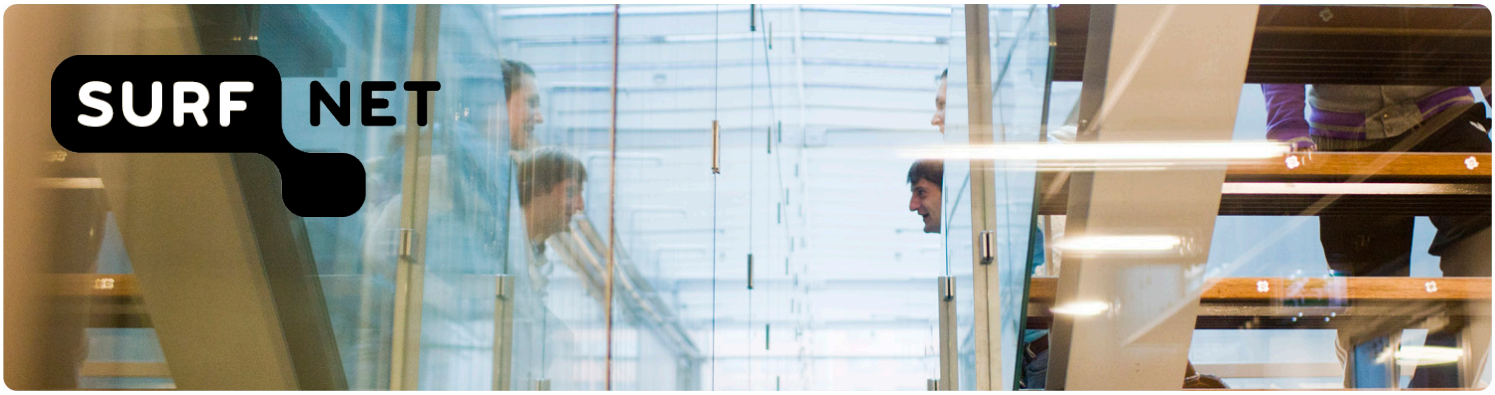


Modelbeleid en procedure responsible disclosure hoger onderwijs

Auteur(s):	SURFnet
Versie:	1.0
Datum:	9 april 2014

Moreelsepark 48
3511 EP Utrecht

Postbus 19035
3501 DA Utrecht

088 - 787 30 00
admin@surfnet.nl
www.surfnet.nl

ING Bank NL54INGB0005936709
KvK Utrecht 30090777
BTW NL 0089.60.173.B01

Inhoudsopgave

Definities **3**

1 Aanleiding **3**

2 Doel responsible disclosure **3**

3 Beleid responsible disclosure **4**

4 Procedure responsible disclosure **6**

4.1 Uitgangspunten 6
4.2 Rollen en verantwoordelijkheden 6
4.3 Ontvangen melding 6
4.4 Identificatie kwetsbaarheid 7
4.5 Beëindiging onderzoek 8
4.6 Bevestigen validiteit 8
4.7 Schade indamming en beoordeling blootstelling 8
4.8 Remediatie en herstel 8
4.9 Openbaar maken 8
4.10 Informeren betrokkenen 8
4.11 Belonen melder 9
4.12 Publiceren 9
4.13 Rapportage en evalueren 9

5 Versiebeheer, revisies **10**

6 Bronnen **10**

6.1 Beleid 10
6.2 Procedure 10

Bijlage A: Flowchart proces responsible disclosure **11**

Bijlage B: Beveiligingsadvies **12**

Definities

A. Responsible disclosure is het op een verantwoorde wijze en in gezamenlijkheid tussen melder en organisatie openbaar maken van kwetsbaarheden op basis van een door organisaties hiervoor vastgesteld beleid voor responsible disclosure.
B. Een kwetsbaarheid is een (vermoedelijke) zwakte in of inbreuk op de beveiliging van de infrastructuur of ICT-systeem van <<INSTELLING>>.
C. De melder is de persoon of instantie die die via responsible disclosure een kwetsbaarheid meldt.
D. De organisatie, <<INSTELLING>>, is de eigenaar en/of beheerder van het systeem en de ontvanger van de responsible disclosure melding.
E. Het responsible disclosure beleid is het document waarin de spelregels zijn waaraan de melder en organisatie zich moeten houden. Zie hoofdstuk 3.
F. De responsible disclosure procedure is de procedure waarin de verantwoordelijkheden en operationele acties voor responsible disclosure zijn beschreven. Zie hoofdstuk 4.

1 Aanleiding

Uit voorbeelden uit de praktijk (zoals de zaak Henk Krol[1] en de melding over het netwerk van KPN door ethische hackers[2]) blijkt dat het belangrijk is voor organisaties om een responsible disclosure beleid uit te dragen. Voor zowel de organisatie als voor de melder schept het duidelijkheid in de verantwoordelijkheden die beide partijen hebben.

<<INSTELLING>> heeft besloten om een responsible disclosure beleid en procedure te ontwerpen en deze toe te passen voor haar eigen organisatie. Het model voor beleid en procedure wordt vervolgens beschikbaar gesteld aan hoger onderwijsinstellingen.

2 Doel responsible disclosure

Het kan natuurlijk gebeuren dat een zwakheid in een product of dienst over het hoofd gezien wordt door de organisatie, die door iemand anders wel wordt opgemerkt. <<INSTELLING>> vindt het daarom belangrijk om meldingen van kwetsbaarheden aan te nemen en samen te werken (eventueel met de melder) om die kwetsbaarheden te verhelpen. Op deze wijze kan het niveau van informatiebeveiliging verhoogd worden en kan schade worden voorkomen.

Veiligheid en het voorkomen van schade staat voorop. Daarom wil <<INSTELLING>> de kwetsbaarheid oplossen voordat deze extern bekend gemaakt wordt. De melder moet <<INSTELLING>> dus voldoende tijd geven om het lek te dichten voordat de kwetsbaarheid eventueel openbaar kan worden.

Door het opstellen van een beleid voor responsible disclosure kan een deel van de onduidelijkheid omtrent vervolging weggenomen worden. Het responsible disclosure beleid zorgt ervoor dat er spelregels zijn voor de melder en voor <<INSTELLING>>. Hierbij is het wel van belang om te melden

[1] Rechtbank Oost-Brabant (2013), *Vonnis zaak Henk Krol*. Geraadpleegd via http://www.rechtspraak.nl/Organisatie/Rechtbanken/Oost-Brabant/Nieuws/Documents/eindhovenaar%20vonnis%20anoniem.pdf
[2] KPN (2013), *Ethisch hackersbeleid helpt KPN*. Geraadpleegd via http://corporate.kpn.com/kpn-actueel/nieuwsberichten-1/ethisch-hackersbeleid-helpt-kpn.htm

dat het OM en een eventuele betrokken derde partij (zoals een student of webhoster) altijd zelfstandig over kan gaan tot juridische stappen, ongeacht de inhoud van het beleid van de organisatie.

3 Beleid responsible disclosure

Het responsible disclosure beleid geeft de spelregels aan voor de melder en geeft aan wat er van de organisatie verwacht kan worden. Om de melder en het publiek de juiste verwachtingen te geven wordt het beleid gepubliceerd op de website. Het beleid hangt samen met de responsible disclosure procedure. De procedure is te vinden in hoofdstuk 4.

Het beleid is gebaseerd op het voorbeeldbeleid van Floor Terra.

---------- Beleid zoals te publiceren op website ----------

Bij <<INSTELLING>> vinden wij de veiligheid van onze systemen erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek is.

Als u een zwakke plek in één van onze systemen heeft gevonden horen, 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.

Ons beleid voor responsible disclosure is geen uitnodiging om ons universiteitsnetwerk uitgebreid actief te scannen om zwakke plekken te ontdekken. Wij monitoren ons bedrijfsnetwerk. Hierdoor is de kans groot dat een scan wordt opgepikt, dat er door onze CERT onderzoek wordt gedaan en er mogelijk onnodige kosten worden gemaakt.

Er bestaat een kans dat u tijdens uw onderzoek handeling uitvoert die volgens het strafrecht strafbaar zijn. Als u zich aan de onderstaande voorwaarden heeft gehouden zullen wij geen juridische stappen tegen u ondernemen betreffende de melding. Het Openbaar Ministerie behoudt altijd het recht om zelf te beslissen of u strafrechtelijk vervolgt wordt. Het Openbaar Ministerie heeft hierover een beleidsbrief (http://www.om.nl/@161174/beleid-ethische/) gepubliceerd.

Wij vragen u:

Uw bevindingen zo snel mogelijk te mailen naar security@<<Instelling>>.nl. Versleutel uw bevindingen met onze PGP key (fingerprint <invullen>) om te voorkomen dat de informatie in verkeerde handen valt.

De zwakheid niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of door het veranderen of verwijderen van gegevens en extra terughoudendheid te betrachten bij persoonsgegevens.

De zwakheid niet met anderen te delen totdat het is opgelost.

Geen gebruik te maken van aanvallen op fysieke beveiliging of applicaties van derden, van social engineering, distributed denial-of-service, of spam.

Voldoende informatie te geven om de zwakheid te reproduceren zodat wij het zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid en de uitgevoerde handelingen voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.

Wat wij beloven:

Wij reageren binnen 3 werkdagen op uw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing,

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.

Wij houden u op de hoogte van de voortgang van het oplossen van de zwakheid.

Anoniem of onder een pseudoniem melden is mogelijk. Het is voor u goed om te weten dat dit wel betekent dat wij dan geen contact kunnen opnemen over bijvoorbeeld de vervolgstappen, voortgang van het dichten van het lek, publicatie of de eventuele beloning voor de melding.

In berichtgeving over de gemelde zwakheid zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker van de kwetsbaarheid.

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 streven er naar om alle problemen zo snel mogelijk op te lossen, alle betrokken partijen op de hoogte te houden en wij worden graag betrokken bij een eventuele publicatie over de zwakheid nadat het is opgelost.

---------- Einde beleid ----------

4 Procedure responsible disclosure

Het responsible disclosure beleid hangt samen met de responsible disclosure procedure. Het beleid is te vinden in hoofdstuk 3. De stroomdiagram van deze procedure is te vinden in bijlage A.

4.1 Uitgangspunten

A. <<INSTELLING>> stelt een beleid en procedure voor responsible disclosure vast en publiceert beleid en procedure op haar website. Beleid en procedure zijn te bereiken via http://www.<<Instelling>>.nl/security.
B. De organisatie reserveert capaciteit om adequaat op meldingen te kunnen reageren. Met name incidentafhandeling en mandaat van de procesverantwoordelijke vergen extra aandacht.
C. De informatiebeveiliging die wordt toegepast op de meldingen is gelijk aan de standaard die wordt gehanteerd bij vertrouwelijke informatie, tenzij dit niet noodzakelijk blijkt na inschaling van de melding.
D. Wederzijds vertrouwen is de basis van responsible disclosure, vooral in het geval van een langlopende behandeling van de kwetsbaarheid. De organisatie moet de melder en overige betrokkenen met regelmaat op de hoogte houden van de voortgang van het proces. Grote wijzigingen in de voortgang moeten aan de melder worden aangegeven omdat deze impact kunnen hebben op de publicatie van de melder.
E. Als de melder zich houdt aan de spelregels zoals gesteld in het responsible disclosure beleid worden er door <<INSTELLING>> geen juridische (vervolg)stappen ondernomen. Als blijkt dat de melder zich niet conform de spelregels heeft gehandeld, kunnen er alsnog juridische vervolgstappen worden ondernomen.
F. Responsible disclosure en het niet naleven van de spelregels van responsible disclosure kunnen vergaande juridische implicaties hebben voor de organisatie en melder. Tijdige juridische consultatie door een bedrijfsjurist bij civielrechtelijke, strafrechtelijke en privacyvraagstukken is daarom essentieel.
G. Responsible disclosure is primair een zaak tussen de melder en de eigenaar/beheerder van het systeem. Meldingen over een systeem van derden kunnen niet behandeld worden door <<INSTELLING>>.
H. Indien mogelijk moeten er afspraken gemaakt worden met leveranciers van goederen en diensten waarop de responsible disclosure procedure eventueel betrekking tot heeft.

4.2 Rollen en verantwoordelijkheden

A. <<INSTELLING>>cert is verantwoordelijk voor het doorzetten van meldingen van kwetsbaarheden naar de juiste Security Officier van de werkmaatschappij. <<INSTELLING>>cert kan advies bieden bij het oplossen van de kwetsbaarheid en kan betrokken partijen informeren over een kwetsbaarheid.
B. Security Officer: De Security Officer van de werkmaatschappij waar de kwetsbaarheid zich bevindt is verantwoordelijk voor het bewaken van de procesvoortgang en het onderzoeken en verhelpen van de kwetsbaarheid. Daarnaast is onderhoudt de Security Officer het contact met de melder.
C. De communicatieafdeling kan de Security Officer steunen bij de communicatie met de melder en wordt betrokken bij publicatie van een kwetsbaarheid.
D. De centrale telefoniste en IT-helpdesk van de werkmaatschappij moeten op de hoogte zijn van de responsible disclosure procedure en moeten een melder kunnen verwijzen naar <<INSTELLING>>cert in het geval een melding binnenkomt bij de centrale telefoniste of IT-helpdesk.
E. De melder is verantwoordelijk voor het eigen handelen en heeft zich te houden aan de spelregels zoals die zijn gesteld in het responsible disclosure beleid van de organisatie.

4.3 Ontvangen melding

A. Een melding over een kwetsbaarheid komt binnen via e-mail. Meldingen via e-mail komen binnen op security@<<Instelling>>.nl en dienen te worden versleuteld met de bijbehorende openbare PGP sleutel.

B. De melding kan anoniem, onder een pseudoniem of via een tussen-/vertrouwenspersoon gedaan worden. Dit kan betekenen dat er geen communicatie mogelijk is met de melder.
C. Er wordt door <<INSTELLING>>cert een ontvangstbevestiging van de melding gestuurd naar de melder. Dit is geen bevestiging van de validiteit van het lek maar bevestiging van de start van het onderzoek.
D. <<INSTELLING>>cert zorgt er voor dat de melding zo snel mogelijk terecht komt bij de afdeling die de melding het beste kan beoordelen en in behandeling kan nemen en er wordt bij <<INSTELLING>>cert een ticket aangemaakt.

4.4 Identificatie kwetsbaarheid

A. Binnen drie werkdagen stuurt de Security Officer een digitaal ondertekende ontvangstbevestiging van de melding van de kwetsbaarheid. In de e-mail staat minimaal:
    a) De bevestiging van de melding
    b) Een eerste inschatting van legitimiteit en ernst van de gemelde kwetsbaarheid
        a. Er dient een inschatting te worden gemaakt van de legitimiteit en ernst van de gemelde kwetsbaarheid. Daaruit komt een termijn waarop de kwetsbaarheid verholpen wordt. Standaardtermijnen voor kwetsbaarheden zijn 60 dagen in configuratie en software en 6 maanden in hardware.
    c) Eventuele vervolgstappen voor het traject
    d) Eventuele behandeltermijn voor het oplossen van het lek.
B. De Security Officer probeert de mogelijke kwetsbaarheid te verifiëren. Als er sprake is van een melding van een kwetsbaarheid in niet meer ondersteunde software, service of website, moet er worden vastgesteld of deze kwetsbaarheid zich niet ook bevindt in andere, wél ondersteunde producten of diensten. Daarnaast zal; een inschatting gemaakt moeten worden of deze zelfde kwetsbaarheid ook bij andere organisaties, binnen of buiten de sector , zou kunnen voorkomen en dienen betrokkenen via de daartoe geëigende kanalen ingelicht te worden.
C. De prioritering moet worden vastgesteld. Deze wordt herleid uit een tweetal factoren: urgentie en impact. De prioritering die moet worden gevolgd is de incident prioritering uit het ‘Draaiboek informatiebeveiligingsincidenten’. Bij een prioriteringsklasse van medium of hoger moet de Corporate Security Officer worden betrokken bij het onderzoek.
D. Er moet een eerste inschatting gemaakt worden of de melder zich heeft gehouden aan de spelregels uit het beleid. Als er mogelijk sprake is van overtreding van de spelregels moet de Corporate Privacy Officer worden ingeschakeld voor een juridische beoordeling.
E. Bij het bepalen van een prioritering van de melding moet rekening worden gehouden met de informatie die op dat moment beschikbaar is. Hieronder kunnen de volgende aspecten worden overwogen:
    a) **De agenda van de melder**: De melder kan van plan zijn om de kwetsbaarheid openbaar te maken via een bijvoorbeeld een onderzoeksverslag of een presentatie tijdens een conferentie. De organisatie moet de kwetsbaarheid openbaar maken voor of direct na de openbaarmaking door de melder. De organisatie moet dus op de hoogte zijn van de gewenste publicatiedatum van de melder.
    b) **Algemene kennis over de kwetsbaarheid**: Als de kwetsbaarheid algemeen bekend is de kans groter dat de kwetsbaarheid uitgebuit zal worden.
    c) **Het karakter van mogelijke aanvallen**: De kosten en de slaagkans van een aanval hangen af van de kwetsbaarheid die moet worden uitgebuit. Kwetsbaarheden met lage aanvalskosten en hoge slaagkans moeten snel worden opgelost.
    d) **Het bestaan en volwassenheid van aanvalsmiddelen**: Wanneer er goedwerkende methodes beschikbaar zijn om gebruik te maken van de kwetsbaarheid, kunnen er aanvalstools ontwikkeld worden.
    e) **Het karakter van potentiele schade**: Het karakter van het product en de potentiele schade bepalen de ernst voor de gebruikers. Een kwetsbaarheid in een intranet kan bijvoorbeeld grote impact hebben door het lekken van persoonlijke informatie.
    f) **Bewijzen van aanvallen (incidenten)**: Incidenten waarbij de kwetsbaarheid wordt uitgebuit kunnen wijzen op een vergroot risico voor de gebruikers. Afhankelijk van de beschikbare

informatie kan er een tijdelijke oplossing worden ontwikkeld, ook als er nog geen complete oplossing beschikbaar is.

4.5 Beëindiging onderzoek

Er zijn verschillende mogelijkheden waarop een onderzoek kan worden afgerond. De melder moet op de hoogte worden gesteld waarom het onderzoek wordt gestaakt.

A. Dubbele melding: Het probleem is als eerder gemeld en wordt al behandeld via een responsible disclosure procedure, via een andere incident afhandelingsprocedure, via gepland onderhoud, of is al verholpen.
B. Verouderd product: De kwetsbaarheid is alleen aanwezig in een product of dienst die niet meer wordt ondersteund door de organisatie.
C. Non-security kwetsbaarheid: De kwetsbaarheid die is gemeld heeft geen implicaties voor de informatiebeveiliging of is niet te misbruiken door middel van bestaande technieken.
D. Kwetsbaarheid bij derde partij: De kwetsbaarheid is aanwezig in een product of dienst van een derde partij. Er kan in overleg met de melder contact worden gezocht met de derde partij.

4.6 Bevestigen validiteit

A. Nadat de verificatie van de kwetsbaarheid is afgerond moet de melder geïnformeerd worden over de bevindingen en de vervolgstappen van het onderzoek.
B. Mogelijk kan de organisatie de kwetsbaarheid niet reproduceren op basis van de informatie uit de melding. De organisatie moet dan de melder vragen om meer bewijs om aan te tonen dat het daadwerkelijk om een informatiebeveiligingsprobleem gaat.

4.7 Schade indamming en beoordeling blootstelling

A. Onderdeel gelijk aan ‘Draaiboek informatiebeveiligingsincidenten’.
B. Aanvulling: De melder moet op de hoogte worden gesteld van de voortgang van het onderzoek. Indien mogelijk wordt de melder een globale planning voor remediatie en herstel gestuurd.

4.8 Remediatie en herstel

A. Onderdeel gelijk aan ‘Draaiboek informatiebeveiligingsincidenten’.

4.9 Openbaar maken

A. Als er een update beschikbaar is voor de kwetsbaarheid in een online omgeving, moet deze update geïmplementeerd worden.
B. De melder maakt de kwetsbaarheid pas openbaar als de melder en organisatie zijn overeengekomen dat de kwetsbaarheid openbaar wordt gemaakt, alle betrokken organisaties goed zijn geïnformeerd en de organisatie heeft aangegeven dat de kwetsbaarheid is opgelost conform de gemaakte afspraken.
C. Als een kwetsbaarheid niet of moeilijk op te lossen is, of indien er hoge kosten mee gemoeid zijn, kan <<INSTELLING>> in overleg met de melder afspreken om de kwetsbaarheid niet openbaar te maken.
D. Zodra de organisatie tevreden is met de effectiviteit van de update moeten medewerkers, gebruikers en klanten via een beveiligingsadvies (zie bijlage B) worden geïnformeerd. De oplossing moet beschikbaar worden gesteld via de website van de organisatie.
E. Nadat er een beveiligingsadvies is gepubliceerd kunnen er verdere aanpassingen noodzakelijk zijn. Deze aanpassingen moeten duidelijk worden bijgehouden.
F. Indien er een ticket bij <<INSTELLING>>cert is aangemaakt moet er worden aangegeven dat deze is afgehandeld.

4.10 Informeren betrokkenen

A. Indien de kwetsbaarheid mogelijk ook op andere plaatsen aanwezig is, kan Security Officer met de melder afspreken om via <<INSTELLING>>cert een bredere ICT-community of het algemene publiek te informeren over de kwetsbaarheid.

4.11 Belonen melder

A. De organisatie bepaalt zelfstandig per geval of er een beloning wordt toegekend en welke vorm de beloning heeft. Een toegekende beloning wordt uitgekeerd zodra met voldoende zekerheid is vastgesteld dat de melder zich heeft gehouden aan de voorwaarden uit het responsible disclosure beleid en de responsible disclosure procedure.

4.12 Publiceren

A. Er worden met de melder afspraken gemaakt over hoe de publiciteit wordt gezocht. De communicatieafdeling wordt betrokken in de besluitvoering omtrent een publicatie.
B. In overleg met de melder kan er toe besloten worden om tezamen naar buiten te treden. Te denken valt aan een gezamenlijke presentatie op een beveiligingscongres of een publicatie op <<INSTELLING>>blog.
C. Indien de melder de kwetsbaarheid niet zelf wil publiceren wordt de melder via een e-mail op de hoogte gesteld van de afronding, de eventuele beloning en bedankt voor zijn melding en inzet .

4.13 Rapportage en evalueren

A. Evaluatie wordt uitgevoerd zoals beschreven in het *'Draaiboek informatiebeveiligingsincidenten'*.
B. Resultaten van de responsible disclosure procedure en de oorzaken van de kwetsbaarheid worden geëvalueerd door het <<INSTELLING>> Security Kernteam.

5 Versiebeheer, revisies

- 9 juli 2014 v 1.0 David van Es en Milla Cuperus
  Gewijzigd: feedback SURFibo leden
- 9 april 2014 v 0.6 David van Es
  Gewijzigd: feedback Alf Moens
- 2 april 2014 v 0.5 David van Es
  Gewijzigd: feedback Evelijn Jeunink en Security Kernteam verwerkt, escalatie en Corporate Security/Privacy Officer toegevoegd
- 28 februari 2014 v 0.4 David van Es
  Gewijzigd: ervaringen responsible disclosure Rabobank Kelvin Rorive verwerkt
- 28 februari 2014 v 0.3 David van Es
  Gewijzigd: feedback Security Kernteam
- 11 februari 2014 v 0.2 David van Es
  Gewijzigd: feedback Alf Moens en Evelijn Jeunink
- 23 januari 2014 v 0.1 David van Es

6 Bronnen

6.1 Beleid

Floor Terra (2013), *Responsible Disclosure voorbeeld tekst*. Geraadpleegd via www.responsibledisclosure.nl

NCSC (2013), Leidraad om te komen tot een praktijk van Responsible Disclosure. Geraadpleegd via https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html

Nederland ICT (2013), *Gedragscode Responsible disclosure*. Geraadpleegd via http://www.nederlandict.nl/Files/TER/Gedragscode_responsible_disclosure_2013.pdf

6.2 Procedure

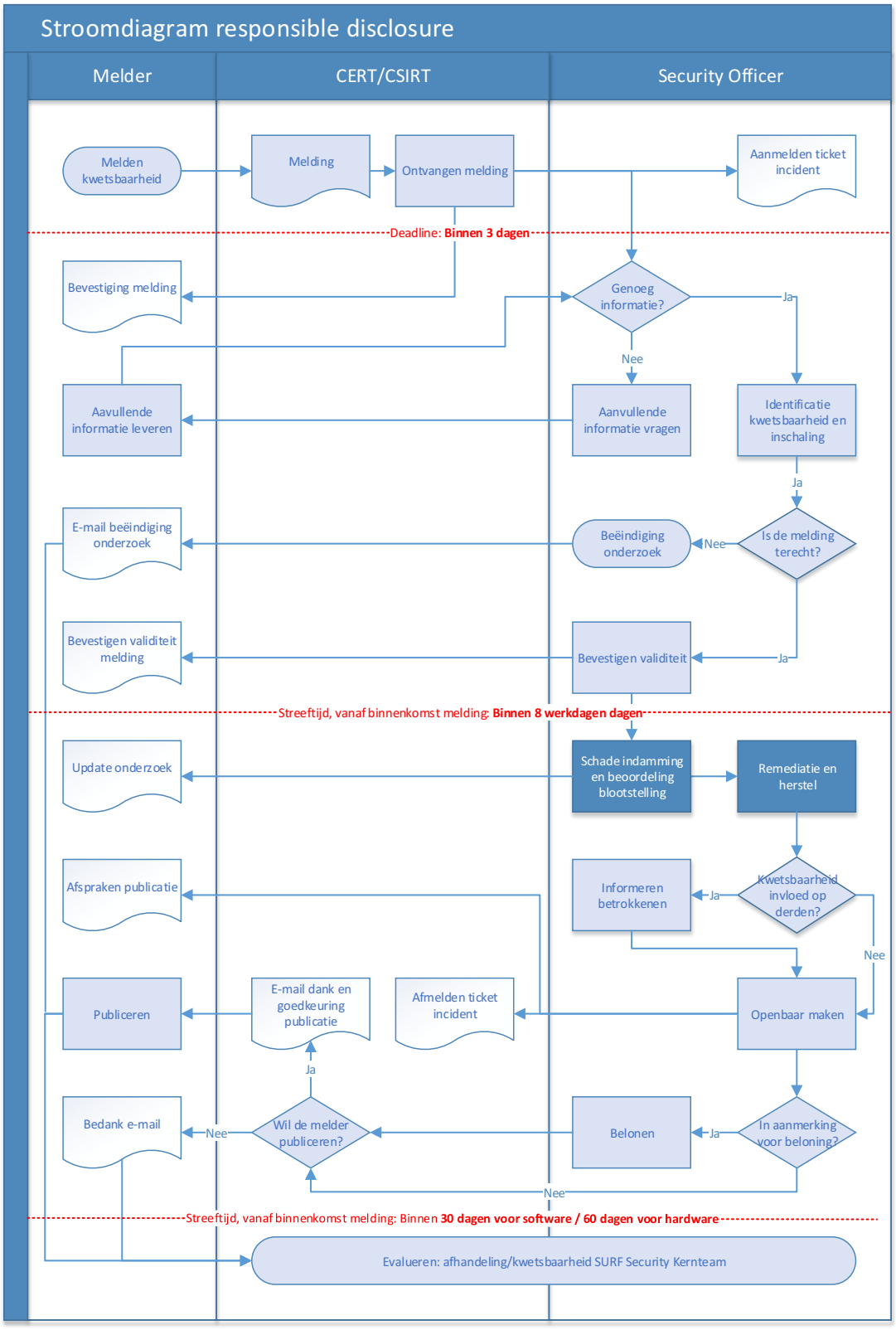
NEN-ISO/IEC (2014), *NEN-ISO/IEC 29147:2014 Vulnerability disclosure*. Genève: ISO/IEC

NEN-ISO/IEC (2013), *NEN-ISO/IEC 30111:2013 Vulnerability handling processes*. Genève: ISO/IEC

SURFnet (2014), *Draaiboek informatiebeveiligingsincidenten*. Utrecht: SURFnet

Bijlage A: Flowchart proces responsible disclosure

Deze flowchart geeft de volgorde aan waarop de verschillende stappen van de responsible disclosure procedure kan worden uitgevoerd.



Bijlage B: Formulier

Voorbeelden voor de inhoud voor formulier melding kwetsbaarheid zijn te vinden in ISO 29147; Annex A of https://forms.cert.org/VulReport/. Een voorbeeld van een formulier:

Dit formulier is alleen bedoeld voor het melden van beveiligingslekken. Graag zo compleet mogelijk invullen.

- Naam
- E-mail
- Public key
- Telefoonnummer
- Wil je publiceren over de kwetsbaarheid (ja/nee)
- Beschrijving kwetsbaarheid en de uitgevoerde handelingen
- Selecteer bestand

Bijlage C: Beveiligingsadvies

Voorbeelden voor beveiligingsadviezen (advisories) zijn te vinden in ISO/IEC 29147:2014; Annex A of https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen-toelichting.html.

Het NCSC hanteert de volgende opbouw voor een beveiligingsadvies:

- Titel
- Advisory-ID
- Versie
- Kans
- CVE-ID
- Schade
- Uitgiftedatum
- Toepassing
- Versie(s)
- Platform
- Update
- Samenvatting
- Gevolgen
- Beschrijving
- Mogelijke oplossingen
- Links