

Annexe 2

Charte du RSSI d'IFPEN

Exigences et besoins techniques

Ergonomie

Une attention toute 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 rendue simple par une ergonomie adaptée :

- Limiter le nombre de pages et clic permettant la saisie et gestion des données personnelles et professionnelles d'un salarié
- 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 proscrire.
- 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. Les développements et paramétrages réalisés au cours du projet devront prendre en compte autant que possible les recommandations du référentiel RG2A (version active au moment de la réalisation) . Les détails des critères et tests associés au RG2A 4 sont accessibles sur <https://accessibilite.numerique.gouv.fr>.

Hébergement

Les lieux d'hébergement des données doivent satisfaire aux exigences de sécurité d'IFPEN et de son ministère de tutelle, soit un hébergement de préférence en France puis, à défaut, dans un pays de l'Union Européenne.

L'hébergement des données doit se faire à minima sur un site principal et un site de redondance. Le mémoire technique devra indiquer la liste de tous les lieux de stockage de données (site d'hébergement principal, site(s) de secours, mode de redondance entre les sites, etc...).

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.

- Identification et authentification

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 la personne qui tente de se connecter est bien celle qu'elle 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 IFPEN, selon une technologie compatible avec l'environnement technique actuellement en place chez IFPEN, décrite dans le tableau ci-dessous :

| Application | Progiciel | Version | Editeur |
|------------------------------|--------------------------|--------------|-----------|
| Annuaire d'entreprise | eDirectory | V8.8.8 | NetIQ |
| | NIM | V4.0.2 | |
| | -- Usercube (à venir) | | |
| Gestion des comptes | Active Directory | Version 2019 | Microsoft |
| Fédération d'identités / SSO | ADFS Azure AD SSO | | Microsoft |

A noter,

- un projet de changement d'annuaire d'entreprise au profit de la solution Usercube est en cours. La solution proposée devra être compatible avec l'annuaire eDirectory et l'annuaire Usercube.
- IFPEN dispose d'un SSO basé sur la technologie Microsoft ADFS compatible SAML v2 et est en cours de migration vers la technologie AZUR AD.

La connexion à la solution ne devra être autorisée que pour les adresses IP publiques IFPEN. (Règle recommandée)

Inversement, seule une plage d'adresse IP précise et bien identifiée sera configurée pour des demandes d'authentification à notre SSO.

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

La solution devra respecter 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).

Un utilisateur pourra se déconnecter afin de fermer sa session ; une nouvelle authentification sera alors nécessaire afin d'accéder à la solution. Une déconnexion automatique au bout de 30 minutes aura le même effet.

Les accès utilisateurs 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.

- Gestion des profils

La solution devra proposer des mécanismes simples, sûrs et cohérents de gestion des utilisateurs et de leurs habilitations au sein de l'outil lui-même. Cela permettra de définir pour chaque type de donnée au sein de la solution, qui pourra y avoir accès, avec quels droits (lecture, écriture, création, etc.).

Un mécanisme interne devra pouvoir fournir un listing des profils ainsi que le détail des profils attribués à quel utilisateur.

NOMBRES D'UTILISATEURS

L'accès à l'outil se fera selon des privilèges gérés par profil utilisateur qui seront à minima :

- LISTE DES PROFILS ATTENDUS

Le mémoire devra préciser le modèle financier lié aux volumes d'utilisateurs déclarés dans ce cahier des charges et à l'augmentation possible de ces volumes.

- Restriction d'accès

Lorsque des mesures d'identification, d'authentification et de contrôle d'accès sont prises pour la solution, elles devront être complétées de fonctions qui restreignent les conditions de ces accès : limitation des points d'accès (adresses IP IFPEN), du 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 durée de vie de 8 heures. A l'issue de ces 08h00 d'activité, le système devra redemander une authentification. En cas d'inactivité au bout de 30 minutes, le système forcera à se réauthentifier.

- 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.

- Chiffrement des données

Dans l'idéal, la solution proposera du chiffrement des données en base de données. Ce chiffrement de données doit pouvoir être activable dès le début ou par la suite sur décision d'IFPEN via une opération technique ne nécessitant pas une interruption de services de plus de 1 jour ouvré.

- 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.

- Finalité du traitement

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).

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

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 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 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.

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.

Protection de type défense en profondeur

L'architecture matérielle et logicielle du site web et de son infrastructure d'hébergement doit respecter le principe de défense en profondeur.

Par exemple :

- Architecture n-tiers (par exemple : séparation du serveur web, du serveur applicatif et de la base de données)
- Création d'une ou plusieurs DMZ pour isoler les différentes composantes de l'architecture n-tiers,

- Firewall périmétrique avec filtrage sur les ports http et https uniquement pour les accès depuis internet,
- Web Application Firewall pour filtrer les requêtes entrantes sur les ports autorisés (80 et 443),
- Logiciel antimalware sur le serveur pour analyser les fichiers uploadés,
- Firewall de type logiciel ou de l'OS pour restreindre les flux entre les serveurs composant l'architecture)
- Etc

Le titulaire détaillera le fonctionnement de ces différentes briques de sécurité en fournissant un diagramme réseau et un diagramme de flux entre celles-ci (de l'accès à internet au serveur de base de données). Cette matrice des flux précisera, tant en entrée qu'en sortie, et son respect devra être imposé par un filtrage réseau dissociant l'instance applicative IFPEN des autres clients du titulaire.

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.

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.

Exploitation du système

Supervision

Le titulaire présentera la supervision qu'il compte mettre en œuvre afin de garantir à IFPEN :

- la disponibilité de la solution et de l'ensemble des composants techniques
- le suivi des temps de réponse
- la bonne exécution de l'exploitation
- la mise à disposition des données sortantes (envoi des données vers IFPEN) et l'intégration des données entrantes au travers de la plateforme d'échange
- les alertes

IFPEN souhaite disposer d'un tableau de bord de suivi des indicateurs de supervision.

Journalisation

La solution devra prévoir des mécanismes d'enregistrement des opérations et des événements liés ou qui peuvent avoir des conséquences sur la sécurité de l'information (tentatives d'accès non-autorisées, opérations d'administration, erreurs, dysfonctionnements, modification ou tentative de modification des paramètres et des mesures de sécurité du système, etc.).

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.

Sauvegarde/restauration

La solution devra proposer des fonctions permettant de sauvegarder les données, ainsi que les configurations des équipements et des logiciels système selon une périodicité permettant de garantir la disponibilité du service selon le délai exprimé par IFPEN.

Une perte des données 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 présentera dans sa réponse, un plan de continuité d'activité (PCA) décrivant :

- Son délai maximal acceptable d'interruption de service
- Les données et applications qui concernées
- Les sites de secours utilisés
- Les procédures de restauration des données et des systèmes
- Les tests qui doivent être réalisés pour s'assurer que ce PCA est efficace

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

Administration des serveurs

L'administration des serveurs hébergeurs devra être effectuée de manière sécurisée :

- utilisation de protocoles faisant appel à du chiffrement : SSH au lieu de Telnet, SFTP au lieu de FTP, RDP sur TLS, etc,
- l'accès aux mécanismes d'administration doit être restreint aux seuls postes d'administration autorisés,
- les administrateurs doivent être authentifiés de manière sûre.

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.

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.

Environnement mis à disposition

Dans l'idéal, les différents environnements à mettre à disposition pour l'IFPEN sont les suivants :

- Environnement de production

- Environnement de recette permettant d'y dérouler la VABF ainsi que les formations et permettant une fois l'application en place, de faire des tests.
- Environnement de préproduction : IFPEN souhaite également disposer d'un environnement sur lequel il y aura une duplication régulière des données et du paramétrage de l'environnement de production

Le titulaire s'engage à fournir l'ensemble des prérequis techniques des différentes plateformes.

Performances

Disponibilité du service

La solution devra être disponible :

- 24/7 ou HO ?

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

Les interventions nécessitant une interruption de service pour maintenance applicative devront être faites en priorité les jours non ouvrés., IFPEN devra être informé des indisponibilités de la plateforme quel que 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.

Compatibilité

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

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

Informatique d'entreprise (IE)

- PC Windows 10 et 11 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)

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 : 5 jours ouvrés.

Niveau de service

Le titulaire devra proposer une architecture permettant d'atteindre les niveaux de services attendus pour l'ensemble des composants de la solution (serveur, liaison Internet, site web).

Temps de réponse

Le titulaire s'engagera à respecter les temps de réponse suivants au niveau du poste de travail :

- Connexion au système : 3 secondes maximum
- Affichage des écrans standards : 3 secondes maximum
- Enregistrement d'une modification de données : 3 secondes maximum
- Modification, création, enregistrement de paramétrage (fonctionnalité pour les administrateurs) : entre 5 et 10 secondes.
- Génération d'un rapport : 4 secondes maximum

Ces temps de réponse doivent être observés dans au moins 90% des transactions.

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 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.

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

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.