BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 447

24 februari 2025

Officiële uitgave van de gemeenschappelijke regeling Veiligheidsregio Noord-Holland Noord

Strategisch Informatiebeveiligingsbeleid VRNHN

Wijzigingshistorie

Versie	Datum	Door	Opmerkingen
1.0	09-06-2017	Ciso	Brondocument van de IBD aangepast voor gebruik binnen VRNHN
2.0	04-10-2024	Ciso	Aangepast aan de Algemene Verordening Gegevensbescherming (AVG), Baseline Informatiebeveiliging Overheid (BIO) en de NEN7510:2017

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid en vervangt het in 2017 vastgestelde 'Informatiebeveiligingsbeleid VRNHN versie 1.0'.
Dit beleid is richtinggevend en kaderstellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en richtlijnen op tactisch en operationeel niveau.[1]
Dit beleid hangt samen met de wettelijke kaders die aan informatieverwerking binnen specifieke onderdelen zijn gesteld, zoals de Algemene Verordening Gegevensbescherming (AVG), de NIS2-richtlijn, het besluit elektronische gegevensverwerking door zorgaanbieders en de wet elektronische gegevensuitwisseling in de zorg. Voor bepaalde taken gelden op grond van deze wet- en regelgeving specifieke beveiligingseisen. Deze zijn in aanvullende documenten geformuleerd.

Het strategisch informatiebeveiligingsbeleid is in een tactisch informatiebeveiligingsbeleid in 18 hoofdstukken nader uitgewerkt en zijn beveiligingseisen en -maatregelen opgenomen, die voor VRNHN voor alle processen en systemen gelden en die in de pas lopen met de hoofdstukken in de BIO en de NEN7510. Een onderdeel van dit strategisch document is ook, een beheerstructuur (ISMS) voor informatiebeveiliging,

Dit document is tevens gericht op alle overige belanghebbenden van VRNHN, zoals burgers, bedrijven en leveranciers van goederen en diensten om op die manier duidelijk te maken wat de basisprincipes en -eisen zijn ten aanzien van informatiebeveiliging.

Met dit 'Strategisch Informatiebeveiligingsbeleid VRNHN zet VRNHN een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen VRNHN te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. Om dat de bewerkstelligen zijn de 10 bestuurlijke principes voor informatiebeveiliging zoals uitgewerkt door de Vereniging van Nederlandse Gemeenten (VNG) van belang (zie bijlage A).

Wetgeving is aan verandering onderhevig en dat kan inhouden dat er wetswijzigingen zijn die tot gevolg hebben dat het VRNHN informatiebeveiligingsbeleid moet veranderen.

2. Over dit document

Documentinformatie
Dit document:

1) Zie structuur Informatiebeveiligingsbeleid VRNHN

- is vastgesteld door het Dagelijks Bestuur Veiligheidsregio NHN;
- is opgesteld door Expert Informatieveiligheid/CISO VRNHN;
- is opgesteld op basis van de normen van NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO), de NEN7510: 2017 Informatiebeveiliging in de zorg en de Algemene Verordening Gegevensbescherming (AVG);
- geeft algemene beleidsuitgangspunten over informatiebeveiliging. Deze uitgangspunten hebben een sterk normerend karakter waarbinnen, middels risicomanagement keuzes gemaakt kunnen worden.

Doel
De hoofddoelstelling van informatiebeveiligingsbeleid is het richting geven aan het inrichten van informatiebeveiliging binnen VRNHN.
Dit informatiebeveiligingsbeleid is erop gericht de beschikbaarheid, de integriteit en de vertrouwelijkheid van de (geautomatiseerde) gegevensverwerking binnen VRNHN en de (geautomatiseerde) uitwisseling van gegevens tussen VRNHN en derden te waarborgen.
Dit informatiebeveiligingsbeleid geeft algemene beleidsuitgangspunten over informatiebeveiliging van VRNHN. Geformuleerde beleidsdocumenten hebben als doel te beschrijven wat directie en management van VRNHN belangrijk vinden in het realiseren van de organisatiedoelen en het passend beheersen van informatiebeveiligingsrisico's.
Informatiebeveiligingsbeleid is tevens de basis voor het inrichten van een procesgerichte benadering van informatiebeveiliging, ook wel het Information Security Management System (ISMS) genaamd. Dit proces hanteert een Plan Do Check Act Cyclus (PDCA)

Voor wie
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?
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.

Informatiebeveiliging en daarmee ook dit informatiebeveiligingsbeleid geldt voor alle medewerkers (ook uitzend- en inhuurkrachten) van VRNHN. Kortom, allen die te maken hebben met het verwerken van informatie. Indien bij samenwerking met derden sprake is van uitwisseling van informatie, waarvan VRNHN eigenaar of beheerder is, dient informatiebeveiliging een onderdeel te zijn in de samenwerkingsovereenkomst en mag deze niet strijdig zijn met het informatiebeveiligingsbeleid van VRNHN en overige van toepassing zijnde wet- en regelgeving.

Plaats van het strategisch beleid
Het strategisch informatiebeveiligingsbeleid wordt gebruikt als basis voor tactische- en operationele beleidsplannen en geeft daarmee richting voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau.

3. Algemeen

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 en vertrouwelijkheid van persoonsgegevens en andere informatie.
- beschikbaarheid / continuïteit: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- exclusiviteit / vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
- integriteit / betrouwbaarheid: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

Het informatiebeveiligingsbeleid geldt voor alle processen van VRNHN 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 alle medewerkers, burgers en externe relaties.

Waarom Informatiebeveiliging?
Informatie is één van de belangrijkste bedrijfsmiddelen van VRNHN. Toegankelijke en betrouwbare informatie is essentieel voor VRNHN, die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt aan burgers en aan de burgemeesters van de inliggende gemeenten (het bestuur) en die met de beschikbare middelen maximale resultaten wil behalen.
Er zijn nog meer overwegingen die de doelen van informatiebeveiliging vormgeven, waaronder:

a. aan wettelijke verplichtingen voldoen, die zijn vervat in de toepasselijke wet- en regelgeving (b.v. Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en het Besluit elektronische gegevensverwerking door zorgaanbieders);
b. b) ethische verplichtingen[2] met betrekking tot gezondheidsinformatie; D.w.z. In de zorg vastgestelde professionele normen en ethiek handhaven (voor zover informatiebeveiliging de vertrouwelijkheid en integriteit van gezondheidsinformatie handhaaft;
c. exploitatiekosten verlagen door gebruik van technologie op een veilige, beveiligde en goed geregelde wijze mogelijk te maken, die activiteiten ondersteunt maar deze niet beperkt;
d. Interoperabiliteit tussen informatiesystemen mogelijk maken.

De bescherming van waardevolle informatie is hierbij belangrijk. Hoe waardevoller de informatie is, hoe meer maatregelen er getroffen moeten worden.

Reikwijdte en afbakening van informatiebeveiliging
Zoals eerder opgemerkt is Informatiebeveiliging meer dan ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, spraak, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, beeldscherm et cetera) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook om mensen en processen. Studies[3] laten zien dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral door menselijk handelen en een tekort schietende organisatie.

Organisatorische aspecten

- Toetsing op IB-beleid is onderdeel van de toets voor projecten met een ICT-component en onderdeel van de project start en eind architectuur (PSA en PEA[4]).
- ICT projecten met een hoog risicoprofiel dienen ter beoordeling en eventuele met input van de afdeling ICT gerealiseerd te worden. Toetsing op architectuur en informatiebeveiliging is hier onderdeel van.
- Projecten worden voorzien van een advies op informatiebeveiliging.
- In het programma van eisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen worden relevante beveiligingseisen opgenomen.

Risicomanagement is de basis
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 de directie is om te bepalen hoeveel of welk risico acceptabel is.
En de risico's zijn talrijk: privacyschendingen door een datalek, imagoschade schade door het uitlekken van vertrouwelijke informatie, fysieke schade door storingen in systemen, belemmeringen in incidentbestrijding door het niet op het juiste moment beschikbaar zijn van de juiste informatie, etc. Risicomanagement geeft ruimte tot interpretatie.
Het is dan ook noodzakelijk om te controleren of de maatregelen die genomen worden de risico's terugbrengen tot een acceptabel niveau. Overschrijding van dat niveau vereist expliciete besluitvorming.

Relatie met privacy
Informatiebeveiliging en privacy zijn termen die soms door elkaar worden gebruikt en vaak hand in hand gaan. Het zijn twee verschillende begrippen, echter met een gemeenschappelijk raakvlak. Informatiebeveiliging heeft namelijk een bredere scope dan de bescherming van enkel persoonsgegevens.

2) Informatie over ethische verplichtingen met betrekking tot gezondheidsinformatie is veelal beschikbaar in gedragscode van een gezondheidsorganisatie. Deze ethische verplichtingen kunnen in bepaalde omstandigheden ook gevolgen hebben voor informatiebeveiliging
3) INSIDER THREAT IN IT (de factor mens beschouwd), Erasmus Universiteit Rotterdam (EURAC) Drs. A.J.A.M. Spee, Colwill C, Human factors in information security: The insider threat e Who can you trust these days?, Inform. Secur. Tech. Rep. (2010), doi:10.1016/j.istr.2010.04.004
4) Dit zijn Prince2 termen, zie hiervoor de projectmanagement methodiek Prince2

Informatiebeveiliging draait om de bescherming van alle gevoelige informatie(systemen) tegen aantasting van integriteit, vertrouwelijkheid en beschikbaarheid. Bijvoorbeeld ook de beveiliging van politiek-gevoelige of financiële gegevens. Een informatiebeveiligingsincident hoeft daarom niet altijd een datalek te betreffen. Dat is enkel het geval wanneer er persoonsgegevens betrokken zijn. Een adequate informatiebeveiliging (van persoonsgegevens) is wettelijk verplicht voor VRNHN om te kunnen voldoen aan de Algemene Verordening Gegevensbescherming (AVG), de Europese privacyverordening. Artikel 32 van de AVG schrijft voor dat:

"*Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen*".

Informatiebeveiliging maakt daarmee een onderdeel uit van de AVG. De AVG laat de inschatting van risico's en het bepalen van de benodigde maatregelen over aan de verwerkingsverantwoordelijke (VRNHN). Normenkaders als de BIO helpen VRNHN om de risico's goed in te schatten en de benodigde maatregelen te treffen. In de praktijk betekent dit dat de CISO en de Functionaris Gegevensbescherming (FG) nauw samenwerken. Hoe VRNHN omgaat met privacy en de AVG is beschreven in het 'Strategisch privacybeleid VRNHN'.

Taken, verantwoordelijkheden en bevoegdheden

Wie	**Relevantie voor IB-beleid**
Directie VRNHN	Integrale verantwoordelijkheid
Management Teams (MT's)	Kaderstelling en implementatie
Lijnmanagement (direct leidinggevende)	Sturing op Informatieveiligheid en controle op naleving
Medewerkers	Gedrag en naleving
Proceseigenaren	Classificatie: bepalen van beschermingseisen van informatie, het implementeren en beheersen van IB maatregelen.
Informatiebeveiligingsfunctionaris(sen)	Coördinatie van en toezicht informatiebeveiliging
HR-team	Arbeidsvoorwaardelijke zaken v.w.b. de onderdelen binnen de IB norm "Veilig personeel"
Managing Agent, gebouwbeheerders, BSP	Fysieke toegangsbeveiliging
ICT-team	Logische/technisch beveiliging ICT bedrijfsmiddelen
Auditors	Onafhankelijke toetsing
Leveranciers en ketenpartners	Compliance (werkt in overeenstemming met de geldende wet- en regelgeving)

4. Strategisch Informatiebeveiligingsbeleid Veiligheidsregio Noord-Holland Noord (VRNHN)

VRNHN is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het informatiebeveiligingsbeleid. Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals (niet uitputtend): de AVG, de Woo (Informatie over security en privacy aangelegenheden vallen hier ook onder), de Wbni[5] maar ook de archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Overheid (BIO) en de NEN7510.
- De Ministerraad voor de Rijksoverheid stelt het BIO normenkader vast, waarbij er ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.
- De NEN7510 is wettelijk verplicht In het kader van de 'Besluit elektronische gegevensverwerking door zorgaanbieders'.

5) De Wet beveiliging netwerk- en informatiesystemen (wordt vervangen door de NIS-2 richtlijn

De directie en het management spelen een cruciale rol bij het uitvoeren van dit informatiebeveiligingsbeleid. Zo maakt het management een inschatting van het belang dat de verschillende delen van de informatievoorziening voor VRNHN hebben, de risico's die VRNHN 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 VRNHN-management geeft 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 VRNHN. 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 VRNHN en de relevante landelijke en Europese wet- en regelgeving.

De strategische doelen van het informatiebeveiligingsbeleid zijn:
- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen[6].
- 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.

De belangrijkst uitgangspunten gelden en zijn ontleend aan de Code voor Informatiebeveiliging (NEN/ISO 27001:2023, 27002:2022), de BIO en de NEN7510:2017
- Alle informatie en informatiesystemen zijn van belang voor VRNHN, bepaalde informatie is van kritiek belang. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn)management, met de directie als eindverantwoordelijke. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door VRNHN hebben een interne verantwoordelijke 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 verantwoordelijke 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 informatiebeveiligingsplannen het fundament onder een betrouwbare informatievoorziening. In een informatiebeveiligingsplan wordt de betrouwbaarheid[7] van de informatievoorziening benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande of herziene risicoanalyses.
- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het management systeem van informatiebeveiliging.
- VRNHN stelt mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze 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 Dagelijks Bestuur stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- De directie beoordeelt met geplande tussenpozen het managementsysteem (ISMS) voor informatiebeveiliging om de continue geschiktheid, adequaatheid en doeltreffendheid te bewerkstelligen.

6) Informatie en andere bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten
7) Het gezamenlijk niveau van Beschikbaarheid, Integriteit en vertrouwelijkheid

- De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerpspecifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- De directie 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, informatiesystemen en procesautomatiseringsystemen 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.
- Tijdens MT VR overleggen dient er aandacht te zijn voor de informatiebeveiliging. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- De afdelingsmanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De afdelingsmanagers zijn verantwoordelijk voor het oefenen met informatiebeveiligings-incidenten en bedrijfscontinuïteit.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Afdelingsmanagers dienen erop toe te zien dat de controle op het verwerken of kennisnemen van (persoons)gegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende de juiste (persoons)gegevens op basis van need-to-know ingezien en/of verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Afdelingsmanagers voeren quickscans informatiebeveiliging uit op basis van de BIO of de NEN7510 om deze risicoafwegingen te kunnen maken.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Informatiebeveiliging maakt deel uit van de beoordelingssystematiek en wordt besproken tussen de manager en de medewerker.
- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.

Aansturing: directieteam
De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingsmanager. De directie zorgt dat de afdelingsmanagers zich verantwoorden over de beveiliging van de informatie die onder hen berust.
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. Het onderwerp informatiebeveiliging wordt binnen VRNHN gezien als een integraal onderdeel van risicomanagement.

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 directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten en risico's. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp informatiebeveiliging te bespreken in het Managementteam overleg.
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.
- Het (laten) uitvoeren van risicoanalyses en DPIA's voor de processen waar zij verantwoordelijk voor zijn.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

Dit IB-beleid treedt in werking na vaststelling door het dagelijks bestuur Veiligheidsregio NHN.

Aldus vastgesteld door het dagelijks bestuur Veiligheidsregio NHN op 6 februari 2025,

Voorzitter
A.M.C.G. Schouten

Secretaris
K. Taneja

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 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 VRNHN 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 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 [8] 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) 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 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 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.

8) Titulair bestuurder