld wordt aan de informatievoorziening. Informatie die niet beschikbaar is, is niet te gebruiken. Ten aanzien van alle informatiesystemen dient daarom te worden vastgesteld welke mate van beschikbaarheid vereist is. Daarbij moet worden gekeken naar alle aspecten van de informatievoorziening, dus zowel technische infrastructuur als gegevens, applicaties en processen.

3.4.2 Integriteit

Onbevoegde toegang tot informatiesystemen of gegevens resulteert in bedoeld of onbedoeld misbruik en/of verlies van gevoelige informatie. Het onvoldoende borgen van de veiligheid van informatiesystemen, de volledigheid en juistheid van de gegevensverwerking en de toegang tot gegevens, leidt tot uitlekken van informatie naar buiten, inbreuken op privacy wetgeving, aantasting van gegevens en onbetrouwbare gegevens.

3.4.3 Vertrouwelijkheid

Het derde aspect waarop informatieveiligheid zich richt, is het waarborgen dat kennisname en/of mutatie en/of uitreiking van vertrouwelijke en/of privacy gevoelige informatie alleen geschiedt door daarvoor geautoriseerde personen, waarbij de waarborging minimaal zorg draagt voor naleving van de geldende wettelijke bepalingen.

Het treffen van maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te waarborgen, gebeurt op basis van risicomanagement. De maatregelen zijn gericht op:

- voorkomen van inbreuken op de informatieveiligheid (preventieve maatregelen);
- beperken van schade als gevolg van inbreuken op de informatieveiligheid (repressieve maatregelen)
- herstellen van schade als gevolg van inbreuken op de informatieveiligheid (correctieve maatregelen)

Potentiële risico’s van inbreuken op de informatieveiligheid zijn bijvoorbeeld:

- imagoschade door schending van privacy of lekken van vertrouwelijke informatie
- financiële schade als gevolg van verlies of beschadiging van informatie
- schade als gevolg van verstoring van de bedrijfsprocessen (waaronder calamiteitenbestrijding)

3.5 Principes voor informatieveiligheid

Voor de realisatie van informatieveiligheid binnen het waterschap worden de volgende principes gehanteerd:

1. **Het waterschap streeft er naar passend en veilig om te gaan met zijn informatie**
    a. Hierbij maakt het gebruik van gangbare beveiligingsnormen zoals de Code voor Informatiebeveiliging (NEN-ISO 27001/27002) en principes uit referentiearchitecturen zoals de NORA (landelijke overheid) en de WILMA (waterschappen) en de Baseline Informatiebeveiliging Waterschappen (BIWA);
    b. Controle en audits zijn een onderdeel van het bestaande kwaliteitssysteem binnen het waterschap.

2. **Het niveau van beveiliging is in overeenstemming met het belang van informatie**
    a. Het waterschap is realistisch in zijn perceptie ten aanzien van informatieveiligheid. 100% beveiliging van informatie is een utopie;
    b. Beveiligingsmaatregelen worden genomen op basis van een risicoanalyse en deze risico's en maatregelen worden periodiek beoordeeld en geëvalueerd;
    c. Het waterschap werkt continu aan verbetering van zijn beveiligingsmaatregelen maar accepteert dat, ondanks alle getroffen maatregelen, de beveiliging van informatie niet altijd gewaarborgd kan worden;
    d. Het vaststellen van het risicoprofiel van het waterschap en het accepteren van rest-risico's door de organisatie maakt onderdeel uit van het periodiek beoordelen, evalueren en verbeteren van de informatieveiligheid.

3. **Informatieveiligheid is de verantwoordelijkheid van het gehele waterschap**
    a. Het dagelijks bestuur is eindverantwoordelijk voor het onderwerp informatieveiligheid en het vastgestelde informatieveiligheidsbeleid;
    b. Iedere bestuurder en iedere medewerker van het waterschap heeft een persoonlijke verantwoordelijkheid voor informatieveiligheid;
    c. De directie is verantwoordelijk voor invoering en naleving van informatieveiligheid;
    d. De Security Officer coördineert op proces- en projectmatige wijze informatieveiligheid binnen het waterschap.

4. **Beveiligingsmaatregelen binnen het waterschap zijn gebaseerd op classificatie**
    a. Het waterschap voert een publieke taak uit. Alle informatie binnen het waterschap is openbaar, echter bepaalde informatie is vertrouwelijk, zoals kabinetsstukken, persoons- en personeelsinformatie;
    b. De maatregelen die zijn getroffen ter beveiliging van de uitwisseling van informatie tussen het waterschap en ketenpartners/derden zijn gebaseerd op deze classificatie.

5. **Binnen het waterschap bestaat een proces voor het melden en afhandelen van informatieveiligheidsincidenten**
    a. In geval van een incident is procedureel vastgelegd welke acties uitgevoerd dienen te worden en door wie (rol) dit plaatsvindt;
    b. Periodiek wordt door de Security Officer gerapporteerd omtrent de gemelde informatieveiligheidsincidenten, de incidenten welke in behandeling zijn en welke zijn afgehandeld.

6. **Bewustwording van medewerkers omtrent informatieveiligheid en privacygevoelige gegevens wordt blijvend gestimuleerd**
    a. Training in informatieveiligheid, inclusief bewustwording, is voor iedere bestuurder en medewerker van het waterschap beschikbaar;
    b. Periodiek zal er pro-actief over het belang van informatieveiligheid worden gecommuniceerd.

7. **Het waterschap participeert in overlegorganen ten aanzien van informatieveiligheid**
    a. Binnen de waterschapssector wordt op landelijk en regionaal niveau actief kennis gedeeld omtrent informatieveiligheid;
    b. Samen met andere vitale sectoren en het Nationaal Cyber Security Center wordt kennis uitgewisseld.

4 Organisatie van informatieveiligheid

4.1 Verantwoordelijkheden

Het dagelijks bestuur is eindverantwoordelijk voor de informatieveiligheid bij het waterschap en voor het beschikbaar stellen van voldoende middelen en capaciteit ten behoeve van de uitvoering van het beleid. Informatieveiligheid gaat niet alleen over ICT, maar betreft het geheel van mensen, middelen, processen en regels waarbinnen informatie zich beweegt.

Binnen het waterschap is het afdelingshoofd Informatievoorziening verantwoordelijk voor de uitvoering van het informatieveiligheidsbeleid. Het afdelingshoofd zorgt ervoor dat de PDCA-cyclus wordt doorlopen en dat er tijdig wordt gerapporteerd. Het daadwerkelijk rapporteren is een uitvoerende taak van de CISO (Chief Information Security Officer) in opdracht van het afdelingshoofd Informatievoorziening.
De CISO kan daarnaast ongevraagd adviseren aan directie en Concern Controller. De CISO heeft tevens als taak om gemelde beveiligingsincidenten en zwakke plekken in de beveiliging te analyseren en noodzakelijke acties te initiëren.
De Concern Controller en directie kunnen het afdelingshoofd Informatievoorziening aanspreken op het functioneren van de CISO.

Voor het daadwerkelijk uitvoeren van technische beveiligingsmaatregelen is de Operational Security Officer (OSO) verantwoordelijk.

De managers zijn verantwoordelijk voor de beveiligingsmaatregelen binnen hun processen en de naleving ervan door de medewerkers die onder hen vallen.

De Concern Controller is verantwoordelijk voor het laten uitvoeren van audits op het informatieveiligheidsbeleid.

Iedere bestuurder en iedere medewerker van het waterschap heeft een persoonlijke verantwoordelijkheid voor informatieveiligheid en geeft daaraan invulling door het naleven van dit beleid en de daaruit voortvloeiende veiligheidsmaatregelen.

4.2 Kwaliteitszorg

Voor het vertalen van de vastgestelde principes voor informatieveiligheid naar beveiligingsmaatregelen, het implementeren van deze maatregelen binnen de organisatie, het uitvoeren van het beheer hierop en het doorvoeren van verbeteringen hanteert het waterschap een kwaliteitssysteem dat voldoet aan de gangbare eisen op dit gebied.

5 Controle en naleving

5.1 Algemeen

Alle constateringen dan wel vermoedens van inbreuk op de veiligheid dienen te worden gemeld en zullen worden getoetst aan de doelstellingen van het vigerende informatiebeleid.

5.2 Controles

Self assessments en veiligheidscontroles ten aanzien van de effectiviteit van de geïmplementeerde beveiligingsmaatregelen worden uitgevoerd onder verantwoordelijkheid van de managers van het waterschap. Verbeterpunten die naar aanleiding van deze controles worden vastgesteld, worden onderdeel van de reguliere rapportagecyclus.

5.3 Audits

Binnen het waterschap worden in het kader van kwaliteitsmanagement periodiek interne audits uitgevoerd op informatieveiligheidsaspecten. Indien het waterschap niet beschikt over de hiervoor benodigde kennis en expertise kunnen de audits extern worden uitgevoerd. Verder is beoordeling van de informatieveiligheid onderdeel van de jaarlijkse accountantscontrole. Naar eigen inzicht van het waterschap kunnen er ook op ad hoc basis externe audits worden uitgevoerd. Verbeterpunten die naar aanleiding van interne en/of externe audits worden vastgesteld, worden onderdeel van de reguliere rapportagecyclus.

5.4 Sancties

Het niet naleven van dit beleid kan ertoe leiden dat door de directie disciplinaire maatregelen worden opgelegd conform hetgeen daarover is vastgelegd in de SAW.

5.5 Onderhoud

Dit beleid wordt minimaal één keer per jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld en opnieuw vastgesteld. Over de wijzigingen wordt vervolgens gecommuniceerd naar alle belanghebbenden.