PURMEREND

GEMEENTEBLAD

Officiële uitgave van de gemeente Purmerend

Nr. 229712

19 september 2019

Gemeentelijk Informatiebeveiligingsbeleid (GIBB) 2019-2021

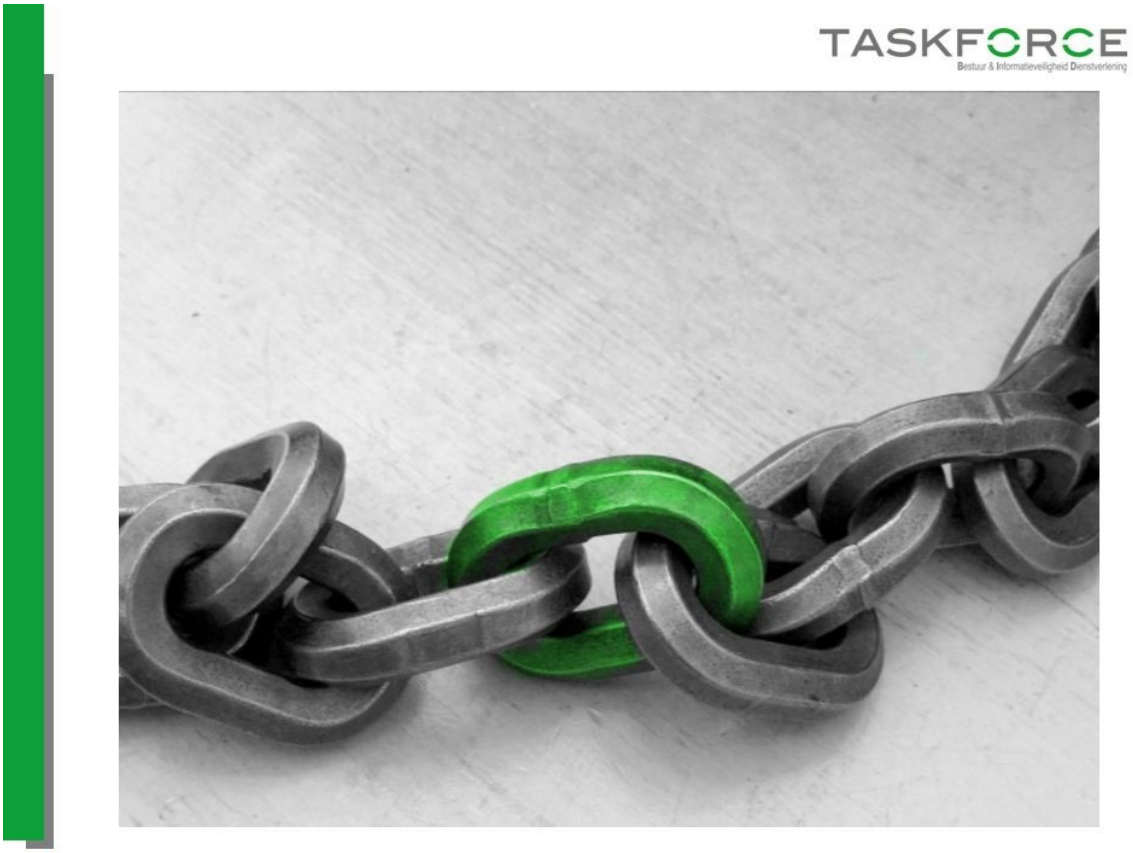
Burgemeester en wethouder van Purmerend,

Gelet op:
- artikel 1.11 lid 1 van de Wet Basisregistratie Personen
- artikel 6 van het Besluit Basisregistratie Personen
- artikel 90 van de Paspoortuitvoeringsregeling Nederland
- norm B.01 van het Specifiek Suwinet-normenkader Afnemers 2017
- resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' (Bijzondere Algemene Ledenvergadering van de Vereniging van Nederlandse Gemeenten 2013)
- norm 5.1.1 van de Tactische Baseline Informatiebeveiliging Gemeenten (BIG)
- control 5.1.1 en 5.1.2 van de Baseline Informatiebeveiliging Overheid (BIO- versie 1.0).

BESLUITEN:

1. het Gemeentelijk Informatiebeveiligingsbeleid 2019-2021 (kenmerk 1454676) vast te stellen;
2. de GS/AD op te dragen het college elk half jaar te informeren over de staat van informatieveiligheid;
3. elk jaar aan de raad verantwoording af te leggen over informatieveiligheid door middel van de ENSIA-methodiek;.
4. met dit besluit het Gemeentelijk Informatiebeveiligingsbeleid 2015 (GIBB 2015 kenmerk 1160182) en Uitvoeringsplan GIBB 2015 (kenmerk1164605) te laten vervallen;
5. dit besluit een dag na publicatie in het gemeenteblad in werking te laten treden.

Gemeentelijk Informatiebeveiligingsbeleid (GIBB) 2019-2021 - Gemeente Purmerend



1 Uitgangspunten informatiebeveiliging Purmerend

1.1 Het waarom en het ambitieniveau van informatiebeveiliging

Informatie is één van de voornaamste bedrijfsmiddelen van de gemeentelijke organisatie. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering. Grote en kleine gebeurtenissen bedreigen de **Beschikbaarheid, Integriteit** (betrouwbaarheid) en/of **Vertrouwelijkheid** van informatie. Deze hebben negatieve gevolgen voor burgers, bedrijven en partners en de bedrijfsvoering van de gemeente. Informatieveiligheid is daarom van groot belang om deze risico's te verminderen.

*Net als het **privacybeleid** en het **integriteitsbeleid** draagt informatiebeveiliging bij aan het bevorderen van het vertrouwen van burgers, bedrijven en partners in de gemeente.*

Het hier voorgestelde beleid is noodzakelijk om als gemeentelijke overheid fatsoenlijk om te gaan met de belangen van de hierboven genoemde betrokkenen. Immers de wereld om ons heen verandert voortdurend en daarmee ook de dreigingen en kwetsbaarheden. Het minstens eenmaal per drie jaar actualiseren van ons informatiebeveiligingsbeleid is daarom een noodzaak vanuit het eigen belang van de gemeente, maar tevens een eis vanuit onze omgeving. [1]
Dit nieuwe IB-beleid treedt in werking een dag na publicatie van het collegebesluit in het gemeenteblad. Hiermee komen het oude Gemeentelijk Informatiebeveiligingsbeleid 2015 (GIBB 2015 kenmerk 1160182) en Uitvoeringsplan GIBB 2015 (kenmerk1164605) te vervallen

1.2 Principes voor informatiebeveiliging

Bij de vaststelling van dit beleid baseert het college zich op "De 10 principes voor informatiebeveiliging" zoals deze geformuleerd zijn door de Informatiebeveiligingsdienst Gemeenten (IBD) en VNG Realisatie:

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

De volledige tekst van deze principes is opgenomen als bijlage 1.

1.3 Uitgangspunten voor het informatiebeveiligingsbeleid

Deze 10 principes krijgen een vertaling in de volgende uitgangspunten:

- Het Informatiebeveiligingsbeleid (IB-beleid) is nu nog gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG) [2] die binnenkort vervangen wordt door de Baseline Informatiebeveiliging Overheid (BIO). [3] Daarom wordt dit beleid al ingericht vanuit de BIO.
- Het IB-beleid heeft een nauwe relatie met het Privacybeleid. Het IB-beleid draagt er aan bij om de vereiste passende technische en organisatorische maatregelen te treffen die de Algemene Verordening Gegevensbescherming van de gemeente vraagt. [4]
- Het realiseren van een 100% veiligheid is een onmogelijkheid. Daarom worden alle specifieke veiligheidsvraagstukken '*risk-based*' benaderd. Dat wil zeggen: beveiligingsmaatregelen worden getroffen op basis van een inschatting van mogelijke risico's.

1) Dit document is gebaseerd op verschillende externe en interne bronnen. De belangrijkste bronnen zijn wel de volgende:
. eindverslag visitatiecommissie Informatieveiligheid "*Durven leren*" (VNG, september 2017).
. *Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten* (IBD 2018)
. *Managementletter onderzoek Baseline informatiebeveiliging Gemeenten* (Duijnborgh Audit, januari 2018)

2) De Baseline Informatiebeveiliging Gemeenten bestaat uit:
Strategische baseline informatiebeveiliging nederlandse gemeenten
Tactische baseline informatiebeveiliging nederlandse-gemeenten

3) Zie: https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/

4) Algemene Verordening Gegevensbescherming art. 32 lid 1.

- Het IB-beleid wordt vastgesteld door het college van B&W voor een periode van drie jaar. Daarnaast stelt het college een jaarlijkse planning vast van de prioriteiten die gemeentebreed van belang zijn. Ook bestaan er (wettelijk verplichte) sectorale plannen Bijvoorbeeld voor de Basisregistratie Personen (BRP), Paspoorten Uitvoeringsregeling Nederland (PUN) en Suwinet.
- De reikwijdte van het informatiebeveiligingsbeleid en -planning bestaat uit:
  - alle werkprocessen, onderliggende informatiesystemen, informatie en gegevens van de gemeente;
  - alle externe partijen die in opdracht van de gemeente met gegevens omgaan;
  - het gebruik van gegevens door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

- Bij de uitvoering van de informatiebeveiliging wordt gebruik gemaakt van een Plan-Do-Check-Act cyclus. Met deze PDCA-cyclus sluit de gemeente aan bij de Eenduidige Normatiek Single Information Audit (ENSIA) die sinds 2017 door alle gemeenten wordt gehanteerd. De resultaten daaruit zijn richtinggevend voor de jaarplanning.

1.4 Risicobewuste informatiebeveiliging

Op verschillende plaatsen in het informatiebeveiligingsbeleid komt het woord "risico" voor. Wat houdt dat in?

We maken een inschatting gemaakt van mogelijke schade voor het geval dat:
informatiesystemen (tijdelijk) niet beschikbaar zijn,
de informatie niet integer is en/of
vertrouwelijke informatie in verkeerde handen valt.
Ook wordt een inschatting gemaakt van de dreigingen waartegen beschermd moet worden. De inschatting van mogelijke schade en dreigingen leidt tot beveiligingseisen om risico's te beperken. Om deze eisen af te dekken worden passende maatregelen getroffen of wordt het (rest)risico geaccepteerd.

Alle gemeenten staan voor deze uitdaging en daarom zijn de Baselines zo nuttig. De BIO is een stelsel van samenhangende "controls". Deze zijn te beschouwen als "*geleerde lessen*" uit de wereldwijde praktijk van deskundigen op het terrein van informatiebeveiliging. Deze lessen zijn verwoord in de ISO-norm 27002. Op basis daarvan en van allerlei wet- en regelgeving onderkent de BIO **verplichte overheidsmaatregelen en optionele handreikingen**.

Eén van de vernieuwingen van de BIO is dat er onderscheid is naar drie **Basis beveiligingsniveaus** (BNN):
BNN1: laag voor systemen waar de beveiligingseisen bewust lager worden gesteld:
BNN2: standaardniveau van beveiliging.
BNN3: hoog niveau van beveiliging. Denk aan: Basisregistratie Personen en de administratie uitvoering Jeugdwet.
Het bepalen van de Basisbeveiligingsniveaus moet gezien worden in relatie tot de implementatie van de baseline. De verwachting is dat de meeste systemen uitkomen op BNN2. Het uitgangspunt van de BIO is dat een organisatie die de baseline volledig heeft geïmplementeerd de generieke beveiliging op orde heeft. Daarom hoeft de organisatie weinig aanvullende maatregelen hoeft te treffen voor de systemen van BNN2 (en 1) maar mogelijkerwijs wel voor de systemen op BNN3. Daarnaast geldt dat het bepalen van de beveiligingsniveaus een project is dat in drie jaar wordt uitgevoerd en telkens per onderzocht systeem inzicht oplevert of en welke aanvullende maatregelen nodig zijn. De uitvoering van die maatregelen kan dus vrijwel meteen beginnen mits gelijktijdig aan de implementatie van de BIO wordt gewerkt.

Het behoort tot de rol van het management van de organisatie om met ondersteuning door de Coördinator Informatiebeveiliging door middel van een risicoanalyse per systeem vast te stellen welk beveiligingsniveau nodig is. Dat geldt voor bestaande en nieuwe informatiesystemen. Het aanpassen van bestaande systemen is echter arbeidsintensief en kostbaar. In het vorig beleidsplan is daarom al de weg gekozen van "security by design". Dit principe houdt in dat elk project voor de vernieuwing of wijziging van informatievoorziening en/of ICT start met een risicoanalyse om te bepalen òf en welke beveiligingsmaatregelen nodig zijn. Vervolgens moeten deze maatregelen ook daadwerkelijk worden uitgevoerd als onderdeel van het project. Vooraf maatregelen treffen is namelijk veel effectiever en goedkoper dan achteraf repareren.

De taakstelling voor deze planperiode is daarom drieledig:
1. toepassing van de volledige BIO op de gehele gemeentelijke informatiehuishouding;
2. in elk IV/ ICT-project wordt het principe van security by design toegepast;

3. uiterlijk aan het eind van de planperiode is voor elk gemeentelijke informatiesysteem bepaald welke Basisbeveiligingsniveau van toepassing is en welke eventuele extra beveiligingsmaatregelen nodig zijn.

1.5 Mensen maken fouten

De mens speelt bij informatiebeveiliging een dubbelrol. Hij/zij is handelend persoon en tegelijkertijd een risicofactor. Volgens het Dreigingsbeeld is dit zelfs de grootste dreiging voor de informatieveiligheid van Nederlandse gemeenten. Dus groter dan cybercrime en andere staten. Onze eigen praktijk van incidenten en datalekken van de afgelopen drie jaar bevestigt dit beeld. Daarom is bewustmaking een belangrijk onderdeel van informatiebeveiliging. Het grootste obstakel is en blijft de vrijblijvendheid op dit terrein. Het is noodzakelijk om bij de bewustmaking twee lijnen naast elkaar te hanteren:

- De '*zachte*' lijn van: informeren en overtuigen. Dit krijgt onder andere vorm in een jaarlijkse gemeentebrede campagne. Deze kan samenvallen met de landelijke campagne Alert Online die jaarlijks in oktober wordt gehouden. Daarnaast zijn incidenten vaak een goede aanleiding om mensen wakker te schudden. Behalve deze middelen die zich richten op de gehele organisatie is het nodig om in de dagelijkse werkpraktijk informatieveiligheid aandacht te geven.
- De '*harde*' lijn van regels en maatregelen. Zo ontbreekt het momenteel aan duidelijkheid welke gedragingen wel en niet van medewerkers verwacht mogen worden. Het Integriteitsprotocol biedt daarvoor alleen algemene aanwijzingen. Aan de andere kant is ook onduidelijk welke waarborgen op privacy de medewerkers hebben als zij werken met geautomatiseerd systemen. Het Privacyreglement Telefoon, e-mail en internetgebruik, dat dateert uit 2004, is dan ook aan vervanging toe. Daarnaast is het nodig om technische en organisatorische maatregelen te treffen die de kans op fouten minder groot maken. Hier ligt de relatie met het bepalen van de Basisbeveiligingsniveaus en het regelen van autorisaties tot systemen en gegevensverzamelingen en gebruik van veilige middelen om te e-mailen en gegevens uit te wisselen..

Bij de bewustmaking spelen teammanagers een belangrijke rol: om het concreet te maken hoort dit onderwerp op de agenda van werkoverleggen

2 Organisatie van de informatiebeveiliging

Het niet expliciet beleggen van verantwoordelijkheden en bijbehorende activiteiten, procedures en instrumenten, vormt een enorm risico voor de gemeente. Het verhindert namelijk het daadwerkelijk en structureel uitvoeren en borgen van de beheersmaatregelen.[5]

2.1 Verantwoordelijkheden en taken

- Het college van burgemeester en wethouders is integraal verantwoordelijk voor de beveiliging (beslissende rol) van informatie binnen vrijwel alle werkprocessen van de gemeente. (De raad heeft hierin een eigen verantwoordelijkheid voor haar eigen informatiehuishouding.)
- Het college
  - o stelt kaders voor informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders door vaststelling van:
    - het Gemeentelijk Informatiebeveiligingsbeleid (driejaarlijks);
    - het Informatiebeveiligingsplan (jaarlijks);
    - sectorale beveiligingsplannen (bijvoorbeeld Basisregistratie Personen, Paspoort Uitvoeringsregeling Nederland en Suwinet).
  - o heeft een portefeuillehouder informatieveiligheid en privacy aangewezen;
  - o legt verantwoording aan af aan de raad en aan externe toezichthouders. Bijvoorbeeld: ministeries van Binnenlandse Zaken en Koninkrijksrelaties, Sociale Zaken en Werkgelegenheid en aan de Autoriteit Persoonsgegevens).
- De Gemeentesecretaris/Algemeen directeur (in sturende rol) is verantwoordelijk voor de uitwerking van de kaders en sturing. Hij/zij:

5) Zie *Durven leren:*
(pag. 12):Versterk de bestuurlijke aandacht door het college en de raad te betrekken.
(pag. 13): Borg een goede positionering van de CISO en zorg dat de CISO kan beschikken over een intern netwerk in de organisatie.

- stuurt op de gemeentebrede risico's;
- stelt de specifieke processen voor informatiebeveiliging vast.
- wijst gegevenseigenaren binnen de ambtelijke organisatie aan;
- controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden;
- evalueert periodiek beleidskaders.

- De voorbereiding van en advisering over de IB taken van de Gemeentesecretaris/Algemeen Directeur (GS/AD) worden opgedragen aan de Coördinator Informatiebeveiliging. (Zie bijlage 2.) Teneinde aan te sluiten bij de gangbare praktijk in gemeenteland wordt de functiebenaming Coördinator Informatiebeveiliging vervangen door Chief Information Security Officer (CISO). De omvang van deze functie is 1,0 FTE.
- De CISO wordt geplaatst binnen het team Beleid en Projecten.
- De directeuren en teammanagers binnen de gemeente (in vragende rol) zijn verantwoordelijk voor de integrale beveiliging van hun organisatieonderdelen, processen en gegevensverzamelingen. Zij worden ook aangeduid als: de **interne gegevenseigenaren, proceseigenaren en "projectopdrachtgevers"**. Voor al deze rollen geldt ten aanzien van hun werkterrein(en):
  - stellen zij op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor de gegevensverzameling vast (hierbij wordt gebruik van de hulpmiddelen die door de VNG Realisatie en de IBD worden beschikbaar gesteld);
  - zijn zij verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
  - sturen zij op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
  - rapporteren zij over naleving van wet- en regelgeving en algemeen beleid van de gemeente in de managementrapportages.

- De teammanager ICT en de teammanager Beleid en Projecten (in uitvoerende rol) zijn verantwoordelijk voor:
  - beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen, die voortvloeien uit de vastgestelde basisbeveiligingsniveaus;
  - beveiliging van de informatievoorziening bij vernieuwing van informatiesystemen en werkprocessen;
  - alle beheeraspecten van informatiebeveiliging, zoals IT security management, incident- en problem management;
  - logging, monitoring en rapportage;
  - technisch beveiligingsadvies leveren aan de andere teams.

- De teammanagers die tevens beheerders zijn van gemeentelijke gebouwen zijn verantwoordelijk voor de fysieke aspecten van de informatiebeveiliging daarvan (bijvoorbeeld toegangsbeveiliging en stroomvoorziening).Voor het Stadhuis is dit de teammanager Facilitair en voor de Koog de teammanager Vastgoed en voor de Purmaryn de teammanager/directeur.

2.2 Functioneel overleg

Op verschillende niveaus vindt overleg plaats over informatieveiligheid. In veel gevallen kan dat samenvallen met het overleg over privacy.

Strategisch overleg met portefeuillehouder

Aansluitend op de periodieke bestuurlijke rapportage (zie hieronder bij 3) vindt er overleg plaatst van de portefeuillehouder met de GS/AD, Functionaris Gegevensbescherming, Concerncontroller en CISO. Dit overleg fungeert tevens als Risk-team zoals geadviseerd in "*De 10 principes voor informatiebeveiliging*".[6]

Tactisch overleg (privacy en) informatieveiligheid

Het Tactisch Overleg adviseert aan de GS/AD over beleidsmatige aspecten van privacy en informatiebeveiliging. Zo vaak als nodig is, maar in elk geval eenmaal per kwartaal komt dit overleg bijeen. Om een brede en gedragen advisering mogelijk te maken bestaat dit overleg in elk geval deel van uit de volgende functionarissen.

- Directeur Bedrijfsvoering

6) 10 Principes voor informatiebeveiliging, Toelichting bij Principe 2.

- Concerncontrollers Beemster en Purmerend
- Functionaris Gegevensbescherming (FG)
- CISO
- Privacyfunctionaris JVZ
- Teammanager IV/Beleid en Projecten
- Teammanager ICT
- Teammanager Burgerzaken (vanwege BRP)
- Een teammanager Maatschappelijk Domein (onder andere vanwege Suwinet)
- Een teammanager Ruimtelijk Domein

Crisisbeheersing
Voor interne crisisbeheersing zijn reeds twee elkaar aanvullende maatregelen getroffen:
- Er is een Computer Security Incident Responseteam (CSIRT) dat belast is met de coördinatie van informatiebeveiligingsincidenten.[7] Hiervan maken in elk geval deel uit: de CISO, de plaatsvervangend CISO, de teammanager ICT, een systeembeheerder en een functioneel beheerder. Het verdient aanbeveling dat deze personen tevens Vertrouwenscontactpersoon bij de IBD (VCIB) zijn. In praktijksituaties zal dit team al naar gelang de situatie uitgebreid worden.
- Er bestaat al een Meldpunt Datalekken dat belast is met de beoordeling en melding van datalekken bij de Autoriteit Persoonsgegevens. Hiervan maken deel uit: de Functionaris Gegevensbescherming, de privacyfunctionaris JVZ, de CISO en plv CISO.

Voor beide groepen zijn procesbeschrijvingen inmiddels vastgesteld.

Samenwerking met andere gemeenten
Onze gemeente erkent het belang van samenwerking. Op **landelijk niveau** speelt de Informatiebeveiligingsdienst (IBD) daarbij een cruciale rol. Onder andere door het delen van informatie over dreigingen en ervaringen met de uitvoering van het informatiebeveiligingsbeleid.

Al eerder is de rol van Vertrouwenscontactpersonen IBD (VCIB) genoemd. Zij worden aangewezen door de GS/AD. Het streven is dat de medewerkers die permanent deel uitmaken van het CSIRT tevens VCIB zijn. Daarnaast zijn er Algemene Contactpersonen IBD (ACIB) die worden aangewezen door de CISO. Hun contact met de IBD is vooral op het gebied van ICT systeembeheer.

Purmerend vervult een actieve rol in het overleg **Privacy en Informatiebeveiliging Zaanstreek-Waterland**. Daarnaast participeert de gemeente in relevante landelijke platforms en onderhoudt contacten met andere sectoraal georganiseerde IB-platforms. Denk hierbij aan deelname in de Vereniging van Informatie- en Automatiseringsprofessionals bij Gemeenten (VIAG), de ontwikkeling van een Gemeenschappelijk Gemeentelijke Infrastructuur en de regionale samenwerking in het Sociaal Domein.

2.3 Externe partijen
In het algemeen geldt dat IB-beleid, landelijke normen en wet- en regelgeving ook gelden voor externe partijen (leveranciers, ketenpartners) waarmee de gemeente samenwerkt (en informatie uitwisselt). Ook voor externe partijen geldt hierbij het '*comply or explain*' beginsel (pas toe of leg uit). Bij de uitvoering hiervan is er echter een gradueel verschil tussen organisaties waarin de gemeente op de een of andere manier participeert (samenwerkingsverbanden) en leveranciers (partijen die in opdracht van de gemeente werken.

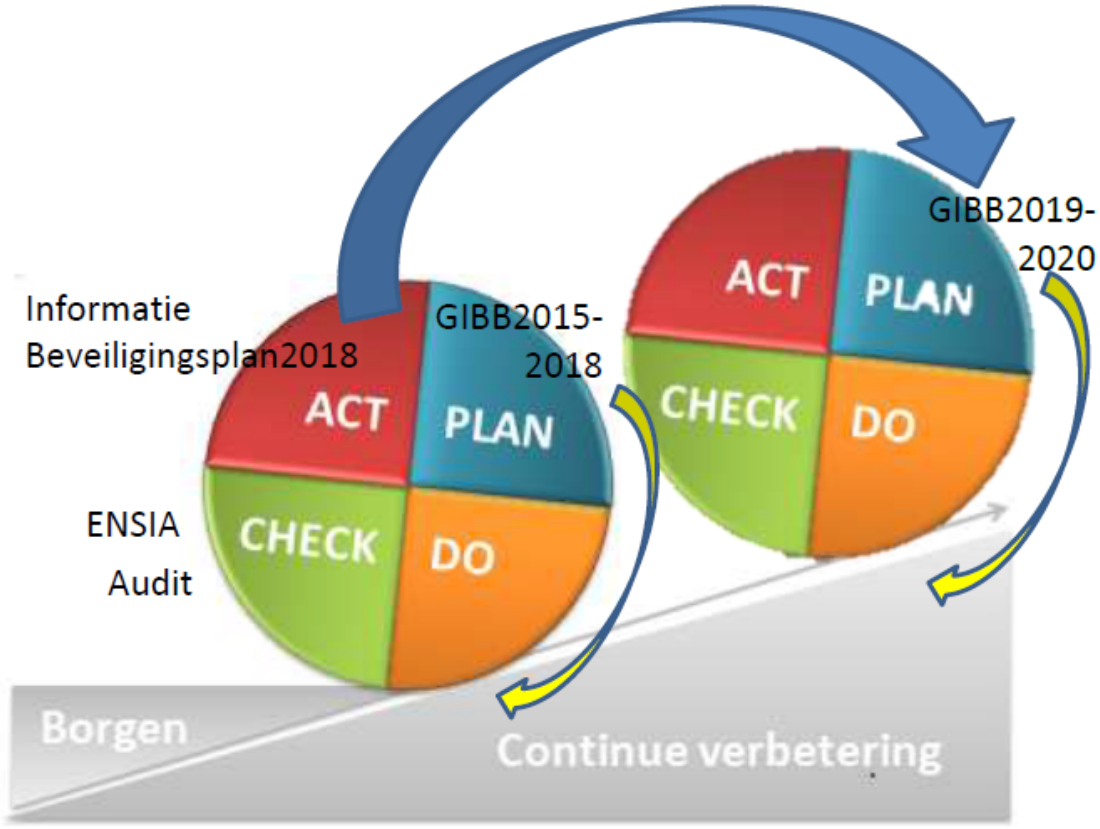
Samenwerkingsverbanden
Het is nodig om beter in beeld te krijgen welke samenwerkingsverbanden er bestaan, welke afspraken gelden en welke aanvullende maatregelen getroffen moeten worden. Dit zal deels aansluiten bij het ingang gezette proces om privacyconvenanten.

Leveranciers
De gemeente is bezig met de overstap naar het gebruik van de Gemeentelijke Inkoopvoorwaarden bij IT-overeenkomsten (GIBIT). Voor externe hosting van data en/of services houden we ons aan de gangbare standaarden zoals voorgesteld door de IBD en het Nationaal Cybersecurity Center (NCSC). Daarnaast sluiten we verwerkersovereenkomsten met leveranciers die persoonsgegevens voor de gemeente verwerken.

7) Conform het advies van de IBD wordt deze term gehanteerd omwille van de herkenbaarheid bij alarmering van buitenaf.

3 Rapportage en verantwoording over Informatiebeveiliging

Informatiebeveiliging is een continu verbeterproces. De cyclische aanpak van 'Plan, do, check en act' vormt het management systeem van informatiebeveiliging. In onderstaand figuur is de PDCA-cyclus voor informatiebeveiliging weergegeven.



Sinds 2017 voeren alle gemeenten jaarlijks de Eenduidige Normatiek Single Information Audit (ENSIA) uit. De verplichten onderdelen van ENSIA 2018 zijn: de informatieveiligheid van Suwinet en DigiD, de Basisregistratie Personen, de Paspoorten Uitvoeringsregeling Nederland, de Basisregistratie Adressen en Gebouwen en de Basisregistratie Grootschalige Topografie. Dit heet de "Verticale verantwoording". Specifiek voor DigiD en Suwinet geldt de verplichting van een oordeel door een IT-auditor. Daarnaast is er de niet-verplichte verantwoording over de algemene informatieveiligheid aan de eigen raad. Dit heet de "horizontale verantwoording". In aanvulling op de verplichte IT audit voor DigiD en Suwinet laat onze gemeente jaarlijks de beantwoording van de gehele vragenlijst over informatiebeveiliging controleren door de IT auditor.

Op grond van de ervaringen met ENSIA 2017 is onderzocht hoe de rapportage naar directie, betrokken colleges van B&W en gemeenteraden verbeterd kan worden. Die verbetering zal bestaan uit twee maatregelen:

- Vereenvoudiging van de verplichte rapportages in samenvattende opleggers;
- Verder gaande integratie van de rapportage over informatieveiligheid (en privacy) in de reguliere P&C cyclus. Dat zal leiden tot twee rapportages in het jaar: de TURAP in september en het jaarverslag/jaarrekening in het voorjaar.

De resultaten uit ENSIA vormen de basis voor de jaarlijkse informatiebeveiligingsplannen.

4 Financiering van informatieveiligheid

Informatieveiligheid kost geld en zal ook meer gaan kosten aangezien gemeenten steeds afhankelijker van ICT worden. Tot op heden worden de kosten van informatieveiligheid grotendeels gedekt vanuit ICT-budgetten. Om meer overzicht te krijgen in de kosten is het noodzakelijk om deze kosten beter in

beeld te krijgen. Tegelijkertijd is het logisch dat informatieveiligheid het beste gediend is door de financiering te beleggen bij de betrokken gegevenseigenaren. Voorgesteld wordt de volgende splitsing aan te brengen:

- De kosten van de beveiliging van de gemeentelijke IT-infrastructuur komt ten laste van het ICT-budget. Deze kosten dienen wel apart gekenmerkt te worden zodat bijgedragen wordt aan inzicht in de kosten van informatieveiligheid.
- Kosten voor aanvullende beveiligingsmaatregelen in IT-vernieuwingsprojecten vormen onderdeel van de projectfinanciering.
- Kosten voor aanvullende beveiligingsmaatregelen van bestaande informatiesystemen worden gedragen door de gegevenseigenaar van het desbetreffende systemen.
- Daarnaast komt er een specifiek budget te komen voor die activiteiten waarbij informatieveiligheid de hoofdzaak is, zoals:
  - Een Information Security Management Systeem;
  - Een systeem voor risicomanagement;
  - ENSIA-traject waaronder IT-audits door externen;
  - Uitvoering van penetratietesten en andere onderzoeken (zowel op de intern als extern gehost systemen)..
  - Activiteiten voor bewustmaking t.a.v. informatieveiligheid;
  - Externe (contra)expertise, forensisch onderzoek en dergelijke.
  - Incidentmanagement.
  - Scholing en kennisopbouw
    De budgethouder hiervan is de CISO.

De financiële consequenties hiervan zijn als budgetneutraal:

- De formatieplaats van coördinator IB binnen Beleid en Projecten wordt hernoemd tot CISO en blijft: 1 fte.
- Het budget voor Informatiebeveiliging (kostenplaats 5534201 Beveiliging infra/9000046 Informatiebeveiliging) gaat over naar Beleid en Projecten voor Informatiebeveiliging. In 2018 bedroeg dit € 87.189.

5 Beslispunten voor het gemeentelijk informatiebeveiligingsbeleid 2019-2021

Burgemeester en wethouders van Purmerend besluiten:

1. het voornemen te hebben het Gemeentelijk Informatiebeveiligingsbeleid 2019-2021 vast te stellen;
2. hierover aan de Ondernemingsraad advies te vragen;
3. de GS/AD op te dragen het college elk half jaar te informeren over de staat van informatieveiligheid;
4. elk jaar aan de raad verantwoording af te leggen over informatieveiligheid door middel van de ENSIA-methodiek;.
5. met dit besluit het Gemeentelijk Informatiebeveiligingsbeleid 2015 (GIBB 2015 kenmerk 1160182) en Uitvoeringsplan GIBB 2015 (kenmerk1164605) te laten vervallen;
6. dit besluit een dag na publicatie in het gemeenteblad in werking te laten treden.

Purmerend, 10 september 2019
Burgemeester en wethouders van Purmerend,
de secretaris
G. Blom
de burgemeester,
D. Bijl

BIJLAGEN

Bijlage 1. De 10 principes voor informatiebeveiliging

Baseline
De 10 principes voor informatiebeveiliging
Behorende bij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en de Baseline Informatiebeveiliging Overheid (BIO)

Colofon
Naam document
De 9 bestuurlijke principes voor informatiebeveiliging
Versienummer
0.7

Versiedatum
13-7-2018

Versiebeheer
Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Met dank aan
De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Wijzigingshistorie:

Versie	Datum	Wijziging / Actie
0.1	Januari 2018	Aanloop naar algehele herziening strategische variant ivm ontwikkelingen BIO
0.3	april 2018	Eerste reviewronde nieuwe strategische baseline
0.4	mei 2018	Brede review intern IBD
0.5	juni 2018	Toelichting toegevoegd
0.6	juni 2018	Commentaar verwerkt, gereed gemaakt voor externe review
0.7	Juli 2018	Externe review commentaar verwerkt

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD beheert de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten

onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruik maken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

Informatiebeveiliging en de gemeentelijke bestuurder

Gemeenten wisselen op alle beleidsterreinen informatie uit en beheren dat op vele manieren. Binnen de eigen organisatie, maar ook daarbuiten: met inwoners, ondernemers, ketenpartners en mede-overheden. Door informatie te delen kunnen gemeenten onder andere hun dienstverlening beter organiseren, de veiligheid van burgers verbeteren en meer mensen aan het werk krijgen. Als professionele organisatie past hierbij dat gemeenten ook de beveiliging van informatie adequaat organiseren. Informatie moet immers beschikbaar, actueel, volledig en betrouwbaar zijn en mag alleen door bevoegden zijn in te zien. Bij de uitwisseling moeten gemeenten te allen tijde rekening houden met beveiligings- en privacyaspecten omdat ze een maatschappelijke en wettelijke verantwoordelijkheid [1] hebben om de gegevens van hun burgers onder alle omstandigheden te beschermen. De risico's rondom de vertrouwelijkheid, integriteit en beschikbaarheid van informatie(systemen) maken dat het onderwerp informatiebeveiliging niet mag ontbreken op de bestuurstafel.

Mens, proces en techniek
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? Gemeentelijke bestuurders zijn verantwoordelijk voor de informatiebeveiliging binnen en buiten de gemeentelijke organisatie. Beveiliging van gegevens en systemen is een zaak van organisatie, procedures, werkprocessen en in de laatste plaats techniek. Het gaat om de mens, de manier waarop deze werkt en het gereedschap waarmee het werk verricht wordt. Dit samenspel vraagt om bestuurlijke visie, focus en draagvlak. De bestuurder geeft hierin het goede voorbeeld.

Risicomanagement is de basis.
Het is aan de bestuurder om de risicobereidheid te bepalen en daarmee ook te controleren of de maatregelen binnen uw organisatie de risico's terugbrengen tot een voor u acceptabel niveau. Overschrijding van dat niveau vereist expliciete besluitvorming van de bestuurder. Risicomanagement staat aan de basis van informatiebeveiliging. Er dient een continu proces van identificatie en beoordeling van risico's plaats te vinden om te bepalen wat nodig is om informatie adequaat te beschermen. Hierbij moet worden opgemerkt dat het risico nul niet bestaat en dat het aan het bestuur is om te bepalen hoeveel of welk risico acceptabel is. En de risico's zijn talrijk: privacyschendingen door een datalek, economische schade door het uitlekken van vertrouwelijke plannen, fysieke schade door storingen in systemen in de openbare ruimte. De bestuurder is niet alleen verantwoordelijk, maar ook aansprakelijk voor schade die voortvloeit uit het ontbreken van een veilige informatievoorziening.

Normen en regels
De internationale norm om informatie(systemen) adequaat te beveiligen is vastgelegd in de ISO27001/2. Voor de Nederlandse overheid is deze norm vertaald naar een zogenaamde baseline informatiebeveiliging gemeenten / overheid (BIG/BIO) met daarin de regels waaraan de verschillende overheidslagen dienen te voldoen. Door middel van een zelfevaluatie (ENSIA) verantwoorden gemeenten zich over deze norm. De ontwikkelingen in de informatietechnologie gaan steeds sneller en de wetgeving rondom de bescherming van persoonsgegevens is aangescherpt.

Bestuurlijke aanvulling op de normen en regels
In aanvulling op de baseline bevat dit document geen regels, maar principes. Daarmee gaat dit document over waarden die u zichzelf als bestuurder oplegt. Deze waarden dienen verbonden te zijn aan de waarden van uw organisatie. Dit document is daarmee de bestuurlijke aanvulling op de baseline en helpen u om de juiste dingen te doen. De principes gaan daarom vooral over u en uw rol bij het borgen van informatiebeveiliging in uw organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Uw organisatie wordt verder dagelijks ondersteund vanuit de IBD bij VNG

1) O.a. de Algemene wet gegevensbescherming, Wet BRP, PUN, DigiD, BAG, BGT en SUWI

en zij hebben daarvoor ondersteuningsproducten geschreven in de vorm van best practice aanwijzingen die helpen bij het invullen van het HOE en zij zijn telefonisch en per mail benaderbaar voor iedere denkbare vraag op het gebied van informatiebeveiliging.

De 10 principes voor informatiebeveiliging

Informatiebeveiliging creëert waarde, voorkomt schade en draagt bij aan de bedrijfsdoelstellingen van de organisatie. Om dat te bewerkstelligen zijn de volgende principes belangrijk:

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

Ik ben mij bewust van de voorbeeldfunctie van een bestuurder en ik draag uit dat risicomanagement van iedereen is. Ik zorg daarom voor een cultuur waarin iedereen vrij is om dreigingen waar te nemen en te melden. In eerste instantie bij de verantwoordelijke, maar indien nodig ook bij mij als bestuurder. Ik spoor managers aan om voorwaarden te scheppen zodat iedereen binnen de organisatie deelgenoot wordt van het proces van risicomanagement. Ik zorg ervoor dat fouten besproken kunnen worden en dat daarmee een lerende organisatie ontstaat. Ten slotte geef ik in mijn eigen doen en laten het goede voorbeeld van hoe je verantwoordelijk omgaat met informatie.

Toelichting
Zonder open cultuur waar iedereen vrij is om te spreken en zonder beperkende factoren als beschermend midden management, heilige huisjes en aanverwante organisatie perikelen is het onmogelijk om risicomanagement goed van de grond te krijgen. Als u er in slaagt om risicodenken en cultuur in alle haarvaten van uw organisatie te laten landen door het geven van voorbeeld gedrag, door het te eisen van uw managers en door helder verwachtingsmanagement, dan heeft u een organisatie die gezond kan reageren op de dagelijkse dreigingen en daarmee samenhangende risico's.

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

Ik maak medewerkers bewust van de risico's van het werken met informatie en ik maak risicomanagement onderdeel van het MT-overleg en laat het anderen in vergaderingen agenderen. Ik zorg ervoor dat iedereen risicomanagement toepast en dat het gezien wordt als vanzelfsprekend en nuttig. Ik ben transparant naar de raad en zorg ervoor dat zij ook hun rol kunnen pakken op dit onderwerp.

Toelichting
Iedereen moet betrokken worden bij risicomanagement, in alle lagen van de organisatie. Maak gebruik van de kennis en verantwoordelijkheid van proces- en systeem eigenaren. Gebruik uw CISO, FG en Controller als onafhankelijke adviseur en laat ze samenwerken in het risk-team, waar u vanzelfsprekend ook zitting in heeft. Laat uw interne communicatie aandacht besteden aan het verspreiden van de boodschap, het belang en het voordeel van risicomanagement binnen uw organisatie. Goed uitgevoerd risicomanagement creëert waarde voor de organisatie omdat de kwaliteit van besluiten toeneemt en de kans op falen afneemt.

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

Ik zorg dat risicomanagement een onderdeel is van het bestuurlijk overleg en dialoog, daarnaast zal ik het integreren in het risicobewustzijn van alle medewerkers en onderdeel laten zijn van de samenwerking met partners en ik zorg ervoor dat risicomanagement integraal onderdeel uitmaakt van uitbestedingen en samenwerkingen. Ik zorg ervoor dat risicomanagement geformaliseerd wordt binnen de hele organisatie met een duidelijke verdeling van verantwoordelijkheden en heldere besluitvorming.

Toelichting
Risicomanagement gaat alleen werken als het geïntegreerd is in alle werkprocessen van de organisatie. Dat kan alleen bereikt worden als het praten over risico's onderwerp is van iedere agenda en daarmee wordt een eerste aanzet gegeven om op een gestructureerde wijze om te gaan met risico's en pro-actief oplossingen te zoeken voor de risico's die aandacht behoeven. Maak lijnmanagers verantwoordelijk voor risicomanagement door afspraken met ze te maken hoe zij risicomanagement in hun dagelijkse praktijk vorm geven en op welke wijze zij daarover rapporteren. Maar bovenal: laat informatiebeveiliging een plek/paragraaf krijgen in alle bestuurlijke documenten.

4. Risicomanagement is onderdeel van de besluitvorming
Risicomanagement is onderdeel van alle besluiten en risicomanagement is chefsache!

Ik maak medewerkers mede-eigenaar van het risicoproces op het vlak van informatieveiligheid en ik maak informatiebeveiliging onderwerp van alle overlegstructuren. Ik draag er zorg voor dat besluiten ten aanzien van de omgang met risico's expliciet genomen en vastgelegd worden. Ik laat risicomanagement naadloos aansluiten op de strategische en beleidsmatige doelstellingen van de organisatie. Op deze wijze bied ik een duidelijk kader waarbinnen mijn medewerkers kunnen opereren.

Toelichting
Iedereen is ervan of zou ervan moeten zijn, u kunt als bestuurder alleen maar de juiste dingen doen als informatie u bereikt, maar vooral als het op de agenda staat. Door risicomanagement of vragen over dreigingen en risico's mee te nemen in de vragen die u stelt aan uw managers kunt u in uw beslissingen ook rekening houden met deze bedreigingen en risico's en ervoor zorgen dat ze behandeld worden voordat ze manifest worden en escalatie voorkomen.

5. 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.

Ik zorg dat ik de risico's ken die een gevaar vormen voor de informatievoorziening van de bedrijfsvoering van de gemeente en ik anticipeer op risico's die voortkomen uit het werken in ketens en ik houd rekening met de complexiteit, de onzekerheid en ambiguïteit in de samenwerking met anderen. Bij samenwerken of uitbesteden van (delen) van de organisatie of processen zorg ik ervoor dat de risico's in kaart gebracht zijn, verantwoordelijkheden verdeeld en dat de juiste maatregelen getroffen worden.

Toelichting
Het risicomanagementproces moet passen bij de organisatie en ondersteunen aan de bedrijfsdoelstellingen. De gemeente kan pro-actief communiceren en laten zien dat risicomanagement bijvoorbeeld in relatie tot privacy belangrijk is en dat ze er naar streven om zorgvuldig (naar goed huisvaderschap) met persoonsgegevens om te gaan. Bij het uitbesteden of delen van informatie moeten de juiste voorzieningen getroffen worden om ervoor te zorgen dat ook buiten de organisatie de juiste dingen worden gedaan.

6. 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.

Ik zorg ervoor dat risicomanagement cyclisch is en daarmee kan ik reageren op veranderingen en toekomstgericht sturen. Het staat daarom regelmatig op de agenda.

Toelichting
Risicomanagement moet een cyclisch, iteratief en terugkerend proces zijn, want dreigingen veranderen, doelstellingen veranderen, de omgeving verandert, klanten gaan meer zorgvuldigheid en of transparantie eisen, wetgeving verandert. Kortom, als risicomanagement geen rekening houdt met een veranderende omgeving en de eigen organisatie, dan doet uw organisatie misschien de verkeerde dingen of teveel of misschien wel te weinig.

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

Ik zorg ervoor dat er voldoende resources beschikbaar zijn om de onderkende risico's op een adequate manier te behandelen. Als gebleken is dat een risico een bedreiging is voor de organisatie doelstellingen en er maatregelen genomen moeten worden, dan zorg ik er ook voor dat de middelen beschikbaar zijn of komen om deze maatregelen uit te voeren.

Toelichting
Risico's ontwijken, mitigeren, verzekeren of wegnemen door het nemen van preventieve-, detectieve-, repressieve- en/of correctieve maatregelen. Welke strategie u ook kiest, ze kosten allemaal resources in termen van tijd, geld en mens capaciteit. Als u niet investeert in informatiebeveiliging dan keert het spook zich op termijn waarschijnlijk tegen uw organisatie en worden alle doelstellingen, hoe goed bedoelt ook, vertaalt in luchtkastelen.

8. 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.

Risicomanagement is gebaseerd op de best beschikbare informatie vanuit mijn organisatie en vanuit mijn samenwerkingen, ik zorg ervoor dat alle belanghebbenden op een gestructureerde en voorspelbare wijze informatie delen die bijdraagt aan een gezonde risicomanagement cultuur.

Toelichting
Zonder goede informatie geen goede risico-inschattingen en besluiten. Zonder goede en tijdige informatie lopen uw organisatie en uw primaire processen een mogelijk risico met mogelijk zelfs een verstoring waar uw klanten last van krijgen. Zonder goede en tijdige informatie neemt u de verkeerde beslissingen en doet uw organisatie de verkeerde dingen.

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

Door mijn inzet zorg ik ervoor dat risicogestuurd werken doorontwikkeld wordt. Ik reflecteer op ervaringen en ik nodig medewerkers uit tot het delen van ervaringen met betrekking tot de risico's die de informatievoorziening bedreigen. Ik zorg ervoor dat de organisatie kan leren van incidenten en dat de organisatie leert te ontdekken wat wel en wat niet werkt.

Toelichting
Risicomanagement is ook de wil om te leren en de wil om te verbeteren. Als die wil er niet is dan heeft u een ad-hoc organisatie die alleen maar kan reageren op incidenten waarbij de energie ontbreekt om te leren en te verbeteren. Incidenten kunnen voorkomen worden door te leren en te verbeteren, het voordeel voor u is geen verassingen, geen raadsvragen en geen pers die u kritische vragen stelt. Als de organisatie verbeterd kunt u ieder risico aan en kunt u aantonen dat uw organisatie (en u) de juiste dingen hebben gedaan.

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

Ik controleer actief binnen mijn organisatie doordat ik opdracht geef om de werking van risicomanagement binnen mijn organisatie op effectiviteit en efficiency te (laten) controleren. Naast management rapportages zijn (externe) controles de manier om te weten te komen of en hoe mijn uitgedragen beleid in de praktijk werkt. Als bestuurder weeg ik goed geïnformeerd risico's en belangen af en neem ik mijn verantwoordelijkheid om knopen door te hakken.

Toelichting
Controle is belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn in de organisatie. Naast verslagen en managementrapportages zijn incidenten en dan vooral de manier waarop ze afgewikkeld worden een goede graadmeter om signalen te krijgen over de wijze waarop de organisatie omgaat met het onderwerp. Medewerkers kunnen er op vertrouwen dat besluiten op bestuurdersniveau genomen worden, wanneer de situatie daar om vraagt.

Kijk voor meer informatie op: www.informatiebeveiligingsdienst.nl
Nassaulaan 12
2514 JS Den Haag
CERT: 070 373 80 11 (9:00 – 17:00 ma – vr)
CERT 24x7: Piketnummer (instructies via voicemail)
info@IBDGemeenten.nl / incident@IBDGemeenten.nl

Bijlage 2. Functieomschrijving CISO

Introductie
Onderstaande omschrijving is gebaseerd op de Handreiking IB-functieprofiel Chief information security officer (CISO) van de IBD (versie 1.0.1 – augustus 2016).

Functienaam
Algemene functienaam: CISO (CISO)

Doel van de functie
Op basis van het gemeentelijk informatiebeveiligingsbeleid zorgdragen voor een samenhangend pakket van maatregelen ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen de gemeente.

Plaats in de organisatie
De CISO maakt deel uit van het team Beleid en Projecten.

Resultaatgebieden

a. Beleid en coördinatie
Het opstellen en actualiseren van het informatiebeveiligingsbeleid (langere termijn).
Het (laten) opstellen van informatiebeveiligingsjaarplannen
Het coördineren van de werkzaamheden van personen, teams en instanties die zijn betrokken bij de uitvoering van het informatiebeveiligingsbeleid.

b. Controle en registratie
Het toezicht houden op de implementatie en naleving van het informatiebeveiligingsbeleid.
Het opstellen van een controleplan, evenals het leveren van ondersteuning bij het uitvoeren van de daarin gedefinieerde taken.
Het (laten) uitvoeren of initiëren van risicoanalyses en interne audits.
Het verzamelen en registreren van informatie over de aanwezige beveiligingsmaatregelen.
Het opzetten of initiëren van een registratie voor beveiligingsincidenten, evenals het afhandelen van opgetreden incidenten en het nemen van preventieve maatregelen ter voorkoming van dergelijke incidenten.

c. Communicatie en voorlichting
Het onderhouden van externe en interne contacten op alle niveaus binnen dit kader.
Het organiseren van en deelnemen aan het Tactisch overleg Informatiebeveiliging.
Het organiseren van en leiden van het Operationeel Overleg Informatiebeveiliging.
Het (laten) verzorgen en coördineren van voorlichting en interne opleidingen van het personeel op het gebied van informatiebeveiliging.
Het stimuleren van het beveiligingsbewustzijn en het opstellen, uitvoeren en onderhouden van een communicatieplan.
Het volgen van nieuwe ontwikkelingen en wetgeving op het gebied van informatiebeveiliging.

d. Advies en rapportage
Het optreden als (mede) opdrachtgever bij beveiligingsprojecten in de organisatie.
Het afstemmen van informatiebeveiliging met lopende projecten binnen de organisatie.
Het (laten) uitwerken van beveiligingsplannen ten aanzien van de maatregelen, evenals het leveren van ondersteuning bij het uitvoeren van de geaccepteerde plannen.
Het geven van gevraagd en ongevraagd advies aan het college van B&W, directie en het lijnmanagement over de te nemen maatregelen.
Het rapporteren aan het college van B&W, directie en het lijnmanagement over het gevoerde beleid met betrekking tot informatiebeveiliging, de voortgang van implementatie van nieuwe maatregelen, opgetreden incidenten, ondernomen acties en resultaten van onderzoeken.

Verantwoordelijkheden en bevoegdheden
De bevoegdheid om op elke plek binnen de organisatie, het IT-netwerk en/of leveranciers van de gemeente gevraagd en ongevraagd onderzoek te kunnen (laten) doen naar de informatiebeveiliging. Op basis daarvan het geven van ongevraagd advies aan het college van B&W, directie en het lijnmanagement over de te nemen maatregelen.

- Bij (grote) beveiligingsincidenten/-risico's heeft de CISO de bevoegdheid, zo nodig, direct in te grijpen (met verantwoording achteraf richting het management. De managementlaag waaraan verantwoording wordt afgelegd, is afhankelijk van type, omvang en impact van het incident. De CISO geeft leiding aan het CSIRT.

- De CISO heeft de bevoegdheid om namens het college aangifte te doen van computerfraude, datalekken en andere incidenten die de informatieveiligheid raken.
- De CISO is budgethouder van het budget voor informatiebeveiliging.

Contacten
a. Extern:
- Informatiebeveiligingsdienst (de CISO is uit hoofde van zijn functie Vertrouwenscontactpersoon IB –VCIB).
- VNG
- Ministeries
- Andere gemeenten (m.n. functionarissen IB en informatievoorziening en ICT)
- Auditors
- Leveranciers'
- Politie en Justitie.

b. Intern:
- Portefeuillehouder Informatiebeveiliging
- Algemeen Directeur en domeindirecteuren
- Concerncontroller en afdelingscontrollers
- Teammanagers, interne gegevenseigenaren, proceseigenaren
- Functionaris(sen) belast met Gegevensbescherming (Privacybescherming)
- Projectleiders, systeembeheerders, functioneel beheerders en gegevensbeheerders
- Alle overige medewerkers

Opleiding, kennis en ervaring
- HBO/Academisch werk- en denkniveau
- Kennis en ervaring op het gebied van bestuurs-/bedrijfskunde en/of informatica
- Kennis van de actuele stand van zaken en mogelijkheden van ICT (besturingssystemen, netwerken, standaarden, ontwikkel- en beheermethoden)
- Kennis en ervaring op het gebied van informatiebeveiliging en risicoanalyse
- Kennis van de Baseline Informatiebeveiliging voor Nederlandse Gemeenten (BIG) en de Baseline Informatiebeveiliging Overheid (BIO)
- Kennis van specialistische beveiligingstechnieken
- Kennis en ervaring op het gebied van adviseren en organisatiekunde
- Kennis van technische infrastructuur, gemeentelijke informatiesystemen en processen
- Kennis en ervaring met projectmatig werken en projectmanagement.

Competenties
- Goede communicatieve vaardigheden, zowel mondeling als schriftelijk
- Goed kunnen samenwerken met verschillende disciplines op verschillende niveaus
- Alert, initiatiefrijk, omgevingsbewust
- Integer
- Overtuigingskracht
- Bereid tot permanente scholing