Sécurité de l'information.

Version 1.0 · en vigueur le 15 novembre 2026

1. Objet et portée

1.1. Ce que couvre cette page. Cette politique décrit les mesures que BONBAY applique pour protéger la confidentialité, l'intégrité et la disponibilité des informations : les siennes, et celles que ses clients lui confient pendant une mission. Elle vaut pour le groupe et ses quatre marques (IA, Cyber, Académie, Design), qui partagent la même équipe, les mêmes outils et les mêmes règles.

1.2. À qui elle s'applique. À chaque personne qui travaille pour BONBAY, salariée ou indépendante, et à nos partenaires Thrive et Qlint lorsqu'ils interviennent sur un de vos projets avec votre accord. Chacune la reçoit et signe une charte et une clause de confidentialité avant son premier accès à une information de client.

1.3. Articulation avec nos documents. Cette page précise l'article 13.4 des conditions générales de vente et la section 10 de notre politique de données personnelles, qu'elle ne remplace pas. Les mesures retenues pour une mission précise sont écrites dans l'annexe D des CGV (tableau D.6) ou dans le devis : pour cette mission, ces documents signés prévalent.

1.4. Ce qui relève d'autres pages. Les règles d'accès à vos systèmes sont détaillées dans Accès à vos systèmes, les sauvegardes et la fin de contrat dans Continuité et réversibilité, la conduite d'un incident dans Incidents et notification, nos référentiels et vos audits dans Conformité et audits.

2. Organisation et responsabilités

2.1. Un responsable nommé. Pierre Marsanne, président de BONBAY, porte la sécurité de l'information, la confidentialité et la protection des données. Il valide cette politique, accorde ou refuse les exceptions, décide des mesures après un incident et répond aux questions des clients. BONBAY n'a pas désigné de délégué à la protection des données : il en est le référent.

2.2. Des règles écrites. Chaque règle de cette page existe sous forme de procédure interne, rangée dans Nexus, notre outil de gestion hébergé dans l'Union européenne, avec la date de sa dernière relecture.

2.3. Des exceptions tracées. Une règle qui ne peut pas s'appliquer, par exemple sur un outil qui ne propose pas la double authentification, donne lieu à une exception écrite : motif, mesure de compensation, durée, accord du président. Les exceptions ouvertes sont relues à chaque revue trimestrielle des accès et fermées dès que leur cause disparaît.

2.4. Un inventaire tenu. Nous tenons la liste de nos postes, de nos comptes, de nos outils, de nos fournisseurs et des accès ouverts chez chaque client. Elle est mise à jour à chaque arrivée, départ ou nouvel outil, et relue chaque trimestre.

SUJET	QUI DÉCIDE	CONTRÔLE
Politique de sécurité	Le président	Revue chaque année, en novembre
Accès ouverts chez les clients	Le client, par écrit, puis le président	Revue chaque trimestre
Exceptions	Le président	Revue chaque trimestre
Choix d'un fournisseur	Le président	À la commande, puis chaque année

3. Les personnes

3.1. Un engagement signé. Chaque personne, chaque partenaire et chaque marque du groupe signe la charte de l'équipe et une clause de confidentialité qui survit à la fin de la collaboration. Ce que nous gardons pour nous est détaillé dans Confidentialité.

3.2. Sensibilisation. Toute l'équipe suit chaque année une session de sensibilisation : hameçonnage, gestion des secrets, usage des outils d'IA, conduite à tenir en cas d'incident. Une personne qui arrive la suit avant son premier accès à un système de client. Les sessions sont datées et la liste des participants est conservée.

3.3. Signaler sans crainte. Chacun signale aussitôt à contact@bonbay.fr un message suspect, un poste perdu, un secret exposé ou sa propre erreur. Une erreur signalée de bonne foi n'est pas sanctionnée : un signalement tardif coûte toujours plus cher qu'une erreur reconnue tout de suite.

3.4. Départ. Les accès d'une personne qui quitte BONBAY sont retirés le jour de son départ, et les secrets qu'elle connaissait sont changés.

4. Postes, comptes et messagerie

Les règles ci-dessous s'appliquent à tout appareil et à tout compte qui sert au travail pour BONBAY.

MESURE	RÈGLE
Chiffrement du disque	Activé sur chaque poste avant tout usage professionnel
Verrouillage	Automatique après 5 minutes d'inactivité
Mises à jour de sécurité	Posées sous 14 jours ; sous 72 heures pour une faille critique déjà exploitée

MESURE	RÈGLE
Protection	Antivirus avec détection et réponse (EDR) sur chaque poste
Supports	Aucune donnée de client sur une clé USB ou un appareil personnel
Comptes	Nominatifs, double authentification obligatoire, droits minimaux
Mots de passe	Uniques par service, générés et rangés dans le coffre d'accès
Perte ou vol d'un poste	Signalement immédiat, effacement à distance, accès révoqués, secrets changés

4.1. Nos outils internes. La double authentification y est obligatoire : nous ne retenons pas un outil interne qui ne la propose pas.

4.2. Messagerie. Notre messagerie et nos documents sont hébergés en France chez OVHcloud. Le domaine bonbay.fr publie des enregistrements SPF, DKIM et DMARC, ce dernier en mode rejet, pour limiter l'usurpation de nos adresses. Aucun mot de passe ni aucune clé ne circule par e-mail.

---

5. Chiffrement, hébergement et journaux

5.1. Chiffrement. Les échanges sont chiffrés en transit avec TLS 1.2 au moins, sur nos sites comme sur les outils que nous livrons. Les données sont chiffrées au repos sur les serveurs, sur les sauvegardes et sur les postes.

5.2. Hébergement. Les sites et bases de données de nos clients sont hébergés en France chez OVHcloud (Roubaix, Gravelines) et produits avec notre partenaire Thrive. Les sauvegardes chiffrées sont confiées à un second fournisseur français, Scaleway, à Paris, dans une autre région. Notre gestion interne (suivi commercial Pilote, coffre d'accès, documents) est assurée par Nexus, hébergé dans l'Union européenne. La liste des prestataires, avec ce qu'ils traitent, figure dans Sous-traitants ultérieurs ; le droit applicable et les options souveraines, dans Souveraineté des données.

5.3. Séparation des environnements. Les essais se font dans un environnement de test séparé de la production. Quand des données fictives, anonymisées ou pseudonymisées suffisent, nous travaillons avec elles.

5.4. Journaux. Nos journaux techniques sont limités à la sécurité (connexions, actions d'administration, erreurs) et conservés 12 mois au plus. Ils servent à détecter un usage anormal et à enquêter sur un incident, pas à surveiller une personne.

5.5. Nos propres sites. Le site www.bonbay.fr ne dépose aucun cookie de mesure ou de publicité sans votre accord, et ne charge Google Analytics qu'après cet accord (page Cookies).

---

6. Logiciels et outils d'IA que nous livrons

6.1. Secrets hors du code. Un mot de passe, une clé d'API ou un jeton n'est jamais écrit dans le code, dans un journal ni dans une page servie au navigateur. Il est lu au démarrage dans la configuration du serveur, elle-même générée depuis le coffre d'accès. Chaque dépôt de code est analysé avant envoi pour détecter un secret oublié.

6.2. Dépendances. Les bibliothèques d'un logiciel que nous livrons sont analysées à chaque livraison. Une vulnérabilité critique connue est corrigée avant la mise en production ; à défaut, la livraison est reportée et vous en êtes informé.

6.3. Mise en production. Une modification passe par l'environnement de test avant la production. Les opérations irréversibles (suppression massive, paiement, changement de sécurité, publication externe) demandent une validation humaine, comme le prévoit l'article 8.2 des CGV.

6.4. Outils d'IA. Nous n'utilisons que des offres professionnelles et des API dont les conditions excluent l'entraînement sur les données transmises, et nous n'envoyons aucune donnée personnelle à un outil d'IA tiers sans votre instruction écrite. Le détail est dans IA et vos données.

---

7. Contrôles réguliers

Une mesure qui n'est pas contrôlée finit par ne plus être appliquée. Nos contrôles sont datés et leurs comptes rendus conservés.

CONTRÔLE	FRÉQUENCE	PAR QUI
Revue des accès et des exceptions	Chaque trimestre	Le président
Test de restauration des sauvegardes	Chaque trimestre	L'équipe technique
Test d'intrusion de nos propres outils	Chaque année	Un prestataire externe indépendant
Test du plan de reprise	Chaque année	L'équipe technique
Revue de l'ensemble des mesures	Chaque année, en novembre	Le président
Sensibilisation	Chaque année	Toute l'équipe

7.1. Référentiels. Nous alignons nos mesures sur l'annexe A de la norme ISO/IEC 27001:2022 et sur le guide d'hygiène informatique de l'ANSSI. S'aligner n'est pas être certifié : ce que nous revendiquons, et ce que nous ne revendiquons pas, est précisé dans Conformité et audits. La norme elle-même est présentée sur notre page ISO 27001.

7.2. Correction. Un écart relevé par un contrôle reçoit un responsable et une date de correction, suivis jusqu'à la clôture. Cette démarche répond à l'article 32.1.d du RGPD, qui demande de tester et d'évaluer régulièrement l'efficacité des mesures.

---

8. Ce que nous ne promettons pas

8.1. Pas de sécurité absolue. Aucune mesure ne rend un système invulnérable. Nous nous engageons sur des moyens, des délais et des contrôles, pas sur l'absence d'incident ; c'est pourquoi la page Incidents et notification dit ce que nous faisons si un incident survient.

8.2. Pas de label que nous n'avons pas. BONBAY n'est pas certifiée ISO 27001, n'est pas qualifiée PASSI ni SecNumCloud et n'est pas hébergeur certifié de données de santé (HDS). Quand une mission l'exige, nous le disons au devis et retenons pour la partie concernée un fournisseur qui détient la certification ou la qualification requise, ou nous déclinons (article 13.3 des CGV).

8.3. Vos systèmes restent les vôtres. Vos comptes, postes, réseaux, configurations et sauvegardes, comme les fournisseurs que vous choisissez, relèvent de vous, sauf prise en charge écrite par BONBAY (article 13.4 des CGV).

8.4. Les fournisseurs. La disponibilité d'OVHcloud, de Scaleway ou d'un fournisseur d'IA dépend d'eux. Nous répondons de nos choix, de nos réglages et des niveaux de service que nous avons acceptés (article 9.4 des CGV).

8.5. Pas d'astreinte implicite. Sans contrat d'astreinte, nous n'assurons pas de surveillance permanente de vos systèmes la nuit et le week-end.

8.6. Cette page n'est pas un audit. Elle décrit notre sécurité, pas la vôtre. Évaluer vos systèmes est une mission distincte : voir Audit de cybersécurité.

---

9. Contact et mise à jour

9.1. Contact. Une question sur cette politique ou une demande de document : contact@bonbay.fr. Réponse écrite sous 2 jours ouvrés.

9.2. Signaler une faille. Une faille se signale à la même adresse, reprise dans le fichier https://www.bonbay.fr/.well-known/security.txt. Notre politique de divulgation coordonnée figure dans Signaler une vulnérabilité.

9.3. Documents remis sur demande. Plan d'assurance sécurité (PAS), synthèse du dernier test d'intrusion, attestations d'assurance responsabilité civile professionnelle et cyber.

9.4. 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. Un changement qui vous concerne vous est annoncé par e-mail. L'ensemble du Centre de confiance est accessible depuis la page Centre de confiance.