Gemeente Smallingerland

Informatiebeveiligingsbeleid 2023 – 2025

Versie:	2.0
Datum:	20-03-2023
Wijzigingen:	20230321: Opname DigiD Beveiligingsbeleid paragraaf 6.10 20230321: Opname bijlage 2 DigiD Randvoorwaarden taken en verantwoordelijkheden 20230327: Opname CLOUD Beveiligingsbeleid paragraaf 6.11 20230914: tekstuele en lay-out aanpassingen en NIS2 toegevoegd in 2.8 Grondslagen

Inhoudsopgave

1.1. Doel en samenvatting van dit document

Informatie is één van de voornaamste bedrijfsmiddelen van gemeente Smallingerland. Het verlies van gegevens, uitval van ICT-voorzieningen , of het door onbevoegden kennisnemen of manipuleren van informatie kan ernstige gevolgen hebben voor de bedrijfsvoering en de dienstverlening richting burgers en bedrijven. Het is van groot belang om informatie in al haar vormen te beschermen om beveiligingsincidenten en/of datalekken te voorkomen.

Incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, de organisatie en bestuurders. Beveiligingsincidenten en gebrekkige opvolging leiden mogelijk tot imagoschade en financiële consequenties in de vorm van een geldboete.

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 Gemeente Smallingerland gelden. Daarnaast zijn de verantwoordelijkheden voor informatiebeveiliging beschreven. De onderwerpen Hybride werken, DigiD en Cloud krijgen de komende tijd de voornaamste aandacht. Deze worden uitgewerkt in het Informatiebeveiligingsplan en het uitvoeringsplan.

1.2. 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.

2. Informatiebeveiliging

2.1. Visie op informatiebeveiliging

Burgers, bedrijven en medewerkers mogen er op vertrouwen dat informatie en (persoons)gegevens bij gemeente Smallingerland in goede handen zijn.

Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en vormt de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, duidelijke verantwoordelijkheden, de juiste maatregelen en risicobewustzijn.

Het proces van informatiebeveiliging is primair gericht op bescherming van informatie, maar is tegelijkertijd een 'vliegwiel'. Het maakt verdergaande elektronische dienstverlening op verantwoorde wijze mogelijk, evenals nieuwe, innovatieve manieren van werken.

2.2. Doel beleid

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.

Gemeente Smallingerland streeft 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 welke niet. De basis voor het afwegen van nog te nemen maatregelen is risicoafweging.

Bijstelling en vaststelling van het informatiebeveiligingsbeleid vindt plaats om de 3 jaar, of eerder indien zich belangrijke wijzigingen voordoen.

2.3. Baseline Informatiebeveiliging Overheid (BIO)

Als leidraad voor de informatiebeveiliging hanteert Gemeente Smallingerland de Baseline Informatiebeveiliging Overheid (BIO). De BIO vormt één gezamenlijk normenkader voor Overheid, Rijk, Waterschappen en Provincies en wordt jaarlijks herzien en/of vernieuwd. 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 BIO-maatregelen verplichte maatregelen zijn. 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.

2.3.1. BBN-niveaus en maatregelen

Om risicomanagement hanteerbaar en efficiënt te houden, kiest de BIO voor risicomanagement dat is gebaseerd op te beschermen belangen en relevante dreigingen. De beschreven belangen en dreigingen worden uitgedrukt in basisbeveiligingsniveau 's: (BBN), namelijk BBN1, BBN2 en BBN3.

Voor BBN1 ligt de nadruk op 'wat mag minimaal verwacht worden?'. Voor BBN2 ligt de nadruk op de bescherming van de meest voorkomende categorieën informatie volgens het principe 'valt de maatregel onder goed huisvaderschap en toont deze beveiliging de betrouwbare overheid?'. BBN3 is van toepassing op gerubriceerde overheidsinformatie waarbij weerstand tegen statelijke actoren of vergelijkbare dreigingen nodig is.

De keuze voor een BBN wordt gemaakt door de proceseigenaar en/of systeemeigenaar en is gebaseerd op risicomanagement. De corresponderende maatregelen voor het bepaalde BBN-niveau zijn vervolgens verplichte maatregelen. De BIO spreekt van overheidsmaatregelen.

2.4. Reikwijdte

De scope van dit beleid omvat alle gemeentelijke processen, informatiesystemen, informatie en gegevens van de gemeente en externe partijen en omvat het gebruik en het beheer door medewerkers en externe partijen, ongeacht locatie, tijdstip en gebruikte systemen en applicaties.

Informatiebeveiliging is meer dan alleen de geautomatiseerde informatiesystemen en ICT-infrastructuur. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, beeldscherm et cetera) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen) maar ook mensen en processen.

2.5. 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:

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

2.6. Algemene Verordening Gegevensbescherming (AVG)

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing als vervanger van de WBP. Op grond van artikel 5 lid 1 onderdeel f dient de organisatie voldoende technische- en organisatorische maatregelen te implementeren om persoonsgegevens te beschermen tegen onopzettelijk verlies, beschadiging of vernietiging.

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.

2.7. Relatie met informatiebeleid en ICT-beleid

Het informatiebeveiligingsbeleid heeft een sterke relatie met het informatiebeleid en het ICT-beleid. Ambities uit het I-jaarplan en aanpassingen in het ICT-landschap worden vertaald naar projecten in de organisatie. Per project of nieuw informatiesysteem wordt in samenspraak met de 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, 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 en/of informatie. Het Informatiebeveiligingsbeleid biedt daarmee de noodzakelijke waarborgen voor vertrouwelijkheid, beschikbaarheid, integriteit en controleerbaarheid van informatie. De CISO heeft zitting in het wijzigingsoverleg tussen informatisering en ICT om te waarborgen dat informatieveiligheid wordt meegewogen bij wijzigingen in het informatie- en ICT-landschap

2.8. Grondslagen

Het informatiebeveiligingsbeleid is gebaseerd op de Baseline Informatiebeveiliging Nederlandse Overheid (BIO) versie 1.03. Een nadere uiteenzetting van de BIO is terug te vinden als bijlage van dit beleidsdocument.

Onderstaande wet- en regelgeving is voor de gemeente Smallingerland van toepassing op het beveiligen van informatie en het waarborgen van de privacy van haar medewerkers en inwoners:

- 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);
- NIS2 , gaat waarschijnlijk in eind 2024.

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);

2.8.1. Suwinet, DIGID en BRP

Suwinet en de Basisregistratie Personen (BRP) zijn informatiesystemen die basisregistraties en persoonsgegevens bevatten van alle inwoners van Nederland. We spreken ook wel van de 'kroonjuwelen' van de informatievoorziening.

Om de informatiebeveiliging van deze systemen te organiseren hanteert Gemeente Smallingerland voor Suwinet en de BRP specifieke beveiligingsplannen. In deze beveiligingsplannen zijn risico`s rollen, verantwoordelijkheden en controles nader beschreven en uitgewerkt.

Gemeente Smallingerland maakt op dit moment gebruik van drie DigiD koppelingen, te weten:

1. Digitaal Loket
2. Parkeren
3. Belastingportaal

DigiD vormt de digitale identiteit van burgers waarmee een groot scala aan diensten kunnen worden aangevraagd bij de overheid en Overheid. Bescherming van de digitale identiteit van inwoners is belangrijk om fraude en misbruik van diensten te voorkomen. Voor DigiD is er een separaat beveiligingsbeleid, zie bijlage 2: DigiD Beveiligingsbeleid. Veder bevat bijlage 3: de DigiD aansluiting randvoorwaarden taken en verantwoordelijkheden.

2.9. Borging van de informatiebeveiliging

De gemeente maakt voor de borging van informatiebeveiliging gebruik van een Information Security Management System (ISMS). Het ISMS 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 inrichten en beheer van een ISMS ligt bij de CISO.

Om verder borging van het informatiebeveiligingsbeleid en de daarvan afgeleide plannen te realiseren, vinden periodiek risicoanalyses plaats om de controle en de kwaliteit van de informatieveiligheid te waarborgen. 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 teammanagers tot stand komt. Het uitvoeringsplan wordt daarbij opgesteld vanuit registraties in het eerder beschreven ISMS.

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

2.10. Risicobenadering

Gemeente Smallingerland volgt een aanpak van informatiebeveiliging op basis van risicobeheersing. Met een aanpak gebaseerd op risicobeheersing is gemeente Smallingerland in staat om een evenwichtige set van beveiligingsmaatregelen te implementeren en in staat om daarbij een goede afweging tussen kosten en noodzaak te maken.

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 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, is de organisatie in staat om haar systemen en bedrijfsprocessen adequaat en doelgericht te beschermen.

2.11. Samenwerking met gemeenten, ketenpartners, leveranciers en instanties

Gemeente Smallingerland werkt nauw samen met andere gemeenten, ketenpartners, bedrijven, en instanties. Zo is de CISO betrokken bij provinciale overlegstructuren in Friesland en Groningen. Andere samenwerkingspartners zijn provincie, politie, ziekenhuizen, scholen en dochterorganisatie Carins, waarin gemeentelijk taken zijn ondergebracht.

Naast deze samenwerkingen betrekt de organisatie ook veel diensten van verschillende leveranciers, bijvoorbeeld voor haar ICT- infrastructuur en informatiesystemen.

Met samenwerkingspartners en leveranciers waar informatiebeveiliging een rol speelt worden op voorhand afspraken gemaakt over het vereiste niveau van informatiebeveiliging dat de gemeente Smallingerland stelt. Afspraken worden vastgelegd in overeenkomsten. Gemeente Smallingerland hanteert hiervoor standaardovereenkomsten, die landelijk beschikbaar zijn, zoals de GIBIT-inkoopvoorwaarden en de standaard verwerkersovereenkomsten van de VNG.

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 maakt daarbij onderscheid tussen de horizontale en de verticale verantwoording, waarbij de horizontale verantwoording als basis dient voor de verticale verantwoording.

3.1. Horizontale verantwoording

De Baseline Informatiebeveiliging Overheid (BIO) vormt de kern van de verantwoording over informatieveiligheid aan de gemeenteraad en wordt jaarlijks herzien. De horizontale verantwoording bestaat uit een zelfevaluatie, een IT-audit, een verklaring van het College van B&W 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 toezichthouders. Dit noemen we de ‘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 gemeente Smallingerland. 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 bedrijfskritisch zijn op basis van classificatie en risicoanalyse. Het overzicht wordt als bijlage aan het informatiebeveiligingsplan toegevoegd.

Het informatiebeveiligingsplan wordt jaarlijks geactualiseerd en besproken in het Informatiebeveiligingsoverleg (IBO) bestaande uit de portefeuillehouder, gemeentesecretaris, concerncontroller en de CISO. Het informatiebeveiligingsplan wordt vervolgens vastgesteld door het college van burgemeester en wethouders en gepresenteerd aan het directieteam (DT). Vervolgens wordt het belegd bij de Teammanagers middels het uitvoeringsplan, zie volgende paragraaf 3.4

3.4. Uitvoeringsplan

Het uitvoeringsplan 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 twee keer per jaar besproken in het Informatiebeveiligingsoverleg bestaande uit de portefeuillehouder, gemeentesecretaris, concerncontroller en de CISO. In het overleg wordt de voortgang van implementatie van maatregelen besproken en vindt waar nodig bijstelling plaats van het uitvoeringsplan.

Bij de BIG was er meer ruimte voor afweging en prioritering op basis van het principe ‘pas toe of leg uit’. Maatregelen uit de BIO zijn, afhankelijk van het BBN-niveau (risiconiveau) verplicht.

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 ISMS en toegevoegd aan het uitvoeringsplan informatiebeveiliging.

4. Uitgangspunten informatiebeveiliging

De gemeente Smallingerland hanteert met betrekking tot informatiebeveiliging de volgende uitgangspunten:

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

2. Een betrouwbare informatievoorziening vormt een essentiële succesfactor voor een efficiënte en effectieve bedrijfsvoering. Omdat de gemeente Smallingerland onderdeel uitmaakt van de totale overheid en ook verbonden is met andere ketenpartijen, heeft een onveilige situatie bij de gemeente Smallingerland 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 bestuur en het management handelt conform de tien bestuurlijke principes informatieveiligheid die zijn opgesteld door de VNG (zie bijlage 2).

7. Periodiek onafhankelijke controle 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.

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

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

10. 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.

11. 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.

12. 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.

13. 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.

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

15. Voor bestaande en nieuwe informatiesystemen is een 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.

16. 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.

17. 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.

5. Organisatie van de informatiebeveiliging

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 deze paragraaf zijn de verantwoordlijkheden voor de interne organisatie en voor de gemeenteraad, als toezichthouder, nader uitgewerkt.

5.1. De gemeenteraad

De gemeenteraad draagt een specifieke bevoegdheid voor de controle en de toetsing op de werking van beleid binnen de gemeente, 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.

5.2. Interne organisatie

In relatie tot informatiebeveiliging onderscheiden we voor de interne organisatie van Gemeente Smallingerland de volgende verantwoordelijkheden.

5.2.1. 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 conform de 10 bestuurlijke principes informatieveiligheid (zie paragraaf 2.5)

5.2.2. 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;
- De directie 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)

5.2.3. Concerncontrol

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.

5.2.4. Teammanagers

Teamleiders zijn verantwoordelijk voor de integrale beveiliging hun organisatieonderdelen, bedrijfsprocessen, gegevensverzamelingen en informatiesystemen. 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 indienst, 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

5.2.5. Team Organisatie en Communicatie, cluster personeel

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 Verklaringen Omtrent Gedrag (VOG)
- het laten ondertekenen en archiveren van geheimhouding- en integriteitsverklaringen

5.2.6. Team I&I

Het team is verantwoordelijk voor:

- verzorgt de beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen die voortvloeien uit de beveiligingseisen en bijbehorende risicoanalyse;
- beheert werkplekken, telefonie, serverplatformen, lokale netwerken, WIFI, externe netwerkverbindingen, zoals VPN-verbindingen, GEMnet, Digikoppeling, servicebus, en verzorgt het technische (wijzigings)beheer van databases, bedrijfsapplicaties en kantoorautomatiseringshulpmiddelen;
- Is medeverantwoordelijk voor alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen;
- Is verantwoordelijk voor alle beheeraspecten van informatiebeveiliging die betrekking hebben op ICT-aangelegen-heden zoals incident- en probleemmanagement, configuratie- en wijzigingsbeheer, hardening, patching, logging van activiteiten, back-up & recovery en uitwijk;
- Acteert actief op acute dreigingen die een gevaar vormen voor de informatievoorziening;

- maatregelen gericht op beveiliging van (toegang tot) gebouwen, en de beveiliging van de publieke ruimte en werkruimte van de gemeente. Onder deze verantwoordelijkheid valt ook het verwijderen en vernietigen van papier.

5.2.7. 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 gevraagd en ongevraagd adviseren van het college, het directieteam, teamleiders, en de concerncontroller;
- stelt het beveiligingsplan en uitvoeringsplan op en zorgt voor de actualisatie van deze plannen
- ziet toe op voortgang van de realisatie van beveiligingsmaatregelen zoals vastgelegd in beveiligingsplannen waaronder ook de specifieke beveiligingsplannen voor de BRP, reisdocumenten en rijbewijzen en Suwinet;
- coördineert de uitvoering van informatieveiligheidsmaatregelen uit het uitvoeringsplan;
- rapporteert twee maal per jaar aan het informatiebeveiligingsoverleg (IBO) over de stand van de informatiebeveiliging en de voortgang;
- neemt deel in een overleg waarbij wijzigingsvoorstellen en projecten vanuit informatisering en ICT kunnen worden beoordeeld op het aspect informatieveiligheid
- 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;
- juiste afhandeling en evaluatie van incidenten en het bijhouden van een registratie van informatiebeveiligingsincidenten.

5.2.8. Functionaris gegevensbescherming

De functionaris gegevensbescherming (FG) is de interne toezichthouder van gemeente Smallingerland waar het gaat om privacy, naleving van de AVG, UAVG, Wpg en de bescherming van persoonsgegevens. 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.

5.2.9. De beveiligingsbeheerder

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

5.2.10. Security Officer Suwinet

De Security Officer beheert beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen en normenkaders is geïmplementeerd. De Security Officer 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 heeft formeel wat betreft rapportages een bijzondere rol. Deze rapporteert namelijk rechtstreeks aan de bestuurlijk verantwoordelijke.

6. Gerelateerde beleidsstukken informatiebeveiliging

Het informatiebeveiligingsbeleid beschrijft de algemene kaders, verantwoordelijkheden en uitgangspunten rond informatiebeveiliging. Naast het informatiebeveiligingsbeleid zijn er andere beleidsstukken opgesteld die een nadere uitwerking zijn van, of een sterke relatie hebben met het informatiebeveiligingsbeleid. Hieronder volgt een overzicht van deze beleidsstukken.

6.1. Beleid wachtwoorden en accounts

Het beleid wachtwoorden en accounts stelt kaders voor het gebruik van wachtwoorden, gebruikersaccounts, beheeraccounts, en serviceaccounts. Het beleid zorgt ervoor dat we op een uniforme wijze om kunnen gaan met het gebruik en beheer van wachtwoorden en accounts om te voorkomen dat onbevoegden toegang kunnen krijgen tot het netwerk en/of de gemeentelijke informatiesystemen.

6.2. Beleid logische toegang

Doelstelling van het beleid logische toegangsbeveiliging is dat de identiteit van een gebruiker, die toegang krijgt tot gegevens, informatiesystemen, portalen of diensten, van de gemeente of van derde partijen, wordt vastgesteld. Het is daarbij van belang dat de autorisatie op een gecontroleerde wijze en via een vastomlijnd proces tot stand komt, waarbij ook de reikwijdte van de acties die een gebruiker uit mag voeren op voorhand zijn bepaald, zijn vastgelegd en zijn ingericht.

6.3. Fysiek toegangsbeleid

Het doel van dit beleid is om duidelijkheid te geven over de wijze waarop het toegangsbeleid binnen gemeente Smallingerland is vormgegeven. Het beleid is mede opgezet om te voorkomen dat onbevoegden toegang krijgen tot ruimtes waartoe zij niet bevoegd zijn, om medewerkers, informatie, informatiesystemen en bedrijfsmiddelen te beschermen. Het toegangsbeleid spitst zich daarnaast toe op de fysieke beveiliging van kantoren, ruimten en faciliteiten.

6.4. Encryptiebeleid

Dit document beschrijft de kaders voor vertrouwde en integere berichtuitwisseling met encryptie tussen, daarvoor geautoriseerde personen en systemen. Het beleid biedt uitgangspunten voor het borgen van onweerlegbaarheid van verzending, ontvangst bij berichtuitwisseling en het vertrouwt kunnen opslaan van bestanden. Het beleid beschrijft ook de kaders voor sleutelbeheer en besteedt specifiek aandacht aan PKI-overheid en certificatiedienstverleners.

6.5. Beleid gebruik van informatie, mobiele apparatuur en gegevensdragers

Dit beleidsdocument is bedoeld om medewerkers van gemeente Smallingerland kaders te bieden waarbinnen een veilige uitwisseling van informatie, het gebruik van mobiele apparatuur en het gebruik van gegevensdragers en verwijderbare media plaats kan vinden.

6.6. Richtlijn dataclassificatie

De classificatierichtlijn drukt het belang van informatie en informatiesystemen uit in classificatieniveaus voor beschikbaarheid, vertrouwelijkheid en integriteit. Per classificatie-niveau wordt een basisset aan maatregelen voorgesteld die het minimale beveiligingsniveau voor het betreffende classificatieniveau beschrijven voor de systeemeigenaar.

6.7. Hardeningbeleid

Het hardeningbeleid van de gemeente geeft richting aan de wijze waarop de gemeente maatregelen wenst te treffen voor hardening. Hardening is het proces waarbij overbodige functies in besturingssystemen uitgeschakeld worden en/of van het systeem verwijderd worden. Door beveiligingsinstellingen te optimaliseren worden mogelijkheden om een systeem te compromitteren verlaagd.

6.8. Patchbeleid

Patchmanagement is het proces waarmee patches op gecontroleerde beheerste (risico beperkende) wijze uitgerold kunnen worden. Patches zijn doorgaans kleine programma's die aanpassingen maken om fouten op te lossen of verbeteringen aan te brengen in bestaande programmatuur en/of hardware. Patchmanagement wordt uitgevoerd door de ICT-afdeling. Het doel van Patchmanagement is tweeledig. Ten eerste is het gericht op het inzichtelijk maken van de actuele stand van kwetsbaarheden en toegepaste patches binnen de beheerde infrastructuur. Het tweede doel is op een zo efficiënt en effectief mogelijke wijze met zo min mogelijk verstoringen stabiele (veilige) systemen te creëren en te houden.

6.9. Hybride werken (te actualiseren)

Dit document beschrijft en uitgangspunten om op een veilige manier op afstand te kunnen werken en veilig gebruik te maken van email en agenda-functionaliteit. Daarbij beschrijft het documenten op welke plaatsen op afstand kan worden gewerkt en stelt het eisen aan de werkplek en de te gebruiken apparatuur.

6.10. DigiD Beveiligingsbeleid

In aanvulling op dit informatiebeveiligingsbeleid (dat integraal van toepassing is op al onze DigiD aansluitingen) zijn er voor DigiD enkele aanvullende maatregelen en verantwoordelijkheden van toepassing:

Normen

- We conformeren ons aan de laatste door Logius gepubliceerde **Norm ICT-beveiligingsassessments DigiD**.
- Jaarlijks wordt dit normenstelsel in het kader van ENSIA door een externe auditor en CISO getoetst.
- Over deze toetsing vindt horizontaal (van college aan de raad) en verticaal (naar Logius) verantwoording plaats.

Eigenaarschap

- Geheel in lijn met de BIO is het eigenaarschap van de DigiD webapplicaties (de webapplicaties die de DigiD functionaliteit als module aanroepen) belegd in de lijnorganisatie en is de betreffende teammanager eindverantwoordelijk voor het goed functioneren van de applicatie en de te treffen maatregelen.

Functioneel beheer

- Per DigiD aansluiting is door de genoemde teammanager een functioneel beheerder aangewezen die de verantwoordelijkheid heeft de door Logius opgetelde beveiligingsnormen te implementeren, controleren (middels een jaarlijks TPM verklaring) en bewijslast ervan op te bouwen in een auditdossier.
- Het auditdossier wordt jaarlijks aan onze externe auditor beschikbaar gesteld en bevat tenminste de contracten en servicerapportages van onze SaaS-leverancier (norm B.05), de incidentprocedure en een overzicht van de incidenten (U/WA.02), de dataclassificatie (U/WA.05), bewijs dat de webapplicatie gehardend is (U/NW.06, ten aanzien van DNSSEC) en de beoordeelde releases (C.08).
- Twee maal per jaar (geagendeerd) wordt er door functioneel beheer beoordeeld of alle autorisaties compleet en actueel zijn; hierover wordt verslag (autorisatiematrix) gedaan richting verantwoordelijk leidinggevende en CISO.

Technisch

- Wij maken – voor wat betreft DigiD aansluitingen - uitsluitend gebruik van cloud-applicaties die door SaaS leveranciers worden geleverd. Derhalve wordt een groot deel van de door Logius afgekondigde normen ingevuld door de SaaS leverancier die hiervan middels een jaarlijkse – door een onafhankelijk auditor opgestelde - TPM-verklaring verantwoording over aflegt.

6.11. CLOUD Beveiligingsbeleid

Het Cloud beveiligingsbeleid is gebaseerd op de 5 adviezen voor veilige inkoop van clouddiensten gepubliceerd door het Nationaal Cyber Security Centrum (NCSC)

Het NCSC adviseert om geen clouddienst in te kopen zonder vooraf vijf maatregelen te treffen:

1. Risicoanalyse
2. Configuratie en monitoring
3. Exit strategie
4. Functioneel beheer
5. Audittoegang

De vijf bovenstaande maatregelen worden hieronder nader uitgelegd:

Risicoanalyse:
Maak proceseigenaar in de organisatie verantwoordelijk voor de in te kopen clouddienst en laat deze verantwoordelijke een risicoanalyse uitvoeren. Voer een risicoanalyse uit per clouddienst op het gebied van privacy, compliance, security en financiering. De risicoanalyse stelt ons in staat om te besluiten welke gegevens we naar de clouddienst willen migreren. Hanteer hierbij het uitgangspunt dat de clouddienstverlener de gegevens in kan zien. Zorg in dit geval ook voor een verwerkersovereenkomst.

Configuratie en monitoring:
Beveiligingsincidenten in cloudomgevingen ontstaan vaak door misconfiguratie aan de gebruikerszijde. Wanneer functioneel beheerders dataopslag bijvoorbeeld onvoldoende afschermen, kunnen datalekken ontstaan. Vanwege het open karakter van veel clouddiensten, kan opgeslagen informatie dan zelfs voor elke internetgebruiker toegankelijk zijn (kans op een datalek). We dienen daarom te zorgen voor passende configuratieprocessen van de betreffende dienst, voordat er data naar clouddiensten gemigreerd zal worden.

Exit strategie:
Het is belangrijk om bij het afnemen en afsluiten van een clouddienst na te denken over een exit strategie. Wanneer er besloten wordt om niet langer gebruik te maken van een clouddienst is het noodzakelijk om de betreffende data te kunnen migreren. Het is daarom aan te bevelen om in de dienstverleningsovereenkomst afspraken te maken over de mogelijkheden om onze data weg te kunnen migreren. Er bestaan standaarden die het mogelijk maken om relatief eenvoudig over te stappen van clouddienstverlener. Een bekende standaard is SWIPO (Switching Providers and Porting Data). Dit is een Europees initiatief dat gedragscodes heeft ontwikkeld die helpen bij eenvoudiger overstappen tussen clouddienstverleners. Informeer bij een clouddienstverlener of er een standaard aanwezig is om over te stappen naar een andere clouddienstverlener. Maak tevens afspraken over het eigenaarschap van de data.

Functioneel beheer:
Stem functioneel beheer af op de clouddienst en tref hiermee passende maatregelen voor authenticatie en autorisatie. Hoewel het gebruik van een clouddienst beveiligingsvoordelen kan hebben, maakt het ook nieuwe vormen van misbruik mogelijk. Gebruiken we bijvoorbeeld geen streng toegangsbeleid in een cloudomgeving, dan kan dat leiden tot datalekken. Ook kan het dan

voorkomen dat elke medewerker toegang heeft tot alle informatie en functionaliteit. Pas toegangsbeheer toe gebaseerd op Role-based access control (RBAC). Het is aan te raden om beleid op te stellen dat beschrijft wie toegang heeft tot welke gegevens en functionaliteiten in de clouddienst. De clouddienstverlener heeft in de meeste gevallen templates oftewel standaarden die in sommige gevallen over genomen kunnen worden. Dit dient per clouddienst beoordeeld te worden. Pas ook het gebruik van Two-Factor Authentication (2FA) toe bij elke clouddienst.

Audittoegang:
Spreek met de clouddienstverlener af op welke manier we met behulp van audits inzicht kunnen krijgen in de kwaliteit van de geboden dienstverlening. In vrijwel alle gevallen is zelfstandige audittoegang beperkt of niet mogelijk. Hiervoor dienen dan audits door derde partijen aangevraagd te worden. De rapporten van deze partijen kunnen een bepaalde mate van zekerheid geven, het zogenaamde assurance level. Bespreek met de clouddienstverlener of er bepaalde normen gehanteerd worden, zoals bijvoorbeeld ISO27017 etc. Hetzelfde geldt voor de locatie waar onze gegevens verwerkt of opgeslagen worden.

Bijlage 1: Beschrijving tien bestuurlijk principes informatiebeveiliging

Baseline

De 10 bestuurlijke principes voor informatiebeveiliging

Behorende bij de Baseline Informatiebeveiliging Overheid (BIO)

Medio 2019 heeft de VNG de tien bestuurlijke principes voor informatiebeveiliging opgesteld. De BIO positioneert de bestuurder en het management sterker dan voorheen in de rol waarin hij of zij risico-gebaseerd stuurt op het gebied van informatieveiligheid. Ter ondersteuning daarbij zijn 'De tien bestuurlijke principes voor informatiebeveiliging' vastgesteld.

- *Bestuurders bevorderen een veilige cultuur*
  Menselijk gedrag en cultuur beïnvloeden op significante wijze alle aspecten van risicomanagement op elk niveau en in elk stadium.

- *Informatiebeveiliging is van iedereen*
  Passende en tijdige betrokkenheid van alle belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties in aanmerking worden genomen. Dit resulteert in een verbeter bewustzijn en goed geïnformeerd risicomanagement.

- *Informatiebeveiliging is risicomanagement*
  Risicomanagement wordt bewust toegepast bij alle organisatie activiteiten.

- *Risicomanagement is onderdeel van de besluitvorming*
  Risicomanagement is onderdeel van alle besluiten en risicomanagement is chefsache.

- *Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking*
  Het Risicomanagementproces is aangepast en staat in verhouding tot de externe en interne context van de organisatie die verband houdt met haar doelstellingen.

- *Informatiebeveiliging is een proces*
  Risico's kunnen ontstaan, veranderen of verdwijnen als de externe en interne context van een organisatie verandert. Risicomanagement detecteert en anticipeert op die veranderingen en gebeurtenissen op een gepaste en tijdige manier.

- *Informatiebeveiliging kost geld*
  Risico's moeten behandeld worden en er zijn vele manieren om veiligheid te realiseren, maar aan alle zijn kosten verbonden.

- *Onzekerheid dient te worden ingecalculeerd*
  De input voor risicomanagement is gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen. Risicomanagement houdt expliciet rekening met eventuele beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn verbonden. Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden.

- *Verbetering komt voort uit leren en ervaring*
  Risicobeheer wordt voortdurend verbeterd door leren en ervaring.

- *Het bestuur controleert en evalueert*
  Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen.

Bijlage 2: DigiD Randvoorwaarden, taken en verantwoordelijkheden

DigiD aansluiting: Randvoorwaarden, taken en verantwoordelijkheden

Gemeente Smallingerland

Documentversie en -historie

Versie	Status	Classificatie	Datum	Type documentatie	Auteur	Opmerking
1.0	Definitief	Intern	21-03-2023	Randvoorwaarden, taken en verantwoordelijkheden	Hans de Vries	

Inleiding

Digitale persoonsidentificatie (DigiD) is een authenticatiemiddel dat wordt ingezet voor onze digitale dienstverlening. Dit is een veilig en betrouwbaar middel waarmee met zekerheid de identiteit van de gebruikers van onze digitale dienstverlening vastgesteld kan worden.

Het aanschaffen en onderhouden van een DigiD aansluiting vergt veel inspanning. Daarnaast kost het geld en manuren. Om zo efficiënt mogelijk te kunnen werken is het belangrijk dat de taken en verantwoordelijkheden bekend en belegd zijn. In het laatste hoofdstuk wordt kort uitleg gegeven waar men rekening mee moet houden bij een nieuwe DigD aansluiting.

Doel

Het doel van dit document is tweeledig

- Het kenbaar maken van de randvoorwaarden voor het aanvragen en behouden van een DigiD aansluiting.
- Het kenbaar maken van de taken en verantwoordelijkheden voor desbetreffende DigiD producteigenaar.

Uitgangspunten gebruik DigiD

- DigiD wordt gebruikt voor alle online dienstverlening van onze gemeente waar met zekerheid de identiteit van de gebruiker vastgesteld moet worden.
- Gezien de werklast en kosten rondom DigiD audits, heeft het de voorkeur om zoveel mogelijk online dienstverlening aan te bieden binnen de bestaande digitale loket functionaliteit (met de bestaande DigiD aansluitingen)

DigiD audit

Iedere online dienst dat aangeboden wordt via DigiD, moet jaarlijks worden getoetst(audit)of het voldoet aan informatiebeveiligingsnormen. Hiermee houdt Logius(toezichthouder DigiD) toezicht op veilig gebruik van de DigiD-aansluitingen. Het betreft een audit van de dienst die wordt aangeboden achter DigiD (bijvoorbeeld een online paspoortaanvraag). Binnen 2 maanden na aansluiting op de productieomgeving van DigiD moet het ICT-beveiligingsassessment-rapport worden aangeleverd bij Logius. Daarna dient de aansluiting jaarlijks geaudit te worden. Dit gebeurt binnen de gemeente middels de ENSIA-verantwoordingssystematiek.

Het DigiD-Normenkader omschrijft de normen waaraan de DigiD-aansluiting moet voldoen. Op de website van Logius of NOREA zijn deze normen te vinden.

Een DigiD aansluithouder kan een deel van de DigiD omgeving of het beheer uitbesteden aan een leverancier (serviceorganisatie). De Serviceorganisatie valt hierdoor binnen de scope van het DigiD assessment. Hierdoor wordt een deel van de normen niet meer bij de aansluithouder maar bij de Serviceorganisatie, of bij beide, getoetst. Een Serviceorganisatie kan voor zijn gedeelte van de DigiD normen een DigiD Assessment uit laten voeren en het resultaat daarvan ter beschikking stellen aan de DigiD aansluithouder in de vorm van een TPM. Veelal is dit het geval en dient dit meegenomen worden in opdracht voor leverancier.

Meer informatie over de DigiD Assessment staat op de website van Logius en NOREA.

Randvoorwaarden DigiD aansluiting

1. Elke DigiD aansluiting dient een producteigenaar te hebben.
2. De producteigenaar draagt zorg dat:
    a. de taken uit het volgende hoofdstuk goed geborgd zijn en worden nageleefd;
    b. er wordt voldaan aan alle (actuele) Logius DigiD normen;
    c. Beheer taken wordt uitgevoerd door een functioneel- of applicatiebeheerder;
    d. de kosten (audits en uren) belegd zijn bij de vakafdeling

Taken en verantwoordelijkheden producteigenaar

De DigiD producteigenaar is eindverantwoordelijk voor de (nieuwe) DigiD aansluiting. Dit betekent dat hij/zij zorg moet dragen en er op toe ziet dat er uitvoering wordt gegeven en daarbij horen de volgende taken:

- Zorg dragen dat er wordt voldaan aan alle (actuele) Logius DigiD normen.
- Opstellen en onderhouden van contracten(afspraken) met de leverancier(s)
    - Hoofdovereenkomst
        - o.a. afspraken over informatiebeveiliging: ISO27001/BBN2+
        - gemeente wordt geïnformeerd wanneer niet aan ISO/BBN2+ (niet meer) kan worden voldaan.
        - Tijdig (uiterlijk 15 okt) aanleveren van een TPM (zonder extra offerte)
        - Dat er geen kosten in rekening worden gebracht voor certificeringen van leverancier.
    - SLA
    - Verwerkersovereenkomst
- Dataclassificatie moet bepaald worden d.m.v. een BIO toets.
- Er op toezien dat gedurende de samenwerking de leverancier zich houdt aan de gemaakte afspraken.
- Dat er een functioneel/applicatiebeheerder aanwezig is dat zorgdraagt voor de borging van de normen gedurende het hele jaar.
- Dat er een functioneel/applicatiebeheerder aanwezig is dat verantwoording aflegt tijdens de DigiD audit en in ENSIA.
- Dat er tijdig (uiterlijk 15 okt) een TPM wordt opgeleverd door de leverancier(s) aan producteigenaar. De producteigenaar levert de TPM intern aan bij de ENSIA coördinator.
- Wanneer er niet voldaan wordt aan de DigiD normen(TPM) dan dient de producteigenaar contact op te nemen met de leverancier en dan zijn de volgende vragen relevant:
    - Wat is de reden voor het niet voldoen aan de norm(en)
    - Kunnen we onze diensten achter DigiD nog veilig aanbieden?
    - Wat is het verbeterplan?
    - Wanneer kunnen wij een nieuwe(schone) TPM verwachten?
- Wanneer er niet voldaan wordt aan de DigiD normen(TPM) dan:
    - moet door de producteigenaar bestuurlijk verantwoording afgelegd worden aan de portefeuillehouder en bestuurlijk ENSIA coördinator;

    - moet door de producteigenaar aan de bestuurlijk ENSIA coördinator een verbeterplan aangeleverd worden;
    - moet door de producteigenaar erop toegezien worden dat de verbeteringen tijdig (binnen de afgesproken termijn) worden doorgevoerd.
- In geval dat de producteigenaar de organisatie verlaat of van functie wisselt dan moet er bij de overdracht(document) duidelijk verwezen te worden naar de bovenstaande verantwoordelijkheden.

Nieuwe DigiD aansluiting

Bij elke nieuwe DigiD aansluiting zijn verschillend disciplines nodig van het IT bedrijf(cluster interne Dienstverlening). Het is daarom belangrijk om als opdrachtgever een I-adviseur te betrekken.
De aanvraag van een nieuwe DigiD aansluiting wordt gedaan via een projectleider en volgens de richtlijnen die door Logius gesteld worden. De I-adviseur en/of projectleider betrekt een informatiebeveiligingsfunctionaris bij de start van een DigiD project. Wanneer een DigiD live gaat dan dient er binnen 2 maanden een DigiD audit plaats te vinden. Er moet kunnen worden aangetoond dat er voldaan wordt aan de door Logius gestelde DigiD normen (zie hoofdstuk 3). Een informatiebeveiligingsfunctionaris coördineert de audit en ondersteund bij de voorbereiding.

Belangrijk is dat de opdrachtgever verantwoordelijk is dat er een producteigenaar en applicatie- of functioneel beheerder aangesteld wordt en dat hoofdstuk 2 en 3 van dit document bekend zijn bij deze personen. Is de producteigenaar een inhuurkracht (dus tijdelijk) dan blijft de opdrachtgever eindverantwoordelijk wanneer de producteigenaar vertrekken en er geen vervanging of overdracht heeft plaatsgevonden.

DigiD eigenaren

Hieronder is een lijst te vinden met de product eigenaren. De lijst word jaarlijks vernieuwd.

DigiD aansluiting:	Producteigenaar/Eindverantwoordelijke:	Taken gedelegeerd aan:
Digitaal Loket	Functie: Teammanager I&I Naam: Simon Wiersma	Functie: Business Informatie Analist Naam: Klaas van der Ploeg
CityPermit	Functie: Teammanager I&I Naam: Simon Wiersma	Functie: Business Informatie Analist Naam: Petra Bies
Belastingportaal	Functie: Teammanager Financiën Naam: Lieuwe Schotanus	Functie: Medewerker Beleid & Kwaliteit Belastingen Naam: Jacqueline Malawau