# Responsible Disclosure Policy House of Trust

Versie: 1.0
Datum: 26.09.2024

House of Trust B.V.
Veenweg 71 H
1701 HC Heerhugowaard

E-mail: info@houseoftrust.nl
BTW-nr: NL866936774B01

KvK: 94919720
IBAN: NL97ABNA0137041578

# Versiebeheer

| Datum | Versie | Wijziging | Auteur |
|---|---|---|---|
| 26.09.2024 | 1.0 | Eerste opzet | Mr. Lennert D. Ouwerkerk (LL.M.) |

# Inhoudsopgave

**Versiebeheer** ..... 2

**Inhoudsopgave** ..... 3

**Scope** ..... 4

**Inleiding** ..... 4

**Wij vragen u:** ..... 4

**Wat wij beloven:** ..... 4

**Wat wordt er in ieder geval niet gezien als kwetsbaarheid:** ..... 5

# Scope

Deze Responsible Disclosure Policy is geschreven voor de systemen van de besloten vennootschap:

- House of Trust B.V.

# Inleiding

Bij House of Trust 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 wij dit graag zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met u samenwerken om onze klanten en onze systemen beter te kunnen beschermen.

**Let op:** dit beleid voor Responsible Disclosure is geen uitnodiging om ons bedrijfsnetwerk uitgebreid actief te scannen om kwetsbaarheden te ontdekken. Wij monitoren ons netwerk zelf continue. Hierdoor is de kans groot dat een scan wordt opgepikt, en dat eventuele problemen daarbij door onze CERT (Computer Emergency Response Team) onderzocht wordt, en voorkomt dat er onnodig kosten worden gemaakt.

# Wij vragen u:

- Uw bevindingen te mailen naar info@houseoftrust.nl.
- 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, verwijderen of aanpassen;
- 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; en
- 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.

# Wat wij beloven:

- Wij reageren binnen drie (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 in beginsel geen juridische stappen tegen u ondernemen betreffende de melding, wij zeggen hier uitdrukkelijk “in beginsel” omdat wij ons het recht willen voorbehouden om wel juridische stappen te ondernemen als bijvoorbeeld: (i) de wijze waarop u het probleem heeft ontdekt niet samenhangt met uw

persoonlijke skills, maar bijvoorbeeld samenhangt met het gebruik van onoorbare of illegale programmatuur; (ii) u een bedrijf of mensen heeft ingehuurd om het probleem te ontdekken; (iii) u het probleem ter berde brengt om ons te chanteren; en (iv) u bent ingehuurd en bent betaald door een derde om het probleem te ontdekken;

- 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 houden u op de hoogte van de voortgang van het oplossen van het probleem;
- In berichtgeving over het gemelde probleem zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker; en
- Als dank voor uw hulp bieden wij een beloning aan voor elke melding van een ons nog onbekend beveiligingsprobleem. De grootte van de beloning bepalen wij aan de hand van de ernst van het lek en de kwaliteit van de melding, wij geven geen beloning voor problemen die niet misbruikt kunnen worden (zie hieronder – volgende kopje);
- Wij streven ernaar 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.

# Wat wordt er in ieder geval niet gezien als kwetsbaarheid:

- HTTP-pagina's met returncode 404 of andere codes die niet zijn 200;
- versievermelding van gebruikte programmatuur;
- open directories met ongevoelige inhoud;
- geen secure flag of HTTPS only flag op ongevoelige cookies;
- problemen met SPF, DKIM, DMARC of andere DNS-records;
- domeinnamen zonder DNSSEC;
- of rapporteren van verouderde versies van programmatuur zonder aantonen van een werkende kwetsbaarheid.

Dit document is gebaseerd op het voorbeelddocument zoals dit staat op: http://www.responsibledisclosure.nl/. Dat voorbeelddocument is geschreven door Floor Terra en is gepubliceerd onder een Creative Commons Naamsvermelding 3.0 licentie. Dat voorbeelddocument is -blijkens de tekst van de aangehaalde website- mede tot stand gekomen dankzij feedback van en discussie(s) met: Deloitte, Rickey Gevers, Oscar Koeroo, Ronald Prins (Fox IT), @JeroenSlobbe, NCSC, @WhatSecurity en anderen.

Wij hebben dat voorbeelddocument gewijzigd om het te laten voldoen aan onze eisen en wensen.