V A D E M E C U M

# C&P 10 – Responsible disclosure medewerkers (AVG)

| | |
|---|---|
| Domein | Communicatie & PR |
| Vastgesteld | December 2020 (AVG-werkgroep, DB en GMR) |
| Evaluatie | December 2022 |

**Bron:**
Floor Tessa (responsibledisclosure.nl)

**Bewerkt door:**
Kennisnet, Ronald van Rooijen en Michel van den Berg

**Inleiding:**
Bij Stichting Delta De Bilt 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, 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 privacy@deltadebilt.nl of telefonisch contact op te nemen met onze Privacy medewerker;

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, te 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.

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 werkdagen 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 met betrekking tot 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.

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 de 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.

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 een handeling uitvoert die volgens het strafrecht strafbaar zijn. Het feit dat Stichting Delta De Bilt mogelijk 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.