

# Responsible disclosure Your Next Concepts

Your Next Concepts hecht veel waarde aan de veiligheid van haar systemen c.q. producten. Wij besteden dan ook veel zorg aan de beveiliging hiervan, door dit een integraal onderdeel te laten zijn van zowel software ontwikkeling, onderhoud alsook bijbehorende dienstverlening. Desondanks kan het voorkomen dat er toch een zwakke plek kan voorkomen in deze systemen.

Wanneer je zo'n zwakke plek of fout vindt in onze systemen, horen we hier graag over. Op deze manier kunnen we ervoor zorgen dat de nodige maatregelen getroffen worden om de veiligheid van onze gebruikers en systemen te waarborgen. Let op: dit is geen uitnodiging om actief onze systemen en producten te testen op zwakke plekken.

Het is mogelijk dat je tijdens je onderzoek handelingen uitvoert die volgens het strafrecht strafbaar zijn. Heb je je aan onderstaande voorwaarden gehouden, dan ondernemen wij geen juridische stappen tegen je. Het Openbaar Ministerie heeft echter altijd het recht om zelf te beslissen of het je strafrechtelijk vervolgt. Lees hierover de [beleidsbrief van het Openbaar Ministerie](#).

## Wij vragen je

- Je bevindingen te mailen naar [security@yournextconcepts.com](mailto:security@yournextconcepts.com). Versleutel indien mogelijk je bevindingen met onze [PGP key](#) (fingerprint D2F9 9650 00A9 6148 5894 575E 5FCD CA3C 9543 8383) om te voorkomen dat de informatie in verkeerde handen valt.
- Het probleem niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of gegevens van derden in te kijken, te verwijderen of aan te passen.
- Wees extra voorzichtig met persoonsgegevens.
- Het probleem niet met anderen te delen totdat het is opgelost en alle vertrouwelijke gegevens die zijn verkregen via het lek direct na het dichten van het 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 oplossen. 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

- Binnen 5 dagen te reageren op de melding met onze beoordeling van de melding en een verwachte datum voor een oplossing.
- Geen juridische stappen te ondernemen betreffende de melding als je je aan bovenstaande voorwaarden hebt gehouden.
- Je melding vertrouwelijk te behandelen en je persoonlijke gegevens niet zonder je toestemming met derden te delen tenzij dat noodzakelijk is om een wettelijke verplichting na te komen. Anoniem of onder een pseudoniem melden is mogelijk. Wij kunnen dan echter geen contact met je opnemen over

bijvoorbeeld de vervolgstappen, voortgang van het dichten van het lek, publicatie of de eventuele beloning voor de melding.

- Je op de hoogte te houden van de voortgang van het oplossen van het probleem.
- In berichtgeving over de gemelde zwakheid zullen wij, als je dit wilt, je naam vermelden als de ontdekker van de kwetsbaarheid.
- Wij kunnen je een beloning geven voor je onderzoek, maar zijn hiertoe niet verplicht. Je hebt dus niet zonder meer recht op een vergoeding. De vorm van deze beloning staat niet van tevoren vast en wordt door ons per geval bepaald. Of we een beloning geven en de vorm waarin dat gebeurt, hangen af van de zorgvuldigheid van je onderzoek, de kwaliteit van de melding en de ernst van het lek.