# Politique de divulgation des vulnérabilités - Vulnerability Disclosure policy

## Introduction

Poka accueille les signalements de vulnérabilités de sécurité provenant de chercheurs, de clients et de toute autre personne qui en découvre une, et s'engage à collaborer avec eux pour les corriger. La protection des données de nos clients est au cœur de la façon dont nous concevons et exploitons la plateforme Poka.

Cette politique explique ce que vous pouvez tester, comment signaler ce que vous trouvez et ce à quoi vous pouvez vous attendre de notre part. Si vous la respectez de bonne foi, nous travaillerons avec vous pour comprendre et régler le problème rapidement.

## Portée

Cette politique couvre la plateforme Poka : le logiciel que Poka développe, exploite et fournit à ses clients.

### Inclus

- L'application Poka et ses API, utilisées au moyen d'un locataire (*tenant*) Poka auquel vous avez légitimement accès
- L'application Web installable Poka, à l'adresse `pwa.poka.io`
- Poka App pour iOS (App Store d'Apple)
- Poka pour Android (Google Play)
- Poka pour Windows (Microsoft Store)

Poka est une plateforme interentreprises et n'offre pas d'inscription publique. Ne testez qu'avec un compte que vous êtes autorisé à utiliser, par exemple le locataire Poka de votre organisation, avec la permission de votre administrateur. N'accédez jamais, et ne tentez jamais d'accéder, au locataire ou aux données d'un autre client.

Si vous n'avez accès à aucun locataire Poka, vous pouvez tout de même nous signaler une vulnérabilité que vous avez remarquée dans les services Poka, mais ne les testez pas activement.

### Exclus

- Le site Web marketing `poka.io` et ses formulaires (vos signalements sont les bienvenus, mais ne le testez pas)
- Les services tiers et fournisseurs SaaS que Poka utilise; signalez-leur directement tout problème

- Les systèmes appartenant à nos clients, à nos partenaires et à d'autres parties prenantes, y compris leurs fournisseurs d'identité et leurs intégrations
- Les bureaux, les employés et les sous-traitants de Poka (piratage psychologique)

**Constats que nous n'acceptons généralement pas**, à moins que vous démontriez un réel impact sur la sécurité :

- En-têtes de sécurité, attributs de témoins (*cookies*) ou paramètres TLS manquants, sans possibilité d'exploitation
- Usurpation de courriel ou configuration SPF, DKIM et DMARC
- Détournement de clic (*clickjacking*) sur des pages sans action sensible
- XSS sur soi-même (*self-XSS*), CSRF de déconnexion, ou problèmes qui exigent un appareil ou un navigateur déjà compromis
- Problèmes qui touchent seulement des navigateurs ou des systèmes d'exploitation désuets ou non pris en charge
- Divulgation de la version d'un logiciel, collecte de bannières ou pages d'erreur trop détaillées
- Absence de limite de requêtes sur des points de terminaison autres que l'authentification
- Rapports produits uniquement par des outils de balayage automatisés, sans validation

Tout système qui n'est pas énuméré ci-dessus est exclu. En cas de doute, écrivez-nous à security+reports@poka.io avant de tester.

## Mentions légales

Vous devez respecter toutes les lois applicables lorsque vous effectuez des recherches et des signalements en vertu de cette politique. Cette politique ne vous donne pas la permission d'accéder à des données appartenant à nos clients ou à des tiers.

## Lignes directrices

Lorsque vous effectuez des recherches et des signalements en vertu de cette politique, vous devez :

- Nous signaler la vulnérabilité le plus tôt possible après l'avoir découverte.
- Utiliser seulement l'accès minimal nécessaire pour démontrer que la vulnérabilité existe. Dès que vous confirmez un accès à des données ou à un autre compte, arrêtez.
- Ne jamais consulter, copier, modifier ou supprimer des données qui ne vous appartiennent pas. Si vous accédez par accident à des données d'un client ou à des renseignements personnels, arrêtez, signalez-le et supprimez toute copie que vous détenez.
- Ne conserver aucun accès : aucune porte dérobée, aucun compte persistant et aucun déplacement latéral.
- Garder les détails confidentiels jusqu'à ce que nous nous entendions sur leur divulgation (voir Divulgation coordonnée).

**Méthodes de test interdites**

- Déni de service, tests de charge ou de stress, ou toute action qui dégrade le service pour d'autres utilisateurs
- Balayage automatisé à haut volume; l'utilisation légère et ciblée d'outils est permise
- Piratage psychologique (hameçonnage par courriel ou par téléphone) ou tests physiques visant les bureaux, le personnel ou les sous-traitants de Poka
- Pourriel, attaque par force brute ou bourrage d'identifiants
- Tests qui modifient ou suppriment des données, ou qui créent du contenu visible par d'autres utilisateurs
- Exploitation d'une vulnérabilité au-delà de ce qui est nécessaire pour la démontrer

## Comment signaler une vulnérabilité

Envoyez votre signalement par courriel à **security+reports@poka.io**, en français ou en anglais. Les signalements anonymes sont acceptés, mais sans moyen de vous joindre, nous ne pourrons pas vous tenir au courant ni vous remercier.

Le chiffrement de votre signalement est facultatif, mais recommandé s'il contient des détails sensibles. Utilisez notre clé publique PGP :

- Clé : keys.openpgp.org
- Empreinte : `9BA8 4E7A 6C33 8CFF 615B 2364 349E 9F28 6EB7 EE07`

Votre signalement doit obligatoirement inclure:

1. Le produit, l'URL ou l'application touchés, avec la version
2. Une description de la vulnérabilité et de son impact sur la sécurité, selon vous
3. Les étapes pour la reproduire, avec tout code de preuve de concept, requête ou capture d'écran
4. La date de votre découverte, et si vous croyez que d'autres personnes la connaissent ou l'exploitent
5. La façon dont vous souhaitez être remercié, le cas échéant

N'incluez aucune donnée appartenant aux clients de Poka ou à leurs utilisateurs. Décrivez plutôt ce à quoi vous avez pu accéder.

Nos coordonnées sont aussi publiées dans un format lisible par machine à l'adresse `https://poka.io/.well-known/security.txt`.

## Ce à quoi vous pouvez vous attendre

Nous accusons réception de chaque signalement dans un délai de 5 jours ouvrables et vous tenons informé jusqu'à ce que le problème soit réglé.

| Étape | Délai |
|---|---|
| Accuser réception de votre signalement | Dans les 5 jours ouvrables |
| Confirmer si la vulnérabilité est valide, et sa gravité | Nous visons un délai de 10 jours ouvrables |
| Faire le point pendant la correction | Nous visons au moins une mise à jour tous les 30 jours |
| Vous aviser de la publication du correctif | Lorsque nous avons confirmé que la vulnérabilité est corrigée |

Nous priorisons les correctifs selon la gravité, évaluée avec le Common Vulnerability Scoring System (CVSS) et ajustée selon l'impact réel sur la plateforme Poka, et nous corrigeons les problèmes critiques le plus rapidement possible. Une fois votre signalement confirmé, nous vous donnerons une date cible pour le correctif et vous aviserons de tout changement.

Certains correctifs dépendent d'un fournisseur tiers ou de l'examen d'une boutique d'applications; si cela retarde un correctif, nous vous expliquerons pourquoi. Nous serons transparents quant à notre décision, y compris lorsque nous concluons qu'un signalement ne constitue pas une vulnérabilité ou qu'il est hors de la portée.

## Divulgation coordonnée

Nous vous demandons de garder une vulnérabilité confidentielle jusqu'à ce qu'elle soit corrigée, ou pendant 90 jours après votre signalement, selon la première éventualité. Si un correctif exige plus de temps, nous vous expliquerons pourquoi et conviendrons d'une nouvelle date avec vous. Nous ne vous demanderons jamais de garder le silence indéfiniment.

- **Avant de publier**, veuillez nous transmettre votre texte afin que nous puissions vérifier qu'il ne contient aucune donnée client et que le correctif est en place.
- **Avis de sécurité.** Lorsqu'une vulnérabilité confirmée touche nos clients, nous avisons directement les clients concernés et pouvons publier un avis de sécurité. Pour les vulnérabilités touchant nos applications mobiles et de bureau, nous pouvons demander un identifiant CVE et vous y mentionner si vous le souhaitez.
- **Exploitation active.** Si nous avons des preuves qu'une vulnérabilité est exploitée, nous pouvons aviser les clients et les autorités compétentes avant la publication du correctif, comme l'exige la loi, notamment le règlement européen sur la cyberrésilience (Cyber Resilience Act). Nous vous en informerons au préalable.
- **Composants tiers.** Si la vulnérabilité se trouve dans un composant qui ne nous appartient pas, nous pouvons transmettre votre signalement à son responsable pour coordonner un correctif, et nous vous en informerons d'abord.

## Reconnaissance

Poka n'a pas de programme de primes aux bogues et ne rémunère pas les signalements. Avec votre permission, nous vous remercierons par votre nom ou votre pseudonyme dans tout avis de sécurité ou toute CVE liés à la vulnérabilité que vous avez signalée.

## Questions

Envoyez vos questions sur cette politique à security+reports@poka.io. Si une partie de cette politique vous semble floue ou pourrait être améliorée, dites-le-nous. D'autres renseignements sur la sécurité et la conformité de Poka se trouvent dans notre centre de confiance (Trust Center).

En cas de divergence entre la version française et la version anglaise de cette politique, la version anglaise prévaut.

## Introduction

Poka welcomes reports of security vulnerabilities from researchers, customers and anyone else who finds one, and commits to working with reporters to fix them. Keeping our customers' frontline data safe is central to how we build and run the Poka platform.

This policy explains what you may test, how to report what you find, and what you can expect from us in return. If you follow it in good faith, we will work with you to understand and resolve the issue quickly.

## Scope

This policy covers the Poka platform: the software Poka builds, operates and ships to customers.

**In scope**

- The Poka application and its APIs, accessed through a Poka tenant you are authorized to use
- The installable Poka web app at `pwa.poka.io`
- Poka App for iOS (Apple App Store)
- Poka for Android (Google Play)
- Poka for Windows (Microsoft Store)

Poka is a business-to-business platform and does not offer public sign-up. Only test with an account you are authorized to use, such as your own organization's Poka tenant with your administrator's permission. Never access, or try to access, another customer's tenant or data.

If you don't have access to a Poka tenant, you can still report a vulnerability you come across in Poka services, but do not actively test them.

**Out of scope**

- The `poka.io` marketing website and its forms (we still welcome reports about it, but do not test it)
- Third-party services and SaaS providers Poka uses; report these to the vendor directly
- Systems owned by our customers, partners and other stakeholders, including their identity providers and integrations
- Physical offices, employees and contractors (social engineering)

**Findings we usually do not accept**, unless you show a real security impact:

- Missing security headers, cookie flags or TLS settings with no exploit path
- Email spoofing or SPF, DKIM and DMARC configuration
- Clickjacking on pages with no sensitive action
- Self-XSS, logout CSRF, or issues that need a compromised device or browser
- Issues that only affect outdated or unsupported browsers or operating systems

- Software version disclosure, banner grabbing or verbose error pages
- Missing rate limits on non-authentication endpoints
- Reports generated only by automated scanners, without validation

Any system not listed above is out of scope. If you are unsure whether a system is covered, ask us at security+reports@poka.io before testing.

## Legal

You must comply with all applicable laws when you research and report under this policy. This policy does not give you permission to access data that belongs to our customers or to third parties.

## Guidelines

When you research and report under this policy, you must:

- Report the vulnerability to us as soon as possible after you find it.
- Use only the minimum access needed to show the vulnerability exists. Once you confirm access to data or to another account, stop.
- Never view, copy, change or delete data that is not yours. If you reach customer or personal data by accident, stop, report it, and delete any copy you hold.
- Not keep a foothold: no backdoors, persistent accounts or lateral movement.
- Keep the details confidential until we agree on disclosure (see Coordinated disclosure).

**Test methods that are not allowed**

- Denial of service, load or stress testing, or anything that degrades the service for others
- High-volume automated scanning; light, targeted use of tools is fine
- Social engineering (phishing, vishing) or physical testing of Poka offices, staff or contractors
- Spam, brute force or credential stuffing
- Tests that change or delete data, or create content visible to other users
- Exploiting a vulnerability beyond what is needed to prove it

## How to report a vulnerability

Email your report to **security+reports@poka.io**, in English or French. Reports may be anonymous, but we cannot keep you updated or credit you without a way to reach you.

Encrypting your report is optional but recommended when it holds sensitive details. Use our PGP public key:

- Key: keys.openpgp.org
- Fingerprint: `9BA8 4E7A 6C33 8CFF 615B 2364 349E 9F28 6EB7 EE07`

Your report must include the following:

1. The affected product, URL or app, with its version
2. A description of the vulnerability and the security impact you believe it has
3. Step-by-step instructions to reproduce it, with any proof-of-concept code, requests or screenshots
4. When you found it, and whether you believe anyone else knows about it or is exploiting it
5. How you would like to be credited, if at all

Do not include data belonging to Poka customers or their users. Describe what you were able to reach instead.

Our contact details are also published in machine-readable form at `https://poka.io/.well-known/security.txt`.

## What you can expect from us

We acknowledge every report within 5 business days and keep you informed until the issue is resolved.

| Step | Timing |
| --- | --- |
| Acknowledge your report | Within 5 business days |
| Confirm whether the vulnerability is valid, and its severity | We aim to do this within 10 business days |
| Status updates while we work on a fix | We aim to update you at least every 30 days |
| Tell you when the fix is released | Once we have confirmed the vulnerability has been resolved |

We prioritize fixes by severity, using the Common Vulnerability Scoring System (CVSS) adjusted for the real impact on the Poka platform, and fix critical issues as quickly as possible. Once we confirm your report, we will give you a target date for the fix and tell you if it changes.

Some fixes depend on a third-party vendor or an app store review; if that delays a fix, we will tell you why. We will be open with you about our decision, including when we conclude that a report is not a vulnerability or is out of scope.

## Coordinated disclosure

We ask you to keep a vulnerability confidential until it is fixed, or for 90 days after your report, whichever comes first. If a fix needs more time, we will explain why and agree a new date with you. We will not ask you to stay silent indefinitely.

- **Before you publish**, please share your write-up with us so we can check it holds no customer data and that the fix is live.
- **Advisories.** When a confirmed vulnerability affects our customers, we notify affected customers directly and may publish an advisory. For vulnerabilities in our mobile and desktop apps, we may request a CVE identifier and will credit you in it if you wish.
- **Active exploitation.** If we have evidence that a vulnerability is being exploited, we may notify customers and the relevant authorities before the fix is released, as the law requires, including under the EU Cyber Resilience Act. We will tell you before we do.
- **Third-party components.** If the vulnerability is in a component we do not own, we may share your report with its maintainer to coordinate a fix, and will tell you first.

## Recognition

Poka does not run a paid bug bounty program and does not pay for reports. With your permission, we will thank you by name or handle in any advisory or CVE for the vulnerability you reported.

## Questions

Send questions about this policy to security+reports@poka.io. If you think part of this policy is unclear, or could be improved, tell us. Poka's wider security and compliance information is on our Trust Center.

If the English and French versions of this policy differ, the English version prevails.

## Revision History

| Version | Date du changement/Date of change | Responsable/Responsible | Résumé des changements/Summary of change |
|---|---|---|---|
| 0.1 | 2026-11-10 | Serge Thibault | Ébauche initiale, en révision avant publication sur le Trust Center / Initial draft, in review before publication on the Trust Center |
| 1.0 | 2026-11-26 | Mathieu Marcotte | Version finalisée / Finalized version |