RESSOURCES RELATIONNELLES

Déploiement et sécurité

MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
Liberté
Égalité
Fraternité

Olivia Lahary – Emma Scheuber – Rachel Tcha – Simon Vallero

Table des matières

Contexte

Dans le cadre de la mise en œuvre de la politique du Gouvernement, le ministère des Solidarités et de la Santé veut mettre en place une plateforme de partage de ressources entre citoyens.

Cette plateforme vise à prévenir les situations d'isolement ainsi que la précarité de l'information sur les domaines du social, de la santé publique et de d'organisation du système de santé.

Les applicatifs développés s'adressent à tous les citoyens, sans distinction. Ceux- ci devront alors être adaptés à tous en mettant l'accent sur leur ergonomie et simplicité d'utilisation. Le projet présentera une application mobile et une version site web desktop.

Contraintes

La phase de recette doit débuter 12 mois après la signature du marché.

Les applicatifs doivent respecter les RGAA et les RGPD.

Le chiffrement des données sensibles.

Il doit y avoir deux applicatifs, un mobile et un desktop.

Ressources

Un budget de 170 000 € pour un MVP.

Identité graphique

Équipe développeurs avec des compétences techniques maitrisant les langages de développement.

Serveur et hébergement chez infogérent.

Outils de développement (intelliJ IDEA)

Git (contrôle de version).

Documentation

Stratégie de déploiement

Environnement requis

Ces exigences techniques constituent une liste de références minimums pour configurer un environnement adéquat pour exécuter l'application.

Serveurs :

Application web Ubuntu pour le front et le back

- 12Go RAM
- Espace de stockage : 150 Go de stockage SSD
- Bande passante illimité
- Sauvegarde quotidienne

Base de données Ubuntu

- 12Go RAM
- 300 Go de stockage SSD
- Bande passante illimité
- Sauvegarde quotidienne

Applicatif :

Serveur base de données

Base de données MariaDB version 10.

Backend :

Installation des versions et librairie :

- JDK 17
- Maven apache 3.8.7
- Spring Boot 3
- Lombok

Frontend :

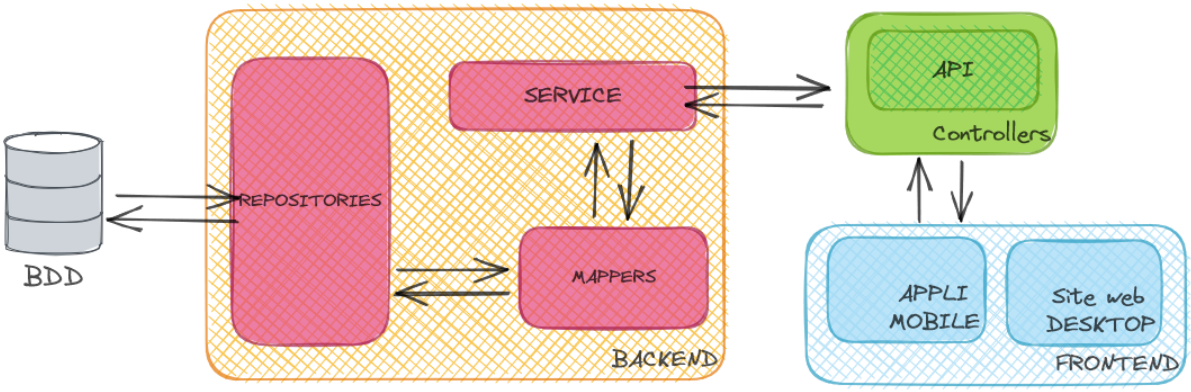
Installation des versions :

- AngularCLI 15.2.2
- Npm 8.13.2
- Node.js 18.13

Plan de déploiement

Caractéristiques des applicatifs :

Ressources Relationnelles est composé de deux interfaces utilisateurs : Un site web desktop et une application mobile. Les deux frontend communiquent avec le backend via la même API.



Le Ministère prévoit environ 1 million d'utilisateurs finaux sur les deux plateformes dans les 6 premiers mois. Puis, à l'ouverture au public d'ici 1 ans, une augmentation de 20% par an.

Parties-prenantes

L'agence ROSE assurera le déploiement des applicatifs Ressources Relationnelles en collaboration avec l'infogérant responsable des serveurs.

	Chef de projet	Développeurs Backend / Frontend	Testeurs	Infogérant	PO Client
Plannification du déploiement	R	I	I	I	A / C
Livraison	C	R	I	I	I
Installation	I	A	I	R	I
Tests en recette	I	I	R / A	N/A	I
Report des bugs	I	I	R	N/A	C / I
Démonstration	R / A	C	I	N/A	A

R : Responsible, celui qui réalise la tâche

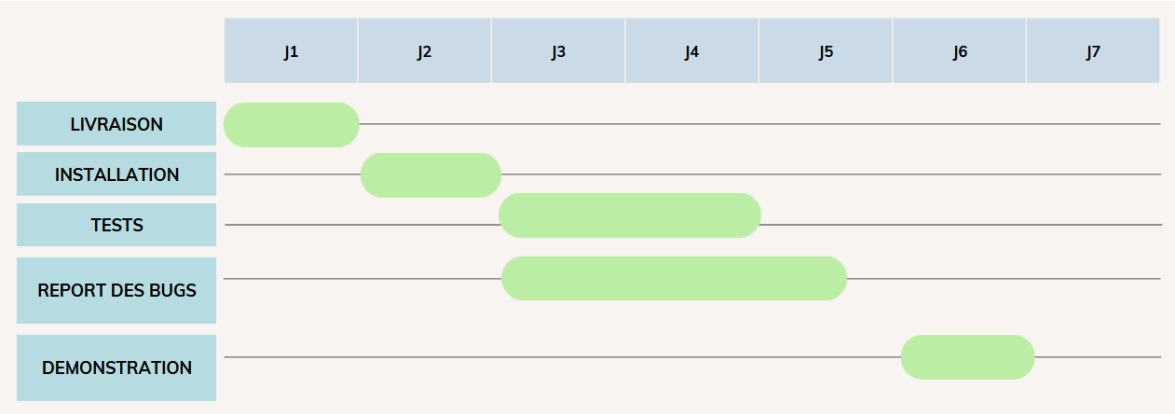
A : Accountable, celui qui approuve la tâche

C : Consulted, celui qui est consulté

I : Informed, celui qui doit être informé

Planning type

Les durées ici sont mesurées en jour et à titre indicatives, elles seront adaptées selon la taille des livraisons.



Analyse de risques

#	Risques identifiés	Probabilité	Gravité	Criticité	Responsable	Prévention
1	Perte de connexion internet	Peu probable	Majeur	Très critique	Equipe infra	Identifier des fournisseurs Internet alternatifs. Mettre en place un mécanisme de bascule automatique.
2	Panne matérielle du serveur	Peu probable	Majeur	Critique	Equipe infra	Stratégie de sauvegarde régulière. Identifier un centre de données alternatif. Plan de récupération après sinistre.
3	Attaque de sécurité par ransomware	Probable	Grave	Très critique	Responsable sécurité	Plan de sécurité robuste, des pares-feux, détection des intrusions, … Former régulièrement les employés.
4	Erreur humaine entraînant la perte de données	Peu probable	Modéré	Critique	Equipe informatique	Former les employés. Automatiser les sauvegardes régulières. Mettre en place des mécanismes de validation.

5	Mauvaise sauvegarde	Peu probable	Majeur	Critique	Infogérant / Responsable de la sécurité	Stratégie de sauvegarde. Tester la restauration des sauvegardes. Documenter les procédures de sauvegarde. Former le personnel.
6	Perte d'intégrité des sauvegardes	Probable	Majeur	Très critique	Infogérant / Responsable de la sécurité	Mettre en œuvre des mécanismes de chiffrement. Contrôles d'authentification et d'autorisation. Vérifier régulièrement l'intégrité des sauvegardes.
7	Risque pandémique	Improbable	Grave	Critique	Direction Générale	Plan de continuité des activités. Prévoir des ressources financières.
8	Destruction des serveurs	Peu probable	Grave	Très critique	Infogérant	Réaliser des sauvegardes régulières des données et les stocker dans un lieu sûr. Plan de reprise après sinistre.
9	Violation de données sensibles	Probable	Grave	Très critique	RSI	Authentification multi-facteurs et gestion des privilèges. Utiliser des méthodes de chiffrement. Mettre en place des systèmes de détection d'intrusion et de surveillance. Sensibilisation des employés sur les pratiques de sécurité.

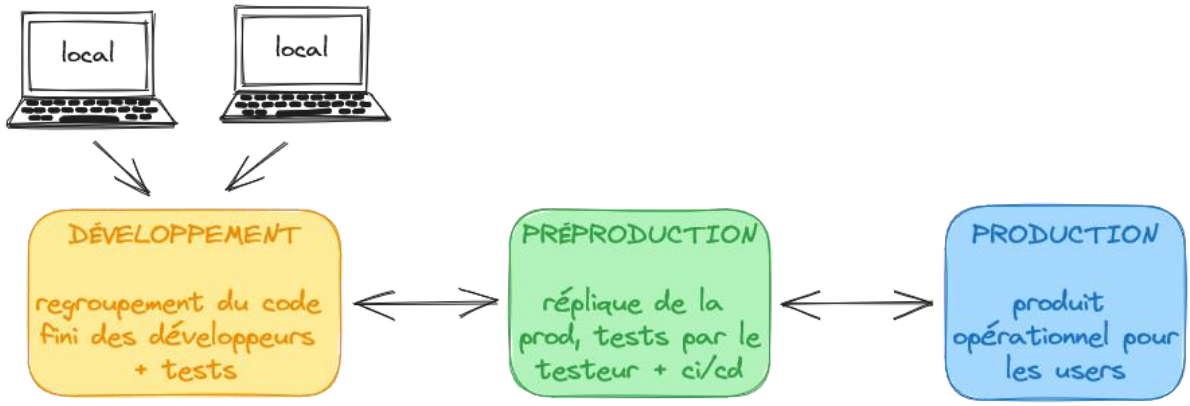
Livraison des applicatifs

Nous avons mis en place 3 environnements pour le projet Ressources Relationnelles :

L'environnement de développement : Il est utilisé par les développeurs pour centraliser leur travail et le tester avant de la livrer.

L'environnement de préproduction (recette) : L'environnement est une réplique de la production où on teste les livraisons.

L'environnement de production : Le produit stable, disponible aux utilisateurs.



Réduire le nombre d'environnements sur le projet vise à faire plus attention à la qualité du travail produit :

Nous mettons en place une stratégie de test dès les développements jusqu'à la livraison. Par exemple, nous mesurons la couverture de tests des tests suivants :

- Les tests unitaires (back et front)
- Les tests fonctionnels
- Les tests de performance
- Les tests end-to-end

Puisqu'une livraison n'est pas infaillible, nous comprenons l'importance de pouvoir faire un rollback le plus rapidement possible. Pour cela il sera possible de faire des rollback en revenant à la version antérieure grâce à un plan de reprise d'activité.

Lors des livraisons nous pourrons décider à quels groupes d'utilisateurs la livraison sera disponible. Et incrémenter les utilisateurs au fur et à mesure, jusqu'à 100%.

Nous avons opté pour une stratégie de déploiement canary :

La nouvelle version sera livrée dans un premier temps à 15% des utilisateurs. Cela nous permettra d'avoir un retour sur les bugs et l'expérience utilisateur. Au fil du temps nous incrémenterons le pourcentage de user auxquels nous livrerons. Cette

stratégie nous donne un grand niveau de contrôle sur le déploiement. Ça nous demande moins de ressources et réduit les risques par rapport à d'autres stratégies comme le bleu/vert.
Cela nous permettra aussi, au besoin, de livrer des évolutions ciblées pour certains utilisateurs par région, par exemple.

Processus d'intégration et de déploiement continu

Développements

Nos développements seront analysés par l'outil SonarQube qui nous aide à détecter les vulnérabilité, code smells, bugs, couverture de tests, …

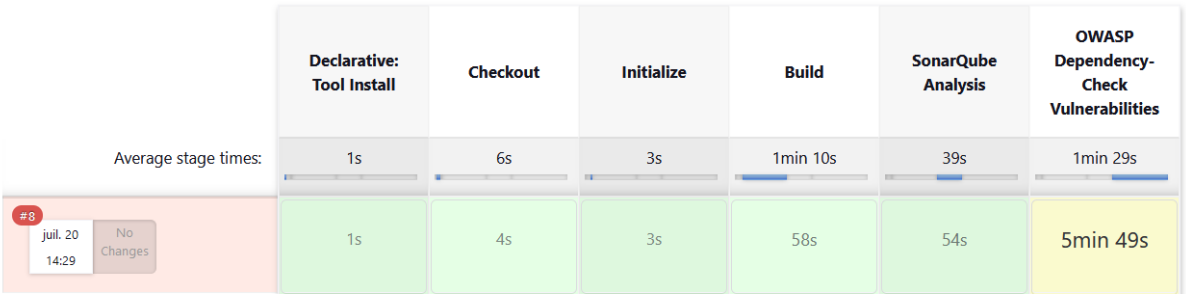
Backend

Pour s'inscrire dans une démarche d'intégration de code continue, nous avons mis en place l'outil Jenkins. Il nous permet d'automatiser certaines tâches comme la pipeline.

La pipeline se décompose comme suit :

- Checkout des sources sur gitllab
- Build de l'application
- Analyse code sonarqube
- Analyse sécurité OWASP
- Exécution des tests
- Package
- Déploiement

Ella sera déclenchée à chaque push dans le repository et à chaque demande de MR. Cela nous permet de savoir si le code produit est valide sur les points cités plus haut. Cet outil à l'avantage d'être compatible avec tous les OS.



Frontend

Pour automatiser les tests du frontend, nous avons mis en place Cypress. Il nous permet d'écrire des tests en javaScript. Il est intégrable à Jenkins.

Il permet de tester le frontend sur tous les navigateurs internet, cela nous assure que l'application répond aux principes de responsivité et de RGAA demandé par le commanditaire.

Une pipeline Jenkins pour le front est également mise en place avec une étape de Build, de tests et de lint.

Déploiement et infrastructure

Les environnements sont conteneurisés à l'aide de docker. Cela les rend plus légers pour le serveur et plus modulables. Nous recommandons les images suivantes :

- Base de données `mariadb:11.1.1-rc-jammy`
- Backend `eclipse-temurin:17-jdk-jammy`
- Frontend `20-alpine3.17`
- Jenkins `jenkins/jenkins:2.401.2-jdk17`
- SonarQube `sonarqube:community`
- SonarQube bdd `postgres:15`

Docker nous permet de devoir écrire moins de configurations.

Pour la gestion des artefacts nous utiliserons nexus. Qui nous permet d'appliquer le principe de Single Source of Truth. Qui rend les artefacts fiables et facilement trouvable. Également il nous permet e bien sécuriser nos livrables.

Maintenance

Gestion des versions

Afin de gérer les versions du code source de manière optimale, nous utilisons GitLab.

Le workflow définit sera celui du fonctionnement des 'feature branch'. Chaque développement est fait sur une branche feature tirée de develop, puis mergée à develop quand la feature est finie.

Chaque merge request sera relue par au moins un autre développeur que celui qui a travaillé sur la feature. Et seul un maintainer pourra la valider.

A chaque fois que du code sera intégré dans la branche develop (reflet de l'environnement de recette), un tag de numéro de version y sera appliqué.

GitLab nous permet de sécuriser le code source, nous avons mis en place un groupe propriétaire des repositories du projet. Au sein de ces repositories et de ce groupe, chaque membre à un rôle défini en fonction de son périmètre sur le projet.

Nous avons mis en place une protection des branches :

- Il est impossible de push sur les branches main et develop. Seule une merge request permet d'y intégrer du code, celui oblige à une relecture.
- Seuls les rôle maintainer peuvent valider une merge vers develop et main.

Ainsi nous limitons le risque de mauvaises manipulations.

C'est une solution grandement compatible avec l'intégration et le déploiement continu.

Gestion des évolutions

La gestion des évolutions de l'application repose sur l'utilisation du logiciel JIRA. Notre processus repose sur un système de tickets, avec des tickets de bug pour signaler les problèmes de l'application, ainsi que des tickets d'évolution pour toutes les améliorations à apporter.

Ces tickets sont attribués différentes priorités pour faciliter le tri et la priorisation. Certains tickets peuvent également avoir une date limite pour affiner leur priorité. Chaque ticket est assigné directement aux personnes responsables dans leur domaine.

Une fois qu'un ticket est créé, il est classé dans la colonne "À faire". La personne en charge du ticket doit alors estimer le nombre d'heures nécessaires pour résoudre le problème.

Ensuite, le ticket passe à l'étape "Dev" lorsqu'il est en cours de résolution, puis à l'étape "Test" pour vérifier la conformité. Ensuite, il passe à l'étape "Recette" avant d'être finalement déployé en production ("Prod").

Les tickets sont soumis à des contraintes strictes pour éviter toute interruption du workflow. Par conséquent, il n'est pas possible qu'un ticket passe directement de l'étape "À chiffrer" à l'étape "Recette", par exemple.

Ces contraintes garantissent une progression logique du processus et permettent de maintenir l'intégrité du workflow. Chaque ticket doit passer par toutes les étapes intermédiaires, telles que "Dev" et "Test", avant d'atteindre l'étape finale de "Recette" et ultimement la mise en production ("Prod").

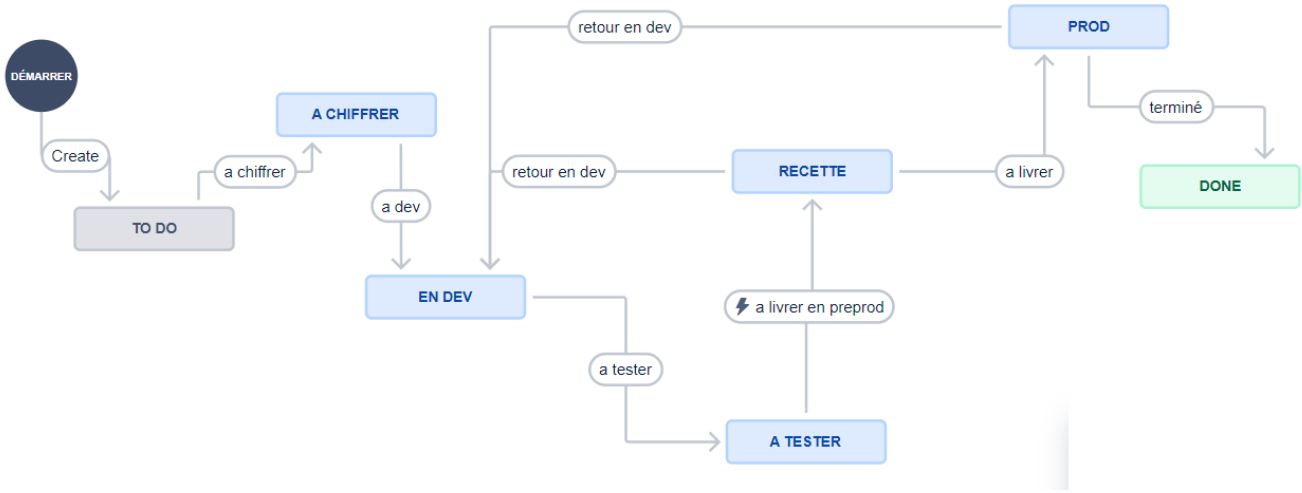
Cette approche séquentielle garantit que chaque étape du processus est soigneusement exécutée et que les problèmes potentiels sont identifiés et résolus avant de passer à l'étape suivante. Ainsi, le workflow reste cohérent et les risques d'erreurs ou de conflits sont réduits au minimum.

Les tickets sont créés et attribués par le chef de projet. Le chef de projet joue un rôle central dans la gestion du processus de tickets. Il est responsable de la création des tickets, en tenant compte des besoins et des demandes de l'équipe ou des utilisateurs de l'application.

Une fois les tickets créés, le chef de projet les attribue aux membres de l'équipe qui sont responsables de leur résolution. Cette attribution se fait en fonction du domaine de compétence et des responsabilités de chaque membre de l'équipe.

Le chef de projet s'assure également de la cohérence et de la priorisation des tickets. Il peut utiliser des critères tels que l'urgence, l'impact sur l'application ou les besoins des utilisateurs pour déterminer l'ordre de résolution des tickets.

Voici le Workflow :



Monitoring de la maintenance :

Une fois le déploiement effectué, il est important de surveiller le système en production pour détecter les problèmes éventuels.

Des outils de surveillance et de journalisation pourront être utilités pour collecter des métriques et des journaux afin d'assurer la stabilité et la performance de l'application.

Comme pistes : Datadog qui permet de monitorer les logs et de générer des statistiques.

Sécurité

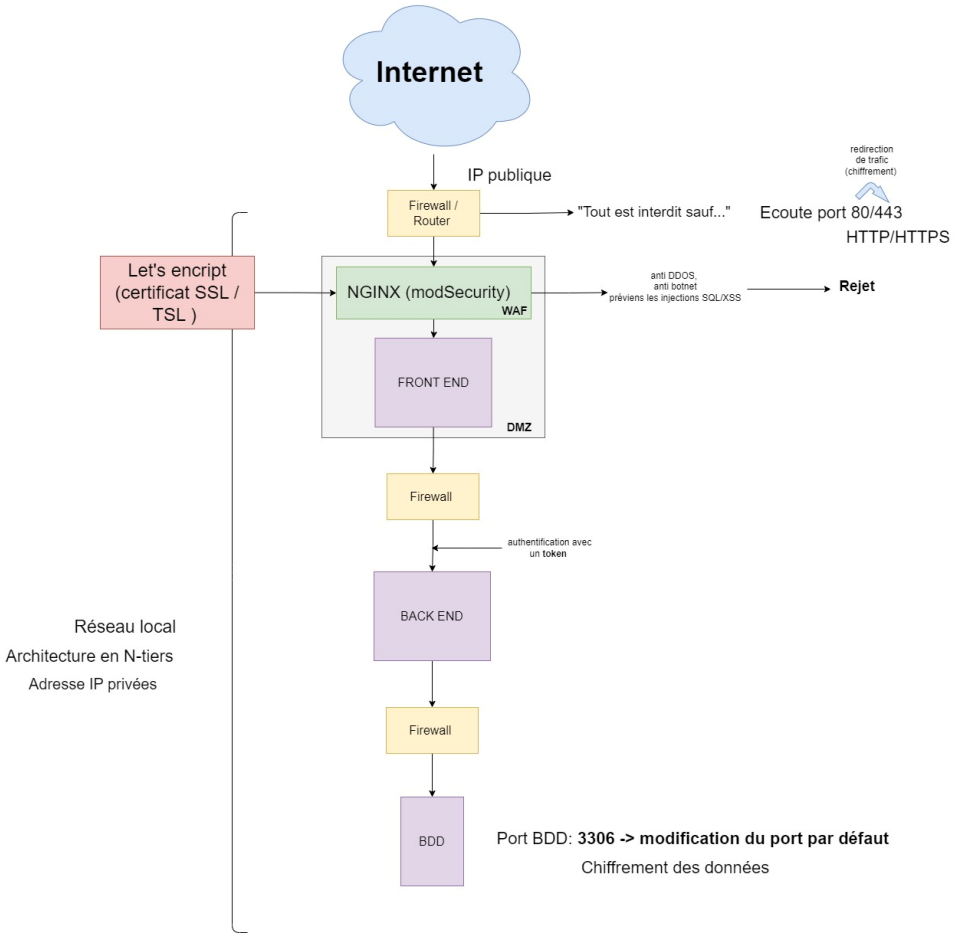
Afin de garantir la sécurité des données des utilisateurs de notre application et assurer son bon fonctionnement, nous préconisons la mise en place d'un système DNS, protégé par Cloudflare, ainsi que le respect des règlementations RGPD et des politiques de sécurité du système d'information PSSI.

La première mesure consiste à utiliser un DNS protégé par Cloudflare. Cloudfare est un service réputé qui offre une protection avancée contre les attaques (DDos) Déni de service distribué, la sécurisation des connexions HTTPS et d'autre menaces potentielles. En intégrant notre système à cloudflare , nous renforçons la sécurité des données en filtrant le trafic malveillant et en améliorant la résilience de notre application.

Parallèlement, il est essentiel de se conformer aux règlementation RGPD qui est une législation européenne visant à protéger les droits et la confidentialité des utilisateurs en matière de leurs données personnelles.

En mettant en œuvre les principes et les obligations du RGPD, nous garantissons que les données des utilisateurs sont collectées, traitées et stockées de manière légale, transparente et sécurisée.

Nous mettons en place une politique de sécurité du système d'information PSSI qui va définir un cadre de gestion de la sécurité de l'information, en identifiant les risques potentiels, en mettant en place des contrôles de sécurité approprié et en assurant une gestion proactive de la sécurité. En l'adoptant, nous nous engageons à maintenir la confidentialité, l'intégrité et la disponibilité des données des utilisateurs, tout en réduisant les risques de violations de sécurité et en garantissant une réponse adéquate en cas d'incident.



L'adresse IP publique est une adresse unique et identifiée à un périphérique qui est connecté à internet. Elle permet à ce périphérique de communiquer avec d'autres appareils sur internet et d'être accessible.

Le routeur est un appareil permettant la communication entre un réseau local domestique et Internet, il permet de protéger le réseau d'une éventuelle intrusion. Il dispose d'un **firewall** intégré. De plus nous avons mis en place un firewall avant tous les blocs : le Front-End (il fait aussi office de routeur), il sera configuré pour laisser passer le flux nécessaire soit une seule route ("tout est interdit sauf …. "), avant le Back-End (il laisse passer uniquement le flux nécessaire) et sur la base de données (comme sur les 2 premiers blocs il laisse passer le flux nécessaire).

Nous allons mettre en place une redirection du port d'écoute. Si l'URL écrite est HTTP://www.resources-relationnelles.fr, cela signifie que le port d'écoute est le port 80. Il n'est pas crypté et donc peu sécurisé. La redirection du port sera la port 443, correspondant au port HTTPS, l'URL de ressources relationnelles sera donc : HTTPS://www.resources-relationnelles.fr. Il s'agit d'un protocole sécurisé qui crypte les connexions via les protocoles SSL (Secure Sockets Layer) /TLS (Transport Layer Security) et garantit que toutes les données transférées restent privées.

Let's encript est une autorité de certification qui fournit des certificat SSL/ TLS gratuits. Il s'agit d'un protocole sécurisé qui crypte les connexions via les protocoles SSL (Secure Sockets Layer) /TLS (Transport Layer Security) et garantit que toutes les données transférées restent privées.

Les certificats SSL fonctionnent comme suit :

Un certificat SSL établit une connexion chiffrée entre un serveur/site web et un navigateur lors d'un processus invisible et instantané appelé négociation SSL.

Authentification : Chaque fois qu'un visiteur lance une nouvelle session sur votre site, le serveur s'identifie au moyen d'un certificat SSL, dont la validité est vérifiée par le navigateur du visiteur.

Chiffrement : Le serveur partage sa clé publique avec le navigateur qui l'utilise pour créer et chiffrer une clé « pré-master ». C'est ce que l'on appelle l'échange de clés.

Déchiffrement : Le serveur déchiffre le pré-master à l'aide de sa clé privée pour établir une connexion chiffrée et sécurisée pendant toute la durée de la session.

Les protocoles TLS/SSL fonctionnent sur tous les principaux systèmes d'exploitation installés sur des appareils récents. De plus, Les moteurs de recherche tels que Google donnent la priorité aux sites web sécurisés HTTPS dans leurs résultats de recherche.

NGINX (modSecurity) en tant que Serveur proxy inverse interviendra pour répartir la charge du trafic entre plusieurs serveurs d'application en amont. Il peut équilibrer la charge entre les serveurs, améliorant ainsi la disponibilité et les performances globales du système. Il est capable de détecter les tentatives d'exploitation, les attaques par injection SQL, les attaques par cross-site scripting (XSS), les tentatives d'accès non autorisées et d'autres types d'attaques courantes contre les applications web. Il utilise des règles basées sur des signatures et des modèles pour identifier les modèles de trafic malveillant. ModSecurity peut filtrer les requêtes HTTP entrantes et sortantes en se basant sur divers critères tels que les en-têtes, les paramètres de requête, les cookies, etc. Il permet de bloquer les requêtes malveillantes avant qu'elles n'atteignent l'application web, réduisant ainsi les risques de compromission.

ModSecurity est un module de sécurité puissant pour Nginx, permettant de renforcer la protection des applications web contre les attaques courantes. Il aide à détecter, bloquer et filtrer les requêtes malveillantes, contribuant ainsi à améliorer la sécurité globale de l'infrastructure web.

WAF : (web application firewall) est conçue pour protéger les applications web contre diverses menaces et attaques en ligne. Il agit comme un filtre entre le serveur web et le trafic web entrant, en surveillant et en analysant les requêtes et les réponses pour identifier et bloquer les activités malveillantes ou suspectes.

Ses principales options : Il peut filtrer le trafic HTTP/HTTPS et filtrer des requêtes malveillantes et les bloquer. Il a une capacité de détection basée sur des signatures, l'analyse du comportement et la détection des anomalies, pour identifier les menaces connues et inconnues, y compris les vulnérabilités courantes des applications web telles que l'injection SQL, les attaques DDoS (botnet), ... Il est particulièrement efficace pour atténuer les attaques répertoriées dans le top 10 de l'**OWASP** (Open Web Application Security Project), permet une surveillance du trafic, et une personnalisation des règles de sécurité si besoin.

La **DMZ** : (zone démilitarisée) est un sous réseau isolé et sécurisé qui se situe entre le réseau interne d'une organisation et internet, tout en limitant l'accès direct, aux ressources sensibles du réseau interne. Son but est de renforcer la sécurité en séparant les services accessibles au public, du réseau interne où se trouvent les données et les systèmes sensibles.

Les principales caractéristiques du DMZ : Elle fournit une couche d'isolement entre internet et le réseau, permet de contrôler les flux de données et de filtrer les attaques potentielles. Les services destinés à être accessibles depuis Internet, tels que les sites web, les serveurs de messagerie, peuvent être hébergés dans la DMZ pour offrir une accessibilité externe tout en minimisant les risques pour le réseau interne. LA DMZ facilite la surveillance et la journalisation du trafic entrant et sortant.

L'accès au **Back-End et à l'API** se fait avec une demande de **token**, Nous avons mis en place un système d'authentification robuste pour tous les utilisateurs en incluant des protocoles d'authentification qui permettrons de vérifier l'identité des utilisateurs et de générer des tokens d'accès.

Lorsque l'utilisateur se sera identifié avec succès (login et mot de passe robuste), un token se génèrera pour valider l'accès. Les tokens sont des chaines de caractères aléatoires, uniques, cryptés et qui contiennent des informations telles que l'identifiant de l'utilisateur, la durée de validité et les autorisations associées. Ces informations sont conservées dans une BDD sous forme d'informations chiffrées.

Lorsque l'utilisateur voudra accéder au Back-end, la validité de la signature et de l'intégrité du token sera vérifiée, ainsi que sa date d'expiration et plusieurs autres paramètres seront vérifiés. Si le token d'accès est vérifié, l'utilisateur aura accès au Back-end. Les tokens doivent avoir une durée de vie limitée. Il faut mettre en place des mécanismes de renouvellement des tokens expirés.

Le chiffrement des données sera un chiffrement asymétrique, d'une clé publique et d'une clé privée. La clé publique est partagée aux utilisateurs et la clé privée est conservée en sécurité et elle n'est accessible qu'a l'entité responsable du décryptage des données.

Seules les entités qui ont la clé privée correspondante seront en mesure de décrypter les données et de restaurer les données.

Enfin le port d'écoute par défaut de la base de données MariaDB (3306) est modifié afin de rendre la base de données moins visible pour les attaques automatisées. Cela renforce la défense en profondeur et oblige les attaquant à deviner le port exact d'accès à la BDD.

RGPD

Ressources relationnelles traite les données personnelles suivantes :

La table User est utilisée pour renseigner l'identité de l'utilisateur, elle contient les éléments suivants :

Nom, prénom, email, nom utilisateur, le pays.

Toutes ces données sont sensibles et indispensables pour retrouver une personne.

Nous avons instauré un formulaire de consentement éclairé pour les utilisateurs, Le consentement doit être librement donné, spécifique, éclairé et révocable à tout moment. Le ministère doit fournir des informations claires et compréhensibles sur la manière dont les données sont collectées, utilisées, partagées, et conservées. Une politique de confidentialité doit être fournie à tous les utilisateurs. (Voir annexe 1)

Le ministère doit fournir aux utilisateurs de l'application, un droit d'accès à leurs données personnelles, le droit de les rectifier, de les supprimer, le droit à la portabilité des données et le droit de s'opposer au traitement des données.

Les mesures de sécurité qui sont mises en place pour protéger les données personnelles contre les accès non autorisés, les fuites, les pertes ou les altérations sont :

La gestion des accès avec la mise en place de contrôles d'accès comme par exemple l'utilisation de mots de passe forts, d'authentification à deux facteurs, et des restrictions d'accès basés sur les rôles : dans notre cas les utilisateurs ont des rôles de citoyens et des rôles restreints.

Le chiffrement des données, notamment le chiffrement des mots de passes.

La mise en place de pare feu, de systèmes de détection d'intrusion et d'autres mesures de sécurité pour protéger les réseaux utilisés pour stocker et transmettre des données personnelles.

La protection des serveurs, en réalisant régulièrement des sauvegardes, des contrôles d'accès…

Le personnel de l'entreprise doit aussi être sensibilisé à l'importance de la protection des données.

De plus un signalement aux autorités des violations des données ainsi qu'aux individus concernés doivent être faites dans un délai de 72h suivant leur découverte.

Le ministère doit tenir des registres des activités de traitement des données. Ce registre doit contenir les renseignements suivantes (renseignements non exhaustifs)

Identifier les activités de traitement

Collecte des informations pertinentes

Documenter les bases légales

Identifier les responsables du traitement

Il est recommandé aussi de faire appel à un professionnel du droit ou un spécialiste du traitement des données.

Un délégué RGPD doit être nommé au sein du ministère, (DPO). Il sera chargé de veiller à l'application des principes des RGPD, et aura un rôle consultatif sur tout questionnement relatif à la protection des données.

Tout manquement à ce règlement peut entrainer des sanctions allant jusqu'à 4% du chiffre d'affaires annuel mondial, ou 20 millions d'euros, selon le montant le plus élevé.

Bonnes pratiques

La sécurité informatique est une préoccupation majeure. Afin de préserver l'intégrité, la confidentialité et la disponibilité des informations sensibles, il est essentiel d'adopter de bonnes pratiques :

- Appliquer des pratiques de développement sécurisé, telles que la validation des entrées, l'échappement des sorties, la protection contre les attaques par injection et la gestion appropriée des droits d'accès.
- Effectuer des tests de sécurité réguliers, y compris des tests de pénétration, pour identifier les éventuelles vulnérabilités.
- Utiliser un système de contrôle de version (GIT par exemple) pour suivre les modifications apportées au code source permet de travail collaboratif et revenir en arrière si nécessaire.
- Documenter le code simplifie la maintenance future
- Arborescence propre (organisation des fichiers adaptée au projet, au langage et ou Framework utilisées).
- Nommer correctement les fichiers
- Front (performance de chargement en minimisant la taille des fichiers CSS, Javascript et d'images)
- Accessibilité pour tous les utilisateurs (personnes malvoyantes ou ayant des problèmes de motricité)
- Automatiser les tests (unitaires, intégration et régressions).
- Optimiser le SEO de l'application frontend pour une meilleure visibilité
- Utiliser les outils de suivi de performance pour améliorer la vitesse de chargement (PagesSpeedInsights, Lighthouse).
- Concevoir l'interface utilisateur adaptable sur d'autres appareils : Responsive design.

Plan de continuité des activités (PCA)

Analyse des impacts :

Dans le cadre de notre Plan de continuité des activités (PCA), nous avons effectué une analyse approfondie des impacts potentiels de l'interruption des activités critiques de notre organisation. Cette analyse vise à identifier les activités et les ressources essentielles, à évaluer les conséquences de leur interruption et à déterminer les délais de reprise acceptables. Voici les résultats de cette analyse :

	Production	**Service clientèle**	**Systèmes informatiques**	**Opérations financières**	**Partenariats stratégies**

Ressources critiques	Baisse de la capacité à répondre à la demande du marché, des retards de livraison des produits	Détérioration de la satisfaction client	Retards dans les opérations internes, une perte de productivité et des erreurs dans la gestion des ressources	Retards dans le recouvrement des créances, problèmes de trésorerie et une perturbation des relations avec les fournisseurs et les partenaires commerciaux	Perte de collaborations commerciales, une diminution des opportunités de croissance et une altération de notre position concurrentielle
Impact financier	Perte de revenus significative				
Impact opérationnel	Baisse de la capacité de réponse à la demande				
Impact de réputation	Mauvais impact sur la satisfaction clients				
Délai de reprise acceptable	48h	24h	12h	48h	72h

Stratégies de continuité :

Afin de garantir la continuité de nos activités critiques en cas de sinistre, nous avons développé des stratégies spécifiques pour chaque activité et ressource essentielle. Ces stratégies visent à maintenir nos opérations ou à les rétablir le plus rapidement possible en identifiant des alternatives et des mesures de préparation appropriées. Voici les stratégies clés que nous avons mises en place pour nos activités critiques

	Production	Service clientèle	Systèmes informatiques	Opérations financières	Partenariats stratégiques
Stratégie	Stratégie de relocalisation vers un site alternatif prééquipé avec des machines similaires et des ressources nécessaires	Stratégie de redirection des appels vers une équipe dédiée travaillant à distance, capable de fournir un soutien continu aux clients.	Stratégie de sauvegarde et de récupération régulière des données, ainsi qu'un plan de reprise après sinistre pour restaurer rapidement les services essentiels.	Stratégie de sauvegarde régulière des données financières et des procédures de récupération pour minimiser les pertes et faciliter la reprise.	Stratégie de communicatio n régulière avec les partenaires, afin de les informer du plan de continuité des activités et de coordonner en cas d'incident.
Alternative	Identification d'un fournisseur externe capable de prendre en charge la production en cas d'urgence	Communicatio n en ligne, assistance aux clients via des canaux virtuels,	Partenariat avec un fournisseur de cloud computing pour héberger les systèmes de manière redondante, ce qui permet de basculer rapidement vers une infrastructure alternative en cas de panne ou d'indisponibilité.	Arrangements avec une banque partenaire pour assurer la continuité des opérations financières, afin de garantir les transactions et les paiements essentiels.	Identification des partenaires alternatifs dans des régions géographiques différentes

Plan d'urgence :

Notre Plan de continuité des activités (PCA) comprend également un Plan d'urgence détaillé pour guider nos actions en cas de sinistre. Ce plan fournit des procédures claires et détaillées à suivre pour assurer une réponse rapide et coordonnée. Voici comment nous avons élaboré notre Plan d'urgence en utilisant les mêmes exemples :

	Production	Service clientèle	Systèmes informatiques	Opérations financières	Partenariats stratégiques

Alerte et notification	Système d'alerte sonore, Notifications mobiles	Système d'alerte par e-mail, Messages d'urgence sur le site web	Outils de surveillance des systèmes, Système de gestion des incidents	Système d'alerte bancaire, Système de détection des fraudes.	Réseau de communication d'urgence, Contacts d'urgence
Sauvegarde des équipements / données	En cas d'évacuation des locaux de production, prévoir des **procédures** pour **sauvegarder** les **équipements** et les données critiques, en particulier en isolant les machines et en effectuant des copies de sauvegarde hors site si possible.	Procédures pour sauvegarder les données client et les systèmes de gestion des tickets, en s'assurant que les informations critiques sont accessibles et protégées en cas d'évacuation ou de sinistre.	Procédures pour effectuer des sauvegardes régulières des données, des configurations système et des paramètres critiques, en veillant à ce que les sauvegardes soient stockées de manière sécurisée et accessibles en cas d'urgence.	Mettre en place des procédures de sauvegarde régulières des données financières, en veillant à leur intégrité et à leur accessibilité en cas de sinistre.	
Activation et alternatives	Désigner une équipe responsable de coordonner la relocalisation vers le site alternatif prééquipé, en suivant un plan préétabli comprenant les délais et les étapes nécessaires.	Prévoir des mesures pour activer les canaux de communication en ligne	Désigner une équipe chargée de suivre le plan de reprise après sinistre, comprenant la restauration des systèmes à partir des sauvegardes, la réaffectation des ressources et la vérification de l'intégrité des données.	Désigner une équipe responsable de contacter la banque partenaire et d'activer les arrangements préétablis pour assurer la continuité des opérations financières.	Plan pour réaffecter les activités ou trouver des alternatives pour maintenir les relations commerciales critiques.

Plan de reprise après sinistre

Notre Plan de reprise après sinistre (PRS) vise à rétablir nos activités normales le plus rapidement possible après un sinistre. Il comprend des étapes spécifiques pour restaurer les systèmes, récupérer les données, réaffecter les ressources et effectuer des tests réguliers pour assurer sa faisabilité et son efficacité.

	Production	**Service clientèle**	**Systèmes informatiques**	**Opérations financières**	**Partenariats stratégiques**
Restauration	Évaluer les dommages causés aux installations de production et planifier les travaux de réparation et de remise en état	Réactiver les canaux de communication traditionnels tels que les lignes téléphoniques et les e-mails après s'être assuré de leur fonctionnement normal. Informer les clients de la reprise des opérations via des messages de communication clairs et précis.	Identifier les serveurs et les systèmes endommagés et coordonner leur restauration ou leur remplacement. Réinstaller les logiciels et les applications nécessaires pour le fonctionnement des systèmes.	Réinstaller les logiciels financiers et les applications nécessaires pour le traitement des transactions et des opérations financières. Vérifier l'intégrité des données financières et leur conformité avec les sauvegardes réalisées.	Informer rapidement les partenaires stratégiques de la situation après le sinistre et de la reprise des activités normales. Coordonner les actions nécessaires pour minimiser les perturbations et maintenir les collaborations fructueuses.

Récupération	Identifier les machines endommagées ou perdues et coordonner leur remplacement ou leur réparation. Assurer la disponibilité des pièces de rechange critiques pour minimiser les temps d'arrêt.	Restaurer les bases de données client à partir des sauvegardes réalisées pendant la période d'interruption. Vérifier l'intégrité des données et s'assurer de leur disponibilité pour une continuité fluide du service clientèle.	Restaurer les données à partir des sauvegardes réalisées avant le sinistre. Effectuer des tests de récupération pour vérifier l'intégrité des données et s'assurer qu'elles sont complètes et exploitables.	Examiner les transactions en attente ou non traitées pendant la période d'interruption et les traiter selon les procédures de récupération prévues. Coordonner avec les banques partenaires pour s'assurer de la continuité des opérations financières.	Rétablir les activités conjointes avec les partenaires, en s'assurant de la disponibilité des ressources nécessaires, de la coordination des équipes et de la résolution des problèmes éventuels.
Réaffectation	Affecter le personnel nécessaire à la reprise de la production. Fournir une formation supplémentaire si nécessaire pour s'adapter aux nouvelles installations ou équipements.	Affecter les membres du personnel du service clientèle à leurs fonctions habituelles et fournir des directives claires sur les procédures mises à jour après le sinistre.	Affecter les équipes informatiques et les administrateurs système à leurs rôles respectifs.	Affecter les membres du personnel des opérations financières à leurs tâches habituelles. Fournir des directives sur les procédures mises à jour après	Réaffecter les membres du personnel chargés de la gestion des partenariats à leurs rôles respectifs et s'assurer qu'ils

				le sinistre et effectuer des formations si nécessaire.	sont informés des procédures et des mesures mises en place après le sinistre.

Formation et communication :

La formation et la communication jouent un rôle crucial dans la mise en œuvre réussie du Plan de continuité des activités (PCA). Voici les étapes clés à suivre pour sensibiliser le personnel et les parties prenantes et garantir leur compréhension des procédures de continuité des activités

	Production	**Service clientèle**	**Systèmes informatiques**	**Opérations financières**	**Partenariats stratégiques**

Sensibilisation du personnel	Organiser des sessions de sensibilisation pour le personnel de production afin de les informer sur l'importance du PCA, les risques potentiels et les mesures d'urgence à prendre en cas de sinistre. Mettre l'accent sur les procédures spécifiques de relocalisation et de réaffectation des ressources.	Dispenser une formation approfondie aux membres du personnel du service clientèle sur les procédures de continuité des activités, l'utilisation des canaux de communication alternatifs et la résolution des problèmes courants liés à la continuité des services.	Fournir une formation approfondie au personnel informatique sur les procédures de sauvegarde, de récupération des données et de reprise après sinistre. Assurez-vous qu'ils sont familiarisés avec les outils et les logiciels nécessaires à la mise en œuvre du PCA.	Dispenser une formation approfondie au personnel financier sur les procédures de continuité des activités, notamment la façon de traiter les transactions en cas d'interruption des systèmes, la gestion des réserves de trésorerie et l'utilisation des arrangements avec les banques partenaires.	Fournir une formation spécifique aux équipes de gestion des partenariats sur les procédures de continuité des activités liées aux partenariats stratégiques. Cela inclut la communication en cas d'incident, la coordination des actions d'urgence avec les partenaires et l'adaptation des accords commerciaux en cas de sinistre.
Formation pratique	Organiser des exercices pratiques pour permettre au personnel de se familiariser avec les procédures de reprise après sinistre, y compris la mise en place d'une ligne de production temporaire dans un site alternatif et l'utilisation d'équipements de remplacement.	Établir des canaux de communication internes dédiés pour diffuser des informations importantes sur les situations d'urgence, les mises à jour du PCA et les changements dans les procédures de service clientèle.	Documenter les procédures de reprise après sinistre de manière claire et accessible à tous les membres de l'équipe informatique. Mettre à disposition des manuels d'utilisation, des guides pas à pas et des ressources en ligne pour référence ultérieure.	Établir des lignes directrices claires sur les procédures financières d'urgence et les responsabilités de chaque membre du personnel financier. Assurez-vous que tous les employés ont accès à ces directives et sont capables de les comprendre et de les suivre en cas de sinistre.	Organiser des réunions régulières avec les partenaires stratégiques pour discuter des procédures de continuité des activités, partager les plans d'urgence respectifs et mettre à jour les informations de contact en cas d'urgence.

Communication continue	Maintenir une communication régulière avec le personnel de production en diffusant des rappels sur les procédures de continuité des activités, en organisant des réunions périodiques pour discuter des mises à jour et en encourageant le partage d'expériences et de bonnes pratiques.	Développer un plan de communication externe pour informer les clients des mesures prises pour assurer la continuité des services en cas de sinistre. Cela peut inclure des communiqués de presse, des mises à jour sur le site web de l'entreprise ou des messages sur les réseaux sociaux.	Organiser régulièrement des exercices de simulation pour le personnel informatique, où ils peuvent mettre en pratique les procédures de reprise après sinistre, tester les sauvegardes et les systèmes de récupération, et résoudre les problèmes éventuels.	Sensibiliser le personnel financier sur l'importance de la confidentialité des informations financières et des mesures de sécurité appropriées à prendre en cas de sinistre. Mettre en place des formations régulières sur la gestion des données sensibles et les protocoles de sécurité financière.	Établir un système de gestion des connaissances ou une plateforme en ligne pour stocker et partager les informations pertinentes sur les partenariats stratégiques, y compris les procédures de continuité des activités spécifiques à chaque partenaire.

Annexes

Annexe 1 : Politique de confidentialité

1. Informations collectées

1.1 Données personnelles : Lors de votre utilisation de notre application, nous pouvons collecter des informations personnelles vous concernant, telles que votre nom, votre adresse e-mail, votre numéro de téléphone et toute autre information que vous choisissez de nous fournir.

1.2 Données de ressources : Notre application peut également collecter des informations sur les ressources que vous traitez, telles que des fichiers, des documents ou des médias. Ces données de ressources sont traitées et stockées de manière sécurisée.

1.3 Données d'utilisation : Nous recueillons des informations sur votre utilisation de l'application, telles que les actions que vous effectuez, les fonctionnalités que vous utilisez et les préférences que vous configurez. Ces données d'utilisation peuvent inclure des informations telles que votre adresse IP, le type de navigateur que vous utilisez, les pages que vous visitez, les horaires d'accès et d'autres statistiques.

2. Utilisation des informations

2.1 Fourniture des services : Nous utilisons les informations collectées pour fournir, maintenir et améliorer notre application de traitement de ressources, ainsi que pour répondre à vos demandes et vous fournir un support technique.

2.2 Communication : Nous pouvons utiliser vos informations personnelles pour vous contacter concernant des mises à jour, des alertes de sécurité, des annonces ou d'autres informations importantes relatives à l'application. Nous pouvons également vous envoyer des communications promotionnelles, mais vous pouvez vous désabonner de ces communications à tout moment.

2.3 Amélioration de l'expérience utilisateur : Nous utilisons les données d'utilisation pour comprendre comment nos utilisateurs interagissent avec l'application, afin d'améliorer et d'optimiser leur expérience.

3. Stockage et sécurité des données

3.1 Conservation des données : Nous conservons vos données personnelles aussi longtemps que nécessaire pour atteindre les finalités décrites dans cette politique de confidentialité, sauf si la loi exige ou permet une conservation plus longue.

3.2 Sécurité des données : Nous prenons des mesures de sécurité appropriées pour protéger vos données personnelles contre tout accès non autorisé, toute divulgation, altération ou destruction. Cela inclut l'utilisation de techniques de cryptage, de pare-feu et de contrôles d'accès stricts.

4. Divulgation des informations

4.1 Partage avec des tiers : Nous ne partageons pas vos informations personnelles avec des tiers, sauf dans les cas suivants :

- Lorsque vous donnez votre consentement explicite pour le partage.

- Lorsque cela est nécessaire pour fournir les services demandés.

- Conformément à la loi, à une procédure judiciaire ou à une demande des autorités gouvernementales compétentes.

- Pour protéger nos droits, notre sécurité ou notre propriété, ainsi que ceux de nos utilisateurs ou du public.

4.2 Transferts internationaux : Dans le cadre de nos activités, vos informations personnelles peuvent être transférées et stockées dans des pays situés en dehors de votre pays de résidence. Nous nous engageons à prendre les mesures nécessaires pour assurer un niveau adéquat de protection des données lors de ces transferts.

4.3 Partenaires et prestataires de services : Nous pouvons faire appel à des partenaires et des prestataires de services tiers pour nous aider à fournir et à améliorer notre application. Ces tiers peuvent avoir accès à vos informations personnelles, mais ils sont tenus de les traiter conformément à nos instructions et dans le respect de cette politique de confidentialité.

4.4 Anonymisation des données : Nous pouvons agréger et anonymiser les informations collectées auprès des utilisateurs de manière à ce qu'elles ne puissent plus être associées à des individus identifiables. Ces données anonymisées peuvent être utilisées à des fins d'analyse, de statistiques ou de recherche.

5. Vos droits et choix

5.1 Accès et mise à jour : Vous avez le droit d'accéder aux informations personnelles que nous détenons à votre sujet et de demander leur correction, leur mise à jour ou leur suppression si elles sont inexactes ou périmées.

5.2 Désinscription : Vous pouvez choisir de ne plus recevoir de communications promotionnelles de notre part en suivant les instructions de désinscription fournies dans ces communications ou en nous contactant directement.

5.3 Cookies et technologies similaires : Notre application peut utiliser des cookies et d'autres technologies similaires pour collecter des informations sur votre utilisation. Vous pouvez configurer votre navigateur pour refuser les cookies ou vous alerter lorsqu'ils sont utilisés, mais cela peut limiter certaines fonctionnalités de l'application.

6. Modifications de la politique de confidentialité

Nous nous réservons le droit de modifier cette politique de confidentialité à tout moment. Toute modification sera publiée dans l'application et sera effective dès sa publication. Nous vous encourageons à consulter régulièrement cette politique de confidentialité pour rester informé des pratiques de protection des données.

7. Nous contacter

Si vous avez des questions, des préoccupations ou des demandes concernant cette politique de confidentialité ou nos pratiques de protection des données, veuillez nous contacter à contact@rose.fr

Date d'entrée en vigueur de la politique de confidentialité : 07/2023.