**DOCUMENT DE SPÉCIFICATIONS TECHNIQUES**

1. **INTRODUCTION**
   1. **Contexte**

La société INTIA Assurance souhaite développer une application web permettant la gestion des informations relatives aux clients et aux assurances. L'application devra offrir des fonctionnalités de création, modification, suppression et consultation des données.

* 1. **Objectifs**
* Permettre une gestion centralisée des clients et de leurs assurances.
* Assurer un accès sécurisé et une interface intuitive.
* Fournir des fonctionnalités pour les directions et les succursales INTIA-Yaoundé et INTIA-Douala.

1. **DESCRIPTION GÉNÉRALE**
   1. **Acteurs du Système**

* **Administrateur** : Gestion des utilisateurs et paramètres généraux.
* **Agent Assurance** : Gestion des clients et contrats d’assurance.
* **Client** : Consultation de ses informations et contrats.
  1. **Fonctionnalités**
* **Gestion des clients** : Ajout, modification, suppression et consultation.
* **Gestion des assurances** : Création, mise à jour, suppression et suivi des contrats.
* **Authentification et autorisations** : Système de connexion avec rôles et permissions.
* **Recherche et filtres avancés** : Permettre la recherche rapide des informations.
* **Génération de rapports** : Extraction des données sous format PDF ou Excel.

1. **ARCHITECTURE TECHNIQUE**
   1. **Technologies Utilisées**

* **Front-end** : Angular avec Angular Material pour l'interface utilisateur.
* **Back-end** : Spring Boot (Java) pour la gestion des services.
* **Base de données** : MySQL pour le stockage des données.
* **Authentification** : JWT (JSON Web Token) pour la gestion des sessions.
  1. **Modélisation de la Base de Données**
* **Table Clients** : ID, Nom, Prénom, Email, Téléphone, Adresse.
* **Table Assurances** : ID, Type d'assurance, Montant, Date de début, Date d'expiration, Client\_ID (Clé étrangère).
* **Table Utilisateurs** : ID, Nom, Email, Mot de passe (haché), Rôle.

1. **SÉCURITÉ ET PERFORMANCES**

* **Gestion des droits d'accès** : Protection des données selon le profil utilisateur.
* **Chiffrement des données sensibles** : Utilisation de bcrypt pour les mots de passe.
* **Optimisation des requêtes SQL** : Indexation et normalisation des tables.
* **Sauvegarde régulière** : Mise en place d'un système de backup automatique.