gemeente Tubbergen

GEMEENTEBLAD

Officiële uitgave van de gemeente Tubbergen

Nr. 281850

3 november 2020

Besluit van het college van burgemeester en wethouders van de gemeente Tubbergen houdende regels omtrent Strategisch Informatieveiligheidsbeleid 2020

Definitief besluit college

1. Het 'Strategisch Informatieveiligheidsbeleid 2020' vast te stellen.
2. Het op 21 februari 2017 in werking getreden Informatieveiligheidsbeleid in te trekken, en het 'Strategisch Informatieveiligheidsbeleid 2020' te publiceren.

1. Inleiding

In dit document is het strategisch informatieveiligheidsbeleid beschreven van de gemeenten Dinkelland en Tubbergen alsmede de bedrijfsvoeringorganisatie Noaberkracht Dinkelland Tubbergen. Omwille van de leesbaarheid van dit informatiebeveiligingsbeleid zijn de gemeentenamen en de naam van de bedrijfsvoeringorganisatie samengevoegd tot Noaberkracht. In alle gevallen worden de gemeenten Dinkelland en Tubbergen en de bedrijfsvoeringorganisatie Noaberkracht Dinkelland Tubbergen bedoeld. Met dit beleid zetten de organisaties een volgende stap om de beveiliging van persoonsgegevens en andere informatie 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 Informatieveiligheid Overheid (BIO).
In de komende paragrafen wordt de kern van het strategisch beleid uiteengezet. In het jaarlijks uit te brengen organisatie brede informatieveiligheidsplan (vastgesteld door de directie) worden vervolgens tactische en operationele aspecten van de informatieveiligheid verder uitgewerkt en geconcretiseerd. Dit wordt o.a. gedaan op basis van input van de teamcoaches, de CISO, het dreigingsbeeld van de IBD en de uitkomsten van ENSIA.
Dit strategisch beleid is gebaseerd op het operationele kennisproduct 'Strategisch Informatieveiligheidsbeleid' van de informatiebeveiligingsdienst (IBD) voor gemeenten.

1.1 Definitie

Onder informatieveiligheid 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 informatie, waaronder persoonsgegevens.
Het informatieveiligheidsbeleid geldt voor alle processen van de gemeente 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, burgers, gasten, bezoekers en externe relaties.

2. Ambitie en visie op het gebied van informatieveiligheid

De dreigingen met betrekking tot informatiebeveiliging zijn de afgelopen jaren flink toegenomen. Zowel de kans van optreden alsmede de impact van incidenten zijn dusdanig dat een organisatie zijn informatiebeveiliging op orde moet hebben, wil de organisatie geen onacceptabele risico's lopen. Belangrijke vragen in dit kader zijn dan ook: "Hoe staat het met de informatiebeveiliging?", en, "Wat moet er nog gebeuren?". Het gewenste niveau is daarom sterk afhankelijk van de ambities van de organisatie.
De visie van Noaberkracht is om door te ontwikkelen naar een wendbare, toekomstbestendige organisatie die van betekenis is voor de samenleving en meebeweegt met veranderingen in de samenleving. Om met de organisatie mee te groeien (of andersom) dient er de komende jaren een stevig fundament onder informatieveiligheid te worden gebouwd. Het streven is daarom dat beheersingsmaatregelen nog sterker op basis van risicomanagement worden bepaald, worden gedocumenteerd en op gestructureerde en geformaliseerde wijze worden uitgevoerd. De uitvoering van informatieveiligheid is in deze situatie aantoonbaar en wordt getoetst.

3. Uitgangspunten

3.1 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatieveiligheidsbeleid zijn de volgende:

De BIO
De BIO (Baseline Informatieveiligheid Overheid) is het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement dan de oude baseline. 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 is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

De 10 principes voor informatieveiligheid
De 10 principes voor informatieveiligheid 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. Informatieveiligheid is van iedereen.
3. Informatieveiligheid is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatieveiligheid behoeft ook aandacht in (keten)samenwerking.
6. Informatieveiligheid is een proces.
7. Informatieveiligheid kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatieveiligheid in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatieveiligheid nadrukkelijk gewenst op de bestuurstafel.

Dreigingsbeeld Informatieveiligheid Nederlandse Gemeenten
Het Dreigingsbeeld Informatieveiligheid Nederlandse Gemeenten 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 informatieveiligheid.
Informatie uit incidenten en inbreuken op de beveiliging
Noaberkracht 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.

3.2 Standaarden informatieveiligheid
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 informatieveiligheidsbeleid heeft een interbestuurlijke werkgroep in 2018 de Baseline Informatieveiligheid Overheid (BIO) uitgebracht. Deze BIO bestaat uit een baseline met verschillende niveaus. Ook zijn praktische operationele handreikingen uitgebracht, zoals een handleiding voor het uitvoeren van een risicoanalyse en voor het opstellen van een beveiligingsplan.
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 informatieveiligheid op tactisch en operationeel niveau. Dit beleid beschrijft op strategisch niveau het informatieveiligheidsbeleid. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen.

3.3 Scope informatieveiligheid
De scope van dit beleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van de organisaties 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 (zowel analoog als digitaal).
Dit strategisch Informatieveiligheidsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de BRP, PNIK en SUWI . Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties). Deze worden in aanvullende documenten geformuleerd.

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

3.4 Beleid

Het bestuur, de directie en de teamcoaches spelen een cruciale rol bij het uitvoeren van dit strategische informatieveiligheidsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de organisaties hebben, de risico's die worden gelopen en welke van deze risico's onacceptabel hoog zijn.
Op basis hiervan zet het management dit beleid voor informatieveiligheid op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.
Het gehele management geeft een duidelijke richting aan informatieveiligheid en demonstreert dat zij informatieveiligheid ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatieveiligheidsbeleid van en voor de hele gemeente. Het informatieveiligheidsbeleid is in lijn met het algemene beleid van Noaberkracht en de relevante landelijke en Europese wet- en regelgeving.

Doelen
De strategische doelen van het informatieveiligheidsbeleid zijn:

- Het managen van de informatieveiligheid.
- 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.

Uitgangspunten
- Alle informatie en informatiesystemen zijn van belang voor de organisaties, echter is bepaalde informatie van vitaal en kritiek belang.
- Het college van B&W is eindverantwoordelijke voor de informatieveiligheid.
- De uitvoering van de informatieveiligheid is een verantwoordelijkheid van de teamcoaches. Alle informatiebronnen en -systemen die gebruikt worden 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 informatieveiligheidsbeleid vormt samen met het informatieveiligheidsplan het fundament onder een betrouwbare informatievoorziening. In het informatieveiligheidsplan wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses.
- Informatieveiligheid is een continu verbeterproces. 'Plan, Do, Check en Act' vormen samen het managementsysteem van informatieveiligheid.
- Noaberkracht 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.

Praktische invulling
Aan de uitgangspunten wordt op volgende wijze invulling gegeven:

- Het college van B&W en het bestuur van Noaberkracht stellen als eindverantwoordelijke het strategisch informatieveiligheidsbeleid vast.
- De directie stelt jaarlijks het informatieveiligheidsplan 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 teamcoaches en ziet erop toe dat de deze 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.
- De onderwerpen, die als risicovol worden gezien, moeten worden opgenomen in de auditplannen.
- De teamcoaches zijn verantwoordelijk voor de uitvoering van de informatieveiligheid voor de processen waarvoor zij verantwoordelijk zijn.
- Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, BAG, BGT) en toekomstige basisregistraties belangrijk zijn in het kader van informatieveiligheid, krijgen zij niet meer of minder voorrang dan andere (primaire) processen. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk het behalen van de doelen die zijn gesteld.
- Alle medewerkers van de organisaties worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Teamcoaches dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat medewerkers de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Teamcoaches voeren risicoanalyses uit op basis van de BIO om afwegingen te kunnen maken.

Randvoorwaarden
Belangrijke randvoorwaarden zijn:

- De informatieveiligheid maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatieveiligheid en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een informatieveiligheidsplan opgesteld onder leiding van de CISO, gebaseerd op:
  - de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
  - het dreigingsbeeld gemeenten van de IBD;
  - De door de afdelingsmanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

4. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatieveiligheid 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, beveiligingsbeheerders) 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.

4.1 Aansturing: directie
De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teamcoach. De directie zorgt dat de teamcoaches zich verantwoorden over de beveiliging van de informatie die onder hen berust. De directie zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatieveiligheid een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.
De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directie draagt zorg voor het uitwerken van tactische informatieveiligheidsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatieveiligheid wordt gezien als een integraal onderdeel van risicomanagement.

4.2 Uitvoering: teamcoaches
Informatieveiligheid valt onder de verantwoordelijkheden van alle teamcoaches. 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 één eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn.

Teamcoaches rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatieveiligheid activiteiten. Taken van de teamcoaches in het kader van informatieveiligheid zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het binnen het eigen organisatieonderdeel 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.

4.3 Controle en verantwoording

Dit strategisch beleid is een verantwoordelijkheid van het bestuur van de organisaties. De bestuurders en directeuren zullen richting en sturing geven aan het onderwerp informatieveiligheid door het geven van voorbeeldgedrag en het vragen om informatie.
De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatieveiligheid aan respectievelijke portefeuillehouders. 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.

Datum college 12-05-2020