CENTRE DE CONFIANCE

Sécurité & confiance

Des accès vérifiés, des validations humaines et un périmètre explicite pour les usages de l'IA.

Démonstration vérifiée : HTTPS/TLS et parcours fonctionnels ciblés. La démonstration utilise des modèles cloud. Chaque installation client fait l'objet de son propre cadrage.

Contrôles observés dans les parcours testés

01 Accès côté serveur

Comptes authentifiés, autorisations et contexte d'espace sont contrôlés par le serveur. Les accès refusés ont été testés.

02 Boîte email choisie

Une boîte explicitement sélectionnée est vérifiée avant usage, sans repli silencieux. La lecture d'un en-tête a été testée en lecture seule.

03 Emails à valider

Les brouillons de la file d'actions attendent une validation. Deux approbations simultanées du même brouillon sont protégées.

04 Appels d'outils contrôlés

Dans les workflows MCP, l'outil et ses arguments sont présentés avant exécution. L'accès et les paramètres sont revérifiés à la reprise.

05 Reprises encadrées

L'état du workflow et les décisions sont enregistrés. Des limites d'étapes et d'appels encadrent l'exécution et ses reprises.

06 Historique disponible

Les actions instrumentées sont horodatées et associées à un acteur. Les workflows conservent leur historique et leur résultat.

Ces constats décrivent des contrôles et des tests ciblés. Ils ne valent pas certification, audit indépendant ou garantie d'absence de vulnérabilité.

DÉPLOIEMENT & RESPONSABILITÉS

Un périmètre clair pour chaque installation

01 Une instance dédiée, selon le projet

Notre règle d'offre est une instance dédiée par entreprise, hébergée pour le client ou installée dans son environnement. Le lieu d'hébergement, les accès d'administration et les responsabilités d'exploitation sont précisés avant le déploiement.

02 Modèle local ou cloud : un choix explicite

Le fournisseur et le mode de traitement sont identifiés. Avec une API cloud, les données nécessaires à la requête sont transmises au fournisseur. Un stockage local ne rend pas ce traitement local. Une installation entièrement locale exige un dimensionnement et une recette spécifiques.

03 Sauvegarde, conservation et contrat

La fréquence des sauvegardes, leur protection, les objectifs de reprise et les tests de restauration sont définis selon le contrat ; ils ne sont pas garantis par cette fiche. Les durées de conservation, la suppression, les sous-traitants et les responsabilités RGPD restent à cadrer avec le client et sa DSI.

Certifications : aucune revendication

Pixel Agent Suite ne revendique ici aucune certification ISO 27001, ISO 27701, SOC 2 ou HDS. Les labels éventuels d'un fournisseur ne sont pas ceux de Pixel Agent.

POUR PRÉPARER VOTRE DÉPLOIEMENT

Précisez le cas d'usage, les données nécessaires, les personnes autorisées et les systèmes à raccorder. Nous cadrons ensuite le périmètre, les contrôles et la recette attendue.

Pixel Drop Technologies · contact@pixel-drop.com
01 83 64 17 41 · 58 Rue de la Chaussée d'Antin, 75009 Paris

Centre de confiance : pixel-drop.com/pixel-agent-confiance
Référence CNIL : cnil.fr/fr/sous-traitant
Travailler avec un sous-traitant. Cette référence ne constitue pas une approbation de Pixel Agent par la CNIL.