Dutch Institute for Vulnerability Disclosure

Informatiebeveiligings beleid

v1.0 – 26-05-2021

Dutch Institute for Vulnerability Disclosure

Colofon

Versie: 1.0

Datum: 26-05-2021

Auteur: Fleur van Leusden (Chief Information Security Officer)

In afstemming met: Bestuur en deelnemers DIVD

Vastgesteld door: Astrid Oosenbrug & Victor Gevers

Op datum: 26-05-2021

Versiebeheer

Datum	Versie	Auteur	Opmerkingen	Verstrekt aan
26-05-2021	1.0	Fleur van Leusden	Definitieve versie	Alle deelnemers DIVD en bestuur. Publicatie website.

Dutch Institute for Vulnerability Disclosure

Inleiding

In het informatiebeveiligingsbeleid staat hoe informatiebeveiliging binnen DIVD is ingericht. Het is een weergave van de verschillende rollen en verantwoordelijkheden en hoe de werkwijze en beleidsstructuur is opgebouwd.

Dit is noodzakelijk om te zorgen dat helder is wie verantwoordelijk is voor welke onderdelen op informatiebeveiligingsgebied en hoe de interne informatiebeveiliging is geborgd.

Dit beleid is voornamelijk bedoeld voor alle vrijwilligers van DIVD. Echter, aangezien DIVD streeft naar transparantie over eigen informatiebeveiliging is dit een openbaar beleid dat ook mag worden gedeeld met externen.

Dutch Institute for Vulnerability Disclosure

Inhoudsopgave

Dutch Institute for Vulnerability Disclosure

RACI/ Verantwoordelijkheidsmatrix Informatiebeveiliging DIVD

	Verantwoordelijk	Eindverantwoordelijk	Geraadpleegd	Geïnformeerd
Raad van Toezicht	-	-	O	X
Bestuur	X	X	O	X
CISO	X	O	X	X
Projectleiders	X	-	O	X
Onderzoekers/ vrijwilligers	X	-	O	X

X = altijd van toepassing

O = soms van toepassing, dat hangt af van het onderdeel

- = niet van toepassing

Rolverdeling

Hieronder staat de rolverdeling op informatiebeveiligingsgebied binnen DIVD nader toegelicht.

Bestuur

Het bestuur van DIVD is eindverantwoordelijk voor de interne informatiebeveiliging. Dat betekent dat zij verantwoording moeten afleggen aan de Raad van Toezicht bij incidenten en de het algehele reilen en zeilen wat betreft de interne informatiebeveiliging. Zij moeten werkwijzen en beleidsstukken goedkeuren en vaststellen. Tevens sturen zij de CISO en de projectleiders aan.

Chief Information Security Officer (CISO)

De Chief Information Security Officer (CISO) legt verantwoording af aan het bestuur. De CISO is verantwoordelijk voor:

- Up to date houden van de informatiebeveiligingsvisie en bijbehorende strategie
- Up to date houden van het informatiebeveiligingsbeleid
- Opstellen van een Vulnerability Disclosure beleid
- Toezicht houden op de uitvoering van de informatiebeveiligingsstrategie
- Toezicht houden op het opvolgen van vastgestelde werkwijzen en beleid door deelnemers
- Opstellen van veilige werkwijzen

- Zicht houden op gebruikte tooling en het signaleren wanneer deze moeten worden ge-update bij kwetsbaarheden
- Zicht houden op de (vertrouwelijke) data van DIVD
- Signaleren van risico's en deze melden bij de betreffende deelnemers/bestuur/raad van toezicht
- Afhandelen en coördineren bij informatiebeveiligingsincidenten
- Zorgen voor bewustwording en kennis binnen de stichting op het gebied van informatiebeveiliging

De CISO maakt ieder jaar een jaarplan waarin diens werkzaamheden staan. Het bestuur stelt dit jaarplan vast en geeft daarmee goedkeuring aan de door de CISO geplande werkzaamheden.

De CISO heeft het recht om op eigen inschatting te escaleren naar de Raad van Toezicht, als deze ernstige misstanden of risico's ziet waarvan de CISO van mening is dat het bestuur hier niet adequaat op reageert. De CISO dient hiervoor wel vooraf het bestuur op de hoogte te stellen dat deze zal gaan escaleren naar de Raad van Toezicht.

Wanneer de CISO ernstige misstanden of risico's signaleert tijdens onderzoeken, heeft de CISO het mandaat van het bestuur om onderzoeken (tijdelijk) stil te laten leggen.

De CISO werkt nauw samen met de Functionaris Gegevensbescherming bij datalekken en privacy aangelegenheden. De CISO is echter niet verantwoordelijk voor naleving van de AVG en bijbehorende taken en verantwoordelijkheden.

Projectleiders

Projectleiders zijn verantwoordelijk voor het aansturen op het volgen van vastgestelde werkwijzen aan onderzoekers en vrijwilligers tijdens de onderzoeken waar zij projectleider van zijn. Wanneer zij signaleren dat onderzoekers niet conform beleid of werkwijzen werken, dienen zij hen hierop te wijzen.

Wanneer projectleiders ernstige misstanden of risico's signaleren op informatiebeveiligingsgebied signaleren informeren zij de CISO en/of het bestuur zo snel mogelijk.

Zij dragen er zorg voor dat incidenten zo snel mogelijk worden gemeld bij de CISO.

Onderzoekers en vrijwilligers

Onderzoekers en vrijwilligers zijn verantwoordelijk voor het veilig omgaan met de (vertrouwelijke) informatie van DIVD. Zij dienen hierbij de code of conduct, vastgestelde werkwijzen en beleid op te volgen. Indien dit niet mogelijk is, dienen zij hiervoor advies te vragen bij hun projectleider of de CISO.

Wanneer een onderzoeker zich niet houdt aan interne regels, kan een projectleider/CISO/bestuurslid in gesprek gaan met de onderzoeker hierover. Wanneer een onderzoeker voornemens is om data die de onderzoeker heeft verzameld binnen de context van DIVD te gebruiken, dan dient de data ook verzameld te zijn volgens de interne regels van DIVD. De onderzoeker heeft daarin een zekere vrijheid om binnen te bewegen en keuzes te maken, maar wel binnen de vastgestelde kaders.

Wanneer zij ernstige misstanden of risico's signaleren op informatiebeveiligingsgebied informeren zij de CISO en/of het bestuur zo snel mogelijk.

Zij melden incidenten zo snel mogelijk bij de CISO en hun projectleider. Zij volgen bij incidenten de instructies op van de CISO en/of hun projectleider.

Dutch Institute for Vulnerability Disclosure

Welk beleid en/of stukken zijn er en wie is daar verantwoordelijk voor

DIVD kent een aantal beleidsstukken en werkwijzen op informatiebeveiligingsgebied. Deze staan hieronder genoemd met daarbij een korte omschrijving alsook wie er verantwoordelijk voor is.

Informatiebeveiligingsvisie

De informatiebeveiligingsvisie verwoordt de visie van DIVD op hoe de stichting omgaat met de eigen informatiebeveiliging en welke uitgangspunten moeten worden gebruikt voor alle beleid en werkwijzen die worden vastgesteld.

De CISO is verantwoordelijk voor het opstellen van de informatiebeveiligingsvisie. Het bestuur is verantwoordelijk voor het goedkeuring van de visie. De Raad van Toezicht stelt de visie vast.

Informatiebeveiligingsstrategie

De informatiebeveiligingsstrategie is een uitwerking van hoe de visie in de praktijk dient te worden gebracht. Hoe gaat DIVD invulling geven aan de uitgangspunten uit de visie? Dat staat weergegeven in de strategie.

De CISO is verantwoordelijk voor het opstellen van de informatiebeveiligingsstrategie. Het bestuur is verantwoordelijk voor het vaststellen van de strategie.

Informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid geeft weer wat de verschillende rollen en verantwoordelijkheden zijn op informatiebeveiligingsgebied en hoe de informatiebeveiliging is ingericht.

De CISO is verantwoordelijk voor het opstellen van het informatiebeveiligingsbeleid. Het bestuur is verantwoordelijk voor het vaststellen van het informatiebeveiligingsbeleid.

Logisch toegangsbeleid

In het logisch toegangsbeleid is onderdeel van het Identity & Access Management (IAM). In dit beleid staat hoe DIVD omgaat met de toegang tot alle gebruikte (gedeelde) systemen.

De Identity en Access management expert is verantwoordelijk voor het logisch toegangsbeleid. De CISO zorgt dat deze up to date blijft en conform de visie en strategie is opgesteld. Het bestuur is verantwoordelijk voor het vaststellen van het logisch toegangsbeleid.

Toolkit

De toolkit is een inventarisatie van alle gebruikte software door DIVD zowel bij onderzoek als interne bedrijfsvoering. Deze toolkit kan worden gebruikt om inzicht te krijgen in gebruikte tooling en is voor de CISO belangrijk om deelnemers tijdig te kunnen informeren bij nieuwe kwetsbaarheden en belangrijke updates.

De CISO is verantwoordelijk voor het up to date houden van de toolkit. Deelnemers van DIVD dienen bij het gebruik van een nieuwe tool om deze in de toolkit te zetten of de CISO op de hoogte te stellen.

Dataopslag inventarisatie

De dataopslag inventarisatie houdt bij welke data DIVD heeft en waar deze op verschillende momenten is opgeslagen. Tevens staat er weergegeven of het (mogelijk) om persoonsgegevens gaat. Dit document is belangrijk om zicht te krijgen op welke data DIVD heeft en hoe deze beveiligd is. Bij

datalekken is het handig om te zien waar data zich op welk moment mogelijk heeft bevonden en wie er mogelijk betrokkenen zijn.

De CISO is verantwoordelijk voor het up to date houden van de dataopslag inventarisatie. Deelnemers van DIVD dienen de CISO op de hoogte te stellen als zij data ergens anders opslaan dan in de huidige versie staat en als zij typen data gaan verwerken.

Vulnerability Disclosure Beleid

In het Vulnerability Disclosure beleid staat wat wij verwachten van personen die kwetsbaarheden van DIVD bij ons komen melden. Er staat praktische informatie in over waar meldingen kunnen worden gedaan en hoe wij deze het liefst ontvangen. Verder staat er in hoe DIVD omgaat en reageert op meldingen.

De CISO is verantwoordelijk voor het opstellen van het Vulnerability Disclosure beleid. Het bestuur stelt het Vulnerability Disclosure beleid vast.

Uitzonderingen op beleid

Wanneer van vastgesteld beleid of werkwijzen afgeweken moet worden, dient dit altijd volgens de volgende voorwaarden te gebeuren:

- De CISO dient hiervan zo snel als mogelijk op de hoogte te worden gesteld. Dat betekent in gevallen waarin dat mogelijk is, met werkzaamheden gewacht dient te worden totdat de CISO op de hoogte is gesteld.
- De CISO dient indien mogelijk vooraf goedkeuring te verlenen voor de uitzondering. Hierbij kan de CISO besluiten het bestuur te betrekken bij de beslissing.
- Indien goedkeuring vooraf niet kan worden afgewacht, dan dient zo goed mogelijk te worden vastgelegd welke afwijkingen zijn toegepast en waarom. Zodat de CISO achteraf kan toetsen of de uitzondering terecht is toegepast.
- De CISO dient een gemotiveerde goedkeuring of afkeuring aan de aanvrager te geven en een afschrift hiervan aan het bestuur te sturen ter informatie.
- Het bestuur heeft het recht om tegen de beslissing van de CISO in te gaan en een uitzondering alsnog goed te keuren of af te keuren. Een bestuurslid mag niet zijn/haar eigen aanvraag goedkeuren of afkeuren.
- Uitzonderingen zijn per definitie tijdelijk van aard. Er dient afgesproken te worden en vastgelegd welke uitzonderingen zijn toegestaan, met motivatie en de duur waarvoor de uitzondering is toegestaan.
- Als een uitzondering voor langere tijd of definitief blijkt, dient het bijbehorende beleid of werkwijze te worden aangepast. Zodat het niet langer een uitzondering is.

Auditing

De CISO is verantwoordelijk voor het toezicht op alle informatiebeveiligingsstukken. Om dit effectief te kunnen doen mag de CISO gevraagd en ongevraagd deelnemers onderwerpen aan een audit. Deelnemers dienen de CISO bij een audit toegang te geven tot alle informatie en stukken waar deze om vraagt.

De CISO audit minimaal één informatiebeveiligingsstuk per kalenderjaar.

De CISO zorgt dat bij elke audit een rapportage met bevindingen wordt opgesteld en deze zal worden gedeeld met de betrokken deelnemers en het bestuur. Het bestuur besluit of het rapport met alle deelnemers wordt gedeeld en welk vervolg zij geven aan de rapportages.