

Responsible disclosure

Een kwetsbaarheid melden bij Boekmee

Versie 1.0 · 27 oktober 2026

In het kort: vind je een zwakke plek in de beveiliging van Boekmee? Meld het vertrouwelijk aan security@boekmee.nl. Doe geen schade, bekijk geen gegevens van leerlingen en geef ons tijd om het op te lossen. Houd je je aan deze regels, dan doen we geen aangifte en bedanken we je graag.

In Boekmee staan gegevens van scholen, hun medewerkers en hun leerlingen. We beveiligen die zo goed als we kunnen, maar geen systeem is helemaal veilig. Vind je toch een zwakke plek, meld het ons dan, zodat we het kunnen oplossen voordat iemand er misbruik van maakt. Deze regeling volgt de Leidraad Coordinated Vulnerability Disclosure van het Nationaal Cyber Security Centrum (NCSC) en geldt vanaf 27 oktober 2026.

1. Waarvoor deze regeling geldt

Deze regeling geldt voor de website <https://boekmee.nl>, voor Boekmee (<https://dashboard.boekmee.nl>), Boekmee Gewend (<https://informatiesysteem.boekmee.nl>), de demo's (<https://demo.boekmee.nl> en <https://demo-gewend.boekmee.nl>) en voor andere systemen die aantoonbaar van Boekmee zijn, zoals onze interne beheeromgeving. Diensten van andere partijen vallen er niet onder (paragraaf 5).

2. Zo meld je een kwetsbaarheid

Mail je melding naar **security@boekmee.nl**. Zet in je melding:

- wat het probleem is en waar het zit, bijvoorbeeld het webadres;
- hoe we het kunnen nadoen, en welke hulpmiddelen je gebruikte;
- wat iemand er volgens jou mee zou kunnen doen, en hoe we je kunnen bereiken.

Zet geen persoonsgegevens die je hebt gezien in je melding, maar beschrijf ze, bijvoorbeeld: 'ik kon namen van leerlingen van een andere school zien'. Wil je details versleuteld sturen, vraag dan eerst in een korte mail om een veilige manier. Je mag ook anoniem melden, maar dan kunnen we je niet op de hoogte houden.

3. Wat we van je vragen

1. Meld het probleem zo snel mogelijk, en alleen aan ons.
2. Doe geen schade: verander, verwijder of versleutel geen gegevens en verstoor de dienst niet. Bekijk, kopieer of download niet meer gegevens dan nodig is om het probleem aan te tonen; één voorbeeld is genoeg.
3. Bekijk geen gegevens van leerlingen. Zie je toch gegevens van leerlingen, medewerkers of scholen, stop dan meteen, maak geen kopie en meld het ons. Verwijder wat je toch hebt verkregen zodra je het hebt gemeld.

4. Test zo veel mogelijk in de openbare demo op <https://demo.boekmee.nl>. Daar staan voorbeeldgegevens met verzonden namen, die elke nacht teruggaan naar de beginstand. Gebruik nergens het account van een ander en verander geen wachtwoorden of instellingen van anderen.
5. Gebruik geen social engineering of phishing tegen medewerkers van Boekmee of van scholen. Doe geen aanvallen die de dienst kunnen verstoren, zoals een (D)DoS-aanval, het raden van wachtwoorden of scans die veel verkeer geven. Doe geen fysieke aanvallen op kantoren, apparaten of datacenters, en verstuur geen spam, ook niet via onze formulieren.
6. Plaats geen malware, achterdeur of andere software en laat niets achter in onze systemen.
7. Deel het probleem met niemand anders tot het is opgelost en geef ons de tijd uit paragraaf 4. Wil je er daarna over publiceren, overleg dan eerst met ons over de inhoud en het moment.
8. Houd je verder aan de wet. Wij kunnen geen toestemming geven voor systemen van anderen.

4. Wat wij beloven

- Binnen 3 werkdagen bevestigen we dat we je melding hebben ontvangen. Binnen 10 werkdagen laten we weten of het om een kwetsbaarheid gaat, hoe ernstig die is en wanneer we een oplossing verwachten.
- We streven ernaar het probleem binnen 60 dagen na je melding op te lossen. Lukt dat niet, bijvoorbeeld omdat een leverancier iets moet aanpassen, dan leggen we uit waarom en spreken we samen een nieuwe termijn af. We houden je op de hoogte en laten je weten wanneer het is opgelost.
- We behandelen je melding vertrouwelijk. Je naam en contactgegevens delen we niet zonder jouw toestemming, tenzij de wet ons daartoe verplicht. Meer hierover staat in onze privacyverklaring op <https://boekmee.nl/privacy>.
- Heb je je aan de regels uit paragraaf 3 gehouden, dan doen we geen aangifte en stellen we je niet aansprakelijk. Het Openbaar Ministerie beslist zelf over vervolging; vraagt het ons om informatie, dan laten we weten dat je volgens deze regeling hebt gemeld.
- Wil je dat, dan noemen we na de oplossing je naam of schuilnaam als dank op deze pagina. Voor een nieuwe en serieuze melding kunnen we je een bol.com-cadeaubon geven als dank. Daar heb je geen recht op, en een melding mag niet afhangen van een beloning.

Blijkt uit je melding dat iemand zonder toestemming persoonsgegevens kon inzien, dan volgen we ons datalekprotocol. We informeren dan binnen 24 uur de scholen om wie het gaat; zij beslissen over een melding aan de toezichthouder. Gaat het om onze eigen gegevens, dan melden we het waar dat moet aan de Autoriteit Persoonsgegevens. Je naam noemen we daarbij alleen met jouw toestemming.

5. Wat buiten deze regeling valt

Diensten van andere partijen, zoals de betaalpagina van Stripe, Cloudflare, Hostinger en sociale media, vallen niet onder deze regeling, ook niet als Boekmee ze gebruikt. Meld een kwetsbaarheid daarin bij die partij zelf.

Deze meldingen zien we meestal niet als kwetsbaarheid, en daarvoor geven we geen beloning:

- dat de demo werkt met de accounts op de inlogpagina van de demo; die zijn bewust openbaar;

- ontbrekende beveiligingsheaders of cookie-instellingen, zichtbare versienummers en instellingen voor SPF, DKIM of DMARC, zolang er geen misbruik is aangetoond;
- uitkomsten van automatische scanners zonder bewijs van echt misbruik, en clickjacking op pagina's waar je niets kunt wijzigen;
- problemen die alleen je eigen account raken (self-XSS) of die een ontgrendeld apparaat van een gebruiker vereisen;
- problemen die we al kennen; dat laten we je dan weten.

6. security.txt

Op <https://boekmee.nl/.well-known/security.txt> staat een klein tekstbestand volgens de internationale standaard RFC 9116. Daarin vinden onderzoekers en hun hulpmiddelen waar ze een kwetsbaarheid kunnen melden. Elke regel heeft de vorm veld, dubbele punt, spatie, waarde, bijvoorbeeld Contact: <mailto:security@boekmee.nl>. Het bestand bevat deze regels:

Veld	Waarde
Contact	mailto:security@boekmee.nl
Expires	2027-10-26T23:00:00.000Z
Preferred-Languages	nl, en
Policy	https://boekmee.nl/responsible-disclosure
Canonical	https://boekmee.nl/.well-known/security.txt

Expires is verplicht en ligt minder dan een jaar na de plaatsing van het bestand; we vernieuwen het bestand elk jaar vóór die datum. Het bestand staat alleen op [https](https://boekmee.nl), als platte tekst (text/plain; charset=utf-8). Een gelijk bestand, met het eigen adres bij Canonical, staat ook op dashboard.boekmee.nl, informatiesysteem.boekmee.nl, demo.boekmee.nl en demo-gewend.boekmee.nl.

Vragen over deze regeling stel je aan security@boekmee.nl. We kunnen deze regeling aanpassen; de versie op <https://boekmee.nl/responsible-disclosure> geldt.