

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	1/40

Direction du Système d'information

Cahier des charges

DATA CONNECT

IFPEN

C3 - CONFIDENTIEL

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	2/40

Direction du Système d'information

Suivi des versions

Version	Date	Résumé des modifications	Auteurs	Relecteurs	Société
1	14/11/2024	Création document	API RRA	MBA HDU MME	IFPEN

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	3/40

Direction du Système d'information

SOMMAIRE

1 CONTEXTE 4

- 1.1 OBJET DU DOCUMENT 4
- 1.2 TERMINOLOGIE ET ABREVIATIONS 5
- 1.3 PRESENTATION DE L'ENTREPRISE 6

2 PRESENTATION DU PROJET ET DE SES ENJEUX 8

- 2.1 CONTEXTE ET OBJECTIF 8
- 2.2 BENEFICES ATTENDUS DU PROJET 8
- 2.3 PERIMETRE DU PROJET 9

3 DESCRIPTION DES FONCTIONNALITES ATTENDUES 10

- 3.1 DATA MOUVEMENT 10
- 3.2 DATA MANAGEMENT 12
- 3.3 MODE D'INTERFAÇAGE 14
- 3.4 ORDONNANCEMENT 15
- 3.5 CAS D'USAGES 16

4 EXIGENCES ET BESOINS TECHNIQUES 24

- 4.1 PREREQUIS TECHNIQUES 24
- 4.2 ARCHITECTURE ENVISAGEE 24
- 4.3 ENVIRONNEMENTS MIS A DISPOSITION 26
- 4.4 MODE DE DEPLOIEMENT 26
- 4.5 FACILITE D'UTILISATION 26
- 4.6 PERFORMANCES 27
- 4.7 SECURITE, CONFIDENTIALITE, INTEGRITE, CONTROLE D'ACCES ET OBLIGATIONS REGLEMENTAIRES 30

5 PRESTATIONS DU PRESENT MARCHE 37

- 5.1 PHASE PROJET 38
- 5.2 PHASE D'EXPLOITATION 39

6 ANNEXES 40

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	4/40

Direction du Système d'information

1 Contexte

1.1 Objet du document

Le présent document constitue le cahier des charges pour la mise en place d'une solution permettant :

- La Gestion de l'échange, le partage et l'exposition des données entre les applications du Système d'informations IFPEN (on premise ou en SAAS)
- La gestion de données de référence et notamment les données métiers

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	5/40

Direction du Système d'information

1.2 Terminologie et abréviations

Terminologie et abréviations utilisées dans le présent document	
Terme / sigle	Définition
Data Steward	Il est le responsable opérationnel pour la gestion des données d'un domaine
DSI	Direction du Système d'Information
EPIC	Etablissement Public à Caractère Industriel et Commercial
IFPEN	IFP Energies Nouvelles
MCO	Maintenance en Conditions Opérationnelles
MOA	Maîtrise d'Ouvrage
MOE	Maîtrise d'Œuvre
PSSIE	Politique de Sécurité des Systèmes d'Information de l'Etat
RDD	Responsable de domaine data, expert métier nommé par sa direction pour gérer et optimiser son domaine de données
RMA	Responsable Métier d'Application. Il(s) assure(nt) pour son métier le rôle d'administrateurs fonctionnels du logiciel. Les RMA font appel au RSIA dès lors qu'ils rencontrent des problèmes nécessitant des paramétrages, des interventions d'ordre informatique, etc.
RPO	Recovery Point Objective : durée maximale acceptable de perte de données après un incident conduisant à une indisponibilité
RSIA	Responsable SI d'Application. Il est le contact privilégié de l'éditeur pour les questions liées à la maintenance, les évolutions, le paramétrage et les éventuels développements du logiciel.
RSSI	Responsable de la Sécurité des Systèmes d'Information
RTO	Recovery Time Objective : temps maximum admissible pour reprendre le service après un incident conduisant à une indisponibilité
SAAS	Software As A Service
SI	Système d'Information
SIS	Système d'Information Support
SSO	Single Sign On

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	6/40

Direction du Système d'information

1.3 Présentation de l'entreprise

IFPEN est un acteur majeur de la recherche et de la formation dans les domaines de l'énergie, du transport et de l'environnement. De la recherche à l'industrie, l'innovation technologique est au cœur de son action, articulée autour de trois priorités stratégiques : mobilité durable, énergies nouvelles et hydrocarbures responsables.

Dans le cadre de la mission d'intérêt général confiée par les pouvoirs publics, l'IFPEN concentre ses efforts sur :

- L'apport de solutions aux défis sociétaux de l'énergie et du climat, en favorisant la transition vers une mobilité durable et l'émergence d'un mix énergétique plus diversifié ;
- La création de richesse et d'emplois, en soutenant l'activité économique française et européenne et la compétitivité des filières industrielles associées.

Ses programmes sont structurés autour de 3 priorités stratégiques :

- Mobilité durable : Développer des solutions pour des transports efficaces et à faible impact environnemental.
- Énergies nouvelles : Produire, à partir de sources renouvelables, des carburants, des intermédiaires chimiques et de l'énergie.
- Hydrocarbures responsables : Proposer des technologies visant à satisfaire la demande en énergie et en produits chimiques en consommant moins d'énergie et en réduisant l'impact environnemental.

Partie intégrante d'IFPEN, son école d'ingénieurs IFP School prépare les générations futures à relever ces défis.

IFPEN dispose d'un capital unique de connaissances issues de plusieurs dizaines d'années de recherche et d'expertise scientifique et industrielle. La mise à disposition de ce socle de connaissances auprès du plus grand nombre vise à éclairer et enrichir les choix collectifs et individuels face aux enjeux énergétiques et environnementaux actuels et futurs :

- 1800 salariés environ (1600 ETP) basés à Rueil-Malmaison et Solaize (banlieue lyonnaise) au 31/12/2022
- Dont plus de 1000 chercheurs et techniciens de R&I (ETP).
- IFP Energies nouvelles a accueilli 170 doctorants, post-docs et stagiaires (ETPT) sur l'année 2022.
- IFP Energies nouvelles fait également régulièrement appel à des vacataires.

Le pivot de la politique de valorisation d'IFPEN réside dans son portefeuille de filiales et de participations, qui rassemble aujourd'hui des acteurs industriels de référence au niveau mondial (Axens, Beicip-Franlab, IFP Training, etc.) et de jeunes entreprises innovantes. Ce modèle, qui a fait ses preuves dans le domaine des hydrocarbures, peut répondre au besoin actuel de création de filières dans les secteurs des énergies nouvelles et de la mobilité durable.

IFPEN oriente aujourd'hui ses efforts en ce sens, avec la création et la prise de participations au capital de sociétés centrées sur les NTE.

Vous trouverez des informations complémentaires sur l'IFPEN sur son site institutionnel : www.ifpenergiesnouvelles.fr.

1.3.1 Le système d'information de l'IFPEN

Le système d'information (SI) d'IFPEN se compose :

- des domaines de production de la R&D (modélisation et simulation, réalisation d'essais et d'analyses, conception de logiciels, etc.),

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	7/40

Direction du Système d'information

- des domaines du support et de pilotage de l'entreprise (stratégie, programmes & projets, partenariats, ...) et des domaines de support (achats, budget, comptabilité, ressources humaines, etc.).
- de domaines d'échanges et partage qui regroupent les fonctionnalités facilitant le travail collaboratif, l'accès à l'information et sa circulation entre les acteurs du SI dans le respect des habilitations de chacun.
- de domaines référentiels d'information qui identifient les données de référence partagées par plusieurs processus et applications du SI.
- de domaines techniques qui constituent les infrastructures informatiques : réseau et télécommunications, serveurs, stockage, poste de travail, etc.

1.3.2 Présentation de la Direction du Système d'Information IFPEN, commanditaire du projet

La DSI a pour missions, pour le système d'information de IFPEN (SI) :

- D'élaborer et mettre en œuvre la politique SI en cohérence avec la stratégie globale de l'entreprise,
- De mettre en place et entretenir un partenariat fort et équilibré avec les directions métiers, écouter leurs besoins et proposer des solutions adaptées,
- De conduire les projets d'évolution et les déployer,
- D'assurer le maintien en conditions opérationnelles des applications informatiques, entretenir et développer les infrastructures informatiques, assurer le support aux utilisateurs,
- D'optimiser les coûts de fonctionnement,
- De garantir la sécurité du SI en relation avec le responsable de la sécurité du système d'information (RSSI).

Ces missions s'exercent dans le cadre d'un schéma directeur du système d'information (SDSI) et d'une gouvernance SI d'entreprise.

La DSI emploie une cinquantaine de collaborateurs répartis entre les sites IFPEN de Lyon et Rueil-Malmaison.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	8/40

Direction du Système d'information

2 Présentation du projet et de ses enjeux

2.1 Contexte et objectif

Dans le cadre de son cœur de métier à savoir la recherche, et dans le cadre d'une gestion administrative de toute entreprise, le système d'informations IFPEN se doit de permettre :

- L'échange de données entre applications. Cet échange de données doit aussi prendre en compte parfois la transformation de ces données.
- De consolider et harmoniser la gestion des données
- De mettre en place une architecture data adaptée et performante pour répondre aux besoins métiers remontés par les RDD : Construction de Dataset avec une exposition maîtrisée et sécurisée pour des nouveaux produits data interne ou externe à l'entreprise

Le SI IFPEN est aujourd'hui équipé d'outils de type solution ETL ou de programmes spécifiques. L'objectif de ce projet est d'acquérir une solution permettant de gérer nos données intégrant des fonctionnalités d'ETL mais aussi de référencées celles-ci (MDM) permettant de répondre à nos deux besoins simultanément.

2.2 Bénéfices attendus du projet

Les bénéfices attendus de ce projet sont :

Des bénéfices métiers :

- Centralisation de l'accès aux données
- Traitements simplifiés tels que le filtrage, la jointure et le tri des données
- Partage des données avec gestion de la confidentialité à travers des API
- Intégration de traitement complexe en faisant appel à des programmes développés en interne
- Traçabilités de l'utilisation des données
- Amélioration de la qualité des données
- Recopie des données complètes, partielles, par delta
- Gestion des référentiels et métadonnées
- Masquages, chiffrements ou anonymisations de toute ou partie des données exposées.

Des bénéfices SI :

- Une rationalisation des flux vers les données applicatives sources avec un seul flux sortant d'une application contenant toutes les données à transmettre à l'ensemble des applications du SI IFPEN et un seul flux entrant contenant toutes les informations nécessaires à l'application alimentée quel que soit la source de ces données
- Une supervision de l'utilisation des données
- Une traçabilité des accès en cas d'audit ou de faille

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	9/40

Direction du Système d'information

2.3 Périmètre du projet

Le périmètre du projet vise à acquérir et installer techniquement une solution répondant à nos besoins

- De gestion de flux pour s'assurer que les données circulent de manière fluide et sécurisée entre les différentes applications du SI et les utilisateurs en minimisant les risques d'erreurs et de pertes d'information
- D'adoption de bonnes pratiques dans la gestion des données pour permettre non seulement de maintenir leur intégrité, mais aussi d'optimiser leur utilisation pour les consommateurs.
- De mise en place des processus rigoureux pour garantir que les informations soient précises, complètes et à jour.
- De gestion des référentiels pour assurer la cohérence et la fiabilité des données au sein de l'entreprise.
- De mise à disposition des données transformées, agrégées pour la création de nouveaux produits data et applications métier
- D'accélérer la construction de dataset, exposer ces données dans un cadre sécurisé
- D'autonomiser les acteurs de la DSI et les relais clés métiers de notre organisation à l'utilisation de ce type de solution.

Le projet est garant du respect des principes du DICT (Disponibilité, Intégrité, Confidentialité, Traçabilité) qui sont essentiels pour assurer la sécurité et la gestion efficace des données.

Le présent cahier des charges cible donc le choix d'une solution avec la prestation d'installation technique de la solution et des formations pour être autonome dans l'utilisation de cette solution.

A noter dans le cadre de projets en cours, des flux seront à mettre en place entre de nouvelles applications entrant dans le SI et d'anciennes applications ou des flux seront à migrer de la solution ETL actuelle vers la nouvelle solution mais ces prestations ne se feront pas dans le cadre de cet appel d'offres.

Un autre appel d'offres pourra éventuellement être émis pour spécifiquement des prestations de mise en œuvre de nouveaux flux ou migration de flux.

Toutefois afin de bien spécifier en détails les besoins attendus, ce cahier des charges fera référence à certains cas d'usages actuels ou futurs.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	10/40

Direction du Système d'information

3 Description des fonctionnalités attendues

3.1 Data mouvement

Le data mouvement regroupe toutes les fonctionnalités attendues pour ce projet Data Connect d'un ETL.

3.1.1 Extraction des données

La solution doit avoir la capacité d'extraire des données de diverses sources, telles que des bases de données relationnelles ou noSQL, des fichiers plats, des API, et des systèmes cloud.

3.1.2 Transformation des données

La solution doit permettre les actions, pour rendre les données cohérentes et utilisables, de

- Filtrage
- Nettoyage
- Normalisation
- Agrégation, notamment agrégation de données de différentes sources à destination d'une seule source
- Enrichissement des données
- Calcul à l'aide de fonction. Le titulaire donnera dans sa réponse des indications sur son catalogue de fonctions/formules incluses à la solution

IFPEN dispose de plusieurs référentiels et la solution doit être capable de les utiliser via des API ou des connexions à la base de données pendant les transformations.

La possibilité d'intégrer des traitements complexes (calculs et/ou algorithmes spécifiques) au sein des workflows est fortement attendu lors des processus de transformation.

Il est essentiel que chaque donnée puisse faire l'objet de plusieurs processus de transformation à la suite. Cela signifie que la solution doit être conçue pour permettre des modifications successives et adaptées aux besoins spécifiques de chaque étape.

3.1.3 Utilisation de programmes internes

Il est indispensable que la solution puisse exécuter des programmes créés en interne, tels que des codes Python ou des exécutables en Java. Cette fonctionnalité est obligatoire du fait que de nombreux traitements de données existent déjà et qu'il n'est pas envisageable de les réécrire dans la nouvelle solution. La solution devra donc être capable d'appeler et d'exécuter ces traitements

De plus, il sera nécessaire de pouvoir utiliser des bibliothèques internes standardisées, notamment pour certains calculs, comme les conversions d'unités de mesure, par exemple.

Il est attendu du titulaire qu'il présente dans sa réponse comment ces appels de code interne ou de bibliothèque seront effectués. À défaut, nous sommes ouverts à des propositions qui pourraient répondre à cette fonctionnalité.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	11/40

Direction du Système d'information

3.1.4 Virtualisation et persistance des données

La solution doit permettre la visualisation virtuelle des données brutes, transformées ou agrégées. Selon le choix de l'utilisateur, la solution doit permettre la persistance de ces vues virtuelles.

3.1.5 Gestion de version de données et des workflows

Pour garantir l'intégrité et la reproductibilité des analyses et la traçabilité des données utilisées dans les projets, la solution doit offrir la gestion de version de données persistées ou des workflows pour suivre précisément les versions des jeux de données et des traitements (filtres, calculs) appliqués pour les générer. La solution doit permettre ainsi de gérer les changements dans un jeu de données et de faire des traitements différentiels afin de ne capturer que les changements.

La solution doit également permettre de revenir à un jeu de données dans une version précédente.

3.1.6 Surveillance et gestion des erreurs

La supervision et la gestion des erreurs sont cruciales pour assurer la fiabilité et la sécurité de la solution. La solution doit permettre une surveillance continue afin de détecter les anomalies et les erreurs dès qu'elles surviennent. La supervision doit permettre d'alerter et/ou notifier les équipes responsables.

Un enregistrement des actions et événements dans des logs détaillés est attendu. Ces journaux permettront de retracer les étapes ayant conduit à une erreur pour identifier les causes et reconstruire les données dans l'état où elles étaient avant l'incident.

Le suivi des processus doit aussi être accessible aux RSIA et aux développeurs de flux pour assurer la gestion des erreurs et apporter des corrections si nécessaire dans le but de garantir l'intégrité des données.

3.1.7 Performance

A noter, le volume de données et de mouvement de données sera progressif. En effet comme indiqué précédemment la solution sera utilisée progressivement par la DSI avec tout d'abord la mise en œuvre de flux d'échanges pour de nouvelles applications du SI puis des migrations de flux présents dans un précédent ETL seront opérées. En parallèle, l'accès à la solution sera donné progressivement aux différents directions métiers pour la gestion de leurs données.

Il serait souhaitable que l'architecture de la solution soit évolutive afin de s'adapter à l'augmentation des volumes de traitements ou de données et qu'elle soit capable d'assurer une bonne performance, malgré de ponctuelle forte sollicitation.

3.1.8 Sécurité des données

La solution doit assurer la protection des données en transit ainsi qu'au repos quand celles-ci sont hébergées par le titulaire via un chiffrement des données au moyen d'un algorithme robuste.

Quand la solution est hébergée par le titulaire, elle doit permettre l'accès aux données avec des adresses IP internes ou connues et autorisées par le SI IFPEN, en plus de la politique d'accès nominative que la solution doit porter. Pour les mêmes raisons et dans les mêmes conditions, la solution doit avoir la capacité de fixer une adresse IP pour les interfaces avec les autres applications.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	12/40

Direction du Système d'information

Au vu de la confidentialité des données, IFPEN sera particulièrement sensible à la gestion de la sécurité de l'infrastructure hébergeant/traitant les données (Certifications, Audit de sécurité, gestion des failles, bonnes pratiques de développement, etc...)

3.1.9 Gérer efficacement les fichiers volumineux

Certains domaines de recherche génèrent des fichiers très volumineux, comme la modélisation moléculaire, la génomique, ou l'imagerie, des fichiers allant jusqu'à plusieurs centaines de Gigaoctets. Il est souhaitable que la solution permette l'envoi de ces fichiers depuis la source vers notre lac de données et le téléchargement depuis le lac de données.

3.1.10 Partage de données

Dans le cadre d'un projet, d'une activité, plusieurs directions ou départements sont amenés à travailler sur les mêmes données ou partager des données.

Il est fortement attendu que la solution mette à disposition un catalogue de données ou un data marketplace afin de parcourir les sources, les jeux de données et les API disponibles.

Ayant un fort intérêt sur le self-service data, cette marketplace sera un point d'entrée pour nos métiers pour la création d'autres applications ou produits data.

Sur certains projets, les directions IFPEN sont souvent amenés à travailler avec des partenaires externes. Il est fortement apprécié si le titulaire dispose de solution de partage de données, en dehors du SI IFPEN, qui répond aux contraintes de sécurité suivantes :

- Séparation des services pour limiter les impacts en cas de compromission
- Contrôle des adresses IP autorisées à faire transiter des données, si le titulaire propose un déploiement en SAAS
- Contrôle d'accès avec compte et mot de passe sécurisé avec une gestion des droits d'accès

Le titulaire devra indiquer le coût de ce catalogue de données en option si ce dernier n'est pas inclus au tarif de base de la solution. IFPEN se réservant alors le droit de ne pas commander cette option.

3.2 Data Management

3.2.1 Gestion centralisée des droits d'accès aux données

La solution doit permettre la gestion centralisée des droits d'accès. Cette gestion de droit permettra de définir, ajuster et contrôler qui peut consulter, modifier, supprimer des données ou chiffrer la donnée.

A noter dans un dataset de données, il faut pouvoir masquer certaines données pour certains profils. Le paramétrage de droits doit être au niveau de chacun des données d'un dataset et non pour un dataset entier.

Cette gestion doit être flexible et permettre à des profils variés (chercheurs, ingénieurs, data scientists, etc.) d'interagir avec les données selon des règles prédéfinies.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	13/40

Direction du Système d'information

La solution doit garantir la cohérence des données critiques de l'organisation, ce qui est essentiel pour maintenir la qualité et l'intégrité des informations à travers les systèmes et projets.

Ce système de gestion des droits est obligatoire pour s'adapter aux différents besoins d'accès des utilisateurs notamment lors du développement de webapp par les directions où les droits d'accès doivent être garantis, ou lors de l'utilisation des données en mode « self data ».

3.2.2 Traçabilité et linéage des données

La solution doit permettre de visualiser le linéage des données afin d'identifier facilement les sources utilisées mais également les traitements effectués sur une donnée et la consommation faite de cette donnée

3.2.3 Qualité des données

La solution doit inclure la possibilité de valider des données (vérification des formats, des doublons, des valeurs manquantes, etc.), la correction des erreurs, et la mise en place de règles de validation et de nettoyage automatique.

La solution doit permettre la création et la maintenance d'un référentiel unique pour les données de référence, ainsi que la mise en place de processus de gouvernance des données pour assurer leur exactitude, cohérence et accessibilité. Il est également nécessaire d'inclure des outils de surveillance et de reporting pour suivre la qualité des données et identifier les écarts ou les problèmes potentiels de manière proactive.

Pour faciliter ce processus, il est nécessaire de définir et d'implémenter des connecteurs vers les "points de vérité", c'est-à-dire les références qui sont considérés comme exacts et fiables dans l'organisation. Ces points de vérité servent de base pour évaluer l'exactitude des données et identifier les anomalies potentielles. La solution doit permettre le signalement des problèmes en fournissant un accès facile aux données de référence fiables.

3.2.4 Gestion des Métadonnées

La solution doit fournir la gestion des métadonnées, ces métadonnées permettront d'assurer que les informations contextuelles (descriptions des jeux de données, provenance des données, transformations subies, etc...) sont correctement documentées.

Pour garantir une gestion efficace des métadonnées, la solution doit fournir des fonctionnalités robustes permettant de capturer, stocker et gérer les informations contextuelles relatives aux jeux de données. Ces métadonnées comprennent des descriptions détaillées, l'origine des données, les transformations subies, ainsi que les usages et les consommations effectuées. En facilitant l'accès à ces informations, la solution contribue à une meilleure compréhension et à une utilisation optimisée des données, tout en renforçant la gouvernance des données et en soutenant les processus décisionnels.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	14/40

Direction du Système d'information

3.2.5 Chiffrement/hachage de la donnée

La solution doit permettre le chiffrement ou le hachage d'une donnée en particulier ou de toutes les données d'une bibliothèque de données. Ainsi le paramétrage de chiffrement/hachage doit pouvoir être fait finement et à la demande.

3.3 Mode d'interfaçage

La solution doit pouvoir faire du data mouvement pour réceptionner ou transmettre des données de différentes manières. Bien évidemment la façon dont les données sont récupérées en entrée de la solution peut varier de la façon dont les données sortent de la solution.

3.3.1 Fichiers

La solution doit permettre les échanges de fichiers de type CSV, TXT, Parquet, Orc, XLS, JSON ou XML. Le format de fichier XML ne doit pas être imposé, la solution doit permettre de paramétrer en entrée comme en sortie un format de fichier XML.

Il ne pourrait pas être accepté que la solution ne gère qu'un seul format de fichier XML qu'il faudrait imposer aux solutions émettant ou réceptionnant le fichier.

Il est attendu que la solution gère efficacement les protocoles de transfert de fichier (FTPS, SFTP, ...) sécurisés.

A noter certains outils de notre système d'information imposent des lignes d'entête et des lignes de fin dans les fichiers échangés. Ainsi la solution doit permettre de paramétrer facilement ces lignes qui peuvent contenir des données statiques ou des données dynamiques calculées à partir des autres données présentes dans le fichier (exemple notamment où la ligne de total doit être la somme des lignes de montant). Le titulaire présentera dans sa réponse la façon de paramétrer ces lignes.

Dans l'idéal la solution à partir d'un fichier en entrée proposera une structuration du dataset pour faciliter sa création.

3.3.2 Base de données relationnelle et NoSQL

Il est souhaitable que la solution dispose des connecteurs nécessaires pour se connecter à différentes bases de données relationnelles ou NoSQL dont :

- Oracle
- Microsoft SQL Server
- MariaDB
- PostgreSQL
- MongoDB
- InfluxDb
- Neo4J

Le titulaire précisera dans sa réponse les bases de données connectables et celles non connectables à la solution.

Si la connexion à certaines bases de données n'est possible qu'en lecture et non en écriture, le titulaire devra impérativement l'indiquer dans sa réponse.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	15/40

Direction du Système d'information

3.3.3 Système de fichier et stockage

Les données sont, dans la majeure partie des cas, stockés sur des zones réseau. La solution doit disposer des connecteurs soit par la capacité de montage sur un conteneur ou un serveur pour lire et écrire sur des systèmes de stockage :

- NFS
- S3
- CIFS

3.3.4 API et Webservices

La solution doit pouvoir interagir avec d'autres solutions via des API ou des webservices en entrée ou en sortie mis à disposition par des applications tierces.

En particulier, la solution doit pouvoir communiquer avec notre ERP CEGID XRP ULTIMATE en lisant des fichiers plats fournis ou en utilisant les API REST fournies par CEGID.

La solution doit également permettre de concevoir des API de manière simplifiée en mode nocode ou à défaut lowcode à partir de données transférées dans la solution.

Dans l'idéal, la solution pourra être utilisée comme une API Management permettant ainsi de garantir que les API sont utilisables et sécurisées. Le titulaire dans sa réponse à ce cahier des charges devra présenter pour chaque fonctionnalité listée ci-dessous si celle-ci est déjà prévue dans la solution, est prévue dans la roadmap d'évolutions de la solution ou n'est pas encore prévue à date :

- Conception d'API
- Passerelle d'API
- Catalogue d'API
- Analyse des API permettant de surveiller l'utilisation des API

Une attention particulière sera portée aux capacités de sécurisation liées à ce service.

3.3.5 Authentification

Les sources de données IFPEN, utilisent plusieurs modes d'authentification. La solution doit pouvoir utiliser ces modes d'authentification (Bearer token, User / mot de passe, Kerberos, Keycloak, ...) afin de collecter les données.

3.4 Ordonnancement

IFPEN a besoin de planifier et d'automatiser des tâches pour une exécution régulière et sans intervention manuelle.

Le titulaire dans sa réponse devra indiquer :

- S'il est possible qu'un ordonnanceur externe à la solution, exemple l'ordonnanceur VTOM déjà présent dans le SI IFPEN, puisse lancer des traitements de la solution tel que des transformations de données, mouvements de données, générations, de données, Le titulaire devra préciser techniquement comment ces traitements doivent être appelés par l'ordonnanceur externe.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	16/40

Direction du Système d'information

- S'il est possible via des API de la solution ou des API externes de déclencher des workflows internes à la solution.
- Si la solution contient un ordonnanceur interne. Dans ce cas de figure le titulaire devra indiquer le coût de cet ordonnanceur en option si ce dernier n'est pas inclus au tarif de base de la solution. IFPEN se réservant alors le droit de ne pas commander cette option.

3.5 Cas d'usages

Afin d'illustrer les besoins que nous avons, le présent document présente quelques cas d'usages qui seront potentiellement implémentés dans la future solution.

3.5.1 Paie RH et ERP Finance

Un des flux de données qui sera à mettre en place dans la nouvelle solution est l'envoi des OD de Paie depuis l'outil de Paie Teams RH vers le nouvel ERP Cegid XRP Ultimate en cours d'implémentation pour IFPEN.

Le fichier généré par l'application Teams RH est un fichier .dat avec position fixe pour les champs
Ce fichier ne comporte pas d'en-tête.

Les données présentes dans ce fichier doivent être transmises à l'ERP Cegid via les webservices mis à disposition par Cegid.

Données fournies par TEAMS	Type	Longueur	Règle d'alimentation
Code rubrique de paie	Char	6	Identifiant unique de la rubrique de paie. Peut être complété par des chiffres à la fin ex PRET01 . Attention le code de la rubrique peut n'être que sur 5 caractères et le champ est complété par un espace pour respecter la longueur de 6. Les éventuels espaces ne doivent pas être transmis à l'ERP.
Compte comptable	Char	6	
Section analytique	Char	6	
Signe du montant	Char	1	montant positif au débit => + montant négatif au débit => - montant positif au crédit => - montant négatif au crédit => +
Montant	Nombre	20	montant en centimes
Matricule du salarié	Char	6	renseigné pour les rubriques et comptes auxiliaisés seulement
Nom du salarié	Char	23	renseigné pour les rubriques et comptes auxiliaisés seulement

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	17/40

Direction du Système d'information

Section d'affectation du salarié	Char	6	renseigné pour les rubriques et comptes auxiliaisés seulement
----------------------------------	------	---	---

3.5.2 Référentiels RH Filiales pour application SANTRA

L'application SANTRA au sein du SI IFPEN est l'application gérant des données de santé. Les filiales IFPEN doivent transmettre à cette application leur fichier RH de collaborateurs. Une transformation est nécessaire entre les fichiers de chacune des filiales qui ont des formats différents vers un format de fichier identique pour SANTRA.

Ci-dessous un exemple de transformation nécessaire.

Le format de fichier en entrée peut être du .csv, du .txt ou autre. Le Fichier en Sortie Fichier SANTRA est un fichier csv avec des séparateurs ;.

A noter dans ce cas d'usage on doit passer par des tables de correspondance. Pour certains champs s'il n'y a pas de correspondance, l'enregistrement est transmis et dans certains cas, il faudra rejeter l'enregistrement.

De plus dans ce cas d'usage, il est nécessaire à partir des fichiers de données à transformer d'alimenter une table de correspondance pour ensuite utiliser cette nouvelle entrée de correspondance. Cf champ Emploi.

Le fichier doit en sortie pour SANTRA également contenir une ligne d'en-tête listant le nom des champs.

Fichier SANTRA	Fichier d'une des filiales	Transformation /contrôles
Matricule	Matricule	
Civilite	Civilité	Transformer la donnée via une table de correspondance propre à la filiale
Nom	Nom	Obligatoire
Nomjeunefille	Nom Patronymique	
Prenom	Prénom	Obligatoire
Datenaissance	Date de naissance	Obligatoire
Paysnaissance		
Deptnaissance		

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	18/40

Direction du Système d'information

Fichier SANTRA	Fichier d'une des filiales	Transformation /contrôles
Villenaissance		
Nationalite		
Adresse1	Adresse	
Adresse2	Complément d'adresse	
Codepostal	Code postal	
Ville	Ville	
Pays	Pays	Transformer selon une table. Si aucune correspondance n'est trouvée, le traitement ne doit pas être interrompu la valeur sera alors vide
Teldomicile		
Telmobile		
Nss	Numéro de sécurité sociale	Supprimer les espaces présents dans le champ reçu de la filiale
Smaritale		
Nbenf		
Nbperscharge		
Handicap		
Dureehandicap		
Datehandicap		
Invalidite		
Dateinvalidite		
Catinvalidite		
Etabl		Valeur fixe à renseigner selon la filiale concernée dans le fichier

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	19/40

Direction du Système d'information

Fichier SANTRA	Fichier d'une des filiales	Transformation /contrôles
Service	Service	Vérifier que le service existe dans la table des services ; obligatoire
Emploi	Nom emploi	Appliquer la correspondance de la table des emplois . A partir du nom emploi prendre l'emploi SANTRA correspondant. Si le nom d'emploi n'existe pas dans la table de correspondance, il faut ajouter une ligne dans cette table : nom emploi Filiale , nom emploi Filiale + « (« + code emploi SANTRA incrémenté + «) », code emploi SANTRA incrémenté à partir du dernier du fichier . Ensuite prendre la valeur créé
Inseeemploi		
Datedeb	Date d'entrée dans le poste	Obligatoire
Dateemb	Date de début de contrat	Obligatoire
Datesite		
Datefin	Date de fin de contrat	
Typeptrc	Type contrat	Appliquer la correspondance ; obligatoire
Temps	Tps travail	Appliquer la correspondance ; non obligatoire ; si la correspondance n'est pas trouvée laisser le champ vide ; mettre un message d'erreur mais ne pas rejeter l'enregistrement
Pourcen	Tps travail	Appliquer la correspondance Temps de travail et prendre le pourcentage associé ; non obligatoire ; si la correspondance n'est pas trouvée laisser le champ vide ; mettre un message d'erreur mais ne pas rejeter l'enregistrement
Cycle		Valeur fixe à renseigner : Normal
Poste		
Amenag		

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	20/40

Direction du Système d'information

Fichier SANTRA	Fichier d'une des filiales	Transformation /contrôles
Astreinte		
Reclasse		
Archive	Date de fin de contrat	Si la date de fin est inférieure ou égale à la fin du mois en cours => , mettre la valeur 1, sinon mettre la valeur 0
Lieu		Valeur fixe à renseigner : Bâtiment Yuccas
Nomurgence		
Prenomurgence		
Lienurgence		
Teldomicileurgence		
Telmobileurgence		
Exempt		
Localisation		Valeur fixe à renseigner : BF
Mailpro	Mail professionnel	
Prenomresp		
Datenaissanceresp Nssresp		
Fct		
Codeempl	Poste	
Nonsuivisst		Valeur fixe à renseigner : 0

3.5.3 Ordre de paiement

La solution doit pouvoir recevoir depuis le nouvel ERP CEGID des ordres de paiements par Webservices et les transmettre en format fichier plat .TXT à notre outil de trésorerie Kyriba.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	21/40

Direction du Système d'information

La solution CEGID étant en cours d'implémentation le format des webservices n'est pas encore connu. En revanche le format de sortie du fichier à transmettre à l'outil de trésorerie devra être sous ce format :

Données à transmettre sur les différents types de lignes

- ligne d'en-tête, Commence par 03
- ligne destinataire, Commence par 06
- ligne total, Commence par 08

Structure enregistrement "entête"

Donnée	Position	Type	Valeur
Date de règlement	26 à 30	Alphanumérique	Format de la date JJMM
Référence de la remise	55 à 61	Alphanumérique	Référence cycle de paiement dans l'ERP, uniquement le n°
Code guichet émetteur	87 à 91	Alphanumérique	Code guichet du compte bancaire sur lequel les virements doivent être débités
N° compte émetteur	92 à 102	Alphanumérique	N° du compte bancaire sur lequel les virements doivent être débités
Code banque émetteur	150 à 154	Alphanumérique	Code banque du compte bancaire sur lequel les virements doivent être débités
BIC	161 à 171	Alphanumérique	Code BIC de la banque émettrice du virement

Structure enregistrement "destinataire"

Donnée	Position	Type	Valeur
Numéro d'émetteur	13 à 18	Alphanumérique	N° émetteur d'IFPEN
Domiciliation	55 à 74	Alphanumérique	Variable. Code guichet du compte bancaire pour NdF ou nom de la banque pour les factures fournisseurs
Code guichet destinataire	87 à 91	Alphanumérique	Variable. Code guichet du compte bancaire du destinataire du virement
N° compte destinataire	92 à 102	Alphanumérique	Variable. N° du compte bancaire du destinataire du virement
Montant	103 à 118	Numérique	Variable. En centime, pas de décimale.
Code banque destinataire	150 à 154	Alphanumérique	Variable. Code banque du compte bancaire du destinataire du virement
BIC	161 à 171	Alphanumérique	Code BIC de la banque destinatrice du virement

Structure enregistrement "total"

Donnée	Position	Type	Valeur
Montant total	103 à 118	Numérique	Somme de tous les montants des enregistrements de type "destinataire". En centime, pas de décimale.

3.5.4 Centralisation de l'accessibilité des données

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	22/40

Direction du Système d'information

Un chercheur qui étudie les propriétés de matériaux doit pouvoir accéder directement aux résultats des essais, aux données de modélisation, et aux métadonnées (comme les conditions expérimentales) sans devoir consulter plusieurs systèmes différents. Cela permet une comparaison rapide et efficace des données issues de différents projets.

Un ingénieur doit pouvoir facilement retrouver les résultats d'expérimentations antérieures et les données calculées à partir de celles-ci, facilitant ainsi l'optimisation de nouveaux procédés sans devoir fouiller dans différents fichiers et rapports.

3.5.5 Traitements donnés sans codage complexe

Dans un souci de la mise en place d'un self-service data, un utilisateur métier doit pouvoir facilement appliquer des filtres sur des données expérimentales mis à disposition dans la solution.

Les utilisateurs formés à l'outil doivent pouvoir mettre en place un workflow de traitement et générer des API de manière simple en no code / low code, sans avoir besoin de demander à un développeur d'écrire une requête SQL ou un programme.

L'utilisateur, disposant des autorisations requises, doit pouvoir utiliser une interface graphique pour trouver et exporter les résultats de ses workflows. Cela permet accélérer le processus d'itération et de décision.

3.5.6 Manipulation des données accessibles

Un chercheur doit pouvoir ajuster ses données en nettoyant et transformant la donnée, directement depuis une interface, sans attendre que la DSI lui fournisse un nouveau jeu de données retravaillé ou réajusté.

L'équipe de conception pourrait importer et ajuster des données externes (comme des fichiers Excel provenant de partenaires industriels) directement dans les outils internes sans l'intervention de la DSI, ce qui permettrait de tester rapidement l'impact de ces nouvelles données dans leurs simulations.

3.5.7 Intégration de traitements complexes

Un utilisateur doit pouvoir intégrer des calculs dans son processus de traitement des données pour automatiser des calculs spécifiques (comme des corrélations).

Un développeur qui a fait un programme de collecte et d'agrégation de données doit pouvoir intégrer son exécutable dans son workflow.

3.5.8 Gestion de version et alertes sur des modifications

Si les données brutes sur un procédé changent (par exemple, une modification des conditions expérimentales), les utilisateurs doivent être alertés immédiatement pour réévaluer les performances ou analyses basées sur ces données modifiées.

Un système de gestion de version permettrait de revenir à une version antérieure d'un jeu de données utilisé pour une simulation si une erreur ou un biais est détecté dans une version plus récente.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	23/40

Direction du Système d'information

Direction du Système d'information

4 Exigences et besoins techniques

4.1 Prérequis techniques

La solution devra impérativement :

- Assurer la data mouvement entre nos applications SAAS et nos applications *On-premise*
- Récupérer les données des applications SAAS et/ou *On-premise* afin de les agréger / consolider et les mettre à disposition à travers des API ou des fichiers d'export
- Être en capacité de traiter ou transférer des données au plus proche de celles-ci
- Sécuriser la data mouvement pour éviter les compromissions, les fuites
- Mettre en œuvre des fonctionnalités de contrôle d'accès aux données (en lecture, écriture et modification) par tout utilisateur et systèmes applicatifs, sur la base de rôles (RBAC ou ABAC) et être compatible avec une authentification SSO (OIDC ou SAMLv2)
- Répondre à un besoin très important de disponibilité, d'intégrité, de confidentialité et de traçabilité (DICT)

Dans le cas où la solution est hébergée par le titulaire, elle devra impérativement :

- Être en capacité de traiter ou transférer des données présentes dans SI IFPEN dans la même localisation (ex : d'une application on-premise vers une autre application on-premise, un utilisateur connecté au SI IFPEN qui manipule des données hébergées dans le SI IFPEN)
- Être hébergée de préférence en France puis, à défaut, dans un pays de l'Union Européenne
- Mettre en œuvre le chiffrement des données au repos et en transit au moyen d'un algorithme robuste
- Être certifiées selon des standards de sécurité reconnus (à minima une parmi les certifications suivantes : SecNumCloud, Soc2 type 2, ISO27001:2013, CSA-STAR level 2.)
- Mettre en œuvre un processus de maintien en conditions de sécurité régulier de ses infrastructures d'hébergement des données
- Permettre l'accès uniquement via des adresses IP autorisées par IFPEN
- Dans les conditions où la source et la destination des données sont sur site, opérer ses actions depuis ce même site
- Assurer un taux de disponibilité à minima de 99%

4.2 Architecture envisagée

IFPEN envisage l'architecture ci-dessous pour répondre aux prérequis techniques.

Le titulaire pourra, s'il le juge utile, proposer une architecture plus en adéquation avec le besoin.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	25/40

Direction du Système d'information

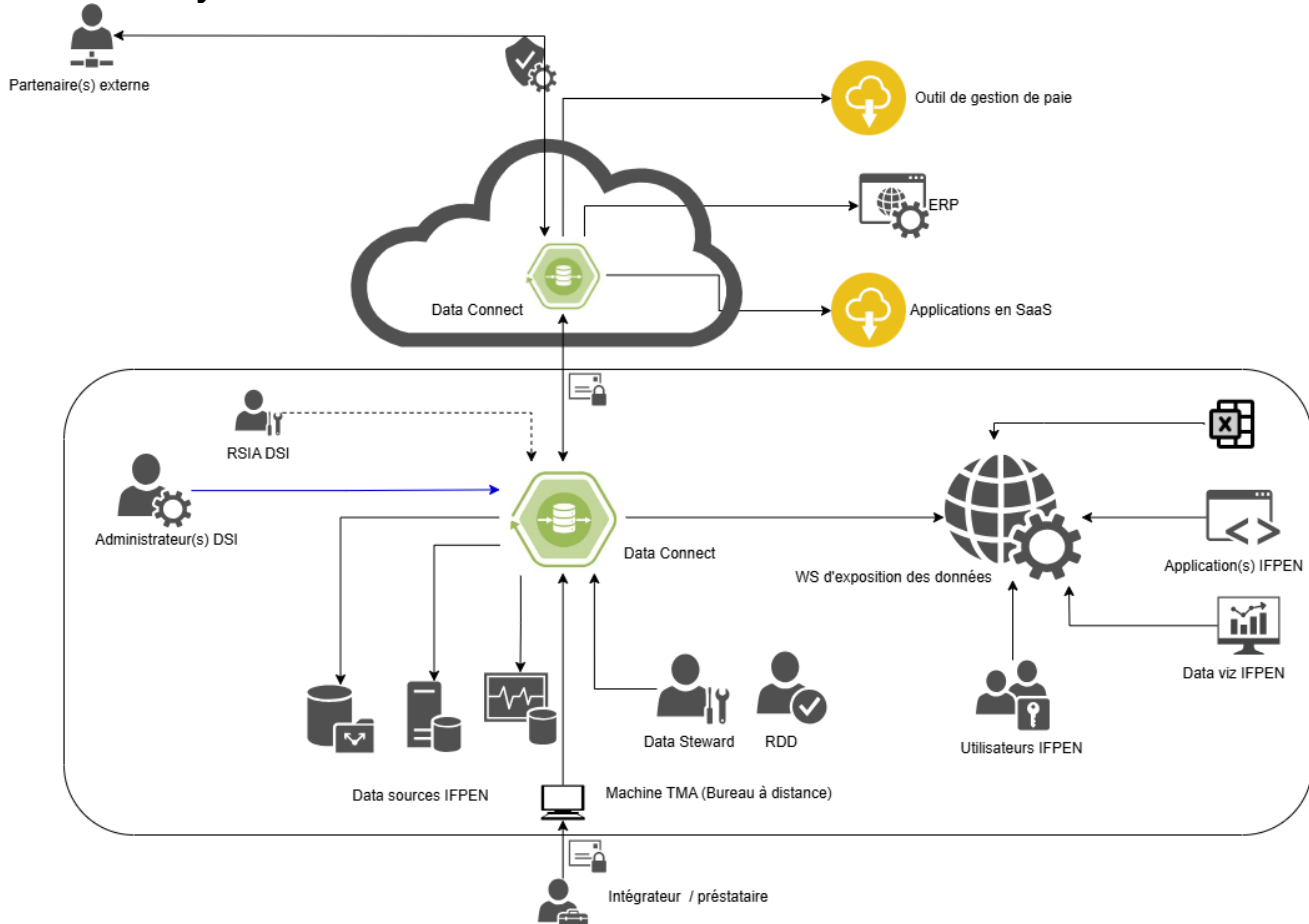


Figure 1 : Architecture envisagée

4.2.1 Architecture Hybride

Le SI IFPEN comprend des applications en SAAS et des applications et des sources de données On Premise. Avec l'objectif de centraliser le data mouvement, la solution doit pouvoir se déployer en mode « cluster » avec des instances dans le cloud et des instances on premise. A défaut de pouvoir se déployer en mode « cluster » deux instances séparées peuvent être considérées avec l'interconnexion des deux instances.

Ex : Les données de notre outil de GA en Saas et de notre outil de Gestion des talents également en Saas doivent pouvoir être agrégées et transmises à notre outil gestion des temps et des absences qui lui est en on-premise.

La solution doit aussi être capable de cloisonner les environnements de développement, de recette et de production.

Dans le cadre du marché, il sera attendue la livraison d'un document présentant l'architecture mise en place après le déploiement de celle-ci.

4.2.2 Hébergement de données

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	26/40

Direction du Système d'information

Si la solution doit héberger ou traiter des données, les lieux d'hébergement des données doivent satisfaire aux exigences de sécurité d'IFPEN, soit un hébergement de préférence en France puis, à défaut, dans un pays de l'Union Européenne.

4.3 Environnements mis à disposition

La solution doit proposer 3 environnements : développement, recette, production. Les données de production doivent pouvoir être mises sur des environnements de développement ou de recette dans certains cas de figure afin de réaliser des tests réels, investiguer sur d'éventuel erreur et apporter des corrections.

4.4 Mode de déploiement

Pour ces déploiements à l'initialisation et/ou mise à jour applicatif, le titulaire s'engage à fournir l'ensemble des prérequis techniques pour le déploiement sur différentes plateformes. Il est aussi demandé de s'engager sur l'architecture technique notamment en termes de dimensionnement et de toutes caractéristiques nécessaires à un fonctionnement performant de l'application (temps de réponses, traitements...).

Le titulaire devra indiquer dans sa réponse comment s'effectue les déploiements de la solution et de ses mises à jour et notamment s'il existe des automatismes.

La mise en place de clients léger (web) est à privilégier pour accéder aux interfaces d'administration et studio de développement des flux et workflows.

4.4.1 Reverse proxy

Pour les flux http/https, IFPEN pourra exposer ces URLs au travers d'un reverse proxy.

4.5 Facilité d'utilisation

4.5.1 Solution avec utilisation en mode low code/no code

L'utilisateur doit pouvoir créer ses workflows / flux de données / création d'API avec un minimum de code voir sans code. Avoir la possibilité d'un mode avancé avec codage est aussi requis.

Pour rappel certains utilisateurs seront des directions métiers et ne sont pas familiarisés avec le développement ou les langages de base de données.

4.5.2 Administration par IFPEN

Il est attendu que la solution puisse être administrée par IFPEN lui-même après une formation aux futurs administrateurs IFPEN prévue dans le cadre de ce marché.

Si la solution ne peut être administrée par IFPEN lui-même et nécessite obligatoirement une administration faite par un intégrateur ou l'éditeur lui-même, le titulaire devra l'indiquer dans sa réponse en précisant les raisons pour laquelle l'administration ne peut être assurée en interne IFPEN.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	27/40

Direction du Système d'information

A noter, le présent marché n'inclut pas cette prestation d'administration de la solution.

4.5.3 Ergonomie

Une attention particulière sera apportée à l'ergonomie proposée qui représente un des atouts majeurs de l'appropriation de la solution par les usagers.

L'utilisation de l'outil doit être rendu simple par une ergonomie adaptée :

- Interface intuitive, cohérente et simple pour l'utilisateur.
- Les écrans, y compris les messages d'erreurs, devront être en français, optimisés et responsive design. La présence d'un ascenseur horizontal est à éviter.
- L'utilisateur devra voir apparaître des messages explicites de confirmation en cas de suppression ou de modification impactante.
- Un message ou un pointeur de souris devra être affiché lors de traitements longs (sablier par exemple).

Le titulaire indiquera ses engagements en matière d'accessibilité au travers des fonctionnalités incluses dans la solution proposée ainsi que la roadmap de développement de l'accessibilité associée. Si une évaluation RG2A (Référentiel Général d'Amélioration de l'Accessibilité) ou d'un autre référentiel international équivalent a été réalisée, la mention obtenue devra être communiquée. Si des développements ou paramétrages sont réalisés au cours du projet, ceux-ci devront prendre en compte autant que possible les recommandations du référentiel RG2A (version active au moment du build). Les détails des critères et tests associés au RG2A 4 sont accessibles sur <https://accessibilite.numerique.gouv.fr>.

4.6 Performances

4.6.1 Disponibilité du service

La solution doit pouvoir être disponible 24h/24 et 7j/7

Le taux de disponibilité calculé en moyenne par le titulaire doit être précisé.

Si des interventions nécessitent une interruption de service pour maintenance applicative, ces dernières devront être faites en priorité les jours non ouvrés., IFPEN devra être informé des indisponibilités de la solution quelque soit l'environnement au moins 5 jours en amont. Dans le cas d'une intervention sur un jour ouvré IFPEN devra donner son accord pour l'intervention.

4.6.2 Compatibilité

L'application doit être accessible à travers le navigateur web Microsoft Edge for Business (Canal de mise à jour mensuelle)

Si un client lourd est disponible il sera uniquement utilisé par les administrateurs de la DSI.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	28/40

Direction du Système d'information

Le titulaire devra prévoir une vérification de la capacité du matériel de IFPEN à supporter les configurations nécessaires pour l'utilisation de la solution sur les postes des utilisateurs, sans coût supplémentaire pour IFPEN.

Les éléments de configuration standard en 2023 sont présentés ci-après :

Informatique d'entreprise (IE)

- PC Windows 10 64 bits (mémoire : 8/16 Go)
- Antivirus McAfee ENS10.x

Informatique scientifique (IS)

- PC Windows 10 64 bits (mémoire : 16 Go ou 32 Go)
- Antivirus McAfee ENS10.x
- PC Linux CentOS 7, Rocky Linux 64bits

Bureautique

- Microsoft 365 E3 (IE et IS Windows)
- OpenOffice version 3.1 (Informatique technique)

Messagerie

- Outlook 365/Exchange 2013 en cours de migration vers Exchange Online

Navigateurs Web

- Microsoft Edge for Business (Canal de mise à jour mensuelle)

Le titulaire devra indiquer dans sa réponse les prérequis techniques des serveurs hébergeant la solution selon l'architecture préconisée par la titulaire.

4.6.3 Continuité et rétablissement du service

La solution nécessitera la mise en œuvre d'une infrastructure et/ou de mécanismes devant être compatibles avec le RTO suivant : 2 heures maximum.

4.6.4 Réversibilité

En cas de cessation de la relation contractuelle, quelle qu'en soit la cause, le titulaire s'engagera à restituer gratuitement à la première demande de IFPEN formulée par lettre recommandée avec accusé de réception et dans un délai de 20 jours à la date de réception de la demande, l'ensemble des données lui appartenant (données des connexions des utilisateurs, algorithme de transformation des données, etc..) sous un format standard lisible sans difficulté dans un environnement équivalent.

Le format précis des données pourra être précisé.

IFPEN collaborera activement avec le titulaire afin de faciliter la récupération des données.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	29/40

Direction du Système d'information

Le titulaire fera en sorte qu'IFPEN puisse poursuivre l'exploitation des données, sans rupture, directement ou avec l'assistance d'un autre titulaire.

4.6.5 Calcul du Bilan Carbone (BGES)

Dans le cadre de sa RSO en conformité avec l'article L 229-25 du code de l'environnement et au décret 2022-982 du 1er juillet 2022 (<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046006338>), IFPEN effectue périodiquement un bilan carbone complet (calcul des émissions directes et indirecte de Gaz à Effet de Serre (Scope 1 à 3) afin de pouvoir suivre les évolutions effectives des plans d'actions mis en place. Pour les solutions informatiques externalisées (SaaS, hébergement), IFPEN doit avoir accès à différentes informations dont notamment :

- A la consommation d'électricité mensuelle (ou annuelle à minima) des équipements informatiques et des utilités nécessaires à leur fonctionnement.
- Aux émissions de gaz à effet de serre mensuelles (ou annuelles à minima) de la solution externalisée.

Rq : Ces consommations et émissions doivent être la résultante de l'activité d'IFPEN.

Si dans l'architecture proposée par le titulaire, une partie de la solution est hébergée par le titulaire ou un sous-traitant, le titulaire devra donner ces informations.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	30/40

Direction du Système d'information

4.7 Sécurité, confidentialité, intégrité, contrôle d'accès et obligations réglementaires

Le titulaire précisera l'organisation et les moyens qu'il mettra en œuvre pour répondre aux exigences de sécurité exprimées par IFPEN.

Dans sa réponse, le titulaire fournira sa politique de sécurité des systèmes d'information. Il décrira dans sa réponse les moyens (audits de sécurité, visite des installations, etc.) permettant d'assurer l'effectivité des garanties offertes par le(s) sous-traitant(s) en matière de protection des données.

4.7.1 Sécurité des accès

Le titulaire devra proposer une solution qui respectera les règles suivantes :

- La connexion aux applications "web" doit utiliser uniquement le protocole HTTPS : non seulement pour protéger les données d'authentification (nom d'utilisateur et mot de passe) des utilisateurs mais aussi l'ensemble du site web (règle obligatoire)
- Le serveur web devra utiliser le mécanisme du HSTS pour forcer toutes les connexions en HTTPS (règle recommandée)
- Le certificat SSL sera généré par IFPEN et l'intégrateur aura la charge de l'installer sur le serveur et de configurer l'applicatif pour le faire fonctionner (règle facultative)
- Les attaques de type « bruteforce » devront pouvoir être « contenues » par la solution en bloquant toute nouvelle tentative d'authentification par exemple pendant 1 minute après 5 tentatives d'authentification échouées (règle recommandée).

Des solutions de sécurité complémentaires seront potentiellement à envisager selon les architectures proposées.

4.7.2 Gestion des droits d'accès à l'application

Un utilisateur pourra se déconnecter afin de fermer sa session ; une nouvelle authentification sera alors nécessaire afin d'accéder à la solution.

Les accès utilisateurs et applicatifs seront tracés dans le cadre de la journalisation de la solution et devront être fournis à IFPEN dans le cadre d'un audit sécurité ou de traitement d'un incident de sécurité.

4.7.2.1 Authentification des utilisateurs

La solution devra proposer des mécanismes d'identification et d'authentification appropriés, afin de s'assurer, lors de l'accès aux données et aux fonctions applicatives, que le compte qui tente de se connecter est bien celui qu'il prétend être.

L'accès à la solution et à ses données devra pouvoir être sécurisé au moyen d'une connexion SSO vers l'Active Directory ou Azure AD IFPEN.

L'accès à la solution et à ses données pourra être sécurisé au moyen d'une authentification multifactorielle (règle recommandée).

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	31/40

Direction du Système d'information

4.7.2.2 Authentification compte local d'administration

Un compte d'administration local à l'application devra permettre une connexion hors Active Directory. Ceci garantira un accès en cas d'incident sur le service SSO d'IFPEN.

Le compte d'administration local à l'application devra pouvoir être paramétré pour une authentification multifactorielle ou à défaut avoir une procédure de bris de glace avec ce compte inaccessible sans celle-ci.

Ce compte pourra se déconnecter afin de fermer sa session ; une nouvelle authentification sera alors nécessaire afin d'accéder à la solution. Une déconnexion automatique doit s'effectuer au bout d'un certain temps.

4.7.2.3 Connexion en tant que ou Audit des droits

Un administrateur doit pouvoir naviguer dans l'appli avec les droits d'un autre utilisateur pour s'assurer du bon niveau de sécurité mise en place pour cet utilisateur.

Ou à défaut la solution doit proposer un outil d'audit des droits pour identifier pour un contenu les droits d'accès et d'actions d'un utilisateur.

4.7.3 Gestion des profils

Il est attendu du titulaire, de présenter une gestion de profil structurée de manière hiérarchique pour assurer une organisation claire et une sécurité renforcée de la solution.

4.7.3.1 Compte et Groupe

Compte : Un compte sera associé à un utilisateur individuel. Chaque utilisateur a un identifiant unique. Une application pourra aussi avoir un compte applicatif. A noter que ces comptes seront à récupérer depuis l'annuaire d'entreprise ou créés directement dans la solution.

Groupe : Les comptes utilisateurs pourront être regroupés en fonction de leurs rôles, directions ou départements. Par exemple, un groupe peut inclure tous les membres de la DSI. Il est attendu que ces groupes puissent être hérités de l'annuaire d'entreprise ou en local sur la solution.

4.7.3.2 Rôle et Habilitation

Rôle : Un rôle doit pouvoir être défini dans la solution pour un ensemble de permissions ou d'actions qu'un utilisateur ou un groupe peut effectuer sur la plateforme. Par exemple, un rôle "Administrateur" pourrait avoir des permissions complètes, tandis qu'un rôle "Analyste" pourrait avoir des permissions limitées à l'exploitation des données.

Habilitation : Les habilitations sont des autorisations spécifiques accordées à un rôle. Elles déterminent ce que les utilisateurs peuvent faire avec les données, comme lire, écrire, modifier ou supprimer des informations.

4.7.3.3 Groupe de données

La définition d'un groupe de données est attendu pour avoir une collection de données qui peut être gérée et sécurisée ensemble.

Par exemple, toutes les données financières peuvent être regroupées dans un groupe de données "Finance". Les rôles et habilitations seront appliqués aux groupes de données pour contrôler l'accès.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	32/40

Direction du Système d'information

Par exemple, seuls les utilisateurs avec le rôle "ERP Finance" pourraient avoir accès au groupe de données "Finance".

4.7.4 Restriction d'accès

Lorsque des mesures d'identification, d'authentification et de contrôle d'accès sont prises pour la solution, elles pourront être complétées de fonctions qui restreignent les conditions de ces accès (ex : le nombre d'accès (correspondant au nombre de comptes créés) ou de sessions de travail simultanées (pas de multi-session pour un même utilisateur)).

Une gestion de session utilisateur côté serveur permettra de valider chaque requête de l'utilisateur. La session pourra avoir une certaine durée de vie. A l'issue de ce délai d'activité, le système devra redemander une authentification. En cas d'inactivité dans un délai prédéfini ou à définir, le système forcera à se réauthentifier.

4.7.5 Contrôle des données

Les données manipulées au sein de la solution doivent être totalement intègres.

La solution devra donc proposer des mécanismes de contrôle des données et de résilience afin d'empêcher qu'une erreur, qu'un dysfonctionnement ou qu'une malveillance se propage et se traduise par une pollution incontrôlée des bases de données.

Ces contrôles doivent notamment porter sur les données entrées/saisies (type, taille, valeurs, format de date, format de nombre, format de coordonnées bancaires, etc...) dans la solution, les processus opératoires et les données de sortie de la solution.

4.7.6 Données à caractère personnel

Une donnée à caractère personnel est «Toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » (RGPD – Article 4.1).

Ainsi, les données à caractère personnel sont celles qui permettent d'identifier une personne en particulier. Autrement dit les noms, les adresses, les numéros de téléphone, les numéros de compte, le NIR, les adresses e-mail et les adresses IP, etc. L'identifiant de connexion au système d'information IFPEN est une donnée à caractère personnel.

4.7.7 Finalité du traitement des données à caractère personnel

Un traitement est «Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction» (RGPD, article 4.2).

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	33/40

Direction du Système d'information

Les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage licite, loyal et transparent. La collecte doit reposer sur une finalité déterminée.

Minimisation et exactitude des données

Seules doivent être traitées les informations pertinentes et juste nécessaires au regard des objectifs et des finalités poursuivis. Seules les données adéquates, pertinentes et non excessives pour la réalisation de la finalité sont collectées.

Durée de conservation des données limitée et archivage

Les informations ne peuvent être conservées de façon indéfinie dans le système d'information. La durée de conservation des données sera établie entre IFPEN et le titulaire. En outre, à la fin de la durée de conservation, les données à caractère personnel doivent automatiquement faire l'objet d'une suppression (purge du système d'information) ou d'une anonymisation des données à caractère personnel.

Si une justification particulière impose de conserver les données plus longtemps (obligation légale de conservation, contentieux potentiel, etc.), la conservation s'effectuera avec des droits restreints aux seules personnes ayant besoin d'accéder aux données.

Sécurité et de confidentialité des données à caractère personnel

Le titulaire responsable de la solution ainsi que le personnel IFPEN utilisateur de la solution doivent assurer la sécurité des données à caractère personnel. Ils doivent prendre les mesures nécessaires pour garantir notamment la confidentialité des données et éviter leur divulgation à des tiers non autorisés.

Ainsi, les données à caractère personnel ne doivent être consultées que par les personnes habilitées à y accéder en raison de leurs fonctions.

Les données peuvent néanmoins être communiquées à des tiers autorisés à en connaître en application de dispositions législatives particulières (Inspections du travail, services fiscaux, services de police...).

Respect des droits des personnes

Le titulaire via la solution proposée doit permettre à l'IFPEN de pouvoir respecter l'intégralité des droits des personnes de manière effective et sécurisée :

- Droits d'accès et de rectification.
- Droit d'opposition.
- Droit à la portabilité.
- Droit à l'effacement.
- Droit à la limitation du traitement.

Information au traitement des données

La solution proposée par le titulaire doit permettre à IFPEN d'exécuter son obligation d'information des personnes concernées par le traitement de données à caractère personnel conformément à l'article 13 du RGPD. La solution proposée par le titulaire devra être en disposition d'apporter à tout moment la preuve qu'elle a fourni à IFPEN les moyens d'informer les personnes concernées

Conformité RGPD du titulaire

Depuis le 25 mai 2018, date d'entrée en vigueur du nouveau règlement européen pour la protection des données à caractère personnel, le sous-traitant doit respecter les exigences posées par l'article 28 du Règlement général sur la protection des données. Par sous-traitant, il faut comprendre la personne physique ou morale, l'autorité publique, le service ou autre organisme qui traite des données à caractère

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	34/40

Direction du Système d'information

personnel pour le compte d'IFPEN et qui reçoit des instructions documentées de la part du responsable du traitement notamment :

- ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ;
- veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- prend toutes les mesures requises afin d'assurer la sécurité des données ;
- tient compte de la nature du traitement, aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits ;
- aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36 (violation de données à caractère personnel), et informe le responsable de traitement, dès connaissance, d'une violation de données à caractère personnel ;
- selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes ;
- met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

Le titulaire transmettra son registre des activités de traitement qui reprendra les traitements réalisés pour le compte de l'IFPEN.

Sous-traitance

Le titulaire ne peut pas sous-traiter les traitements qui lui sont confiés par l'IFPEN sans autorisation écrite spécifique préalable. L'IFPEN doit disposer de tous éléments utiles afin de donner son autorisation à la sous-traitance y compris ceux lui permettant de gérer les conséquences d'une sous-traitance (notamment les questions relatives au transfert de données hors de l'Union européenne).

Le titulaire doit déclarer à l'IFPEN l'ensemble de ses sous-traitants y compris ceux chargés de traiter les données confiées par l'IFPEN auxquels il envisage d'avoir recours.

Localisation des données

Les données à caractère personnel devront être traitées et hébergées sur le territoire français ou à défaut de l'Union européenne (lieu principal et secondaire).

Les données à caractère personnel ne feront l'objet d'aucun transfert de données à caractère personnel y compris entre les entités du groupe auquel le titulaire pourrait appartenir sans information et autorisation préalables de l'IFPEN.

Sécurité des données à caractère personnel

L'accès aux données traitées pour le compte de l'IFPEN doit être sécurisé conformément à l'état de l'art. Le titulaire doit garantir qu'il met en place des mesures afin de s'assurer que les ressources consacrées aux prestations réalisées pour l'IFPEN ne traitent les données que pour lesdites prestations.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	35/40

Direction du Système d'information

La solution du titulaire doit permettre la création et la gestion de profils d'utilisateurs de l'IFPEN afin de gérer les droits attribués à chacun (Par exemple, intégration de fichiers, modifications de la base de données, diffusion des données, etc.).

Le titulaire doit être en mesure d'identifier une violation de données à caractère personnel. Il devra préciser comment et dans quel délai.

Audit et fin du contrat

Le titulaire doit permettre à l'IFPEN de réaliser des audits et/ou de mandater un tiers aux fins de réalisation d'audit de la conformité des traitements qu'il met en œuvre pour son compte y compris les règles de sécurité.

Le titulaire doit s'engager à collaborer lors de la réalisation des audits tant par l'IFPEN que par un tiers qu'il pourrait mandater.

Le titulaire doit s'engager à respecter le choix de l'IFPEN quant à la restitution et/ou la suppression des données à caractère personnel à la fin du contrat.

En cas de sous-traitance, le titulaire doit s'assurer que les obligations de restitution et/ou de suppression sont respectées.

Protection contre les attaques en déni de service

Le titulaire devra avoir mis en place des mesures de protection contre les attaques de type DDoS. Il détaillera le fonctionnement de celles-ci.

Maintien en Condition de Sécurité (MCS)

Les composants applicatifs employés doivent être recensés et maintenus à jour. Cela inclut d'une manière non exhaustive : bases de données, serveurs applicatifs, serveurs webs, OS, BIOS des serveurs physiques, firmware des composants réseaux, etc.

Le titulaire appliquera les correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles (logiciels système ou applicatifs, logiciels embarqués) sur tous les matériels dont il a la charge. En cas d'alerte grave (attaque virale, faille critique) annoncée par le CERT-FR (Computer Emergency Response Team), le correctif devra être appliqué dans un délai de 48 heures sur les infrastructures hébergeant le système.

Si aucun correctif n'est disponible, le titulaire devra suivre les recommandations de l'éditeur ou du CERT-FR dans le cadre d'un contournement provisoire. Si le contournement nécessite la désactivation d'une fonctionnalité indispensable au système, le titulaire s'engagera à proposer des mesures permettant d'éviter l'exploitation de la vulnérabilité.

Le traitement des alertes mineures pourra intervenir durant les périodes de maintenance hebdomadaires ou mensuelles.

Les passages de correctifs devront être précédés d'une sauvegarde spécifique du système et des données qu'il contient, ainsi que de tests sur un environnement de pré-production.

Le titulaire devra mettre à jour le dossier de définition avec la liste des correctifs de sécurité appliqués sur les serveurs et communiquer à la demande du donneur d'ordres la version actualisée du document. La validation du bon fonctionnement du système se fera conjointement avec les équipes techniques du titulaire et le chef de projet responsable de la solution hébergée.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	36/40

Direction du Système d'information

En cas d'alerte donnée par les équipes d'experts du titulaire, par l'administration ou le CERT-FR, l'IFPEN sera notifié par courrier électronique avant toutes opérations. En particulier, le responsable sécurité de la maîtrise d'ouvrage sera le correspondant privilégié pour le suivi des opérations.

Le titulaire s'engage à fournir une adresse mail, un numéro de téléphone et les périodes correspondantes d'opération (H24, heures ouvrables, ...) permettant au maître d'ouvrage de suivre le traitement d'une alerte.

Fuite d'informations

Le titulaire veillera à limiter les renseignements fournis sur le fonctionnement technique du site web. Par exemple, le site web ne devra renvoyer ni les détails sur la version du serveur web, ni de message d'erreurs génériques.

La navigation dans les répertoires devra être désactivée.

Les bases de données ne doivent pas être exposées directement sur internet ; des mécanismes de protection doivent garantir sa sécurité (par ex : filtrage IP, accès par VPN ou bastion, etc.)

Le titulaire devra garantir l'étanchéité des données et en aucun cas permettre à d'autres clients d'avoir accès aux données de l'IFPEN.

Détection et réaction des incidents de sécurité

Une politique antivirale stricte devra être mise en place au niveau des serveurs dont le titulaire à la charge. La mise à jour des signatures devra être automatique et d'une fréquence élevée.

Un contrôle de non-contamination des serveurs Web de production devra être effectué périodiquement. Des mécanismes de supervision et de détection des incidents réseau entre les éléments constitutifs de l'application devra être mis en place (par exemple : IDS/IPS, NDR/EDR/XDR, IPS local, etc)

L'utilisation d'un antivirus de flux pour bloquer les fichiers malveillants en amont est recommandé.

4.7.8 Supervision

Le titulaire présentera la supervision disponible au sein de la solution notamment pour les tâches qui seraient automatisées.

4.7.9 Journalisation

La solution devra prévoir des mécanismes d'enregistrement des opérations que ce soit pour la conception de dataset, de flux d'échanges, d'accès/consultation/modification d'une donnée. Cet enregistrement sous forme d'audit devra pouvoir être consultable et les accès à sa consultation devront pouvoir être paramétrables au même titre que les autres droits d'accès.

Dans l'idéal, la solution proposera différents niveaux de logs. Ces différents niveaux de logs pourront être paramétrés différemment selon les datasets.

La solution devra également enregistrer et restituer toutes les modifications de paramétrage qui ont été effectuées.

La solution devra prévoir des mécanismes de protection des équipements (contrôle d'accès, etc...) de journalisation ainsi que les informations journalisées contre la modification et les accès non autorisés.

4.7.10 Sauvegarde/restauration

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	37/40

Direction du Système d'information

La solution devra proposer des fonctions permettant de sauvegarder les données de l'application (données de connexions des utilisateurs et les algorithmes de transformation de données, workflows),

Une perte des données de l'application saisies **durant les dernières 24 heures** est la tolérance maximale retenue (RPO).

Le titulaire présentera dans sa réponse, le plan de reprise d'activité (PRA) et la politique de sauvegarde mise en place permettant de satisfaire les exigences IFPEN.

Le titulaire devra protéger les sauvegardes archivées de l'altération, de la destruction et des accès non autorisés.

4.7.10.1 Gestion des incidents et des problèmes

Le titulaire devra mettre en place et documenter un processus de remontée et de gestion des incidents liés à la sécurité de l'information qui couvrira :

- le processus de signalement et d'escalade des événements liés à la sécurité de l'information,
- l'ouverture, l'analyse et le traitement des incidents,
- la correction des bugs et des anomalies (MCO),
- la correction des failles de sécurité des différents composants de l'architecture (MCS),
- les temps de traitement et de correction.

IFPEN devra être alerté de tout incident dès que celui-ci a été découvert par le titulaire.

L'ensemble des incidents devra être tracé.

Le titulaire devra également mettre en place et documenter un processus de gestion des incidents et problèmes, au sens ITIL, afin d'analyser les incidents rencontrés et minimiser leur apparition future.

4.7.10.2 Droit d'audit

IFPEN se réserve le droit d'auditer ou de faire auditer par une société tierce l'organisation de la sécurité mise en œuvre chez le titulaire et chez les éventuels titulaires intervenants dans le cadre de la présente prestation. Le titulaire précisera dans sa réponse le délai minimal de prévenance.

IFPEN pourra procéder avant mise en production à un audit sécurité qui vérifiera la conformité de l'infrastructure applicative (systèmes, composants, etc.) aux exigences IFPEN.

5 Prestations du présent marché

Le marché lié à cet appel d'offres comprend :

- En phase Projet
 - L'installation de la solution sur les différents environnements requis : développement, recette et production. Le titulaire devra indiquer dans sa réponse si l'installation sera à faire par IFPEN avec l'accompagnement du titulaire et de la documentation nécessaire ou si la prestation sera faite par le titulaire dans ce cas l'installation sera à faire avec un PC IFPEN fourni au prestataire pour cette prestation.
 - Trois typologies de formations
 - Formation à destination des utilisateurs de la DSI
 - Formation à destination des directions métiers R&I
 - Formation des administrateurs techniques de la solution

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	38/40

Direction du Système d'information

- Accompagnement sur le premier use case : cas d'usage ordre de paiement (de type échange de données entre deux applications)
- En phase d'exploitation
 - La mise à disposition de la solution pour une durée de 5 ans selon les modalités tarifaires du titulaire : achat ou locations de licences, abonnement/souscription aux services, etc...
 - Le support produit
 - La maintenance de la solution
 - Le maintien en condition de sécurité

5.1 Phase projet

5.1.1 Planning

La prestation d'installation de la solution devra être faite dans un délai souhaité de 04 semaines mais dans un délai maximum de 08 semaines après la signature du marché.

Les prestations de formations et d'accompagnement au premier use case, devront elles être réalisées dans un délai souhaité de 06 semaines et dans un délai maximum de 12 semaines.

5.1.2 Livrables

Les livrables attendus en phase de projet sont :

- La solution en elle-même
- Un guide utilisateur
- Un document présentant l'architecture applicative et le mode de fonctionnement ou à défaut une aide à la rédaction si faite par IFPEN
- Des supports de formations pour les 3 formations listées
- Document spécifiant le paramétrage (étapes du workflow, définition des données d'entrées, données de sortie, etc...) pour le premier use case

5.1.3 Recettes

IFPEN réalisera

- Une recette technique suite à l'installation de la solution permettant de vérifier que la solution est correctement installée en mettant en œuvre un premier flux d'échange simple d'exemple qui ne sera pas forcément un cas d'usage fonctionnel à réellement mettre en œuvre.
- Une recette fonctionnelle pour le premier use case qui sera mis en œuvre avec l'accompagnement du titulaire

A l'issue de chaque de recette, un PV de réception de recette sera émis.

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	39/40

Direction du Système d'information

5.1.4 Garantie

Une phase de Garantie de 1 mois est attendu pour les prestations

- d'installation de la solution à partir de la date d'installation de la solution

5.2 Phase d'exploitation

5.2.1 Support technique produit

Il est attendu qu'un support technique produit soit mis en place de la part du titulaire du marché pour répondre aux questions d'utilisation, diagnostique d'anomalie liée au « Produit » dans le cadre du marché et pour toute sa durée : 5 Ans.

La réponse à toute question posée (par courriel ou téléphone ou ticket support) devra être fournie dans les 2 jours ouvrés suivants le dépôt de la question.

Le service support devra être accessible dans la plage horaire suivante : du lundi au vendredi de 8h à 18h (heure française).

5.2.2 Maintenance du produit

Il est attendu de la part du titulaire une maintenance corrective et évolutive sur le « Produit » notamment avec des mises à disposition de nouvelles versions pour répondre à des exigences réglementaires, répondre à des problèmes de performances, dysfonctionnement technique de la solution et un maintien en condition de sécurité (MCS).

Les anomalies détectées par IFPEN devront pouvoir être remontées au titulaire via un outil de ticketing interne IFPEN Pégase, un outil de ticketing du titulaire ou à défaut par courriel et mail)

Le délai de traitement de l'anomalie sera dépendant de la typologie de l'anomalie

	T0	Délai maximal en jour ouvré de résolution
Livraison du correctif d'une Anomalie bloquante (impossibilité de manière permanente ou répétitive d'utiliser la solution)	Signalement par IFPEN	1 jour
Livraison du correctif d'une Anomalie majeure (une fonctionnalité qui est altérée et qui ralentit le processus ou impose des contraintes à l'utilisateur)	Signalement par IFPEN	3 jours
Livraison du correctif d'une Anomalie mineure	Signalement par IFPEN	10 jours

Diffusion	Étude	Référence	Date	Page
Externe	Z0059	458117-24-INF-SOL	11/12/24	40/40

Direction du Système d'information

6 Annexes

Sont annexés à ce cahier des charges :

- Annexe 1 : Grille fonctionnelle à compléter par le titulaire
- Annexe 2 : Question de sécurité, onglet Hébergement-Sécurité et Green-IT à compléter par le titulaire
- Annexe 3 : « Contexte informatique d'IFP Energies nouvelles » présentant l'environnement informatique d'IFP Energies nouvelles