CONTRAT DE DÉVELOPPEMENT D'API (CDAP)

1.1 Parties contractantes

Le présent Contrat de Développement d'API est conclu entre :

- Le Prestataire : Instants Web Agency, spécialisée en conception et intégration de solutions web et d'API.
- Le Client : [Nom – Raison sociale – Adresse], souhaitant faire développer une ou plusieurs API.

1.2 Objet

Le contrat encadre la conception, le développement, l'intégration, la documentation et la mise à disposition d'une API ou d'un ensemble d'API, décrits en détail dans le Cahier des Charges Technique (Annexe A).

1.3 Étendue de la prestation

La prestation comprend notamment :

- L'analyse des besoins fonctionnels et techniques ;
- La conception de l'architecture logique et technique ;
- Le développement des Endpoint prévus ;
- La mise en place des mécanismes d'authentification et de contrôle d'accès ;
- La rédaction de la documentation développeur ;
- La fourniture d'un environnement de test ;
- La livraison de la première version de l'API.

1.4 Livrables

À l'issue de la prestation, le Prestataire remet au Client :

- Le code de l'API ou les modalités d'accès ;
- La documentation technique détaillée ;
- Les informations nécessaires à l'intégration ;
- La description de la version publiée ;
- Le rapport de tests.

1.5 Obligations du Prestataire

Le Prestataire réalise la prestation selon les règles de l'art, en veillant à la robustesse, à la sécurité et à la maintenabilité de l'API.

1.6 Obligations du Client

Le Client fournit les informations nécessaires, donne accès aux environnements requis, valide les étapes intermédiaires et utilise l'API dans le cadre défini par le contrat.

1.7 Durée

Le contrat prend effet à sa signature et reste applicable pendant la durée de réalisation. La maintenance et l'évolution peuvent être prévues dans une convention complémentaire.

– ANNEXE A : CAHIER DES CHARGES TECHNIQUE

2.1 Description générale

Description détaillée de l'API : objectifs, périmètre, contexte d'usage, contraintes techniques et exigences particulières.

2.2 Endpoints et ressources

Pour chaque endpoint : URL, méthode HTTP, paramètres, format de réponse, codes d'erreur, limites d'usage.

2.3 Règles métiers

Description des traitements, validations et conditions appliquées par l'API.

– ANNEXE B : PROPRIÉTÉ INTELLECTUELLE

3.1 Droits accordés au Client

Droit d'utiliser l'API dans le cadre défini (usage interne, mise à disposition de tiers, etc.).

3.2 Éléments conservés par le Prestataire

Conservation des briques logicielles génériques, bibliothèques internes et outils de génération.

3.3 Garantie d'éviction

Garantie que l'API livrée ne viole pas volontairement les droits de propriété intellectuelle de tiers.

– ANNEXE C : POLITIQUE D'UTILISATION DE L'API

4.1 Conditions d'accès
Obtention de clés ou tokens d'accès, à conserver de manière confidentielle.

4.2 Usage autorisé et restrictions
Usage limité au cadre défini, interdiction de surcharge volontaire, détournement ou contournement des protections.

4.3 Gestion des clés
Interdiction de diffusion publique, partage non contrôlé ou stockage non sécurisé des clés.

– ANNEXE D : ACCORD DE CONFIDENTIALITÉ (NDA)

5.1 Informations concernées
Code, documentation, schémas, données métier, secrets d'affaires, et plus largement toute information désignée comme confidentielle.

5.2 Engagements
Non-divulgation à des tiers et mise en place de mesures de protection internes.

5.3 Durée
Obligations de confidentialité maintenues pendant cinq ans après la fin du contrat.

– ANNEXE E : SÉCURITÉ & CONFORMITÉ (POLITIQUE DE SÉCURITÉ AVANCÉE)

6.1 Principes généraux
L'API est pensée avec une approche orientée sécurité : exposition limitée, contrôle des entrées, chiffrement des échanges, séparation des environnements.

6.2 Politique de sécurité avancée pour les API

- Gouvernance de la sécurité : référents techniques, procédures d'escalade, registre des changements et incidents.

- Contrôle des accès : authentification forte, rotation des clés, séparation des comptes par environnement, principe du moindre privilège.
- Protection des données : chiffrement des flux, protection des logs, limitation des données exposées.
- Surveillance : métriques, alertes, détection des comportements anormaux, journalisation des actions sensibles.
- Tests de sécurité : audits, tests d'intrusion, vérification régulière des dépendances et correctifs.
- Gestion des incidents : procédures de réponse, notification du Client, plan d'actions correctrices.

6.3 Conformité
Respect de la réglementation applicable (notamment RGPD) lorsque des données personnelles sont traitées.

– ANNEXE F : MAINTENANCE & GESTION DES VERSIONS

7.1 Numérotation
Schéma de versions explicite (ex. 1.0.0, 1.1.0, 2.0.0).

7.2 Maintenance corrective
Correction de dysfonctionnements, ajustements mineurs.

7.3 Maintenance évolutive
Ajout de capacités, modification de comportements, optimisation.

– ANNEXE G : PROCÉDURE DE LIVRAISON

8.1 Environnement de test
Mise à disposition d'une sandbox, données simulées, scénarios de test.

8.2 Mise en production
Description des responsabilités, planning et opérations techniques.

8.3 Réception
Validation via procès-verbal de recette ou acceptation tacite.

ANNEXE H : RESPONSABILITÉ

9.1 Obligation de moyens renforcée
Mise en œuvre de tous les moyens raisonnables pour assurer le bon fonctionnement de l'API.

9.2 Limitations
Responsabilité limitée aux dommages directs ; exclusion des pertes de profit, de données non sauvegardées et dommages indirects.

– ANNEXE I : RÉSILIATION & RÉCUPÉRATION DES DONNÉES

10.1 Résiliation
Résiliation possible pour manquement grave, non-paiement ou autre motif légitime, selon les modalités prévues.

10.2 Récupération des données et des accès
Remise des éléments convenus au Client, désactivation des accès restants.