**Responsible Disclosure**

**model mbo, vs 2.0**

****

**IBPDOC27**

Verantwoording

**Bron:**

**Starterkit Informatiebeveiliging**

*Stichting SURF*

*Februari 2015*

**Floor Terra**, Responsibledisclosure.nl

**SCIPR**

SCIPR is een community of practice binnen de SURF samenwerkingsorganisatie met als doelen het actief stimuleren van en richting geven aan informatiebeveiliging en privacy binnen het hoger onderwijs en onderzoek (universiteiten, hogescholen, wetenschappelijk onderzoek en universitair medische centra). Dat wordt bereikt door het bevorderen van de samenwerking tussen informatiebeveiligers/kwartiermakers ib en privacy en het leveren van praktisch bruikbare adviezen.

Voor meer informatie zie [www.scipr.nl](http://www.scipr.nl)

**Bewerkt door:**

Kennisnet / saMBO-ICT

**Auteurs/review**

Kiki de Bondt (Kennisnet)

Ludo Cuijpers (saMBO-ICT)

Leo Bakker (Kennisnet)

Job Vos (Kennisnet)

Versie 2.0, september 2017

**Sommige rechten voorbehouden**

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s) en uitgever van Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden.

**Creative commons**

[](http://www.google.nl/url?sa=i&source=images&cd=&cad=rja&uact=8&ved=0CAgQjRw&url=http://creativecommons.org/about/downloads&ei=ViUYVb6yHcbWPPKhgMAM&psig=AFQjCNFD0SQUbum02GpIZCKN9_e8blqrwQ&ust=1427732182559562)Naamsvermelding 3.0 Nederland

(CC BY 3.0)

**De gebruiker mag:**

* Het werk kopiëren, verspreiden en doorgeven
* Remixen – afgeleide werken maken

**Onder de volgende voorwaarde:**

* Naamsvermelding – De gebruiker dient bij het werk de naam van Kennisnet te vermelden (maar niet zodanig dat de indruk gewekt wordt dat zij daarmee instemt met uw werk of uw gebruik van het werk).

Vooraf:

Voor het opzetten van beleid voor Responsible Disclosure is altijd verwezen naar de documentatie van SURF in deze. De verwijzing naar deze documenten vind je nog steeds hieronder.

Intussen is er op basis van een ontwerp van Floor Terra van responsibledisclosure.nl een nieuw model gemaakt door Kiki de Bondt (Kennisnet). Dit model bestaat uit twee delen, een voor medewerkers en één voor studenten. Dit model is voor het mbo zeer goed bruikbaar en wordt hieronder weergegeven.

**Model Responsible Disclosure voor medewerkers**

Bij <schoolbestuur> vinden wij de veiligheid van onze informatiesystemen (internet en bijbehorende hardware en software) erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek (kwetsbaarheid) is. Als u een zwakke plek in één van onze systemen heeft gevonden, dan horen wij dit graag, zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met u samenwerken om onze gebruikers en onze systemen beter te kunnen beschermen.

**Wij vragen u:**

* Uw bevindingen te mailen naar security@<schoolbestuur>.nl of telefonisch contact op te nemen met onze <security officer>,
* De kwetsbaarheid niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of (persoons)gegevens van derden in te kijken, verwijderen of aan te passen,
* De kwetsbaarheid niet met anderen te delen totdat deze is verholpen en alle (vertrouwelijke) gegevens die zijn verkregen via de lek direct na het verhelpen van de lek te wissen,
* Geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden, en
* Voldoende informatie te geven om het probleem te reproduceren zodat wij het zo snel mogelijk kunnen verhelpen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.

**Wij zeggen toe dat:**

* Wij reageren binnen 3 dagen op uw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing,
* Als u zich aan bovenstaande voorwaarden heeft gehouden zullen wij geen juridische stappen tegen u ondernemen betreffende de melding\*,
* Wij behandelen uw melding vertrouwelijk en zullen uw persoonlijke gegevens niet zonder uw toestemming met derden delen tenzij dat noodzakelijk is om een wettelijke verplichting na te komen. Melden onder een pseudoniem is mogelijk,
* (Optioneel) Wij kunnen u een beloning geven voor uw onderzoek. We zijn daartoe echter niet verplicht. U heeft dus niet zonder meer recht op een vergoeding. De vorm van deze beloning staat niet van tevoren vast en zal door ons per geval worden bepaald. Of we een beloning geven en vorm van de beloning hangt af van de zorgvuldigheid van uw onderzoek, de kwaliteit van de melding en ernst van het lek,
* Wij houden u op de hoogte van de voortgang van het verhelpen van de kwetsbaarheid, en
* In berichtgeving over het gemelde probleem zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker. Wij streven er naar om alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.

\* Let op: ons beleid voor responsible disclosure is geen uitnodiging om ons netwerk uitgebreid te scannen om zwakke plekken te ontdekken. Er bestaat een kans dat u tijdens uw onderzoek handeling uitvoert die volgens het strafrecht strafbaar zijn. Het feit dat <schoolbestuur> geen aangifte tegen u zal doen sluit niet uit dat er een strafrechtelijk onderzoek naar uw handelen gehouden kan worden dan wel dat u strafrechtelijk kunt worden veroordeeld.

Cc/by/3.0 NL

Geschreven door Floor Terra (responsibledisclosure.nl), bewerkt door Kennisnet en <schoolbestuur>.

**Model Responsible Disclosure voor leerlingen**

Bij <schoolbestuur> vinden wij de veiligheid van onze informatiesystemen (internet en bijbehorende hardware en software) erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek (kwetsbaarheid) is. Als jij een zwakke plek in één van onze systemen hebt gevonden, dan horen wij dit graag, zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met jou samenwerken om de leerlingen, medewerkers en onze systemen beter te kunnen beschermen.

**Wij vragen jou:**

* Je bevindingen te mailen naar security@<schoolbestuur>.nl of deze door te geven aan je <mentor>. Jouw <mentor> zal je vervolgens in contact brengen met onze <security officer>,
* De kwetsbaarheid niet te misbruiken door bijvoorbeeld meer informatie te downloaden dan nodig is om het lek aan te tonen of informatie van andere leerlingen, docenten of andere medewerkers in te kijken, verwijderen of aan te passen,
* De kwetsbaarheid niet met anderen te delen totdat deze is verholpen en alle informatie die verkregen is via de lek direct na het verhelpen van de lek te wissen,
* Geen gebruik te maken van aanvallen op de beveiliging van de school, en
* De school voldoende informatie te geven om het probleem te kunnen vinden zodat wij het zo snel mogelijk kunnen verhelpen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.

**Wij beloven dat:**

* Je binnen 3 dagen van ons te horen krijgt hoe we de kwetsbaarheid gaan oppakken en wanneer wij hiervoor een oplossing verwachten,
* Als je de kwetsbaarheid netjes gemeld hebt en via de bovenstaande stappen gehandeld hebt, zullen wij geen melding maken bij de politie\*,
* Wij jouw melding vertrouwelijk behandelen en dat jouw persoonlijke gegevens niet zonder jouw toestemming met anderen delen worden tenzij dit wettelijke verplicht is,
* (Optioneel) Als je de kwetsbaarheid gemeld hebt volgens bovenstaande stappen, je ter beloning een taart van de school ontvangt,
* Wij je op de hoogte houden van de voortgang van het verhelpen van de kwetsbaarheid.

\* Let op: ons beleid voor responsible disclosure is geen uitnodiging om ons netwerk uitgebreid te scannen om zwakke plekken te ontdekken. Er bestaat een kans dat je tijdens jouw onderzoek handelingen uitvoert die strafbaar zijn. Het feit dat <schoolbestuur> geen aangifte tegen je zal doen sluit niet uit dat er een strafrechtelijk onderzoek naar jouw handelen gehouden kan worden dan wel dat je strafrechtelijk kunt worden veroordeeld.

Cc/by/3.0 NL

Geschreven door Floor Terra (responsibledisclosure.nl), bewerkt door Kennisnet en <schoolbestuur>.

Verwijzing naar documenten SCIPR

Oorspronkelijk is steeds verwezen naar de documentatie die in het hoger onderwijs wordt gebruikt en die door de ibp community van het hoger onderwijs, SCIPR in beheer wordt gehouden. De verwijzing naar deze documentatie is hieronder weergegeven:

Modelbeleid en procedure responsible disclosure

Implementatie handleiding responsible disclosure

**Bijlage: Framework informatiebeveiliging en privacy in het mbo**

