STRATEGISCH INFORMATIEBEVEILIGINGS-BELEID NWO-I

1 INLEIDING

1.1 NUT EN NOODZAAK

Een betrouwbare informatievoorziening is essentieel voor wetenschappelijk onderzoek en het goed functioneren van de bedrijfsvoering processen. Informatiebeveiliging is het proces dat deze betrouwbare informatievoorziening borgt. Het opnemen van informatiebeveiliging als normaal kwaliteitscriterium voor een gezonde bedrijfsvoering is tegenwoordig niet langer een keuze, maar een noodzaak.

Bedreigingen worden groter

Cybercriminaliteit is de afgelopen jaren zeer sterk toegenomen en daarmee ook de economische schade voor ons land. Criminele organisaties, opportunisten, (internationale) activisten en ook geautomatiseerde malware zijn bedreigingen die door de steeds verdere digitalisering groter blijven worden. Volgens het NCTV zijn daarnaast cyberaanvallen door statelijke actoren het nieuwe normaal waarbij Nederland het doelwit is van een offensief cyberprogramma van landen als Rusland en China. Zij kunnen de genoemde digitale middelen inzetten tegen een breed scala aan mogelijke doelwitten, van lokale verenigingen tot internationale veiligheidsorganisaties en van één individu tot diasporagemeenschappen. Volgens de AIVD blijft de dreiging van offensieve cyberprogramma's tegen Nederland en de Nederlandse belangen onverminderd hoog en zal deze in de toekomst alleen maar toenemen. Deze statelijke actoren hebben meermaals (succesvolle) digitale aanvallen uitgevoerd op een EU-lidstaat. Dit valt binnen het normbeeld van deze statelijke actoren en de aanhoudende digitale (spionage)dreiging die daarvan uitgaat. Deze actoren voeren veelvuldig digitale aanvallen uit op onder andere EU- en NAVO-lidstaten.

Goede informatiebeveiliging is kosteneffectief

Ook de kosten van het bestrijden van cyberaanvallen kunnen snel oplopen. De recente hacks bij de universiteit van Maastricht (2019), Leiden (2021), Eindhoven (2022) en ook de hack van NWO-D in 2021 geven voldoende aanleiding. Volwassen informatiebeveiligingsrisicobeheersing is essentieel om de juiste beheersmaatregelen te selecteren en effectief te implementeren, om zo hogere kosten en schade te voorkomen.

Technologische ontwikkelingen

Technologische ontwikkelingen, zoals cloud computing, veranderen fundamenteel hoe we werken, en beïnvloed de bedrijfsmodellen van leveranciers en kwaadwillenden evenzeer. De maatregelen die een paar jaar geleden nog afdoende beschermde zijn achterhaald in een veranderende wereld. Informatiebeveiliging moet daarom een continu proces zijn om gepast bescherming te blijven bieden.

Ketenafhankelijkheden
Steeds meer informatie wordt gecreëerd, verwerkt en opgeslagen buiten de eigen organisatie, het eigen land of werelddeel, terwijl de verantwoordelijkheid van de beveiliging van deze informatie bij NWO-I blijft. Controle over data en beveiliging in de verschillende ketens is een essentieel onderdeel van de informatiebeveiligingsuitdagingen.

Samenwerking, altijd en overal
Toenemende flexibilisering, hybride werken en grotere mobiliteit vragen om een medewerker die altijd en overal toegang heeft tot de informatie die op dat moment noodzakelijk is. De nauwe samenwerking tussen de NWO-I-instituten en andere (onderzoeks)instellingen vraagt om een veranderende beveiligingshouding en het toepassen van nieuwe middelen om risico's af te dekken. Hierbij krijgen we te maken met uiteenlopende normenkaders, volwassenheidsniveaus en risicoprofielen. Met dit beleid voor informatiebeveiliging is geprobeerd al deze kaders te vatten in één samenhangend geheel.

Wet- en regelgeving
Wetgeving, op nationaal en Europees niveau, richt zich steeds meer op het verplichten van gepaste bescherming van kritieke infrastructuur, medische gegevens en persoonsgegevens. Het ligt in de lijn der verwachtingen dat, zoals in de AVG, de eisen die gesteld worden aan de aantoonbaarheid van deze gepaste bescherming toe zullen nemen.

Maatschappelijke verantwoordelijkheid
Tot slot is er de maatschappelijke verantwoordelijkheid die een organisatie heeft, die tot de basis wetenschappelijke infrastructuur behoort. Van NWO-I mag verwacht worden dat zij zorgvuldig omgaat met de gegevens die zij beheert, en dat de gegevens die zij levert juist, accuraat en tijdig zijn. Kortom, structurele aandacht voor de betrouwbaarheid van de informatievoorziening. Het domein van informatiebeveiliging helpt NWO-I bij een goede invulling van haar maatschappelijke taken. Een goede borging van informatiebeveiliging zorgt voor een betere betrouwbaarheid van de informatievoorziening en een grotere continuïteit van de bedrijfsvoering.

1.2 REIKWIJDTE

Het beleid geldt voor de hele NWO-I organisatie en is van toepassing op NWO-I en alle derden die informatie verwerken namens NWO-I. Voorbeelden zijn: universiteiten, collega-onderzoeksinstituten, bedrijven en dienstenleveranciers.

NWO-I werkt in toenemende mate samen in onderzoeksprogramma’s als gelijkwaardige partners. Het organisatieoverstijgende karakter van dreigingen maakt het noodzakelijk sterk in te zetten op samenwerking. Uitgangspunt is gelijkwaardigheid en betrokkenheid. Veel maatregelen zullen pas effect sorteren als in de gehele keten worden afgestemd dan wel getroffen.

Dit informatiebeveiligingsbeleid heeft betrekking op alle informatie die onder verantwoordelijkheid van NWO-I verwerkt wordt, ongeacht of het om gesproken, geschreven, geprint, digitaal of welk ander medium dan ook, ongeacht of het opengesteld, gelezen, getransporteerd, opgeslagen of vernietigd wordt.

1.3 ONDERDEEL KWALITEITSZORG

Informatiebeveiliging is een onderdeel van de kwaliteitszorg voor bedrijfsvoering en onderzoek. Informatiebeveiliging is een 'gewone' lijnverantwoordelijkheid. Daaraan inhoud geven gebeurt zowel op basis van interne overwegingen betreffende de betrouwbaarheid van de werkprocessen van een organisatie als op basis van externe randvoorwaarden zoals bestaande wet- en regelgeving. Uitgangspunt daarbij vormt de noodzaak om tot een integrale benadering van informatiebeveiliging te komen.

Integrale aanpak
Informatiebeveiliging is vanwege het belang voor de organisatie bij uitstek een onderwerp voor het bestuur. Beveiligingsrisico's moeten onderdeel zijn van het cyclische proces van strategisch risicomanagement, waarbij periodiek belangen, risico's en maatregelen worden geëvalueerd. Digitale beveiliging is daarbij slechts één dimensie waar de organisatie rekening mee moet houden. Een integrale aanpak kijkt ook naar dreigingen en kwetsbaarheden vanuit andere dimensies. Alleen al daarom is deze integrale aanpak nodig, waarbij gestreefd wordt naar synergie en samenwerking met disciplines zoals P&O, facilitaire zaken, financiën, communicatie en juridische zaken. Alleen door deze integrale aanpak kunnen de bestuurders 'in control' zijn over de veiligheid binnen NWO-I.

Kwaliteitscirkel
Voor het effectueren van informatiebeveiliging wordt gewerkt via de Plan Do Check Act cyclus. Na het vaststellen van wat nodig is, worden maatregelen getroffen en gecontroleerd of die maatregelen het gewenste effect sorteren (controle). Deze controle kan direct aanleiding geven tot bijsturing in de maatregelen. Ook kan het totaal van eisen, maatregelen en controle aan revisie toe zijn (evaluatie). Het goed doorlopen van deze kwaliteitscirkel zorgt op elk moment voor controle en verbetering van het beveiligingsniveau.

1.4 VERNIEUWING

Informatiebeveiliging is continu aan vernieuwing onderhevig. Het NWO-I informatiebeveiligingsbeleid wordt zo vaak als nodig – maar minimaal elke 3 jaar – vastgesteld door het stichtingsbestuur.

2 GOVERNANCE

NWO-I past het 'Three Lines' model voor risicobeheersing toe[1].

1ste lijn
De eerste lijn wordt gevormd door het Stichtingsbestuur en de lijnorganisatie. Het Stichtingsbestuur is eindverantwoordelijk voor de gehele risicobeheersing, stelt de risicobereidheid vast, monitort de effectiviteit van het informatiebeveiligingsmanagementsysteem en delegeert de verantwoordelijkheden, en middelen, om de beveiligingsdoelen te bereiken. Een van de leden van het Stichtingsbestuur neemt als portefeuillehouder Informatiebeveiliging deze verantwoordelijkheden op zich.

De lijnorganisatie (1e lijn) is waar de keuzes gemaakt worden om middelen in te zetten (tijd, geld) om organisatorische doelen te behalen en waar de proces- en systeemeigenaren zich bevinden. De lijnorganisatie opereert onder verantwoordelijkheid van de directie en rapporteert aan de Chief Information Security Officer (CISO) over de staat van informatiebeveiligingsrisicobeheersing, waaronder de hoogte en status van actuele informatiebeveiligingsrisico's, de status van de risicobehandelplannen en beveiligingsincidenten. De lijnorganisatie is verantwoordelijk voor de compliance aan interne beleidskaders, contractuele verplichtingen, ethische verplichtingen en geldende wet- en regelgeving. Als het volgens de lijnorganisatie nodig is om af te wijken van het informatiebeveiligingsbeleid of leidraden kan dat middels het exceptieproces (paragraaf 2.2).

Ieder instituut en het bureau NWO-I stelt een eigen Information Security Officer (ISO) aan die adviseert over de implementatie van het informatiebeveiligingsbeleid. De ISO is binnen het onderdeel het primaire aanspreekpunt voor het vertalen van de beveiligingsbeleidskaders in concrete acties, het toezien op de implementatie daarvan, het identificeren van risico's, de opvolging van risicobehandelplannen en het rapporteren over de staat van risicobeheersing aan de instituutsdirectie en de CISO. De ISOs en CISO overleggen regelmatig over trends, ondersteuningsbehoefte, beleidsverbeteringen, de samenwerking en algemene verbetermogelijkheden. De CISO is ervoor verantwoordelijk dat deze overleggen met voldoende frequentie plaatsvinden en de gewenste resultaten bereiken.

[1] https://www.iia.org.au/technical-resources/professionalGuidance/the-iia's-three-lines-model

Binnen de instituten is de ICT Manager verantwoordelijk voor het leveren van de IT-diensten en de daarbij behorende technische beveiligingsmaatregelen. De ICT Manager heeft daarmee veel uitvoeringsverantwoordelijkheden voor informatiebeveiliging. Ook is het de ICT Manager die de middelen heeft om technische maatregelen te implementeren om eventuele informatierisico's te mitigeren, ook als de risico's zelf niet technisch van aard zijn. De ICT Manager wordt daarom nauw betrokken bij de risicobeheersing binnen het instituut en proactief meegenomen bij de risico-identificatie en behandeling. De afhandeling van beveiligingsincidenten binnen het instituut gebeurt ook onder de verantwoordelijkheid van de ICT Manager.

2de lijn
De CISO is een onafhankelijke functionaris, die verantwoordelijk is voor het vertalen van de organisatiedoelen in het informatiebeveiligingsbeleid en leidraden. De CISO faciliteert en ondersteunt de lijnorganisatie in het nemen van hun verantwoordelijkheden. De positie van de CISO is die van adviseur en beleidsverantwoordelijke informatiebeveiliging op strategisch/tactisch niveau. De CISO rapporteert aan de directeur Bedrijfsvoering over de risico's en adequaatheid van de interne risicobeheersing en minimaal jaarlijks aan het Stichtingsbestuur. Het advies van de CISO moet ingewonnen zijn bij alle aangelegenheden die een potentieel grote impact kunnen hebben op de informatiebeveiliging van NWO-I.

3de lijn
De afdeling Internal Audit heeft de rol van 3e lijn en rapporteert onafhankelijk over de effectiviteit van de informatiebeveiligingsrisicobeheersing, zowel in de 1e als 2e lijn. Daarnaast heeft de CISO ook toezichthoudende verantwoordelijkheden en kan deze onderzoek uitvoeren of laten uitvoeren binnen de organisatie om de effectieve werking van het informatiebeveiligingsrisicomanagementsysteem te beoordelen. Ook de Functionaris Gegevensbescherming ziet toe op de gepaste organisatorische en technische beveiligingsmaatregelen waar dit de bescherming van persoonsgegevens betreft.

2.1 VERDELING VERANTWOORDELIJKHEDEN

Risico eigenaarschap
Het eigenaarschap van risico's hangt af van de hoogte van het restrisico. De hoogte van het restrisico wordt bepaald volgens het NWO Risicomanagementbeleid en hangt af van de mitigerende maatregelen die genomen worden. De eigenaar of een organisatorisch hoger gelegen functionaris volgens onderstaande tabel zijn bevoegd om restrisico's te accepteren:

Waardering restrisico	Risico-eigenaar
Zeer klein	Data-eigenaar
Klein	Proces- of systeemeigenaar
Groot	Instituutsmanager, Instituutsdirecteur, Directeur bedrijfsvoering
Zeer Groot	Stichtingsbestuur

De functionaris die de risico-eigenaar zou zijn op basis van het **initiële risico** (dus als er geen mitigerende maatregelen worden genomen) dient wel altijd geïnformeerd te worden over het risico en hoe het risico behandeld wordt.

2.2 EXCEPTIEPROCES

De lijnorganisatie is en blijft verantwoordelijk voor de gepaste risicobeheersing in het onderdeel, waarbij het principe geldt '**Pas toe of leg uit**'. Indien het nodig of wenselijk geacht wordt om van dit beleid, of de leidraden, af te wijken, dan dient daar melding van gemaakt te worden bij de CISO. Deze melding dient voorzien te zijn van een omschrijving met daarin van welk beleidskader afgeweken wordt, welke risico's dit met zich meebrengt, hoe deze risico's (eventueel) gemitigeerd worden en het restrisico van de uitzondering. De lijnorganisatie blijft zelf verantwoordelijk voor de behandeling van risico's. De CISO heeft hierbij een adviserende en signalerende functie als met de afwijking te grote risico's voor NWO-I genomen dreigen te worden.

3 VAN BELEID NAAR UITVOERING

In het informatiebeveiligingsbeleid worden ambitie en strategie van NWO-I op het gebied van informatiebeveiliging benoemd. De gevolgde strategie bij de implementatie van dit beleid wordt door de instituten uitgewerkt in 3-jarenplannen.

Tevens worden de strategische uitgangspunten weergegeven die als kapstok dienen voor het inhoudelijk beleidsraamwerk. Als vervolg hierop stelt de CISO 'leidraden' op die specificeren hoe specifieke beveiligingsonderwerpen binnen NWO-I georganiseerd dienen te worden gebaseerd op de geldende normenkaders (ISO 27000 serie), handreikingen van SURF en *best-practices* van andere (wetenschappelijke) instituten. Deze leidraden volgen eveneens het principe pas-toe-of-leg-uit. Ieder instituut implementeert deze leidraden in de eigen werkprocessen en ziet toe op de handhaving.

3.1 VERWANT BELEID

Het informatiebeveiligingsbeleid heeft relaties met aanverwante beleidskaders zoals het integriteitsbeleid, het personeelsbeleid, het ARBO-beleid, privacy beleid en het beleid op kennisveiligheid. Dit beleid implementeert het NWO Risicomanagementbeleid (22.0733) en het Rapport Governance informatiebeveiliging NWO-I (21.0763) tenzij anders aangegeven.

De verschillende beleidskaders hebben samenhang en de verschillende betrokken disciplines zijn binnen de organisatie vertegenwoordigd in de 'Commissie Integrale Veiligheid' die regelmatig bijeenkomt onder verantwoordelijkheid van de risicomanager voor integrale afstemming over de organisatiebrede risicobeheersing (*Enterprise Risk Management*) en om de gewenste synergie te bewerkstelligen.

3.2 LOPENDE INITIATIEVEN

Vooruitlopend op dit informatiebeveiligingsbeleid is NWO-I gedwongen geweest enkele initiatieven te nemen – onderweg naar gemiddeld volwassenheidsniveau 3 per eind 2025 – die naadloos passen binnen dit Informatiebeveiligingsbeleid:

- De invoering van het SURFsoc stelt instituten in staat bedreigingen te monitoren en alert te reageren wanneer dit tot incidenten leidt (principe 6: paraatheid; alerte detectie en response).
- De periodieke PEN-testen stekt de instituten in staat de technische kwetsbaarheden bloot te leggen en hier maatregelen op te nemen (principe 6: paraatheid; alerte detectie en response).
- De awarenesscampagne versterkt de kennis en het bewustzijn van de medewerkers (principe 2: Iedereen; informatiebeveiliging is een verantwoordelijkheid van iedereen).
- De door de instituten uit te voeren risicoanalyses is een belangrijke basis die randvoorwaardelijk is voor het prioriteren (principe 1: risico-gebaseerd; informatiebeveiliging is risico-gebaseerd).
- De aanstelling van de ISO's ten behoeve van de instituten stelt instituten in staat daadwerkelijk werk te maken van de informatiebeveiliging voor de eigen organisatie en ook voor de context keten waar de organisatieonderdeel van uitmaakt (principe 8: samenwerken; informatiebeveiliging is een gedeelde uitdaging).

4 DE NWO-I BEVEILIGINGSPRINCIPES

4.1 DE 8 PRINCIPES

De volgende principes zijn leidend en dienen als kapstok die in verdere leidraden door de CISO verdiept worden. In situaties dat er geen leidraad beschikbaar is kan de CISO specifieke gevallen toetsen tegen deze strategische principes. Een dergelijke toetsing van de CISO tegen dit beleid dient gezien te worden als een formele beleidsinterpretatie die ofwel opgevolgd moet worden of waarop het exceptieproces moet worden toegepast zoals ook geldt voor de rest van het informatiebeveiligingsbeleid.

Veel kennisinstellingen in Nederland hanteren een groot deel van dezelfde principes. Naast dat deze principes zorgvuldig tot stand zijn gekomen en *best-practices* zijn, zorgen we door dezelfde principes te volgen ook voor herkenbaarheid en congruentie met andere kennisinstellingen.

1	**Risico-gebaseerd** Informatiebeveiliging is risico-gebaseerd 
Kern	We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten.
Achtergrond	Het delen van kennis (openheid) is een belangrijke kernwaarde van het onderzoekproces. Voor een goede risicoafweging bij het beschermen van informatie en het treffen van de juiste maatregelen, is het van belang om de waarde van informatie vast te stellen. Als de waarde van informatie bekend is, kan ook de juiste mate van beveiliging worden bepaald, één die past bij de risico's. Proportionaliteit daarin is gewenst, ook om de beschikbare financiële middelen efficiënt te gebruiken ('Fit for purpose').

2	**Iedereen** Informatiebeveiliging is een verantwoordelijkheid van iedereen 
Kern	Iedereen is en voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.
Achtergrond	Iedereen is zich bewust van de waarde van informatie en handelt daarnaar. Deze waarde wordt bepaald door de mogelijke schade als gevolg van verlies van beschikbaarheid, integriteit of vertrouwelijkheid. Van zowel medewerkers als derden wordt verwacht dat ze bewust omgaan met informatie in welke vorm dan ook en dat ze actief bijdragen aan de veiligheid van de geautomatiseerde systemen en de daarin opgeslagen informatie. Het succes van beveiliging staat of valt met goede communicatie. Goede communicatie wordt daarom actief bevorderd, op en tussen alle niveaus in de organisatie.

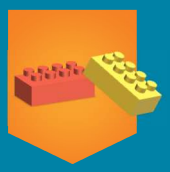
3	**Altijd** Informatiebeveiliging is een continu proces 
Kern	Informatiebeveiliging zit in het DNA van al onze werkzaamheden.
Achtergrond	De omgeving verandert continu: cyberdreigingen nemen toe en af, processen veranderen, medewerkers en studenten veranderen etc. Eenmalig de maatregelen bepalen en implementeren is onvoldoende om een veilig klimaat te behouden. Informatiebeveiliging heeft alleen zin als dit een continu proces is van het nemen van maatregelen, bewustzijn en controles.

4	**Security by Design** Integrale aanpak informatiebeveiliging 
Kern	Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering mbt informatie, processen en IT-faciliteiten.
Achtergrond	Security by design betekent dat al tijdens de start van een project, het ontwerp van een nieuwe applicatie of ICT-omgeving en bij technische of functionele veranderingen rekening wordt gehouden met de beveiliging van gegevens en de continuïteit van de processen. Dit voorkomt (vaak dure) herstelwerkzaamheden achteraf.

5	**Security by Default** Standaard beperkte toegang en veilige instellingen 
Kern	Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een bewuste keuze.
Achtergrond	Security by default betekent dat in elke configuratie die wordt geïmplementeerd de aanwezige security opties standaard aan staan. Dit voorkomt ongewenste en ongecontroleerde toegang tot (persoons)gegevens. Openstellen van informatie is daarmee altijd een bewuste keuze na een zorgvuldige afweging.

6	**Paraatheid** Alerte detectie en response 
Kern	In de wetenschap dat het altijd mis kan gaan zorgen we voor adequate detectie van mogelijke incidenten en dat we kundig kunnen reageren als deze zich voordoen.
Achtergrond	We moeten ervan uitgaan dat onze digitale muren doordringbaar zijn. Wij zullen dan ook het accent van de veiligheidsmaatregelen verschuiven van het steeds hoger maken van de muren (weerbaarheid) naar de capaciteit veerkrachtig op te kunnen treden. Detectie van en response op incidenten is van het grootste belang om passend en voortvarend te handelen wanneer NWO-I doelwit van in- of externe bedreigingen is.

7	**Veilig faciliteren** Van beveiligen naar veilig faciliteren 
Kern	Beveiligingsmaatregelen- en procedures hebben de naam belemmerend te zijn. Dit past niet goed meer bij onze hedendaagse manier van werken. De traditionele manier van inperken wordt waar mogelijk vervangen door een aanpak van veilig faciliteren.
Achtergrond	Bij het implementeren van beveiligingsmaatregelen streven we ernaar om de gebruikers zo min mogelijk hinder te laten ondervinden. De ervaring leert dat dit het draagvlak voor beheersmaatregelen verhoogt en ook een risico-verlagende werking heeft, doordat gebruikers minder gauw maatregelen via omwegen proberen te omzeilen.

8	**Samenwerken** Informatiebeveiliging is een gedeelde uitdaging 
Kern	Door ervaringen uit te wisselen en de samenwerking op te zoeken, zowel in- als extern, wordt het uiteindelijke resultaat voor iedereen beter. Informatiebeveiliging is geen *zero-sum game*, we beschermen ons tegen dezelfde dreigingen en samenwerking verhoogt onze succeskansen.
Achtergrond	Hoe zwakker de sector algemeen is, hoe makkelijker het voor kwaadwillenden zal zijn om in te breken en hoe interessanter onderzoeksinstellingen als doelwit zijn. Net als dat onderzoek ten goede komt van de maatschappij nemen we ook maatschappelijke verantwoordelijkheid door samenwerkingen op te zoeken voor de risicobeheersing, in de wetenschap dat als we onderling informatie delen dit meer voordelen zal bieden dan nadelen.

4.2 TOEPASSEN VAN DE PRINCIPES

De doorvertaling van de beveiligingsprincipes leiden tot de volgende beleidsregels (uitgangspunten):

- Informatieveiligheid draagt bij aan de realisatie van onze maatschappelijke opgaves en doelen op het gebied van onderzoek en bedrijfsvoering. Hierbij houden wij rekening met geldende wet- en regelgeving.
- Het inrichten van de informatievoorziening volgens dit beleid in opzet, bestaan en werking, geeft afdoende zekerheid voor onze digitale weerbaarheid.
- Het primaire uitgangspunt is risicomanagement. Wij hanteren een risicomanagementsystematiek conform de NEN-ISO 27001 waardoor wij continu risico's in beeld brengen, waar nodig passende beheersmaatregelen treffen en monitoren of de beheersmaatregelen over de tijd heen nog steeds effectief en efficiënt werken. De klassieke aanpak waarbij inperking van de mogelijkheden de boventoon voert, maakt plaats voor veilig en verantwoord faciliteren.
- Het beveiligingsniveau is in lagen uit te breiden. In de basis streven wij naar een gemiddeld volwassenheidsniveau 3 op basis van het SURF-toetsingskader. Waar nodig of vereist worden extra (specifieke) maatregelen getroffen boven op dit basisniveau. Een uitgevoerde risicoanalyse kan hiertoe aanleiding geven.
- Informatie wordt geclassificeerd om te bepalen welke beheersmaatregelen nodig en passend zijn. Hierbij is de aard van de informatie in de processen leidend. Er wordt geclassificeerd op de drie betrouwbaarheidsaspecten van informatie: Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). Op basis van een classificatie wordt bepaald hoe deze informatie behandeld dient te worden.
- Bij de start van projecten, het inrichten van processen en het inkopen of uitbesteden van diensten en systemen wordt een risicoanalyse vroegtijdig uitgevoerd. Er wordt een expliciet besluit genomen door de risico-eigenaar op de beheersing van de gevonden risico's en de opvolging van het advies.
- Het beleid is leidend en bepalend voor een adequate bescherming van de betrouwbaarheid van onze informatie bij samenwerkingen met leveranciers en andere (keten)partners met wie wordt samengewerkt. Er zijn afspraken gemaakt op het gebied van informatieveiligheid en op de naleving wordt toegezien.
- Structureel en planmatig wordt gewerkt aan het beveiligingsbewustzijn, waarbij de samenwerking met privacy en kennisveiligheid nauw wordt opgezocht.

- Het systeem van zelfregulering staat centraal, waarbij jaarlijks opzet, bestaan en werking van de beleidsregels worden geëvalueerd. Op basis hiervan wordt een verbeterplan opgesteld en wordt via de *Planning & Control*-cyclus verantwoording afgelegd door het Stichtingsbestuur aan de Raad van Toezicht. Er wordt gewerkt conform de *plan-do-check-act* verbetercyclus.
- We richten onze systemen in volgens *zero-trust*. Dit is een bekend beveiligingsmodel om moderne digitale omgevingen te beschermen.

5 DOCUMENTBEHEER

Voor vragen of opmerkingen over dit document kan contact opgenomen worden met pki-nwoi@nwo.nl (Privacy, Kennisveiligheid en Informatiebeveiliging).

6 VERSIEBEHEER

Versie	Personen	Datum	Actie
0.9	Stijn Hoogervorst (CISO)		Initiële versie
0.9	Mick Deben (ISO), Hans Bloemen (ISO), Erik van Loon (ISO)		Feedback
1.0	Stijn Hoogervorst (CISO)	12-03-2023	Tekstuele wijzigingen, portefeuillehouder vanuit stichtingsbestuur, verduidelijking 3 lines met plaatje, RACI, contactgegevens, versiebeheer en verklarende woordenlijst opgenomen.
1.1	Stijn Hoogervorst (CISO)	18-04-2023	Feedback verwerkt van IM overleg 24 maart
1.2	Stijn Hoogervorst (CISO)	02-05-2023	Feedback verwerkt van IM overleg 26 april

6.1 VERKLARENDE WOORDENLIJST

Afkorting	Definitie
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
CISO	Chief Information Security Officer
Informatiebeveiliging	Het proces van treffen, onderhouden en controleren van een samenhangend pakket van maatregelen om de vereiste betrouwbaarheid van informatie in termen van beschikbaarheid, integriteit en vertrouwelijkheid te borgen;
Informatiesysteem	Een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur, alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie;
ISO	Information Security Officer
ISO27001	Internationale standaard voor het inrichten van een managementsysteem voor informatiebeveiliging van de International Organization for Standardization
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationale Coördinator Terrorisme en Veiligheid
Proces	Een samenhangende serie handelingen met een overkoepelend doel uitgevoerd door personen of informatiesystemen, al dan niet ondersteund door één of meerdere informatiesystemen.