GBTwente

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 51

2 januari 2023

Officiële uitgave van de gemeenschappelijke regeling Gemeenschappelijke Regeling Gemeentelijk Belastingkantoor Twente

AANWIJZINGS- EN BENOEMINGSBESLUIT

Het dagelijks bestuur van de gemeenschappelijke regeling Gemeentelijk Belastingkantoor Twente,

Benoemt:

1. de heer R.H.M. Weusthuis

als Chief Information Security Officer (CISO) voor het Gemeentelijk Belastingkantoor Twente en

1. de heer J.A. Litjens en
2. mevrouw K. van der Ent

als plaatsvervangend Chief Information Security Officer voor het Gemeentelijk Belastingkantoor Twente.

Aldus getekend, te Hengelo, d.d. 14 oktober 2022
Ondertekening
Secretaris
.....
Voorzitter
.....
De heer J.A.G. Cloosterman Mevrouw E. Zinkweg-Ankone

AANVAARDING

1. De heer R.H.M. Weusthuis aanvaart hiermee zijn benoeming als Chief Information Security Officer (CISO) van het Gemeentelijk Belastingkantoor Twente.

Aldus getekend, te Hengelo d.d. 14 oktober 2022

.....

De heer R.H.M. Weusthuis
Stafadviseur IT

2. De heer J.A. Litjens aanvaart hiermee zijn benoeming als plaatsvervangend Chief Information Security Officer van het Gemeentelijk Belastingkantoor Twente.

Aldus getekend, te Hengelo d.d. 14 oktober 2022

.....

De heer J.A. Litjens
Functionaris Gegevensbescherming

3. Mevrouw K. van der Ent aanvaart hiermee haar benoeming als plaatsvervangend Chief Information Security Officer van het Gemeentelijk Belastingkantoor Twente.

Aldus getekend, te Hengelo d.d. 14 oktober 2022

.....

Mevrouw mr. K. van der Ent
Strategisch stafadviseur

Functiebeschrijving Chief Information Security Officer (CISO)

1. Doel van de functie

Doel van de functie is het, op basis van de Baseline Informatiebeveiliging Overheid (BIO), zorgdragen voor een samenhangend pakket van maatregelen ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen GBTwente.
Risicoanalyse, oog voor de bedrijfsvoering en in achtneming van de wettelijke voorschriften zijn daarbij sleutelbegrippen.

2. Plaats van de functie binnen de organisatie

De functie vindt plaats in combinatie met de functie stafadviseur IT en is zowel technisch als organisatorisch gericht. De organisatorische kant richt zich meer op het geheel en de samenhang van beveiligingsmaatregelen, de beleidskant. De technische kant houdt zich bezig met één of meer technische beveiligingsonderwerpen; de uitvoeringskant.
De functie van CISO brengt met zich mee dat er rechtstreeks aan het dagelijks bestuur wordt gerapporteerd en geadviseerd.

3. Taken, verantwoordelijkheden en bevoegdheden

De resultaatgebieden betreffen:
• Beleid en coördinatie
• Controle en registratie
• Communicatie en voorlichting
• Advies en rapportage

Taken en verantwoordelijkheden
1. Verantwoordelijk voor het opstellen, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid en de daaruit voortvloeiende informatiebeveiligings-plannen.
2. Optreden als informatiebeveiligingsadviseur (voor het management) bij nieuwe ICT-voorzieningen en bij ingrijpende veranderingen in de ICT-infrastructuur.
3. Adviseren van het bestuur en (lijn)management bij de uitwerking van het informatie-beveiligingsbeleid in informatiebeveiligingsplannen voor hun verantwoordelijkheidsgebieden, en bij de implementatie van deze plannen.
4. Initiëren of laten uitvoeren van periodieke beveiligingsaudits, risico-, afhankelijkheids- en kwetsbaarheidsanalyses.
5. Coördineren en adviseren bij beveiligingsincidenten en zo nodig optreden bij calamiteiten.
6. Op de hoogte blijven van ontwikkelingen op het gebied van informatiebeveiliging en zo nodig met voorstellen komen voor aanvullingen of verbeteringen van producten, methodieken of werkwijzen met betrekking tot de informatiebeveiliging.
7. Opzetten en initiëren van (periodieke) informatiebeveiligingsbewustzijn programma's en adviseren over voorlichting en training van gebruikers in het correct omgaan met informatie(systemen).
8. Te allen tijde een open deur dienen te hebben voor de gebruikersorganisatie indien deze, buiten de hiërarchie om, een beveiligingsincident wil melden. De CISO is het formele, en bij iedereen in de organisatie bekende, aanspreekpunt voor 'informatie-beveiligingszaken'.
9. Projecten leiden die als doel hebben beveiligingsmaatregelen te implementeren of de kwaliteit van de beveiliging op langere termijn te handhaven en waar nodig te verbeteren.
10. Controleren van de werking en naleving van het informatiebeveiligingsbeleid en daaruit voortvloeiende maatregelen.
11. Periodiek rapporteren van beveiligingsincidenten en de afhandeling daarvan aan het bestuur en (lijn)management.
12. GBTwente vertegenwoordigen in externe overleggremia.
13. Rapportages op het gebied van de beveiliging (laten) beoordelen.

Bevoegdheden
De belangrijkste bevoegdheid is om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen (laten) doen en zo nodig zaken voor te schrijven. Bij informatiebeveiliging is het echter noodzakelijk om centraal keuzes te maken.
Bij (grote) beveiligingsincidenten/-risico's heeft de CISO de bevoegdheid, zo nodig, direct in te grijpen (met verantwoording achteraf richting het management) .
Daarnaast heeft de CISO de bevoegdheid om gevraagd en ongevraagd te mogen rapporteren en adviseren aan de directie en het dagelijks en/of algemeen bestuur van GBTwente.

4. Contacten

Zowel intern als extern
Intern moet de CISO contact onderhouden met andere Security Officers of beveiligings-functionarissen binnen GBTwente. De CISO heeft daarbij de verantwoordelijkheid dit contact te structureren in vaste en ad-hoc overlegvormen.
Verder onderhoudt de CISO intern contact met (lijn-/project-)managers, auditors, coördinatoren, de FG en collega's IT.

Extern contact is er met auditors/toezichthouders (accountant, ministerie, IBD), service providers en politie/justitie.
Extern wisselt de CISO kennis en ervaring uit met vakgenoten van andere gemeenten/gemeentelijke instellingen/samenwerkingsverbanden en met de informatiebeveiligingsdienst (IBD). In dat laatste geval kan de CISO ook VCIB en/of ACIB zijn. De rol ACIB en VCIB zijn van belang binnen het aansluit- en communicatieproces met de IBD.

Om op de hoogte te blijven van nieuwe technologische ontwikkelingen is contact met leveranciers (beurzen, lidmaatschap gebruikersgroepen van bepaalde producten) tevens van belang.

Binnen GBTwente is er naast de CISO nog een aantal functies dat zich bezighoudt met aan informatiebeveiliging, gerelateerde gebieden.

De Functionaris Gegevensbescherming (FG) en de Privacy Officer (PO)
De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Algemene Verordening Gegevensverwerking (AVG). De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. Een gemeentelijke instelling is vanaf mei 2018 verplicht een FG te hebben.

De PO houdt niet alleen toezicht op de omgang met persoonsgegevens, maar bekleedt ook een adviserende rol. De PO adviseert het personeel over privacy gerelateerde zaken en kan eveneens trainingen geven om de interne kennis over dit onderwerp te vergroten. Daarnaast kan de PO net als de FG een (ondersteunende) rol hebben bij het uitvoeren van een Data Protection Impact Assesssment (DPIA) en bij het melden van datalekken. Daarnaast kan de PO fungeren als contactpersoon voor de IBD.

Er vindt veelvuldig overleg plaats tussen de FG, de PO en de CISO. Het aspect 'vertrouwelijkheid van informatie' behoort immers ook tot het taakgebied van de CISO. Bij afwezigheid kunnen alle drie de functionarissen elkaar vervangen.

De (ICT-)auditor
De auditor voert onafhankelijk controleactiviteiten uit, veelal in nauwe samenwerking met de externe accountant. Er is afstemming nodig met betrekking tot de planning van activiteiten. De CISO wordt geïnformeerd over de uitkomsten van de controles. De auditor kan zich bij zijn/haar controles voor een deel baseren op de door de CISO uitgevoerde controles en voortgangsrapportages.

De (bedrijfs-)beveiliger, receptionist(e)
Deze functionaris is belast met de fysieke beveiliging van gebouwen en ruimten binnen een gemeentelijke instelling. Er is zeker een relatie met informatiebeveiliging, bijvoorbeeld daar waar het de beveiliging van computerruimten betreft.
In contacten met politie/justitie is het ook mogelijk dat de bedrijfsbeveiliger en de CISO dit gezamenlijk afhandelen.
In de BIO is één van de onderdelen: de fysieke beveiliging (met als doel 'het voorkomen van ongeautoriseerde toegang tot, schade aan, of verstoring van de gebouwen en informatie van de organisatie.').

Chief Information Officer, directie, (lijn-/project-)manager
Daar waar zij verantwoordelijk zijn voor ICT-beleid, respectievelijk informatiebeleid, is duidelijk dat informatiebeveiliging daarvan een onderdeel is.

Personeelsfunctionaris
Er is een relatie tussen personeelsbeleid en informatiebeveiliging, bijvoorbeeld daar waar het de selectie en het ontslag van personeel betreft. Ook bij het opstellen van gedragsregels met betrekking tot 'het veilig omgaan met informatie' is er overlap. Tenslotte kan personeelszaken een belangrijke bijdrage leveren aan informatiebeveiliging door te zorgen dat bij beoordelingsgesprekken met medewerkers expliciet beoordeeld wordt op, de wijze waarop de betreffende medewerker met zijn/haar verantwoordelijkheid ten aanzien van de beveiliging van informatie van de gemeente is omgegaan.

Stafadviseur Juridische control / strategisch adviseur
Op het gebied van informatiebeveiliging is veel wet- en regelgeving. In het uiterste geval kan het management van een organisatie aansprakelijk worden gesteld als zij onvoldoende heeft gedaan aan in-

formatiebeveiliging. Reden genoeg voor de CISO om bij het, opstellen van beleid en de implementatie van maatregelen, te toetsen of daarmee wordt voldaan aan alle geldende wet- en regelgeving.

Persvoorlichter
In geval van beveiligingsincidenten kan het raadzaam zijn dat er vooraf overleg is geweest tussen CISO en persvoorlichter, en mogelijk nog een jurist/PO/FG, over hoe daar naar buiten mee moet worden omgegaan.

De ACIB en de VCIB
Iedere gemeentelijke instelling die zich officieel aangesloten heeft bij de IBD moet een ACIB (algemeen) en een VCIB (vertrouwd) aangewezen hebben. Het rapporteren van beveiligingsincidenten behoort tot het taakgebied van de CISO. Ook zal de CISO op organisatie niveau een rol hebben in de escalatieprocedure.

De Kwaliteitscoördinator
Kwaliteitszorg richt zich op de continue verbetering van de bedrijfsprocessen teneinde de gewenste kwaliteit te kunnen leveren. Informatiebeveiliging richt zich op de vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Daarmee levert de CISO een bijdrage aan de kwaliteit van de bedrijfsvoering. Afstemming is nodig om 'de neuzen dezelfde kant op te zetten' en om dubbel werk te voorkomen.

5. Opleiding, kennis, ervaring en competenties

Opleiding, kennis en ervaring
• Minimaal HBO/Academisch werk- en denkniveau
• Kennis en ervaring op het gebied van bestuurs-/bedrijfskunde en/of informatica
• Kennis van de actuele stand van zaken en mogelijkheden van ICT (besturingssystemen, netwerken, standaarden, ontwikkel- en beheermethoden)
• Kennis en ervaring op het gebied van informatiebeveiliging en risicoanalyse methoden
• Kennis van de Baseline Informatiebeveiliging Overheid (BIO) en de ISO 27001/27002
• Kennis van specialistische beveiligingstechnieken, zoals encryptie
• Kennis en ervaring op het gebied van adviseren en organisatiekunde
• Kennis en ervaring op het gebied van gemeentelijke dienstverlening
• Kennis van technische infrastructuur samen met de business inschatting van de kwetsbaarheid
• Kennis en ervaring met projectmatig werken en projectmanagement

Competenties
Met competenties wordt bedoeld 'het in staat zijn om weloverwogen de juiste kennis, vaardigheden en houding in te zetten op het juiste moment in authentieke situaties'.
• Goede communicatieve vaardigheden, zowel mondeling als schriftelijk
• Goed kunnen samenwerken met verschillende disciplines op verschillende niveaus
• Alert, initiatiefrijk, omgevingsbewust
• Integer
• Overtuigingskracht
• Bereid tot permanente scholing

Toelichting op en nadere informatie over functiebeschrijving CISO

1. Doel

Doel van de meer technisch gerichte functie is, om met de bij de functie behorende specialistische kennis en kunde het beveiligingsrisico (dus het risico dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van informatie wordt aangetast) als gevolg van de toepassing van (nieuwe) technologieën op een aanvaardbaar niveau te brengen en te houden. Deze functie heeft een rol bij enerzijds de ontwikkeling van nieuwe projecten/systemen, en anderzijds het onderhoud en beheer van bestaande systemen, applicaties en infrastructuur.
De meer beleidsmatig gerichte functie heeft als belangrijkste doel om binnen GBTwente voldoende organisatorische beveiligingsmaatregelen te initiëren, en wel zodanig dat de technische beveiligingsmaatregelen ook daadwerkelijk effectief zijn. Met andere woorden, er dient zorg gedragen te worden voor samenhang tussen de technische en organisatorische maatregelen.
Het is mogelijk dat de CISO zich zowel met beleid als uitvoering bezighoudt, wenselijk is dit niet gezien het feit dat dit er toe kan leiden dat één van beide gebieden dan te weinig aandacht krijgt.

2. Plaats in de organisatie

Het betreft een staffunctie/verbijzonderde functie direct onder het dagelijks bestuur of de directeur.

Bij een kleine gemeente zal er meestal sprake zijn van één CISO en dan wellicht niet fulltime. In combinatie met een andere functie tot één fulltime functie is ook mogelijk. Echter, deze functies moeten elkaar qua taken, verantwoordelijkheden en bevoegdheden niet 'bijten'. Ook moet de positionering van die andere functie conform de gewenste positionering van de CISO-functie zijn.
Gezamenlijke positionering binnen de organisatie met risico-, veiligheids-, continuïteits-, privacy en/of kwaliteitsmanagement kan de functie op een hoger plan brengen.
Positionering bij de (ICT)-auditfunctie heeft niet de voorkeur, omdat controle/toezicht door de (ICT-) auditor op de CISO daardoor wordt bemoeilijkt: de externe auditfunctie (accountant) moet dan een grotere rol krijgen.
Positionering onder een ICT-directeur, informatiemanager of Chief Information Officer (CIO) is mogelijk, zolang er maar altijd de mogelijkheid bestaat tot directe rapportage aan het dagelijks bestuur. Risico van plaatsing onder de ICT-directie is dat de nadruk meer op de technische aspecten van informatiebeveiliging komt te liggen, terwijl juist de mensen in de organisatie veelal de zwakke schakel in het geheel zijn.
De geschetste positie garandeert een zekere, voor de functie noodzakelijke, onafhankelijkheid ten opzichte van de 'gewone' lijnfuncties. Bovendien is deze positie van belang om voldoende gewicht in de schaal te kunnen leggen. Dat is nodig ter compensatie van de 'natuurlijke weerstand' tegen het treffen en handhaven van voldoende beveiligingsmaatregelen.

3. Resultaatgebieden (taken, verantwoordelijkheden en werkzaamheden)

Beleid en coördinatie
• Het opstellen en actualiseren van het informatiebeveiligingsbeleid (langere termijn).
• Het (laten) opstellen van informatiebeveiligingsplannen voor teams of deelgebieden (jaarplannen).
Het coördineren van de werkzaamheden van personen, teams en instanties die zijn betrokken bij de uitvoering van het informatiebeveiligingsbeleid.
• De CISO kan gezien worden als de programmamanager van het strategisch programma informatiebeveiliging.

Controle en registratie
• Het toezicht houden op de implementatie en naleving van het informatiebeveiligingsbeleid.
• Het opstellen van een controleplan, evenals het leveren van ondersteuning bij het uitvoeren van de daarin gedefinieerde taken.
• Het uitvoeren of initiëren van risicoanalyses en interne audits.
• Het verzamelen en registreren van informatie over de aanwezige beveiligingsmaatregelen.
• Het opzetten of initiëren van een registratie voor beveiligingsincidenten, evenals het afhandelen van opgetreden incidenten en het nemen van preventieve maatregelen ter voorkoming van dergelijke incidenten.

Communicatie en voorlichting
• Het onderhouden van externe en interne contacten op alle niveaus binnen dit kader.
• Het organiseren van en deelnemen aan een coördinerend overleg met betrekking tot informatiebeveiliging.
• Het verzorgen en coördineren van voorlichting en interne opleidingen van het personeel op het gebied van informatiebeveiliging.
• Het stimuleren van het beveiligingsbewustzijn en het opstellen, uitvoeren en onderhouden van een communicatieplan.
• Het volgen van nieuwe ontwikkelingen en wetgeving op het gebied van informatiebeveiliging.

Advies en rapportage
• Het optreden als projectmanager bij beveiligingsprojecten, waarbij aansturing wordt gegeven aan projectleiders binnen organisatorische eenheden.
• Het afstemmen van informatiebeveiliging met lopende projecten binnen de organisatie.
• Het uitwerken van beveiligingsplannen ten aanzien van de maatregelen, evenals het leveren van ondersteuning bij het uitvoeren van de geaccepteerde plannen.
• Het geven van gevraagd en ongevraagd advies aan het bestuur, de leiding van de organisatie en het lijnmanagement over de te nemen maatregelen.
• Het rapporteren aan het bestuur en de leiding van de organisatie over het gevoerde beleid met betrekking tot informatiebeveiliging, de voortgang van implementatie van nieuwe maatregelen, opgetreden incidenten, ondernomen acties, resultaten van onderzoeken en resultaten van controles.

Onderstaand nog enkele aandachtspunten bij de diverse resultaatgebieden, waarbinnen ook een budget, een bijbehorend jaarplan en dito rapportage niet vergeten mogen worden.

Beleid
Beleid opstellen, uitvoeren en toetsen/controleren. Uitvoering en controle op uitvoering gaan niet samen.

Coördineren
Informatiebeveiliging is een aspect dat door de hele organisatie van GBTwente heen loopt. Het 'zit in' de infrastructuur, de applicaties, de processen, de beheerders en de gebruikers. Verder gaat het bij informatiebeveiliging om integriteit (zijn/blijven gegevens juist en volledig), beschikbaarheid en vertrouwelijkheid. Dat kan soms tegenstrijdige belangen opleveren.
Fysieke beveiliging en privacy zijn onderwerpen die deels overlap hebben met informatiebeveiliging. Iemand moet dat geheel coördineren, anders werkt het langs elkaar heen of nog erger, elkaar tegen. Dan bereik je niet wat je wilt bereiken en wordt onnodig geld weggegooid.

Adviseren, aan wie en waarover?
De CISO is binnen GBTwente de deskundige bij uitstek op het gebied van informatiebeveiliging. Bij de invoering van nieuwe of vernieuwde systemen, de toepassing van nieuwe technologieën, procedures, maar ook als zaken in de praktijk niet goed blijken te lopen kan/moet de CISO worden ingeschakeld. Informatiebeveiliging achteraf inbouwen is namelijk vaak een lastige en kostbare zaak.
De CISO heeft veel kennis zelf in huis. Waar de eigen kennis onvoldoende is, weet de CISO waar en bij wie deze kennis wel aanwezig is. Het is dus van belang dat een CISO is aangesloten bij een gremium van vakgenoten. Op dit moment wordt nagedacht over een overheid informatiebeveiliging community, maar ook de IBD heeft een besloten community waar ervaringen kunnen worden uitgewisseld. Buiten de overheid is dat het Platform voor Informatiebeveiliging (PvIB).
Bij adviseren gaat het, naast de inhoud van het advies, ook over de wijze waarop een advies wordt gegeven. Een CISO moet over goede adviesvaardigheden beschikken. Bij tegengestelde belangen, deadlines die gehaald moeten worden, et cetera is hij/zij degene die het informatiebeveiligingsaspect steeds weer naar voren brengt. En wel zodanig dat dit ook wordt geaccepteerd.

Rapporteren
Rapportage is een belangrijk onderdeel van de taak van een CISO. Het zorgt ervoor dat het management weet wat er op het gebied van informatiebeveiliging speelt. Hierdoor blijft het management commitment behouden. En dat is misschien wel de belangrijkste voorwaarde om informatiebeveiliging binnen een organisatie van de grond te krijgen en te behouden.

Baseline Informatiebeveiliging Overheid (BIO)
De onderwerpen die behoren tot het taakgebied van de CISO's staan in de Baseline Informatie-beveiliging Overheid (BIO). Ten aanzien van deze onderwerpen moet een CISO een beleid opstellen/coördineren, controleren/registreren, communiceren/voorlichten en adviseren/rapporteren.

Organisatorisch/technisch
De CISO welke zich richt op de organisatie van de informatiebeveiliging is overkoepelend aan de meer technisch gerichte Security Officer. Technisch kan (en moet) er veel geregeld worden op het gebied van informatiebeveiliging. Maar dat is niet voldoende. Uiteindelijk wordt 'de techniek' gebruikt door mensen (medewerkers, externen, gasten). Juist deze kant van informatiebeveiliging (hoe zorg ik dat de dure technische maatregelen effectief worden gebruikt binnen de organisatie) is van belang, maar krijgt vaak nog niet de aandacht die zij verdient.
ICT staat ten dienste van het primaire proces, het lijnmanagement. Zo staat ook informatiebeveiliging ten dienste van de bedrijfsvoering.

Bevoegdheden

Voorwaarde om de functie CISO volledig te kunnen vormgeven, is de bevoegdheid om gevraagd en ongevraagd te mogen rapporteren aan het dagelijks en/of algemeen bestuur van GBTwente.
Bevoegdheid zonder budget werkt in de praktijk niet. Een eigen budget voor informatiebeveiliging is dus een andere belangrijke voorwaarde voor het goed functioneren.