Annexe – recommandations informatiques

Les spécifications techniques

Le titulaire proposera une installation de sa solution en mode SaaS, sur sa propre infrastructure ou celle d'un hébergeur.

1.1 Volumétrie

L'outil devra supporter une capacité de stockage compatible aux besoins de service.
Chaque dossier lié à une convention de portage comporte et comportera une série de documents joints : convention, courriers, photos, plans, etc..)

1.2 Sécurité

La solution et l'organisation du titulaire devront se conformer aux exigences et pratiques de la direction solutions numériques relatives à la sécurité des systèmes numériques.

1.2.1 Définitions

Le Département de Loire-Atlantique s'est engagé dans une démarche globale de sécurité. Il est entendu par sécurité, le traitement de :

- **La disponibilité**, c'est l'aptitude du système à remplir une fonction dans des conditions définies d'horaires (en exemple : 24 heures, 5 jours, 10 jours)
- **La confidentialité**, c'est le caractère réservé d'une information dont l'accès est limité aux seules personnes admises à la connaître pour les besoins du service
  - Exemple de la notion de confidentialité :
  - Données restreintes au niveau d'accès
  - Données nécessitant une protection particulière
  - À cet égard les archives départementales sont en mesure d'apporter les informations nécessaires quant aux délais de communicabilité fixés par la loi du 15 juillet 2008
  - Données stratégiques ou engageant fortement la responsabilité du Département de Loire-Atlantique (et de l'Établissement public Foncier de Loire Atlantique)
- **L'intégrité** du système et de l'information qui garantit que ceux-ci ne sont modifiés que par une action volontaire et légitime. Lorsque l'information est échangée, l'intégrité s'étend à l'authentification du message, c'est-à-dire à la garantie de son origine et de sa destination.
- **La traçabilité** permettant d'identifier l'origine et de reconstituer le parcours d'une information depuis sa production jusqu'à son utilisation

1.2.2 Exigences

L'ensemble des exigences de sécurité ci-dessous doivent pouvoir être mis en œuvre en conformité avec l'Annexe Cadre de cohérence technique :

La DIMA (Durée d'Indisponibilité Maximale Acceptable) est inférieure à 4 heures en heures ouvrées

La PDMA (Perte de Données Max Acceptable) est d'une heure.

Confidentialité des données : diffusion limitée à un nombre réduit de personnes explicitement autorisées

Intégrité des données : les données peuvent contenir des erreurs si on peut les retrouver et les corriger

Traçabilité : les actions sur ce bien doivent pouvoir faire l'objet d'analyse a posteriori et être imputables à leurs auteurs

Authentification et habilitations :

- Mettre en place une authentification personnelle et nominative pour l'accès des utilisateurs.
  L'authentification doit respecter la politique de sécurité du Département en termes de définition et de gestion des mots de passe, soit en s'appuyant sur l'annuaire soit en respectant les règles 45 à 47 des "Règles d'intégration d'un nouveau composant" disponible sur l'espace collaboratif DSN (rubrique Urbanisation)
- Définir et mettre en œuvre différents profils d'accès en conformité avec le besoin d'en connaitre de chacun des utilisateurs (consultation, saisie, validation, administration, etc.)
- S'assurer que le projet formalise un processus de gestion et de revue des habilitations, précisant notamment les opérations de création, de revue et de suppression de comptes et des privilèges utilisateurs
- Mettre en œuvre une authentification forte pour accéder à l'application et effectuer les actions jugées sensibles (par exemple avec un certificat client) pour l'accès par le backoffice depuis internet

Journalisation :

- Identifier par le projet les évènements/actions nécessitant d'être tracés (saisie, modification, etc.)
- Paramétrer les mécanismes de traçabilité et de journalisation des actions identifiées. Assurer la sécurité des traces (interdire l'accès aux journaux en écriture ou centraliser les journaux sur un serveur tiers)
- Purger régulièrement pour une éviter une conservation excessive. Si nécessaire, mettre en œuvre une revue régulière des traces

Sécurité des logiciels :

- S'assurer que la surveillance et le déploiement des patchs de sécurité et des mises à jour des composants techniques qui supportent le service sont pris en compte par les équipes.
  S'assurer régulièrement (au moins annuellement) que le système est mis à jour par l'Editeur et par les équipes en charge du projet.
- S'assurer que les applications utilisées par le projet sont sous contrat de maintenance et que le projet dispose d'un support de l'éditeur
- S'assurer que les développements applicatifs respectent les bonnes pratiques de sécurité dans les développements (Exemple : OWASP pour les applications Web). Le développeur/éditeur doit s'engager à une maintenance corrective pour corriger les bugs, les erreurs de conception et les failles de sécurité de l'application.
- Valider la robustesse de son projet avant exposition sur Internet via un test d'intrusion
  En cas de solution externe, demander à l'hébergeur s'il subit régulièrement des tests d'intrusion

Sécurité des données :

- Etudier l'opportunité d'une solution de chiffrement des données lors de leur stockage en base de données
- Privilégier un hébergement/traitement de données en Europe pour les données à caractère personnelle. Si l'éditeur de la solution a son siège social aux Etats Unis, il conviendra de demander une preuve d'adhésion au "privacy shield" (accord en vigueur au 01/03/18)
- S'assurer que les communications sont chiffrées (exemple : HTTPS) pour garantir la confidentialité et l'intégrité des données.
- S'appuyer sur une offre de sauvegarde qui satisfait le besoin de PDMA d'une heure
  Définir et tester à intervalles réguliers la procédure de restauration des données sauvegardées.
- Mettre en place des dispositifs afin d'assurer une continuité d'activité respectant une DIMA inférieure à 4 heures en heures ouvrées
- Former régulièrement les utilisateurs de l'application pour éviter les erreurs d'utilisation (mauvaises saisies, informations erronées, etc.)
- Utiliser les solutions de la DSN pour l'échange de fichier sécurisée avec l'extérieur (Tiers, partenaires, etc.) & se conformer aux standards de la DSN pour l'interconnexion entre le SI du Tiers et celui du Département. En cas d'impossibilité technique par le prestataire, une dérogation devra être demandée par le projet auprès de son RSSI.
  Prévoir un chiffrement des données transférées
- Intégrer la solution d'archivage numérique proposée par la DSN

Continuité :

- Garantir la redondance des compétences pour permettre de palier à l'indisponibilité d'une personne de la DSN
- S'assurer que les SLA souscrit avec le partenaire hébergeur respecte les besoins en disponibilité de l'application
- Formaliser une documentation permettant de réinstaller l'application en cas de perte complète de celle-ci. Cette procédure devra notamment préciser le temps nécessaire pour être suivi. Tester ponctuellement le bon fonctionnement de la procédure
- Souscrire à l'offre standard de supervision fournie par la DSN (supervision sur socle techniquement uniquement)
- Etudier la mise en place en place d'une supervision applicative supplémentaire afin d'être prévenu au plus vite d'un disfonctionnement applicatif
- Prévoir dans le cahier des charges l'engagement de l'éditeur pour corriger les vulnérabilités identifiées lors des tests d'intrusion
- Prévoir le chiffrement des sauvegardes
- Le titulaire devra intégrer le plan d'assurance sécurité dans son offre
- Le titulaire devra être certifié ISO27001 sur le périmètre du projet
- Le Département doit être en mesure d'auditer la solution du titulaire

1.2.3 Authentification

Le titulaire se conformera aux exigences et pratiques de la DSN, précisées ci-dessous :
Pour procéder à l'authentification des utilisateurs de l'application, il est recommandé de déléguer l'authentification au serveur d'identités utilisée par le département (Keycloak).

Les dispositions et règles relatives à l'authentification sont décrites dans l'Annexe 2 « Règles d'architecture et d'intégration ».
Le Titulaire respectera la politique de sécurité du Département et décrites dans l'Annexe 3 « Politiques techniques de sécurité ».

Le titulaire devra notamment respecter :

- les recommandations de l'ANSSI, notamment les recommandations pour la mise en œuvre d'un site web : Maîtriser les standards de sécurité côté navigateur (https://www.ssi.gouv.fr/uploads/2013/05/anssi-guide-recommandations_mise_en_oeuvre_site_web_maitriser_standards_securite_cote_navigateur-v2.0.pdf);
- les recommandation de l'OWASP ;
- les exigences du référentiel RGS lors du développement de téléservice.

Si le titulaire souhaite utiliser des données de production pour réaliser des tests, le titulaire devra préalablement obtenir l'accord du Département et les anonymiser. Le prestataire devra assurer la confidentialité des données lors de leur anonymisation.

1.3 Accessibilité

Contexte :
L'article 47 de la loi n°2005-102 du 11 février 2005 pour « l'égalité des droits et des chances, la participation et la citoyenneté des personnes » rend obligatoire à tout service de communication publique en ligne d'être accessible à toutes les citoyennes et à tous les citoyens, qu'elles ou qu'ils soient ou non en situation de handicap (visuel, auditif, moteur, trouble divers...). Pour faciliter la mise en œuvre de **l'accessibilité numérique**, la **DINUM** édite depuis 2009 le **référentiel général d'amélioration de l'accessibilité - RGAA**, créé pour mettre en œuvre l'article 47 de la loi handicap de 2005 et son décret d'application n° 2019-768 du 24 juillet 2019 relatif à l'accessibilité aux personnes handicapées des services de communication au public en ligne. L'actuelle version en vigueur du RGAA est la 4.1 datée du 18 février 2021 (www.numerique.gouv.fr/publications/rgaa-accessibilite/).

L'accessibilité du web est une problématique d'accès aux contenus et services numériques web pour les personnes handicapées en particulier et, plus généralement, pour tous les utilisateurs, quels que soient leurs dispositifs d'accès ou d'assistance, leurs aptitudes physiques ou mentales ou leurs conditions d'environnement (matériel, culture, infra réseau, localisation…).

L'application du RGAA concerne à ce jour les services numériques suivants :

- ✓ les sites internet, intranet, extranet, les applications Web (progiciels métiers) dès lors qu'ils constituent des applications utilisées au travers d'un navigateur Web ou d'une application mobile ;
- ✓ les applications mobiles : tout logiciel d'application conçu et développé pour être utilisé sur des téléphones intelligents (smartphone/Iphone), tablette, hors OS ou matériel ;
- ✓ bornes interactives libre-service, pour leur partie applicative, hors OS ou matériel.

Depuis plus de 3 ans, le département de Loire-Atlantique a engagé un vaste chantier de mise en conformité de ses services en ligne internes et externes grâce à **une prise en compte du RGAA pour tout nouveau projet de service numérique**. Ce prérequis est également en vigueur pour son projet de dématérialisation du recrutement sachant que le pourcentage d'agentes et d'agents en situation de handicap y est à ce jour de plus de 8%. Ce nouveau service de recrutement devra ainsi contribuer à maintenir voire à améliorer cet existant.
À titre d'exemple, le site institutionnel présente aujourd'hui un taux de conformité de 84% (www.loire-atlantique.fr/44/accessibilite-partiellement-conforme/declaration-d-accessibilite/c_1364392). Cet excellent résultat a été obtenu en prenant en compte l'accessibilité dès la phase de conception de ce vaste projet de refonte. A cet effet, un « design system » sur lequel s'appuie la majorité des sites satellites du Département a été développé avec ce même niveau d'exigence pour assurer la pérennité de la démarche accessible engagée (https://design.loire-atlantique.fr/).
Au-delà de l'obligation légale, l'inclusion numérique s'inscrit donc pleinement dans les valeurs fondamentales et historiques du département de Loire-Atlantique.

Cadre réglementaire :
Ainsi, tout internaute ou personne agent du CD44 doit pouvoir accéder à l'ensemble des contenus numériques, depuis son navigateur web, sans que son éventuel handicap ne constitue un obstacle.
Afin d'être utilisable par les personnes en situation de handicap utilisant différents moyens de navigation (navigation sans souris, sans clavier), logiciels ou matériels spécialisés (lecteur vocal, plage Braille) ou nécessitant la personnalisation de l'affichage du site (grossissement des caractères, qualité des contrastes), les services en ligne numériques proposés au Département doivent se conformer avec les préconisations du RGAA.
Le Département pourra éventuellement réaliser un audit de vérification du niveau de conformité au RGAA 4.1.
Les corrections liées à l'accessibilité seront prises en charge et intégrées à la maintenance de la solution par le titulaire.

1.4 Performances

Les performances attendues de la solution logicielle sont de 3 secondes pour les opérations courantes.
L'ensemble des fonctionnalités prévues doit pouvoir être activé pour le nombre d'utilisateurs définis au chapitre volumétrie sans que cela n'influe sur les performances générales du système.
Pour atteindre les performances souhaitées, le titulaire indiquera avec précision les composants matériels et logiciels nécessaires ainsi que leurs caractéristiques minimums.