Accès à vos systèmes.

Version 1.0 · en vigueur le 15 novembre 2026

1. Objet et portée

1.1. Ce que couvre cette page. Elle s'applique à tout accès que vous ouvrez à BONBAY : serveur (SSH, SFTP), console d'hébergement, base de données, back-office de site, messagerie, compte publicitaire, logiciel en ligne, clé d'API. Elle couvre aussi les comptes que nous créons pour un agent d'IA ou une automatisation qui agit dans vos outils.

1.2. Qui est concerné. Chaque personne de BONBAY, toutes marques confondues, et nos partenaires Thrive et Qlint lorsqu'ils interviennent sur votre projet avec votre accord écrit. Les mêmes règles s'appliquent à tous.

1.3. Articulation. Cette page précise les articles 8.2 et 13.2 des CGV et la section 6 de notre politique de données personnelles. Si l'accès permet d'atteindre des données personnelles, l'accord de sous-traitance (annexe D des CGV) est signé avant l'ouverture : voir RGPD : sous-traitance. Nos mesures générales (postes, chiffrement, contrôles) sont décrites dans Sécurité de l'information ; ce que nous gardons pour nous de ce que nous voyons chez vous, dans Confidentialité.

2. Avant l'ouverture : la fiche d'accès

2.1. Une demande écrite. Aucun accès n'est ouvert sans une fiche d'accès que vous validez. Elle indique le système, la personne nommée qui l'utilisera, les droits demandés, le motif, l'environnement (test ou production) et la date de fin prévue. Elle est rangée dans le dossier de la mission et sert de référence à la revue des accès.

2.2. Vous créez, nous utilisons. Nous vous demandons de préférence de créer vous-même les comptes à nos noms : vous gardez la main et pouvez les couper à tout moment. Si vous nous demandez de les créer, nous le faisons depuis un compte que vous nous ouvrez à cet effet, et nous vous remettons la liste des comptes créés.

2.3. Le test d'abord. Quand un environnement de test ou une copie existe, nous y travaillons d'abord. Quand des données fictives, anonymisées ou pseudonymisées suffisent, nous vous demandons celles-là plutôt que les vraies (article 13.2 des CGV).

2.4. Remise d'un secret. Si vous devez nous transmettre un mot de passe ou une clé, nous vous envoyons un lien de dépôt à usage unique vers notre coffre d'accès. Ne l'envoyez ni par e-mail, ni par messagerie instantanée, ni dans un document partagé.

---

3. Comptes nominatifs, droits minimaux, double authentification

3.1. Un compte par personne. Chaque intervenant a son propre compte, à son nom. Nous n'utilisons pas de compte générique (« admin », « agence ») et nous ne réutilisons jamais un compte ou une clé d'un client à l'autre. Les clés SSH sont propres à chaque personne et à chaque client, et protégées par une phrase secrète.

3.2. Les droits nécessaires, rien de plus. La lecture avant l'écriture, l'écriture avant l'administration. Un droit d'administration n'est demandé que pour la tâche qui l'exige et il est retiré à la fin de cette tâche.

3.3. Double authentification. Elle est obligatoire sur chaque accès qui la propose, par application d'authentification ou clé physique ; le SMS n'est utilisé que si aucune autre méthode n'existe. Si votre système ne la propose pas, nous vous le disons par écrit et proposons une mesure de compensation : restriction à nos adresses IP, passage par un réseau privé (VPN), ouverture limitée aux plages d'intervention. Cette exception est tracée et relue chaque trimestre.

3.4. Système à compte unique. Si un outil n'autorise qu'un seul compte, celui-ci est attribué à une seule personne nommée, son secret reste dans le coffre et il est changé à la fin de la mission.

---

4. Secrets et coffre d'accès

4.1. Un seul endroit. Mots de passe, clés d'API, jetons, clés SSH et certificats sont rangés dans le coffre d'accès de Nexus, chiffré et hébergé dans l'Union européenne. Ils ne sont jamais copiés dans un e-mail, un document, un ticket, une conversation, un journal ou le code.

4.2. Cloisonnement. Une personne ne voit que les secrets des missions auxquelles elle est affectée. Chaque consultation d'un secret est enregistrée : qui, quand, lequel.

4.3. Dans les outils que nous livrons. Un logiciel lit ses clés au démarrage, dans une configuration générée depuis le coffre. Aucune clé n'apparaît dans le dépôt de code, dans les pages servies au navigateur ni dans les journaux.

4.4. Secret exposé. Un secret envoyé par erreur dans un canal non prévu, y compris par vous, est aussitôt rangé dans le coffre et retiré du canal quand c'est possible ; nous vous demandons de le changer dans la journée.

---

5. Pendant la mission

5.1. Depuis nos postes uniquement. Nous nous connectons à vos systèmes depuis des postes gérés par BONBAY (disque chiffré, antivirus avec détection et réponse, mises à jour suivies), jamais depuis un appareil personnel ou un ordinateur public.

5.2. Journal de nos actions. Nos interventions sont journalisées de notre côté : date, personne, système, action. Sur votre demande, nous vous remettons sous 5 jours ouvrés l'extrait qui concerne vos systèmes. Ces journaux sont limités à la sécurité et conservés 12 mois au plus.

5.3. Interventions sensibles. Une intervention en production vous est annoncée. Une suppression massive, un paiement, un changement de sécurité, une publication externe ou toute opération irréversible attend votre validation, comme le prévoit l'article 8.2 des CGV. Avant une modification importante, un point de restauration est pris (voir Continuité et réversibilité).

5.4. Accès d'urgence. Si un incident impose d'agir hors de la plage prévue, par exemple pour isoler un compte compromis, la mesure est limitée au nécessaire, tracée et vous est notifiée le jour même (article 9.4 des CGV). La suite est décrite dans Incidents et notification.

5.5. Nos partenaires. Thrive ou Qlint n'accèdent à vos systèmes qu'avec votre accord écrit, par leurs propres comptes nominatifs et aux mêmes règles. Ils ne reçoivent jamais un accès qui a été ouvert à BONBAY.

---

6. Agents d'IA et automatisations

Un agent d'IA qui agit dans vos outils est traité comme un intervenant, avec des règles plus strictes.

RÈGLE	CE QUE CELA VEUT DIRE
Son propre compte	Un compte de service au nom de l'agent, jamais celui d'une personne
Lecture seule par défaut	L'écriture n'est ouverte que pour les actions listées au devis
Confirmation humaine	Toute action irréversible attend la validation d'une personne
Plafonds	Nombre d'étapes et durée limités par tâche, coût limité par requête
Journal	Chaque action est enregistrée : consigne reçue, outil appelé, résultat
Bouton d'arrêt	Vous et nous pouvons couper l'agent à tout moment ; l'arrêt est testé avant la mise en service

6.1. Clés à votre nom. Les comptes et clés d'API des fournisseurs d'IA sont ouverts à votre nom chaque fois que c'est possible : vous payez le fournisseur directement et gardez la main. Les budgets, plafonds et alertes sont décrits dans Maîtrise des tokens.

6.2. Données. Un agent n'envoie pas de données personnelles à un outil d'IA tiers sans votre instruction écrite. Ce qui part vers un modèle et ce qui n'y part jamais est décrit dans IA et vos données.

6.3. Pas d'accès illimité. Sauf autorisation écrite donnée après analyse des risques, un agent ne reçoit pas d'accès autonome illimité à la production (article 8.2 des CGV). Le fonctionnement d'un agent est expliqué sur la page Agent IA.

---

7. Revue et fermeture des accès

MOMENT	CE QUE NOUS FAISONS	DÉLAI
Chaque trimestre	Revue de tous les accès ouverts chez nos clients, rapprochés des missions en cours	Accès sans mission fermé le jour même
Fin d'une tâche	Retrait des droits d'administration temporaires	À la fin de la tâche
Fin de la mission	Retrait de tous nos accès et des comptes d'agents	Au plus tard le jour de la fin
Départ d'une personne	Retrait de ses accès, changement des secrets qu'elle connaissait	Le jour du départ
Votre demande	Fermeture de l'accès désigné	Le jour ouvré de la demande

7.1. Fiche de fermeture. À la fin de la mission, nous vous envoyons sous 2 jours ouvrés une fiche qui liste les comptes fermés, les clés supprimées et les secrets que vous nous aviez confiés, que nous vous invitons à changer. Nos copies de ces secrets sont effacées du coffre.

7.2. Contrat récurrent. Pour une maintenance ou un hébergement, la mission dure tant que le contrat court. Les accès restent alors limités aux personnes affectées, et la revue trimestrielle vérifie qu'ils sont toujours nécessaires.

---

8. Ce qui dépend de vous, et nos limites

8.1. Vous gardez la main. Vous administrez vos systèmes : vous pouvez voir nos comptes, les suspendre ou les fermer à tout moment, sans préavis. Nous vous recommandons de garder vous-même les comptes d'administration principaux.

8.2. Vos journaux. Notre journal couvre nos actions avec nos outils. La journalisation de vos propres systèmes dépend de leurs réglages ; si elle manque ou ne suffit pas, nous vous le signalons.

8.3. Vos comptes et vos postes. La sécurité de vos comptes, postes, réseaux et fournisseurs reste la vôtre, sauf prise en charge écrite par BONBAY (article 13.4 des CGV). Si un de vos comptes est compromis, l'accès que vous nous avez ouvert peut l'être aussi : prévenez-nous aussitôt.

8.4. Données sensibles. Un accès qui permet d'atteindre des données de santé, biométriques, pénales ou d'autres catégories particulières n'est ouvert qu'après l'examen préalable prévu à l'article 13.3 des CGV.

8.5. Hors de notre périmètre. Les accès que vous ouvrez directement à un autre prestataire, même recommandé par nous, relèvent de votre contrat avec lui.

---

9. Contact et mise à jour

9.1. Contact. Une demande d'ouverture, de fermeture ou d'extrait du journal : contact@bonbay.fr. Un accès que vous pensez compromis se signale à la même adresse, sans attendre ; une faille se signale aussi à cette adresse, reprise dans le fichier https://www.bonbay.fr/.well-known/security.txt.

9.2. 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. Un changement qui vous concerne vous est annoncé par e-mail. Les autres engagements du groupe sont réunis sur la page Centre de confiance.