RESPONSIBLE DISCLOSURE-BELEID

Versie: 1.0 · **Datum:** 6 november 2026 · **Eigenaar:** directie Vivia B.V.
Kwetsbaarheid melden: security@vivia.nl

Heeft u als klant een beveiligingsincident of een (vermoedelijk) datalek? Meld dit dan niet via dit beleid, maar via ons meldformulier (zie de meldprocedure).

1. Doel

Vivia B.V. (hierna: Vivia) vindt de beveiliging van haar systemen, diensten en de gegevens die daarin worden verwerkt erg belangrijk. Via onze diensten, zoals Vivia-Connect en de STIP-App, verwerken wij gezondheidsgegevens in opdracht van zorgaanbieders. Daarom zijn wij gecertificeerd voor NEN 7510 en ISO/IEC 27001.

Hoe zorgvuldig wij ook werken, een systeem kan toch een kwetsbaarheid bevatten. Met dit beleid bieden wij beveiligingsonderzoekers en anderen een veilige en duidelijke manier om kwetsbaarheden aan ons te melden. Zo kunnen wij ze snel beoordelen en verhelpen, voordat iemand er misbruik van maakt.

Wij werken volgens de principes van Coordinated Vulnerability Disclosure (CVD), zoals beschreven in de Leidraad CVD van het Nationaal Cyber Security Centrum (NCSC).

2. Reikwijdte

Dit beleid geldt voor systemen en diensten die Vivia zelf aanbiedt of beheert:

- de websites van Vivia, waaronder www.vivia.nl;
- Vivia-Connect, inclusief koppelingen en API's;
- de STIP-App;
- overige door Vivia gehoste diensten en de bijbehorende technische infrastructuur.

Buiten de reikwijdte vallen:

- systemen van leveranciers en subverwerkers, zoals de infrastructuur van onze hostingpartij TransIP. Meld kwetsbaarheden daarin bij die partij zelf;
- systemen van onze klanten, zoals hun elektronisch cliëntendossier (ECD). Meld die bij de betreffende zorgaanbieder;
- fysieke locaties en medewerkers van Vivia (zie de regels in hoofdstuk 4).

Bevindingen die op zichzelf geen beveiligingsrisico opleveren, behandelen wij doorgaans niet als kwetsbaarheid. Voorbeelden zijn ontbrekende HTTP-beveiligingsheaders zonder aantoonbaar misbruik, het tonen van softwareversies, ontbrekende SPF-, DKIM- of DMARC-records, clickjacking op pagina's zonder gevoelige acties en self-XSS. U mag ze wel melden.

Twijfelt u of een systeem binnen de reikwijdte valt? Neem dan eerst contact op via security@vivia.nl.

3. Een kwetsbaarheid melden

Meld een (mogelijke) kwetsbaarheid zo snel mogelijk en vertrouwelijk via ons meldformulier (kies "Kwetsbaarheid") of per e-mail aan security@vivia.nl. Wilt u gevoelige details liever versleuteld delen? Vraag ons dan om een beveiligde manier om ze te versturen.

Vermeld in uw melding zo mogelijk:

1. een duidelijke beschrijving van de kwetsbaarheid;
2. het betrokken systeem, de URL of de applicatie;
3. de stappen om de kwetsbaarheid na te bootsen;
4. de mogelijke gevolgen voor de beveiliging;
5. eventueel screenshots, logbestanden of een beperkte proof-of-concept;
6. uw contactgegevens, als u op de hoogte wilt blijven. U mag ook anoniem of onder een pseudoniem melden; wij kunnen u dan alleen niet informeren.

Stuur geen persoonsgegevens, wachtwoorden of andere vertrouwelijke gegevens mee die u tijdens uw onderzoek bent tegengekomen. Beschrijf alleen dat u er toegang toe had.

4. Regels voor uw onderzoek

Wij vragen u zich aan de volgende regels te houden:

- Maak geen misbruik van de kwetsbaarheid.
- Doe niet meer dan nodig is om het bestaan en de gevolgen van de kwetsbaarheid aan te tonen.
- Bekijk, download, wijzig of verwijder geen gegevens van anderen. Onze systemen kunnen gezondheidsgegevens van cliënten en patiënten bevatten; deze mag u nooit inzien of opslaan.
- Gebruik alleen testaccounts of uw eigen account en probeer niet in te loggen met gegevens van anderen. Gebruik geen brute-force-aanvallen.
- Gebruik geen social engineering of phishing en voer geen fysieke tests uit.
- Voer geen (D)DoS-aanvallen of andere tests uit die de beschikbaarheid van onze diensten kunnen verstoren. Zorgsystemen moeten altijd beschikbaar blijven.
- Installeer geen malware, backdoors of andere middelen om toegang te houden.
- Deel informatie over de kwetsbaarheid niet met anderen voordat wij daarover afspraken hebben gemaakt.
- Krijgt u toegang tot vertrouwelijke gegevens of dreigt een verstoring? Stop dan direct met uw onderzoek en meld dit onmiddellijk.
- Verwijder na afloop alle gegevens die u tijdens uw onderzoek heeft verkregen.

5. Zo gaan wij met uw melding om

Wij behandelen elke melding zorgvuldig en vertrouwelijk, en bepalen de prioriteit op basis van het risico. Daarbij streven wij naar de volgende termijnen:

Stap	Streeftermijn
Ontvangstbevestiging	Binnen 3 werkdagen
Eerste inhoudelijke beoordeling	Binnen 5 werkdagen
Terugkoppeling over het vervolg en een verwachte oplosdatum	Binnen 10 werkdagen
Voortgangsupdate	Minimaal elke 14 dagen
Oplossen van de kwetsbaarheid	Afhankelijk van de ernst en complexiteit; in principe binnen 60 dagen na de melding

Ernstige of kritieke kwetsbaarheden pakken wij met voorrang op; waar nodig nemen wij direct tijdelijke maatregelen. De termijnen zijn streeftermijnen en geen garantie.

6. Vertrouwelijkheid en openbaarmaking

Wij vragen u de kwetsbaarheid vertrouwelijk te houden totdat deze is opgelost, of totdat wij samen afspraken hebben gemaakt over openbaarmaking. Publicatie vindt bij voorkeur plaats in onderling overleg. Wij houden een standaardtermijn van 60 dagen na de melding aan; als een oplossing meer tijd vraagt, stemmen wij een nieuwe termijn met u af.

Bij een gezamenlijke publicatie noemen wij u, als u dat wilt, als melder van de kwetsbaarheid.

7. Juridische afspraken

Houdt u zich aan de voorwaarden van dit beleid, dan doen wij geen aangifte en stellen wij u niet aansprakelijk voor uw onderzoek. Let op: deze toezegging bindt het Openbaar Ministerie niet. Het OM kan zelf besluiten om tot vervolging over te gaan.

Is een systeem van een derde betrokken, dan informeren wij die partij over de kwetsbaarheid. Wij geven uw persoonsgegevens alleen met uw toestemming aan anderen door, tenzij wij daartoe wettelijk verplicht zijn.

Uw gegevens gebruiken wij alleen om uw melding af te handelen. Meer hierover leest u in onze privacyverklaring.

8. Datalekken en wettelijke meldplichten

Blijkt uit een melding dat persoonsgegevens onbevoegd zijn ingezien of gebruikt, dan behandelen wij dit als een (mogelijk) datalek. Wij informeren dan onze klanten, zodat zij als verwerkingsverantwoordelijke aan hun meldplicht kunnen voldoen. Waar dat wettelijk nodig is, melden wij het incident ook bij de bevoegde autoriteiten. Uw melding blijft daarbij vertrouwelijk.

9. Beloning

Vivia heeft geen bug-bountyprogramma. Wij waarderen uw hulp wel. Bij een melding van een nieuwe en relevante kwetsbaarheid kunnen wij u daarom een bedankje geven. Of en hoe wij dat doen, bepalen wij per melding. U kunt hieraan geen rechten ontlenen.

10. Wijzigingen en contact

Wij kunnen dit beleid aanpassen. De actuele versie staat altijd op deze pagina. Ons contactadres voor kwetsbaarheden staat ook in security.txt.

Versie	Datum	Wijziging
1.0	6 november 2026	Eerste versie

Vragen over dit beleid kunt u stellen via security@vivia.nl.