



STRATEGISCH INFORMATIEBEVEILIGINGS- BELEID

Informatiebeveiliging 2020-2023

OPSTELLER

Organisatie : Omgevingsdienst Noord-Holland Noord
Opsteller : Jos Engelhart
Telefoon : 06 - 1404 5161
E-mail : jengelhart@odnhn.nl
Kenmerk : 8107280

Adres : Postbus 2095
1620 EB HOORN
Bezoekadres : Dampten 2
1624 NR HOORN

DATUM

22 september 2020

VERSIEHISTORIE

Datum	Auteur	Reden wijziging
27-08-2020	Jos Engelhart	Concept.
22-08-2020	Jos Engelhart	Strategisch IB-beleid besproken met Rob van Doorn en Damir Stajcer

VERZENDLIJST

Wie	Rol	Gevraagde actie
Rob van Doorn	Directeur OD NHN	Instemmen beleid
Damir Stajcer	MT-lid	Kennisnemen beleid
Ed Langereis	MT-lid	Kennisnemen beleid
Mike Goudemond	MT-lid	Kennisnemen beleid
Jeroen Vogel	MT-lid	Kennisnemen beleid

INHOUDSOPGAVE

1.	INLEIDING.....	5
1.1	Leeswijzer.....	5
1.2	Wat is informatiebeveiliging?.....	5
1.3	Ambitie en visie van de OD NHN op het gebied van informatieveiligheid.....	5
2.	STRATEGISCH BELEID.....	7
2.1	Doel.....	7
2.3	Standaarden informatiebeveiliging.....	8
2.4	Plaats van het strategisch informatiebeveiligingsbeleid.....	8
2.5	Scope informatiebeveiliging.....	8
2.6	Uitgangspunten.....	8
3.	ORGANISATIE, TAKEN & VERANTWOORDELIJKHEDEN.....	11
3.1	Aansturing: Directeur OD NHN.....	11
3.2	Uitvoering: afdelingsmanagers.....	11
3.3	Controle en verantwoording.....	12
	BIJLAGE A: DE 10 PRINCIPES VOOR INFORMATIEBEVEILIGING.....	13

1. INLEIDING

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2020 tot en met 2023 en vervangt het in 2019 vastgestelde "Informatiebeveiligingsbeleid versie 2019-07-02".

Dit beleid is richtinggevend en kaderstellend en wordt waar nodig aangevuld met specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

Met dit "Strategisch Informatiebeveiligingsbeleid 2020-2023" zet de Omgevingsdienst Noord-Holland Noord (OD NHN) een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de OD NHN te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO) zie bijlage C.

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen Informatiebeveiligingsplan (vastgesteld door de directie) worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de afdelingsmanagers, de CISO en het dreigingsbeeld van de IBD. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

1.2 Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie.

Het informatiebeveiligingsbeleid geldt voor alle processen van de OD NHN en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politieke bestuur, alle medewerkers, klanten, gasten, bezoekers en externe relaties.

1.3 Ambitie en visie van de OD NHN op het gebied van informatieveiligheid

De visie van de OD NHN is dat het zich voor de komende drie jaar richt op het professioneel, efficiënt en kwalitatief goed uitvoeren van de aan haar opgedragen (milieu)taken.

Dit informatiebeveiligingsbeleid sluit aan bij het professioneel werken en uitvoeren van de taken waarvoor de OD NHN is opgesteld. De klanten (gemeenten, provincie) waaraan de OD NHN haar diensten verleend, moeten immers kunnen vertrouwen op een goede beveiliging van de informatie die de OD NHN verwerkt over hun inwoners en hun organisaties. De OD NHN is hier zelfs wettelijk toe verplicht (wet AVG).

De ambitie die de OD NHN heeft op het gebied van informatiebeveiliging is om medewerkers een veilige werkomgeving te bieden die optimaal wordt gefaciliteerd zonder de beveiliging van de informatie in gevaar te brengen. Dat zal in de praktijk een spanningsveld opleveren omdat (technische) maatregelen beperkend kunnen zijn. Door medewerkers blijvend bewust

te maken van het belang van een goede beveiliging van informatie en de verantwoordelijkheid die zij hier zelf in hebben, wordt continu gewerkt aan het creëren van draagvlak voor de genomen en te nemen maatregelen.

2. STRATEGISCH BELEID

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het "Strategisch Informatiebeveiligingsbeleid voor de jaren 2020 tot 2023". De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan (IBP).

2.2 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid zijn:

- De BIO.
- De 10 principes voor informatiebeveiliging (zie bijlage A).
- Het dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten.
- Informatie uit incidenten en inbreuken op de beveiliging.

2.2.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement dan de oude BIG. Dat wil zeggen dat de afdelingsmanagers nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.2.2 De 10 principes voor informatiebeveiliging (zie bijlage C)

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:

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 ingecalculiseerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van de Directeur OD bij het borgen van informatiebeveiliging in de OD NHN. Deze principes ondersteunen de directeur bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de bedrijfsprocessen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de OD NHN. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de directietafel.

2.2.3 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten, dat jaarlijks door de Informatiebeveiligingsdienst (IBD) wordt geactualiseerd, geeft zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit

dreigingsbeeld wordt gebruikt om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

2.2.4 Informatie uit incidenten en inbreuken op de beveiliging

De OD NHN kent naast het hierboven genoemde dreigingsbeeld een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.3 Standaarden informatiebeveiliging

De OD NHN baseert haar informatiebeveiligingsbeleid op de BIO (Baseline Informatiebeveiliging Overheid). Dit is een standaard die voor de gehele overheid verplicht is gesteld en waarin controls en maatregelen zijn opgenomen waaraan de OD NHN moet voldoen.

De BIO bestaat uit een baseline met drie niveaus van beveiligen: BBN1, BBN2 en BBN3. De OD NHN moet tenminste voldoen aan de controls en maatregelen die op het niveau BBN1 zijn gedefinieerd. Een dataclassificatie op de bedrijfskritische applicaties moet uitwijzen welke aanvullende maatregelen nodig zijn.

2.4 Plaats van het strategisch informatiebeveiligingsbeleid

Dit strategisch informatiebeveiligingsbeleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau.

In dit document wordt op strategisch niveau het informatiebeveiligingsbeleid beschreven en zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven 'Informatiebeveiligingsplan'.

2.5 Scope informatiebeveiliging

De scope van dit strategisch informatiebeveiligingsbeleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van de OD NHN en externe partijen (bijvoorbeeld politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit strategisch Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af.

Bewust wordt in dit strategisch informatiebeveiligingsbeleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

2.6 Uitgangspunten

De directie en het afdelingsmanagement spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de organisatie heeft, de risico's die de OD NHN hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele organisatie. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligings-

beleid is in lijn met het algemene beleid van de OD NHN en de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Strategische doelen

De strategische doelen van het informatiebeveiligingsbeleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van klanten en medewerkers.
- Het waarborgen van de naleving van dit beleid.

2.6.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van dit beleid zijn:

- Alle informatie en informatiesystemen zijn van belang voor de OD NHN. De Directeur OD NHN is eindverantwoordelijke voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de OD NHN hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Informatiebeveiliging is een continu verbeterproces. "Plan, do, check en act" vormen samen het managementsysteem van informatiebeveiliging.
- De OD NHN stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

2.6.3 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- De Directeur OD NHN stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- De Directeur OD NHN stelt jaarlijks het informatiebeveiligingsplan vast.

- De Directeur OD NHN is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- De Directeur OD NHN is verantwoordelijk voor het vragen om informatie bij de afdelingsmanagers en ziet erop toe dat de afdelingsmanagers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie, voorafgaand aan de P&C-gesprekken.
- Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de controleplannen.
- De afdelingsmanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- Alle medewerkers van de OD NHN worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Afdelingsmanagers zien erop toe dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechtgebende medewerkers de juiste persoonsgegevens ingezien en verwerkt hebben.
- De benodigde beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Afdelingsmanagers laten Quick Scans informatiebeveiliging uitvoeren op basis van de BIO om deze risicoafwegingen te kunnen maken. De CISO ondersteunt hierin.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een informatiebeveiligingsplan opgesteld onder leiding van de CISO, gebaseerd op:
 - Het dreigingsbeeld gemeenten van de IBD;
 - De door de afdelingsmanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

3. ORGANISATIE, TAKEN & VERANTWOORDELIJKHEDEN

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn (CISO) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne of externe) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering. Een audit vindt plaats op verzoek van de Directeur OD NHN.

3.1 Aansturing: Directeur OD NHN

De Directeur OD NHN zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingsmanager. De Directeur OD NHN zorgt dat de afdelingsmanagers zich verantwoorden over de beveiliging van de informatie die onder hen berust. De Directeur OD NHN zorgt dat de eindverantwoordelijke portefeuillehouder binnen het Dagelijks Bestuur gevraagd en ongevraagd geïnformeerd kan worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het Dagelijks Bestuur zich ook verantwoorden naar het Algemeen Bestuur.

De Directeur OD NHN stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De Directeur OD NHN draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO. De Directeur OD NHN autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de OD NHN gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: afdelingsmanagers

Informatiebeveiliging valt onder de verantwoordelijkheden van alle afdelingsmanagers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Afdelingsmanagers rapporteren aan de Directeur OD NHN over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in het bedrijfsvoeringsoverleg.

Taken van de afdelingsmanagers in het kader van informatiebeveiliging zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid, de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

De voorbereiding en coördinatie van het overleg ligt bij de CISO.

3.3 Controle en verantwoording

Dit strategisch beleid is een verantwoordelijkheid van de Directeur OD NHN. De Directeur OD NHN zal volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

De Directeur OD NHN is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan de portefeuillehouder. Daarnaast rapporteert de Directeur OD NHN over de mate waarin invulling is gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

Middels deze verantwoordingsrapportage worden het Dagelijks Bestuur van de OD NHN en het Algemeen Bestuur geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de OD NHN informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar klanten adequaat te beschermen.

Vastgesteld op : [datum] door de Directeur OD NHN

[Ondertekening]

BIJLAGE A: 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 in elk stadium.

Ik ben mij bewust van de voorbeeldfunctie van een bestuurder en ik draag uit dat risicomanagement van ieder- een 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 is het niet goed mogelijk om risico's te identificeren en als de risico's niet bekend zijn, kunt u ze ook niet adresseren. Als u in uw organisatie een cultuur bevordert waarin mensen zich vrij voelen om risico's te melden en maatregelen voor te stellen, dan kunt u adequaat reageren op dreigingen en 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 hij ook zijn rol kan 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 Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG) en Controller als onafhankelijke adviseur en laat ze samenwerken in een risicoteam, 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 kwade lichteit 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 het 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 risico-

management geformaliseerd wordt binnen de hele organisatie met een duidelijke verdeling van verantwoordelijkheden en heldere besluitvorming.

Toelichting

Risicomanagement werkt alleen als het geïntegreerd is in alle werkprocessen van de organisatie. Dat kan alleen bereikt worden als risico's regelmatig op de agenda staan en als risico's een plek/paragraaf krijgen in alle bestuurlijke documenten. Maak lijnmanagers verantwoordelijk voor risicomanagement door afspraken met ze te maken over uw risicobereidheid. Lijnmanagers zijn verantwoordelijk voor de maatregelen en rapportage daarover.

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 de medewerkers kunnen opereren.

Toelichting

U kunt als bestuurder alleen de juiste richting aangeven als informatie u bereikt. Door dreigingen en risico's mee te nemen in de vragen die u stelt aan uw managers kunt u er in uw beslissingen ook rekening mee houden. Zo kunt u bijsturen voordat risico's 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 organisatiedoelstellingen. De keten is zo sterk als de zwakste schakel. De gemeente dient met ketenpartners en leveranciers regelmatig het gesprek te voeren over risico's en de maatregelen die ervoor zorgen dat de risico's tot een acceptabel niveau worden teruggebracht.

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, doel- stellingen veranderen, de omgeving verandert en wetgeving verandert. Indien u in uw risicomanagement geen rekening houdt met een veranderende omgeving, dan zijn uw maatregelen op termijn wellicht niet doeltreffend of doelmatig.

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

Toelichting

Risico's kunt u ontwijken, mitigeren, overdragen of wegnemen door het nemen van preventieve-, repressieve- en/of correctieve maatregelen. Welke strategie u ook kiest, ze kosten allemaal middelen in termen van tijd en geld. Voor maatregelen kan derhalve een kosten-batenanalyse worden gemaakt.

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 risicomanagement.

Toelichting

Zonder goede informatie kunt u geen goede risico-inschattingen en besluiten nemen. Zonder goede en tijdige informatie bent u niet bekend met de risico's die uw organisatie loopt.

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 gedijt het beste in een organisatie die leert van ervaringen en op basis hiervan verbeteringen doorvoert. Hoe goed u uw informatiehuishouding ook beveiligt, incidenten zullen altijd voorkomen. Door te zoeken naar verbeterpunten en de wil om te leren bouwt u doorlopend aan het verhogen van uw digitale weerbaarheid.

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 geef opdracht om de werking van risicomanagement binnen mijn organisatie op effectiviteit en efficiency te (laten) controleren. Naast managementrapportages zijn (externe) con-

troles de manier om te weten te komen of en hoe het beleid in de praktijk uitwerkt. 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 risico- management ingebed zijn in de organisatie. Naast verslagen en managementrapportages zijn incidenten, en dan vooral de manier waarop ze afgewikkeld worden, een goede graadmeter om te zien hoe de organisatie omgaat met het onderwerp. Medewerkers kunnen erop vertrouwen dat besluiten op bestuursniveau genomen worden, wanneer de situatie daar om vraagt.