Signaler une vulnérabilité.

Version 1.0 · en vigueur le 15 novembre 2026

1. Objet et portée

1.1. Ce que couvre cette page. C'est notre politique de divulgation coordonnée : la personne qui trouve une faille nous la signale, nous la corrigeons, et la publication éventuelle se fait d'un commun accord, après la correction. Elle s'inspire des normes ISO/IEC 29147 (divulgation des vulnérabilités) et ISO/IEC 30111 (traitement des vulnérabilités) ; notre contact est publié selon le format de la RFC 9116, dans le fichier www.bonbay.fr/.well-known/security.txt.

1.2. À qui elle s'applique. À toute personne : chercheur en sécurité, client, visiteur, partenaire, fournisseur. Les failles que nous trouvons nous-mêmes, par exemple lors du test d'intrusion annuel de nos outils, suivent les mêmes délais.

1.3. Articulation avec les autres documents. Elle détaille la section 10 des mentions légales et la section 11 de notre politique de données personnelles. Une faille qui a été exploitée devient un incident : la procédure et les délais de Incidents et notification s'appliquent alors en plus. Nos mesures générales sont décrites dans Sécurité de l'information. Cette page ne concerne pas nos prestations de test d'intrusion pour vos propres systèmes.

2. Comment nous signaler une faille

2.1. L'adresse. Écrivez à contact@bonbay.fr, adresse reprise dans le fichier www.bonbay.fr/.well-known/security.txt. Indiquez en objet « Vulnérabilité » et le service concerné. Le français et l'anglais sont acceptés.

2.2. Ce qui nous aide.

- l'adresse de la page ou du service touché ;
- le type de faille et l'impact que vous estimez ;
- les étapes pour la reproduire, avec les requêtes ou les captures utiles ;
- la date, l'heure et l'adresse IP de vos essais, pour les distinguer d'une attaque dans nos journaux ;
- vos coordonnées, et si vous souhaitez être cité après la correction.

2.3. Les pièces sensibles. Si vous avez vu des données personnelles ou des secrets, ne les joignez pas : décrivez-les. Si une pièce doit malgré tout nous parvenir, nous vous indiquons un canal chiffré sur simple demande.

2.4. Les autres canaux. Le formulaire de contact du site alimente notre suivi commercial : il n'est pas fait pour un signalement. Ne publiez pas la faille sur un réseau social ou un forum avant la correction (article 8).

3. Ce qui est dans le périmètre

SERVICE	RECHERCHE AUTORISÉE	PRÉCISION
www.bonbay.fr et ses cinq sites (groupe, /ia/, /cyber/, /academie/, /design/)	Oui	Pages, formulaires et outils en ligne : audit IA, test de niveau, diagnostic de cybersécurité, configurateur de formation
Sous-domaines de bonbay.fr exploités par BONBAY	Oui	Y compris la configuration de notre domaine de messagerie (SPF, DKIM, DMARC)
Outils développés et exploités par BONBAY, exposés sur Internet	Oui	Sur demande, nous confirmons si un service est bien le nôtre
Sites et outils de nos clients, même conçus ou maintenus par BONBAY	Non	Voir 3.2
Services de nos fournisseurs (OVHcloud, Scaleway, Nexus, Qonto, Stripe, fournisseurs d'IA)	Non	À signaler à l'éditeur, selon sa propre politique

3.2. Les systèmes de nos clients. Nous ne pouvons pas autoriser une recherche sur un système qui ne nous appartient pas : un test exige l'accord écrit de son titulaire (article 9 des CGV). Si vous tombez sur une faille d'un site que nous maintenons, arrêtez-vous et écrivez-nous : nous prévenons le client sous 2 jours ouvrés et suivons la correction avec lui. Si nous ne le maintenons pas, nous vous indiquons à qui vous adresser.

3.3. Les composants tiers. Si la faille vient d'un logiciel ou d'une bibliothèque d'un éditeur, nous la lui signalons en divulgation coordonnée et appliquons chez nous la correction ou un contournement dans les délais de l'article 6.

4. Ce qui est hors périmètre ou interdit

4.1. Tests interdits.

déni de service, test de charge, envoi massif de requêtes ou de formulaires ;
hameçonnage, appel ou toute manœuvre visant nos équipes, nos partenaires ou nos clients ;
accès physique à nos locaux ou à nos matériels ;
essai systématique de mots de passe ;

consultation, copie, modification ou suppression de données d'autrui au-delà du minimum qui démontre la faille ;
installation d'une porte dérobée, maintien d'un accès, rebond vers un autre système ;
tout test sur les systèmes de nos clients ou de nos fournisseurs.

4.2. Signalements non retenus comme vulnérabilité. Sans démonstration d'un impact réel : un rapport brut d'outil d'analyse automatique ; l'absence d'un en-tête de sécurité sans scénario exploitable ; l'affichage d'un numéro de version sans faille associée ; une attaque qui suppose un appareil ou un compte déjà compromis ; une injection qui ne touche que votre propre navigateur ; l'affichage d'une page dans un cadre quand elle ne permet aucune action sensible. Nous les lisons et pouvons les corriger, sans les délais de l'article 6.

---

5. Règles de bonne foi

Une recherche est de bonne foi, au sens de cette politique, quand la personne :

s'arrête dès que la faille est démontrée ;
utilise ses propres comptes de test et ne vise que le périmètre de l'article 3 ;
ne garde aucune donnée rencontrée, la supprime après le signalement et nous le confirme ;
nous signale la faille sans attendre ;
ne la divulgue pas avant la correction, dans les conditions de l'article 8 ;
ne dégrade pas le service pour les autres utilisateurs ;
ne demande aucune contrepartie. Une demande de paiement posée comme condition du silence n'est pas un signalement et sort du cadre de cette politique.

En cas de doute sur un test, demandez-nous avant de le faire, à la même adresse.

---

6. Nos délais

ÉTAPE	DÉLAI	À COMPTER DE
Accusé de réception, par une personne	2 jours ouvrés	La réception du signalement
Évaluation : faille confirmée ou non, gravité, suite prévue	10 jours ouvrés	La réception du signalement
Correction ou contournement d'une faille critique	7 jours	La confirmation de la faille
Faille élevée	30 jours	La confirmation de la faille

ÉTAPE	DÉLAI	À COMPTER DE
Faille moyenne	90 jours	La confirmation de la faille
Faille faible	Prochaine mise à jour planifiée, au plus tard 180 jours, ou décision écrite et motivée de ne pas corriger	La confirmation de la faille
Point d'avancement	Au moins tous les 15 jours	Jusqu'à la correction

6.2. La gravité. Elle part du score CVSS 4.0 publié par le FIRST : critique de 9,0 à 10, élevée de 7,0 à 8,9, moyenne de 4,0 à 6,9, faible de 0,1 à 3,9. Nous l'ajustons au contexte réel (données exposées, exploitation sans authentification, nombre de personnes touchées), vous donnons le score et son raisonnement, et vous pouvez le contester.

6.3. Le contournement. Quand la correction définitive demande plus de temps, une mesure de contournement est mise en place dans le délai : désactivation d'une fonction, filtrage, coupure d'un accès. Nous vous donnons la date de la correction définitive.

6.4. Une faille exploitée. Si l'évaluation montre que la faille a été exploitée ou que des données ont été exposées, la procédure d'incident s'applique en plus, avec ses délais d'information des clients et de la CNIL.

---

7. Protection de la personne qui signale

7.1. Pas de poursuite. BONBAY ne porte pas plainte et n'engage aucune action contre une personne qui a cherché de bonne foi et respecté cette politique, y compris au titre de l'article 323-1 du Code pénal (accès frauduleux à un système de traitement automatisé de données).

7.2. Face à un tiers. Si un fournisseur ou une autorité nous interroge sur votre recherche, nous confirmons par écrit qu'elle entrait dans le cadre de cette politique. Nous ne pouvons pas engager un tiers ni le ministère public.

7.3. Votre identité. Elle n'est connue que des personnes qui traitent le signalement. Nous ne la communiquons pas sans votre accord, sauf obligation légale.

7.4. Une autre voie. Vous pouvez aussi transmettre la faille à la seule ANSSI, qui préserve la confidentialité de votre identité (article L2321-4 du Code de la défense) : cyber.gouv.fr.

7.5. Remerciements. Il n'y a pas de prime. Nous vous remercions par écrit et, si vous le souhaitez, nommément dans l'avis publié après la correction.

---

8. Divulgation coordonnée et publication

8.1. Une date convenue. Nous fixons avec vous la date de publication, après la correction. Sans accord, nous vous demandons d'attendre la correction, et au plus 90 jours après votre signalement. Avant ce terme, nous vous disons si un délai supplémentaire est justifié, et pourquoi.

8.2. Notre avis. Pour toute faille critique ou élevée corrigée, nous publions dans le Centre de confiance un avis court : service concerné, nature de la faille, dates du signalement et de la correction, et ce que les utilisateurs doivent faire, le cas échéant. L'avis ne donne aucun détail qui permette d'attaquer un système encore vulnérable.

8.3. Les clients concernés. Un client dont les données ou les systèmes ont pu être touchés est prévenu directement, avant toute publication.

---

9. Limites

9.1. Pas de contrat. Cette politique ne crée ni contrat, ni rémunération, ni droit à une prime.

9.2. Pas d'astreinte permanente. Nos délais se comptent en jours ouvrés pour l'accusé de réception et l'évaluation. Pour une faille en cours d'exploitation, écrivez « URGENT » en objet : le message est traité en priorité, sans promesse d'une réponse immédiate la nuit ou le week-end.

9.3. Les failles d'un éditeur. Quand la correction dépend d'un éditeur ou d'un fournisseur, nous ne maîtrisons pas son calendrier. Nous mettons en place un contournement dans nos délais quand c'est possible, et vous le disons quand ça ne l'est pas.

9.4. Les propositions commerciales. Un message qui propose des services d'audit à partir d'une analyse automatique n'est pas un signalement au sens de cette politique.

9.5. Le reste de nos contrôles. Cette politique ne remplace ni notre test d'intrusion annuel ni nos revues, décrits dans Conformité et audits.

---

10. Contact et mise à jour

10.1. Responsable. Pierre Marsanne, président de BONBAY, porte la sécurité, la confidentialité et la protection des données, et reçoit les signalements : contact@bonbay.fr, adresse reprise dans www.bonbay.fr/.well-known/security.txt. BONBAY, SAS au capital de 4 500 €, 38 cours de l'Intendance, 33000 Bordeaux.

10.2. Version. Version 1.0, en vigueur le 15 novembre 2026. Cette page est revue chaque année (prochaine revue : novembre 2027) et à chaque changement important. Le fichier security.txt renvoie à cette page ; son champ d'expiration (Expires) est renouvelé au moins une fois par an. Les clients sont prévenus de tout changement qui les concerne.

10.3. Les autres engagements. L'ensemble des pages est réuni dans le Centre de confiance.