

INFORMATIEBEVEILIGINGSBELEID MGR SDCG

STRATEGISCH INFORMATIEBEVEILIGINGSBELEID 2020-2023 MGR SOCIAAL DOMEIN CENTRAAL GELDERLAND

		datum
versie	1.0	12-09-2019
Auteur	Kees van Galen	
Adviseur	Jos Thijssen (RID)	25-08-2019
Gezien door directie	Hermien Wiselius	1-9-2019
Akkoord directie	Hermien Wiselius	2-9-2019
Besproken in MT		2-9-2019
Besproken in bestuur	DB	28-10-19
Goedgekeurd door bestuur	DB	28-10-19

Inleiding.....	2
Strategisch beleid.....	2
Doel	2
Ontwikkelingen	2
Plaats van het strategisch beleid.....	4
Scope informatiebeveiliging.....	4
Uitgangspunten.....	4
Organisatie, taken & verantwoordelijkheden	6
Aansturing: directie.....	6
Uitvoering: module-managers	7
Controle en verantwoording.....	7
BIJLAGE: De 10 bestuurlijke principes voor informatiebeveiliging	8
De 10 principes voor informatiebeveiliging	9

INLEIDING

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2020 t/m 2023. Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau (informatiebeveiligingsplan) en werkinstructies (gedragsregels) op operationeel niveau.

Vanaf 2020 is de Baseline Informatiebeveiliging Overheid (BIO) leidend voor gemeenten en daarmee ook voor de MGR sociaal domein Centraal Gelderland (MGR SDCG). De MGR SDCG voert ten behoeve van de aangesloten gemeenten in mandaat of delegatie taken uit. In haar strategische beleid committeert zij zich aan het beleid van de gemeenten. Om haar rol en taken goed en professioneel te vervullen is informatieveiligheid een randvoorwaarde. Dat is niet alleen een technische vraag, maar ook een bestuurlijke.

Met dit 'Strategisch Informatiebeveiligingsbeleid 2020-2023' zet de MGR SDCG een belangrijke stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te verwezenlijken. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG.

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 MGR SDCG 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 bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

De MGR SDCG zet in op een passend niveau van informatieveiligheid in de organisatie. Een betrouwbare¹ informatievoorziening is noodzakelijk voor het goed functioneren van de MGR en de aangesloten gemeenten en de basis voor het beschermen van rechten van burgers en bedrijven.

STRATEGISCH BELEID

DOEL

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatiebeveiligingsbeleid voor de jaren 2020 t/m 2023'. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan (IBP).

ONTWIKKELINGEN

De ontwikkelingen die van belang zijn voor het formuleren van het informatiebeveiligingsbeleid zijn de volgende:

DE BIO

¹ Met betrouwbaarheid wordt bedoeld: beschikbaarheid (continuïteit van de bedrijfsvoering), integriteit (juistheid, volledigheid) en vertrouwelijkheid (geautoriseerd gebruik) van gegevens en informatie.

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 modulemanagers 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.

DE 10 PRINCIPES VOOR INFORMATIEBEVEILIGING (ZIE BIJLAGE)

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

1. De directie bevordert een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging heeft 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. De directie controleert en evalueert.

De principes gaan vooral over de rol van de directie bij het borgen van informatiebeveiliging in de organisatie. Deze principes ondersteunen de directie bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de MGR SDCG én voor de aangesloten gemeenten. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuursafdeling.

DREIGINGSBEELD INFORMATIEBEVEILIGING NEDERLANDSE GEMEENTEN

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten² geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

INFORMATIE UIT INCIDENTEN EN INBREUKEN OP DE BEVEILIGING

De MGR SDCG kent naast het hierboven genoemde dreigingsbeeld natuurlijk 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.

STANDAARDEN INFORMATIEBEVEILIGING

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen.

Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek in 2018 de Baseline Informatiebeveiliging Overheid (BIO)

² <https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2019-2020/>

uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. Ook zullen praktische operationele handreikingen worden uitgebracht, zoals een handleiding voor het uitvoeren van een risicoanalyse voor het opstellen van een beveiligingsplan.

De inhoud en structuur van deze nota zijn afgestemd op die van de ISO en de BIO. Ook het Informatiebeveiligingsplan zal deze structuur volgen.

PLAATS VAN HET STRATEGISCH BELEID

Het strategisch beleid 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.

Deze nota beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven 'Informatiebeveiligingsplan MGR SDCG'.

SCOPE INFORMATIEBEVEILIGING

De scope van dit beleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van de MGR SDCG en externe partijen, 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. Indien voor bepaalde kerntaken op grond van wet- en regelgeving ook nog specifieke (aanvullende) beveiligingseisen gelden, worden deze in aanvullende documenten geformuleerd.

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

UITGANGSPUNTEN

De directie en het module-management 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 MGR SDCG heeft, de risico's die de MGR SDCG 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 MGR SDCG. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de MGR SDCG en de relevante landelijke en Europese wet- en regelgeving.

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 burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

BELANGRIJKSTE UITGANGSPUNTEN

De belangrijkste uitgangspunten van het beleid zijn:

- Alle informatie en informatiesystemen zijn van belang voor de MGR SDCG, bepaalde informatie is van vitaal en kritiek belang. De directie 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 MGR SDCG 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, organisatie brede 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 MGR SDCG 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.

INVULLING VAN DE UITGANGSPUNTEN

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het DB stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- De directie stelt jaarlijks het informatiebeveiligingsplan vast.
- De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- De directie is verantwoordelijk voor het vragen om informatie bij de module-managers en ziet erop toe dat de module-managers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO), of degene die deze rol binnen of voor de MGR SDCG vervult, 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 auditplannen.
- De module-managers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de MGR SDCG en het behalen van de doelen die zijn gesteld.
- Alle medewerkers van de MGR SDCG worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Module-managers dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende medewerkers de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Module-managers voeren quickscans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

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 directie, gebaseerd op:
 - de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA) van aangesloten gemeenten en ketenpartners;
 - het dreigingsbeeld gemeenten van de IBD;
 - de door de module-managers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

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, security officers) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

AANSTURING: DIRECTIE

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een module-manager. De directie zorgt dat de module-managers zich verantwoorden over de beveiliging van de informatie die onder hen berust. De directie zorgt dat het DB gevraagd en ongevraagd geïnformeerd wordt over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering.

De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO of degene die binnen of voor de MGR SDCG deze rol vervult. De directie autoriseert de benodigde procedures

en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de MGR SDCG gezien als een integraal onderdeel van risicomanagement.

UITVOERING: MODULE-MANAGERS

Informatiebeveiliging valt onder de verantwoordelijkheden van alle module-managers. 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. Module-managers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de modules over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in het MT.

Taken van de module-managers in het kader van informatiebeveiliging zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het binnen de eigen module 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.

CONTROLE EN VERANTWOORDING

Dit Strategisch Beleid is een verantwoordelijkheid van de directie van de MGR SDCG. De directie 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 directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan het DB. De directie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

De aangesloten gemeenten verantwoorden zich over informatiebeveiliging middels de ENSIA-systematiek. Zij wijzen jaarlijks een ENSIA-coördinator aan en deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de MGR SDCG. De directie en module-managers leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over de informatiebeveiliging van de MGR SDCG komt in het jaarverslag tot uitdrukking. Daarmee geeft de directie aan in hoeverre de MGR SDCG voldoet aan de afspraken die gemaakt zijn voor de Informatiebeveiliging. Ook worden de eventuele verbetermaatregelen vermeld die de MGR SDCG gaat treffen. De ingevulde zelfevaluatievragenlijst (GAP-analyse BIO) vormt de basis voor het opstellen van de paragraaf Informatiebeveiliging in het jaarverslag.

Middels deze verantwoording wordt het bestuur van MGR SDCG geïnformeerd.

Vastgesteld op : 28 oktober 2019 door het DB van de MGR SDCG

BIJLAGE: DE 10 BESTUURLIJKE PRINCIPES VOOR INFORMATIEBEVEILIGING

BEHORENDE BIJ DE BASELINE INFORMATIEBEVEILIGING OVERHEID (BIO)

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 medeoverheden. Door informatie te delen kunnen gemeenten onder andere hun dienstverlening beter organiseren, de veiligheid van inwoners 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 verantwoordelijkheid¹³ hebben om de gegevens van hun inwoners 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 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.

RISICOMANAGEMENT IS DE BASIS

De bestuurder is verantwoordelijk voor een veilige informatievoorziening. Het is daarom aan de bestuurder om de risicobereidheid te bepalen en daarmee ook te controleren of de maatregelen binnen de organisatie de risico's terugbrengen tot een voor de bestuurder acceptabel niveau. Overschrijding van dat niveau vereist expliciete besluitvorming. Risicomanagement staat daarmee 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.

NORMEN EN REGELS

De ontwikkelingen in de informatietechnologie gaan steeds sneller en de wetgeving rondom de bescherming van persoonsgegevens is aangescherpt. 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

³ O.a. de Algemene wet gegevensbescherming, Wet BRP, PUN, DigiD, BAG, BGT en SUWI

zogenaamde Baseline Informatiebeveiliging Overheid (BIO) met daarin de regels waaraan alle overheidslagen dienen te voldoen. Door middel van een zelfevaluatie (ENSIA) verantwoordende gemeenten zich over deze norm.

BESTUURLIJKE AANVULLING OP DE NORMEN EN REGELS

In aanvulling op de baseline bevat dit document de bijbehorende principes voor bestuurders. 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 de bestuurlijke aanvulling op de baseline en helpt 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.

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 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 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 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 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 risicomanagement 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, doelstellingen 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 INGEALCULEERD

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

Risicomangement 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

Risicomangement 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 risicomangement binnen mijn organisatie op effectiviteit en efficiency te (laten) controleren. Naast managementrapportages zijn (externe) controles 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 risicomangement 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.