Nota voor	:	vergadering algemeen bestuur
Datum	:	15 december 2022
Onderwerp	:	Strategisch Informatiebeveiligingsbeleid VNOG
Agendapunt	:	5.
Kenmerk	:	AB/2228

Portefeuillehouder: H.J. van Schaik

Bijlage: Strategisch Informatiebeveiligingsbeleid VNOG

Inleiding
In 2018 heeft uw bestuur de Baseline Informatieveiligheid VNOG vastgesteld. Dit document biedt beleidsmatige kaders voor zowel gegevensbescherming als informatiebeveiliging. Daarnaast is in 2019 het Privacybeleid van de VNOG vastgesteld.

Wijzigingen in de onderliggende regelgeving, waaronder de komst van de Baseline Informatiebeveiliging Overheid (BIO), en recente ontwikkelingen maken dat het beleid met betrekking tot de genoemde onderwerpen aan herziening toe is.

Het nieuwe Gegevensbeschermingsbeleid voor de VNOG, ook Privacybeleid genoemd, is door uw bestuur vastgesteld in de vergadering van 23 juni 2022.

In deze vergadering wordt u het Strategisch Informatiebeveiligingsbeleid VNOG ter vaststelling voorgelegd. Dit besluit is door het dagelijks bestuur voor advies aan de Ondernemingsraad voorgelegd. De OR adviseert …… .

Het vaststellen van (nieuw) Informatiebeveiligingsbeleid is onderdeel van het Actieplan BIO AVG 2022-2024, dat u in de vergadering van 24 maart 2022 heeft vastgesteld.

Advies-voorgenomen besluit
1. Het Strategisch Informatiebeveiligingsbeleid VNOG vast te stellen;
2. De Baseline Informatieveiligheid VNOG 2018 in te trekken.

Beoogd effect
Beschikken over actueel beleid op het gebied van informatiebeveiliging.

Argumenten
1.1 Betrouwbare en veilige informatie is van levensbelang voor de dienstverlening door de VNOG
Uw bestuur heeft het beschikken over ‘een sterke informatiepositie’ aangemerkt als een van de drie pijlers onder de missie en de visie van de VNOG. Dat benadrukt het belang van correcte en betrouwbare informatie voor de advisering en de uitvoering van de operationele taken, maar ook voor de taken op het gebied van de bedrijfsvoering. Een optimale invulling van deze pijler stelt hoge eisen aan de informatieveiligheid en -beveiliging.

1.2 De ambitie van de VNOG is het waarborgen van de vertrouwelijkheid, de integriteit en de beschikbaarheid van de informatievoorziening

Deze ambitie krijgt vorm in alle aspecten van de informatiebeveiliging, waaronder het beschermen van alle fysieke en digitale informatiesystemen binnen de VNOG en het beperken van de risico's van diefstal, verlies, misbruik, uitval of beschadiging van deze informatiesystemen Het creëren van bewustwording en daarmee van gedragsverandering bij het bestuur, de VNOG-medewerkers en externe relaties op het gebied van Informatieveiligheid is eveneens van belang. Als overheids- én veiligheidsorganisatie is het zaak de VNOG-organisatie te beschermen tegen aansprakelijkheid en fysieke- en/of imago- en vertrouwensschade door misbruik van de informatiesystemen en faciliteiten en dient er een adequate continuïteitstrategie te zijn om onderbrekingen van activiteiten tegen te gaan en kritieke processen te beschermen.

1.3 Het beleid stelt de uitgangspunten voor de informatiebeveiliging en de inrichting ervan vast

De strategische en tactische uitgangspunten, die zijn benoemd in de paragrafen 2.5, 2.6 en 2.7 vormen de kaders voor de verder invulling van het beleid in een informatiebeveiligingsplan, dat jaarlijks door de directie wordt vastgesteld. Hiertoe behoren onder meer het verzekeren van de informatiebescherming gedurende de levenscyclus van de informatie, van creatie tot vernietiging, het faciliteren van een veilige informatie-uitwisseling, het continu monitoren op potentiële bedreigingen voor de informatieveiligheid en het aanpassen van de beveiliging aan nieuwe dreigingen.

1.4 De specifieke rollen en functies voor de informatieveiligheid zijn benoemd

Naast de verantwoordelijkheid van het lijnmanagement (directie, afdelingshoofden en teamleiders) zijn er op het gebied van informatieveiligheid twee functionarissen met een specifieke verantwoordelijkheid: de Chief Information Security Officer (CISO) en de Security Officer (SO). De VNOG heeft beide functies ingevuld.

1.5 De Baseline Informatiebeveiliging Overheid (BIO) is verplicht voor de gehele overheid

De Baseline Informatiebeveiliging Overheid (BIO) beschrijft het basisniveau voor informatiebeveiliging voor de overheid in Nederland. Dit betekent dat er voor alle overheidsorganisaties één basisniveau voor informatiebeveiliging is met één gezamenlijke taal. Het vaststellen van en beschikken over informatiebeveiligingsbeleid is een verplichting, die voortvloeit uit de BIO. Daarmee liggen ook de kaders vast. Paragraaf 2.7 en hoofdstuk 3 van het document zijn regiospecifiek voor de VNOG, de overige delen volgen uit de BIO.

1.6 Informatieveiligheid is onderdeel van het Actieplan BIO AVG 2022-2024

Een van de elementen in het Actieplan BIO AVG is het verbeteren van de governance[1] op het gebied van informatieveiligheid. De VNOG legt daarmee in documenten vast hoe zij de informatieveiligheid vormgeeft. De vaststelling van dit Strategisch Informatiebeveiligingsbeleid past hierin. Met de vaststelling van dit beleid zijn geen extra kosten gemoeid. De benodigde financiële middelen voor concrete maatregelen en voorzieningen zijn bij de vaststelling van het Actieplan BIO AVG 2022-2024 al beschikbaar gesteld.

[1] Maatregelen en voorzieningen in de categorieën Governance, Preventie, Detectie en Respons bepalen het volwassenheidsniveau van de informatiebeveiliging. Binnen de VNOG heeft met name de eerste categorie een extra impuls nodig.

2.1 Het Strategisch Informatiebeveiligingsbeleid vervangt de Baseline Informatieveiligheid 2018
In 2018 heeft uw bestuur op basis van de toen geldende regelingen en inzichten, met name de voorloper van de BIO, de Baseline Informatieveiligheid VNOG vastgesteld. Het nieuwe beleidsdocument vervangt de Baseline uit 2018, die daarom kan worden ingetrokken.

Kanttekeningen
1.1 Concrete maatregelen zijn nodig om het beleid in te vullen
Het Strategisch Informatiebeveiligingsbeleid geeft de kaders voor informatieveiligheid. Dit beleid krijgt een uitwerking in concrete maatregelen, waarmee zoveel mogelijk wordt voorkomen dat securityschendingen plaatsvinden, bijvoorbeeld door een datalek, dat informatie niet integer is en/of het in verkeerde handen kan vallen, dat gijzeling van belangrijke data plaatsvindt of dat sprake is van economische schade door het uitlekken van vertrouwelijke plannen en documenten of van fysieke schade door storingen in systemen. In de planperiode 2022-2024 worden deze maatregelen -waar dat nog niet is gebeurd- geïmplementeerd, waarmee de informatieveiligheid gestalte krijgt.

Uitvoering/ communicatie/ inwerkingtreding
De uitvoering van het Strategisch Informatiebeveiligingsbeleid is opgedragen aan de directie en de afdelingshoofden en wordt uitgewerkt in een Informatiebeveiligingsplan, dat jaarlijks door de CISO wordt voorbereid en door de directie wordt vastgesteld.

Het informatiebeveiligingsbeleid wordt daarnaast daar waar nodig vertaald naar maatregelen, procedures en voorzieningen die worden opgenomen in het voor alle medewerkers te raadplegen *Handboek Informatiebeveiliging*.

Voor het bevorderen en borgen van kennis en bewustzijn van informatiebeveiliging organiseert de CISO in samenwerking met de Functionaris Gegevensbescherming (FG) jaarlijks een awarenesstraining voor de medewerkers. Daarnaast zal informatieveiligheid een onderwerp zijn in het verkeer tussen de leidinggevenden en de medewerkers.

Het Strategisch Informatiebeveiligingsbeleid VNOG is met ingang van zijn vaststelling van toepassing.

Rapportage/ evaluatie
De CISO rapporteert periodiek aan de directie en het managementteam over de informatiebeveiliging, die ook onderdeel is van de P&C-gesprekken. De directie rapporteert periodiek aan het bestuur over de stand van de informatiebeveiliging, eveneens in het kader van de P&C-cyclus.

Personele consequenties
Geen.

Financiële consequenties
Geen.

Het algemeen bestuur van de Veiligheidsregio Noord- en Oost-Gelderland;

Bijeen in de vergadering d.d. 15 december 2022;

Gelezen het voorstel van het dagelijks bestuur d.d. 8 september 2022;

Besluit:
1. Het Strategisch Informatiebeveiligingsbeleid VNOG vast te stellen;
2. De Baseline Informatieveiligheid VNOG 2018 in te trekken.

De secretaris | De voorzitter

drs. D.G.L. Kransen | A.J.M. Heerts

Apeldoorn, 15 december 2022

Strategisch Informatiebeveiligingsbeleid

Veiligheidsregio Noord- en Oost-Gelderland

Datum: 24 mei 2022
Versie: 0.2
Zaaknummer:
Auteur: Edwin Moraal
Organisatieonderdeel: Bedrijfsvoering

Inhoud

1. Inleiding

Een van de pijlers onder de missie en de visie van de VNOG ‘Samen werken aan Veiligheid; Veilig en gezond wonen, werken en recreëren’ is het beschikken over een sterke informatiepositie.
De invulling van deze pijler stelt hoge eisen aan het beheer van de informatie, die in de organisatie aanwezig is. Intern ligt de focus op vraagstukken op het gebied van informatie-gestuurd werken, Informatieveiligheid en cyberverstoringen. Extern ligt deze op gegevensuitwisseling met de andere veiligheidsregio's en de (crisis)partners.
Nieuwe ontwikkelingen op het gebied van het hybride werken vergroten het risico dat data en daarmee informatie zich steeds meer en meer gaat verspreiden.
Dit geldt zowel binnen de VNOG als bij opdrachtnemers. Veilige toegang tot (digitale) informatie inclusief gebouwen en personeel vereist actief beheer. Het uitwisselen van (gevoelige) informatie vormt al snel een risicobron voor de privacy van betrokkenen.

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid van de VNOG en is richtinggevend en kaderstellend. De nota wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en procesbeschrijvingen/ werkinstructies op operationeel niveau.

Met dit 'Strategisch Informatiebeveiligingsbeleid’ zet de VNOG een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de VNOG 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 nl en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). De principes zijn gebaseerd op de 10 bestuurlijke principes voor informatiebeveiliging zoals uitgewerkt door de Informatiebeveiligingsdienst van de Vereniging Nederlandse Gemeenten (IBD VNG). Op het niveau van de veiligheidsregio’s kennen we verder de VeRA (Veiligheidsregio’s Referentie Architectuur) en de landelijke Security Architectuur.

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerpspecifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het Informatiebeveiligingsplan, vast te stellen door de directie, worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de afdelingshoofden, de Chief Information Security Officer (CISO) en het dreigingsbeeld vanuit de landelijke gremia zoals Vakgroep Informatieveiligheid, waarin de CISO’s en FG’s van de veiligheidsregio’s samenwerken, het Nationaal Cyber Security Centrum (NCSC) en de Informatiebeveiligingsdienst (IBD) van de Vereniging Nederlandse Gemeenten. De VNOG heeft zich in hun keten aangesloten bij de voor haar relevante informatiebronnen. In het Informatiebeveiligingsplan staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist.
Hoofdstuk 3 beschrijft vervolgens bij welke functionarissen en hoe de taken en verantwoordelijkheden in de organisatie op het gebied van informatiebeveiliging belegd zijn.

1.2 Wat is informatiebeveiliging?

Informatiebeveiliging is het proces van vaststellen van de vereiste beveiliging van informatiesystemen, zowel digitaal als fysiek, in termen van vertrouwelijkheid, beschikbaarheid en integriteit en het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.

De BIO beoogt de beveiliging van informatie(systemen) bij alle bestuurslagen en bestuursorganen van de overheid te bevorderen, zodat alle onderdelen erop kunnen vertrouwen dat onderling uitgewisselde gegevens, in lijn met wet- en regelgeving, passend beveiligd zijn. Het doel is continuïteit in de bedrijfsprocessen door het waarborgen van juiste en tijdige informatie.

1.3 Ambitie en visie van de VNOG op het gebied van informatieveiligheid

De VNOG heeft de ambitie om de vertrouwelijkheid, integriteit en beschikbaarheid van haar informatievoorziening te waarborgen. Een toereikend informatiebeveiligingsbeleid is hierbij een randvoorwaarde. Bij het realiseren van deze ambitie streeft de VNOG de volgende doelen na:

- Het conformeren aan geldende wet- en regelgeving en de normen uit de BIO. In de uitvoering kiest de VNOG voor een pragmatische aanpak, maar deze is uiteraard compliant.
- Het beschermen van alle fysieke en digitale informatiesystemen binnen de VNOG (met inbegrip van, maar niet beperkt tot, alle computers, netwerkapparatuur, Cloud-voorzieningen, software en data) en het beperken van de risico's van diefstal, verlies, misbruik, uitval of beschadiging van deze informatiesystemen. Dit geldt ook voor de fysieke toegang tot informatie.
- Bewustwording/gedragsverandering creëren bij het bestuur, alle medewerkers, gasten, bezoekers en externe relaties met betrekking tot de bekendheid en naleving van alle huidige en relevante interne procedures en richtlijnen, alsmede van wetgeving op het gebied van Informatieveiligheid.
- Zorgen voor een veilige en betrouwbare werking van de informatiesystemen voor in- en externe medewerkers en door leveranciers die deze informatiesystemen namens de VNOG beheren.
- De borging ten aanzien van het beheer (exploitatie) van informatiesystemen om onbedoelde wijzigingen, met mogelijke nieuwe risico's, te voorkomen.
- De VNOG, als organisatie, te beschermen tegen aansprakelijkheid en fysieke- en/of imagoschade door misbruik van haar informatiesystemen en faciliteiten.
- Zorgen voor een systematiek van incidentenregistratie en analyse.
- Het bieden van een kader voor een adequate continuïteitsstrategie om onderbrekingen van activiteiten tegen te gaan en kritieke processen te beschermen tegen de gevolgen van omvangrijke storingen en incidenten in informatiesystemen en om tijdig herstel te bewerkstelligen. In de eerste fase dienen de ICT-technische zaken opgepakt te worden.
- Om informatieveiligheid te realiseren hebben we een systeem nodig wat ons helpt om op een adequaat niveau te komen. We gaan hier uit van een plan-do-check-act cyclus. Hierdoor krijgen we een systeem wat gericht is op het continue verbeteren. In het vakgebied informatiebeveiliging noemen we dat ook wel een Information Security Management System (ISMS).

2. Strategisch beleid

In dit hoofdstuk worden de hoofdlijnen voor het Informatiebeveiligingsbeleid van de VNOG op strategisch niveau benoemd. Onderdeel van dit hoofdstuk zijn het doel van het beleid, de te hanteren uitgangspunten, de scope en de procesinrichting van de informatiebeveiliging. De tactische en operationele vertaling van het beleid vindt plaats in het door de directie vast te stellen informatiebeveiligingsplan en in het (operationele) Handboek informatiebeveiliging.

2.1 Doel

Het doel van dit informatiebeveiligingsbeleid is om formeel invulling te geven aan de manier waarop binnen VNOG wordt omgegaan met security en informatiebeveiliging en bestuurlijk de randvoorwaarden vast te leggen voor verdere uitwerking van dit beleid.

De strategische doelen van het informatiebeveiligingsbeleid, gerelateerd aan de BIO, zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming en beheer 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 inwoners en medewerkers.
- Het waarborgen van de naleving van dit beleid.

2.2 Scope informatiebeveiliging

De scope van dit beleid omvat alle VNOG-processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de VNOG 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 beleid is van toepassing op de gehele organisatie, alle organisatieonderdelen, objecten en gegevens(verzamelingen), inclusief derden die hiertoe door de VNOG worden ingezet. Het informatiebeveiligingsbeleid is in lijn met het overige beleid van de VNOG en de relevante landelijke en Europese wet- en regelgeving.

Dit Strategisch Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit geldende wetgeving. 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.

2.3 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid zijn gebaseerd op de BIO. Dit is het nieuwe normenkader voor de gehele overheid. De werkwijze van de BIO is gericht op risicomanagement. 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.
Risicomanagement is daarbij van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afweegt of informatie in bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.4 De 10 bestuurlijke principes voor informatiebeveiliging

De 10 bestuurlijke principes[1] voor informatiebeveiliging vormen een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden 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 informatiebeveiliging in de overheidsorganisatie en ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de veiligheidsregio-processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de veiligheidsregio. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

Het bestuur van de VNOG heeft zich al eerder gecommitteerd aan de 10 bestuurlijke principes in het kader van de besluitvorming rond het Versnellingsplan BIO AVG 2022-2024 en de evaluatie informatiebeveiliging en gegevensbescherming.

2.5 Strategische uitgangspunten voor informatiebeveiliging

De VNOG opereert 24 uur per dag, 365 dagen per jaar en moet altijd klaar staan. Naast de 10 bestuurlijke principes, hanteert de VNOG daarom een aantal uitgangspunten:

Verificatie voor vertrouwen (zgn. ZERO TRUST)
Nooit (impliciet) vertrouwen, maar verifiëren wanneer geen standaard vertrouwensrelatie bestaat. Dit geldt voor gebruikers, apparaten, applicaties en pakketten, ongeacht wat het is en ongeacht de locatie op of ten opzichte van de VNOG-infrastructuur.

Informatie wordt beschermd
Informatiebescherming moet verzekerd zijn gedurende de hele levenscyclus van de informatie: creatie, wijziging, opslag, transport en vernietiging. Deze bescherming is verder vormgegeven in het separaat vastgestelde Gegevensbeschermingsbeleid van de VNOG.

[1] De VNG heeft in 2019 de 10 bestuurlijke principes opgesteld. https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf

Veilige informatie-uitwisseling
De infrastructuur en applicatie-architecturen moeten veilige informatie-uitwisseling kunnen faciliteren en mogelijk maken. Een veilige infrastructuur die onweerlegbare transacties en transacties van derden ondersteunt, is vereist ter ondersteuning van transacties die aan de regelgeving voldoet.

Continue beveiliging
De beveiligingsinfrastructuur en de beveiligingsorganisatie moeten hierop en op elkaar aansluiten om de operatie te ondersteunen, met andere woorden: continu monitoren, beoordelen en waarschuwen.

Aanpassen op nieuwe bedreigingen
De informatiebeveiligingsarchitectuur en -infrastructuur bieden richtlijnen voor preventieve, opsporings- en corrigerende maatregelen die de verwachte capaciteiten beschrijven om de omgeving up-to-date en veilig te houden. Kennis over dreigingen wordt gedeeld met derden buiten de VNOG, conform daarover afgesproken procedures.

Dreigingsbeeld Informatiebeveiliging
Het dreigingsbeeld informatiebeveiliging vanuit het NCSC (Nationaal Cyber Security Centrum) 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.

Daarnaast krijgt de VNOG informatie van c.q. deelt de VNOG deze met VR-ISAC (VeiligheidsRegio's Information Sharing and Analysis Center), Informatiebeveiligingsdienst (IBD) VNG, SOC (Security Operations Center) van een externe partij, SOC politie en Z-CERT (Zorg – Computer Emergency Responce Team).

Informatie uit incidenten en inbreuken op de beveiliging
De VNOG kent naast het hierboven genoemde dreigingsbeeld een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren. Daarmee zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van dit beleid.

Standaarden voor informatiebeveiliging
De basis voor de inrichting van de informatiebeveiliging is de BIO. De maatregelen worden op basis van best practices bij (lokale) overheden genomen. Voor de ondersteuning van overheden bij het formuleren en realiseren van hun informatiebeveiligingsbeleid is in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht.
Sinds 2020 is de BIO ook voor samenwerkingsverbanden als veiligheidsregio's verplicht. De 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 dit beleid zijn afgestemd op die van de BIO. Het informatiebeveiligingsplan zal ook deze structuur volgen.

2.6 Tactische uitgangspunten voor de informatiebeveiliging

De tactische uitgangspunten van het informatieveiligheidsbeleid gaan in op de beheersdoelstellingen per onderdeel van de BIO. De BIO kent naast het ISMS een aantal inhoudelijke onderwerpen.

Deze onderwerpen staan veelal niet op zich daar de onderwerpen vaak samen zorgen voor een niveau van veiligheid. Zo is er samenhang tussen de HRM processen instroom, doorstroom en uitstroom en het beheer van autorisaties. Op het gebied van communicatie op het internet is er samenhang met het beheer van encryptiesleutels. Wanneer een organisatie excelleert op één gebied kan een ander gebied weer voor onveiligheid zorgen. We zeggen dan ook wel dat de beveiliging zo goed is als de zwakste schakel in de keten. Per onderwerp zullen we op tactisch niveau aangeven wat het doel is van dit beheersaspect.

Veilig Personeel

Doelstelling
Medewerkers dienen geschikt te zijn en geschikt te blijven voor hun functie. De belangrijkste waarborg is het aantrekken van betrouwbaar en geschikt personeel en de zorg dat de medewerkers geschikt blijven voor hun functie, zodat ze op een goede wijze met de informatie van de organisatie om kunnen gaan tijdens en na afloop van hun contract.

Toelichting
Informatieveiligheid valt en staat met de kennis, houding en gedrag van de medewerkers. Om de juiste medewerkers in de organisatie te krijgen, deze gedurende hun loopbaan te trainen en te coachen zodat zij over de kennis en vaardigheden beschikken die nodig zijn om hun functie naar behoren uit te voeren.

Beheer van bedrijfsmiddelen

Doelstelling
De organisatie gebruikt een groot aantal systemen (apparatuur, devices en software) om de informatievoorziening te faciliteren. Het doel van dit beheer aspect is het identificeren van alle hard- en software zodat deze op een adequate wijze beheerd en beveiligd kunnen worden.

Toelichting
Om informatie adequaat te kunnen beheren is het van belang om inzicht te hebben in diverse ICT-componenten die gebruikt worden om informatie te verwerken. Er kan pas adequaat beheer gevoerd worden wanneer je in het zicht hebt wat je moet beheren. De administratie waarin de ICT-componenten worden beschreven (ook wel configuratie management database CMDB) genoemd dient als basis van diverse beheerprocessen zoals patchmanagement, incidentmanagement evenals het informatieclassificatiesysteem waarmee de behoefte, de prioriteit en de mate van beveiliging door de verantwoordelijk manager kan worden bepaald.

Toegangsbeveiliging

Doelstelling
Toegang tot informatie en informatie op een passende wijze beveiligen zodat onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie wordt voorkomen.

Toelichting
Om effectieve toegangscontrole tot vertrouwelijke en privacygevoelige informatie te kunnen invoeren en onderhouden wordt er een toegangsrichtlijn opgesteld. Naast deze toegangsrichtlijn heeft ieder informatiesysteem nog een specifiek gedefinieerde uitwerking omtrent toegang, dat is afgestemd op het beveiligingsniveau van de informatie.

Cryptografie

Doelstelling
Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

Toelichting
Een effectieve manier om informatie te beveiligen tegen onbevoegde inzage is het versleutelen van deze informatie. Dit gebeurt bij voorkeur zowel bij de opslag als het transport. Belangrijk beheeraspect is dat versleuteling wordt toegepast met behulp van sleutels die veilig genoeg zijn conform de actuele standaarden. Om verlies van data te voorkomen is het van belang dat er ten aanzien van het beheer van de sleutels goede maatregelen zijn getroffen.

Fysieke beveiliging

Doelstelling
Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatie verwerkende faciliteiten van de organisatie voorkomen.

Toelichting
Een belangrijk aspect van informatieveiligheid is het voorkomen dat onbevoegden fysiek toegang hebben tot informatie. Ondanks de snelle ontwikkeling van digitale informatieverwerking is veel informatie ook nog analoog beschikbaar. Daarnaast dienen de informatie verwerkende computers en devices beschermd te worden tegen onbevoegde toegang. Fysieke beveiliging wordt ingezet om onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatie verwerkende faciliteiten van de organisatie voorkomen.

Beveiliging bedrijfsvoering

Doelstelling
Correcte en veilige bediening van informatie verwerkende faciliteiten ter voorkoming van ongewenste aanpassingen, verlies en diefstal van gegevens

Toelichting
Informatie wordt door de gehele organisatie heen gebruikt en daarnaast wordt informatie ook gedeeld met andere organisaties. Doordat informatie wordt hergebruikt is het van belang dat informatie goed wordt beheerd. Uitgangspunt hierbij is dat ieder brok aan informatie wordt beheerd vanuit een aangewezen organisatie-onderdeel die daarvoor eenduidige processen en controlemaatregelen heeft ingericht om de kwaliteit van de informatie te kunnen waarborgen.

Communicatiebeveiliging

Doelstelling
Informatie van de organisatie die via het interne netwerk intern dan wel extern wordt getransporteerd dient afdoende te worden beveiligd om onderschepping en/of ongewenste aanpassing van informatie te voorkomen.

Toelichting
Bij het beheer van netwerken moet onderscheid worden gemaakt tussen het eigen netwerk en netwerken die de grens van de organisatie overschrijden. Voor transport van vertrouwelijke en privacygevoelige gegevens via netwerken dienen extra maatregelen ter waarborging van de veiligheid te worden getroffen om te zorgen dat de data-integriteit en de vertrouwelijkheid bij transport is gewaarborgd. Zeker nu we steeds meer met externe partijen samenwerking is het van groot belang te kunnen vertrouwen op de communicatiekanalen.

Aankoop, ontwikkeling en onderhoud van informatiesystemen

Doelstelling
Waarborgen dat informatieveiligheid integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus en bij het testen van systemen. Dit zowel bij interne systemen als bij gebruik van een cloud leverancier.

Toelichting
Bij de ontwikkeling van (informatie)systemen moeten beveiliging en privacy vanaf aanvang in het ontwerpproces of in het pakket aan eisen worden meegenomen. Bij standaardprogrammatuur moet voor aanschaf worden vastgesteld of geautomatiseerde beveiligingsmaatregelen zijn ingebouwd en aan de eisen vanuit de AVG wordt voldaan. Bij het onderhoud van (informatie)systemen moet informatieveiligheid een vast aandachtspunt zijn.

Leveranciers

Doelstelling
Er dienen met leveranciers overeenkomsten te worden gesloten die ervoor zorgen dat de dienstverlening in overeenstemming is met het informatieveiligheidsbeleid en de wettelijke bepalingen.

Toelichting
Organisaties zijn ten aanzien van de verwerking van informatie sterk afhankelijk van diverse leveranciers. Dit niet alleen vanwege de aanschaf en de primaire werking maar vanwege de dienstverlening die verbonden is aan de primaire dienstverlening. Het is van belang om met de leveranciers goede afspraken te maken over de aard van de dienstverlening. Daarnaast dient te worden gecontroleerd of ook aan de eisen wordt voldaan.

Incidentenbeheer

Doelstelling
Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatieveiligheid incidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging

Toelichting
Het beheer van incidenten kent twee gezichtspunten. Ten eerste dienen incidenten snel en adequaat te worden afgehandeld maar daarnaast zijn incidenten ook een signaal dat bestaande maatregelen wellicht niet voldoen. Het is dus van belang dat een incident zowel goed en snel wordt afgehandeld en dat daarnaast een analyse plaatsvindt zodat duidelijk is wat de oorzaak is geweest en hoe we er structureel voor kunnen zorgen dat een dergelijk voorval niet meer plaats kan vinden.

Continuïteitsbeheer

Doelstelling
Beschikbaarheid van informatie verwerkende faciliteiten bewerkstelligen.

Toelichting
Continuïteitsbeheer heeft als doel om er voor te zorgen dat de dienstverlening intern en extern ongestoord kan plaatsvinden. Om de dienstverlening ongestoord doorgang te laten vinden dienen we zowel te kijken naar de systemen die nodig zijn als naar de facilitaire voorzieningen.

Naleving

Doelstelling
Verzekeren dat informatieveiligheid wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie ter voorkoming van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatieveiligheid en beveiligingseisen.

Toelichting
Het uitdragen van beleid en het opstellen van procedures moeten een waarborg bieden voor de kwaliteit. Het controleren van het beleid en de naleving van de procedures zijn erop gericht om te beoordelen of beleid en procedures ook werkbaar zijn in de praktijk. Daarnaast kunnen controles ook gebruikt worden om verdere sturing te geven aan de organisatie en zijn daarmee een essentieel onderdeel van de governance.

2.7 Procesinrichting informatiebeveiliging

Bij de inrichting van de informatiebeveiliging onderscheidt de VNOG de volgende processen en procedures:

- Preventie: het voorkomen van veiligheidsincidenten.
- Detectie: het ontdekken van een incident of kwetsbaarheden en het creëren van mogelijkheden om achteraf vast te kunnen stellen of er sprake is geweest van een inbreuk.
- Isoleren: het beperken van de gevolgen van een veiligheidsincident.
- Analyseren: het onderzoeken van beveiligingsincidenten en de gevolgen ervan.
- Repareren: wanneer ‘besmetting’ plaats heeft gevonden moet herstel mogelijk zijn zoals back-up en re-store, maar ook uitwijkprocedures en externe inhuur van bewaking/bescherming.
- Communiceren: het toelichten van de situatie en het bieden van een handelingsperspectief.

Belangrijkste uitgangspunten
De belangrijkste uitgangspunten, in willekeurige volgorde, van het beleid en de praktische invulling daarvan zijn:

Uitgangspunten	Praktische invulling
Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.	• Het algemeen bestuur stelt als bestuurlijk eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast, met advisering door de Ondernemingsraad. • De directie als ambtelijk eindverantwoordelijke stelt jaarlijks het informatiebeveiligingsplan vast en legt verantwoording af aan het bestuur.
Er wordt een informatiebeveiligingsplan opgesteld onder leiding van de CISO dat, in afstemming met de Security Board, ter vaststelling aan de directie wordt aangeboden	• De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie, voorafgaand aan de P&C-gesprekken.
Alle informatie en informatiesystemen, inclusief alle Proces Automatiseringssystemen (PA) die binnen de gebouwen van de VNOG en in de publieke ruimte van de VNOG worden gebruikt, zijn van belang voor de VNOG, bepaalde informatie is van vitaal en kritiek belang.	• De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerpspecifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. • De afdelingshoofden zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de VNOG, hebben een interne systeemeigenaar 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 eigenaren van de informatie en het systeem.	• De afdelingshoofden zijn samen met de CISO verantwoordelijk voor het oefenen met informatiebeveiligingsincidenten en bedrijfscontinuïteit. • De directie is verantwoordelijk voor het vragen om informatie bij de afdelingshoofden en ziet erop toe dat de afdelingshoofden adequate maatregelen genomen hebben voor de bescherming van de informatie, informatie-systemen en procesautomatiseringssystemen die onder hun verantwoordelijkheid valt.
Kennis en bewustzijn van informatiebeveiliging en omgaan met gegevens binnen de organisatie dienen actief bevorderd en geborgd te worden	• Alle medewerkers van de VNOG worden getraind in het gebruik van beveiligingsprocedures. • De CISO rapporteert periodiek aan MT en directie ten aanzien van informatiebeveiliging.
Iedere medewerker, zowel vast als tijdelijk, intern, extern of ingehuurd en iedere externe gebruiker, 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. Dit geldt ook voor gebruikers van onze informatiesystemen die geen medewerker zijn (zoals bijvoorbeeld bij dashboards).	• Medewerkers dienen verantwoord om te gaan met alle informatie. • Informatiebeveiliging maakt deel uit van de beoordelingssystematiek en wordt besproken tussen de leidinggevende en de medewerker.

Door periodieke controle, organisatiebrede planning en 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 getoetst en zo nodig bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.	• Afdelingshoofden dienen erop toe te zien dat de controle op het verwerken van gegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende medewerkers de juiste gegevens ingezien en verwerkt hebben. • De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Aan de hand van quick scans op basis van de BIO worden deze risico-afwegingen gemaakt. • Het informatiebeveiligingsbeleid wordt periodiek getoetst en zo nodig herzien en vastgesteld. • Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging naar aanleiding van de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
De informatiebeveiliging maakt deel uit van de afspraken met ketenpartners en leveranciers.	• De informatiebeveiliging maakt onderdeel uit van de inkoopvoorwaarden van de VNOG.
De VNOG stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de in dit beleid gestelde wijze.	

3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie.

De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn (Security Board, CISO en Security Officer (SO) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een interne of externe auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

3.1 Uitgangspunten

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

Dit beleid wordt vastgesteld door het algemeen bestuur en vormt ook voor het management de kaders. De directie stelt het informatiebeveiligingsplan als uitvoering van het beleid vast en draagt dit met het afdelingsmanagement uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele management geeft een duidelijke richting aan informatiebeveiliging, demonstreert dat het informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven hiervan voor de gehele VNOG.

3.2 Rollen en functies binnen de informatiebeveiliging

Veel onderdelen binnen onze organisatie zijn bij informatiebeveiliging betrokken. In dit Strategisch informatiebeveiligingsbeleid worden de verantwoordelijkheden van de betreffende functies en rollen beschreven.

Rol	Toelichting
Directie	- is gemandateerd door het dagelijks bestuur; - stelt het informatiebeveiligingsplan vast; - stelt het gewenste niveau van informatiebeveiliging vast en wijst procesverantwoordelijke/systeemeigenaar per informatiesysteem aan; - bevordert de beschikbaarheid van voldoende middelen om informatiebeveiliging passend te waarborgen.
Chief Information Security Officer (CISO)	- is gemandateerd door het dagelijks bestuur; - is aanspreekpunt voor informatiebeveiliging; - is verantwoordelijk voor de afhandelen van informatiebeveiligingsincidenten. Verantwoordelijk voor: - actueel houden en coördineren van de uitvoering van het informatiebeveiligingsbeleid; - bevorderen van informatiebeveiligingsbewustzijn; - (pro) actief adviseren over informatiebeveiliging en het informatiebeveiligingsbeleid; - uitvoeren van analyses en advies over BIO (minimaal benodigde aanpassingen); - ondersteunen bij het uitvoeren van risicoanalyses en DPIA; - adviseren en ondersteunen van de organisatie om het benodigde niveau van informatiebeveiliging te bereiken dat minimaal voldoet aan de wet- en regelgeving; - zorgdragen dat ondersteunende systemen en processen voldoen aan wet- en regelgeving; - samen met de Functionaris voor de Gegevensbescherming adviseren ten aanzien van gegevensbescherming.
Security Officer (SO)	- vormt op het gebied van de informatieveiligheid (security) samen met de CISO het team Security, vergelijkbaar met het team Privacy op het gebied van gegevensbescherming, dat bestaat uit de FG en de Privacy Officer (PO); - vervangt in voorkomende gevallen de CISO in al zijn taken en werkzaamheden, waaronder als vertegenwoordiger van de VNOG in het VR ISAC; - is naast de CISO aanspreekpunt voor de VNOG-medewerkers voor informatieveiligheid. Verantwoordelijk voor : - leveren van een actieve bijdrage aan het door de CISO op te stellen informatieveiligheidsbeleid en adviseert deze daarover; - op diens verzoek adviseren van de CISO en, in samenspraak met de CISO, de organisatie over alle aspecten van de informatieveiligheid; - detecteren van potentiële veiligheidsrisico's in de organisatie en overleggen met de CISO over de te nemen maatregelen ter afwending van de risico's; - gevraagd en ongevraagd rapporteren aan de CISO over zijn taken, werkzaamheden en bevindingen; - ondersteunen van de CISO bij de uitvoering van diens taken en werkzaamheden; - uitvoeren van collegiale toetsingen op het gebied van informatieveiligheid bij andere veiligheidsregio's; - operationele informatieveiligheidstaken, waaronder het beheer van e-Herkenning.

Functionaris voor de Gegevensbescherming (FG)	Heeft een wettelijk mandaat. De taken en verantwoordelijkheden van de FG liggen op het terrein van de gegevensbescherming en zijn vastgelegd in het Gegevensbeschermingsbeleid van de VNOG.
Privacy Officer (PO)	De taken en verantwoordelijkheden van de PO liggen op het terrein van de gegevensbescherming en zijn vastgelegd in het Gegevensbeschermingsbeleid van de VNOG.
Afdelingshoofden en proceseigenaren	Zijn verantwoordelijk voor de inrichting en uitvoering van de primaire en secundaire bedrijfsprocessen, inclusief het uitvoeren van de controles in de eerste lijn en de informatiebeveiliging van dat proces en de risico-indeling/-afweging.
Teamleiders	Zijn verantwoordelijk voor de applicaties die binnen hun team uitgevoerd worden, inclusief de informatiebeveiliging van dat proces en de risico-indeling/-afweging.
Controller	Is belast met toetsing van uitvoer en kwaliteit van controles in de tweede lijn
Security Board (CISO, FG, controller en jurist)	Ziet toe op en adviseert over risico's ten aanzien van informatiebeveiliging en gegevensbescherming, inclusief juridische en organisatorische risico's.
Medewerkers Control	Voeren controles uit in de tweede lijn.
Adviseur informatievoorziening	- implementeert adviezen uit veiligheidsincidenten, onder supervisie van de CISO; - zorgt voor het verbeteren van de informatiebeveiliging binnen team, afdeling en organisatie conform normenkaders; - draagt bij aan het bevorderen van informatiebeveiligingsbewustzijn; - is samen met de CISO aanspreekpunt voor vragen op het gebied van informatiebeveiliging; - draagt bij aan de architectuur van de informatiebeveiliging en de inrichting van het architectuurlandschap.
Adviseur ICT	- implementeert adviezen uit veiligheidsincidenten, onder supervisie van de CISO; - zorgt voor het verbeteren van de informatiebeveiliging binnen team, afdeling en organisatie conform normenkaders; - draagt bij aan het bevorderen van informatiebeveiligingsbewustzijn; - is samen met de CISO aanspreekpunt voor vragen op het gebied van informatiebeveiliging; - draagt bij aan de architectuur van het ICT-landschap met als uitgangspunt de informatiebeveiliging en de inrichting van het architectuurlandschap.
Functioneel beheerders	Zijn verantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid voor de betreffende applicaties.
Medewerkers	- zijn zich bewust van de eigen verantwoordelijkheid en de risico's van het eigen handelen ten aanzien van informatieveiligheid; - gaan binnen de eigen taakuitvoering op juiste wijze om met informatie; - melden geconstateerde risico's en incidenten.
Leveranciers van diensten	Zijn medeverantwoordelijk -primair is de proceseigenaar dit- voor het borgen van de eisen en maatregelen van informatiebeveiliging zonder dat dit een goed gebruik van het informatiesysteem in de weg staat

3.3 Aansturing: directie

De directie zorgt ervoor dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingshoofd. De directie zorgt dat de afdelingshoofden en teamleiders zich verantwoorden over de beveiliging van de informatie die bij hen berust. Op die manier kan de directie zich ook verantwoorden naar het bestuur.

De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligingsonderwerpen (landelijke en regionale initiatieven en scholing) en laat zich hierin bijstaan door de CISO van de VNOG. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de VNOG gezien als een integraal onderdeel van risicomanagement.

3.4 Uitvoering: afdelingshoofden

Informatiebeveiliging valt onder de verantwoordelijkheden van alle afdelingshoofden. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij delen met teamleiders. De bedoeling is dat alle processen, systemen, data en applicaties altijd minimaal één eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Afdelingshoofden rapporteren aan de directie over de door hen op tactisch en operationeel niveau uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal twee keer per jaar het onderwerp Informatiebeveiliging te bespreken in het bedrijfsvoeringsoverleg en in Managementteam.

Taken van de proceseigenaren/leidinggevenden in het kader van informatiebeveiliging zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het voldoen aan wetgeving die op hun processen van toepassing is en invulling geven aan de rollen die binnen die wetgeving benoemd zijn.
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid, de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

3.4 Controle en verantwoording

Dit Strategisch Informatiebeveiligingsbeleid is een verantwoordelijkheid van het bestuur van de VNOG. Het bestuur zal volgens de 10 bestuurlijke 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 bestuur respectievelijk de bestuurlijke portefeuillehouder. De directie rapporteert daarnaast over de mate waarin zij invulling heeft gegeven aan het uitwerken van tactische (deel)beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

Aldus besloten in de vergadering van het algemeen bestuur van [datum]