Een bestuursmanifest voor informatieveiligheid

Principes voor informatieveiligheid

Het thema Informatiebeveiliging is de laatste jaren sterk op de voorgrond gekomen. Door de toegenomen digitalisering zijn onze de kwetsbaarheden toegenomen en zal permanente aandacht nodig blijven voor informatieveiligheid. Terwijl we weten dat Informatieveiligheid een zaak is van de business/de lijnorganisatie en daarmee is verankerd in de bestuursverantwoordelijkheid van de organisatie, zien we tevens dat dit vakgebied is doortrokken van vakjargon en dat het vele technische specialismen omvat. In het algemeen geldt dat dit niet op natuurlijke wijze aansluit bij de wereld van de bestuurder. De VNG-IBD heeft tien principes opgesteld die behulpzaam kunnen zijn bij het beantwoorden van de vraag hoe de bestuurder zich kan verhouden tot het thema informatieveiligheid. Het zijn tips die hij kan gebruiken bij de invulling van zijn rol. Bijgaand is dit document toegevoegd.

In onderstaande vijf ik-boodschappen zijn de tien principes gebundeld tot een soort bestuursmanifest. Wat CIP betreft staat hierin de kern van de rol die bestuurders hebben bij Informatieveiligheid.

Ik bevorder een veilige cultuur

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.

Ik stel risicomanagement centraal

Ik zorg ervoor dat risicomanagement geformaliseerd wordt binnen de hele organisatie en in de ketens waarin wij werken, met een duidelijke verdeling van verantwoordelijkheden en heldere besluitvorming. 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.

Ik zie informatiebeveiliging als een proces

Ik zorg ervoor dat risicomanagement cyclisch is en daarmee kan ik reageren op veranderingen en toekomstgericht sturen. Het staat daarom regelmatig op de agenda. Hiermee adresseer ik het gegeven dat omstandigheden en dientengevolge risico's voortdurend wijzigen en regelmatig nopen tot her-evaluatie. Daarnaast bevorder ik hiermee ook het proces van leren en verbeteren in de organisatie.

Ik zorg voor toereikend budget

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.

Ik controleer en evalueer

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.

INFORMATIE
BEVEILIGINGS
DIENST

Bijlage

Baseline

De 10 bestuurlijke principes voor informatiebeveiliging

Behorende bij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en de Baseline Informatiebeveiliging Overheid (BIO)

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document
De 9 bestuurlijke principes voor informatiebeveiliging

Versienummer
1.0

Versiedatum
21-08-2018

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

Copyright

Rechten en vrijwaring
De IBD is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan de IBD geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. De IBD aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

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
1.0	Augustus 2018	Finale versie ter publicatie

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 informatie-technologie 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 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.

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

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