RESPONSIBLE DISCLOSURE

Kwetsbaarheden veilig en verantwoord aan ons melden

Versie	1.1
Ingangsdatum	18 april 2026
Laatst bijgewerkt	18 april 2026

Inleiding

Wij nemen de beveiliging van onze systemen en die van onze klanten serieus. Ondanks onze inspanningen kan het voorkomen dat er een kwetsbaarheid aanwezig is. Als u een beveiligingsprobleem ontdekt in onze systemen, websites of klantenomgevingen die wij beheren, stellen wij het zeer op prijs als u ons daarover informeert. Zo kunnen wij snel actie ondernemen en onze klanten beschermen.

Dit beleid geldt voor alle systemen, websites en online omgevingen die onder de verantwoordelijkheid van xYnta Hosting B.V. vallen — waaronder onze eigen websites, ons klantenportaal en klantenomgevingen op onze infrastructuur.

Ons responsible disclosure beleid is gebaseerd op de richtlijnen van het Nationaal Cyber Security Centrum (NCSC) en de standaard van responsibledisclosure.nl door Floor Terra, gepubliceerd onder de Creative Commons Naamsvermelding 3.0 licentie.

Wat valt binnen de scope?

Wij ontvangen graag meldingen over kwetsbaarheden in:

- Onze eigen websites en online omgevingen (zoals xynta.com, mijn.xynta.com, orbit.xynta.com, help.xynta.com en xyntastatus.com)
- Onze interne systemen en infrastructuur voor zover deze van buitenaf toegankelijk zijn
- Klantenomgevingen die wij beheren op onze infrastructuur

Kwetsbaarheden in systemen van derden die wij niet beheren, vallen buiten de scope. Neem in dat geval rechtstreeks contact op met de betreffende partij.

Wat vragen wij van u?

Om te zorgen dat wij veilig en zorgvuldig kunnen handelen, vragen wij u het volgende:

- **Meld uw bevinding zo snel mogelijk** via e-mail aan security@xynta.nl. Versleutel uw bericht bij voorkeur met onze PGP-sleutel om te voorkomen dat gevoelige informatie in verkeerde handen valt.
- **Maak geen misbruik van de kwetsbaarheid.** Download niet meer gegevens dan strikt nodig is om het probleem aan te tonen. Bekijk, wijzig of verwijder geen gegevens van derden.
- **Deel de kwetsbaarheid niet met anderen** totdat wij het probleem hebben opgelost. Verwijder alle vertrouwelijke gegevens die u via de kwetsbaarheid heeft verkregen zodra het lek is gedicht.
- **Gebruik geen aanvalstechnieken** die de beschikbaarheid of integriteit van onze systemen in gevaar brengen, zoals denial-of-service aanvallen, brute force, spam of social engineering.
- **Geef ons voldoende informatie** om het probleem te kunnen reproduceren en oplossen. Het IP-adres of de URL van het getroffen systeem en een duidelijke omschrijving van de kwetsbaarheid zijn in de meeste gevallen voldoende. Bij complexere kwetsbaarheden kan meer informatie nodig zijn.
- **Handel te goeder trouw** en volg deze procedure. Melden onder een pseudoniem is toegestaan.

Wat kunt u van ons verwachten?

- **Wij reageren binnen één werkdag** op uw melding met een bevestiging van ontvangst en een eerste beoordeling.
- **Wij lossen het probleem zo snel mogelijk op** en streven naar een oplossing binnen 90 dagen. Als meer tijd nodig is, overleggen wij dit met u. Wij houden u gedurende het proces op de hoogte van de voortgang.
- **Wij ondernemen geen juridische of andere nadelige stappen** tegen u als u te goeder trouw handelt en zich houdt aan de procedure die in dit beleid is beschreven. Dit geldt ook als u daarbij per ongeluk een grens heeft overschreden die u redelijkerwijs niet had kunnen voorzien.
- **Wij behandelen uw melding vertrouwelijk.** Uw persoonsgegevens worden niet zonder uw toestemming gedeeld met derden, tenzij wij daartoe wettelijk verplicht zijn.
- **Wij vermelden uw naam als ontdekker** in onze hall of fame als u dit wenst. Wilt u liever anoniem blijven, dan respecteren wij dat.
- **Wij betrekken u bij eventuele publicatie** over de kwetsbaarheid nadat het probleem is opgelost, als u dat op prijs stelt.

Wat valt buiten dit beleid?

Wij behandelen geen meldingen die betrekking hebben op:

- Reeds bekende kwetsbaarheden of kwetsbaarheden die al eerder aan ons zijn gemeld
- Kwetsbaarheden waarbij actief misbruik is gemaakt of waarbij gegevens van derden zijn ingezien, gewijzigd of gekopieerd buiten hetgeen nodig is voor de melding
- Theoretische kwetsbaarheden zonder aantoonbaar praktisch risico
- Bevindingen afkomstig van geautomatiseerde scantools zonder handmatige verificatie
- Aanvallen op fysieke beveiliging, social engineering of medewerkers van xYnta

Wij behouden ons het recht voor om meldingen die buiten de scope vallen of die niet voldoen aan de voorwaarden van dit beleid niet in behandeling te nemen.

Hoe meldt u een kwetsbaarheid?

Stuur uw melding naar security@xynta.nl. Versleutel uw bericht bij voorkeur met onze PGP-sleutel. Vermeld in uw melding:

- Een duidelijke omschrijving van de kwetsbaarheid
- Het IP-adres, de URL of het systeem waarop de kwetsbaarheid is aangetroffen
- Stappen om het probleem te reproduceren
- Uw contactgegevens of pseudoniem, zodat wij u kunnen bereiken voor vervolgvragen

Wij bevestigen de ontvangst van uw melding binnen één werkdag.

Contact

- **xYnta Hosting B.V.**
- Kapitein Luidingaflat 26
- 3333 CM Zwijndrecht
- Nederland
- E-mail beveiliging: security@xynta.nl
- E-mail algemeen: info@xynta.nl
- Telefoon: 085 400 6666
- KvK-nummer: 64691675

De actuele versie van dit document is altijd beschikbaar op:

https://www.xynta.com/juridisch/responsible-disclosure

Deze PDF is een momentopname van versie 1.1. Controleer altijd of u de meest recente versie leest.