

Annexe : Exigences en matière de sécurité de l'information

Le prestataire devra proposer un concept de sécurité qui doit prendre en compte la mise en œuvre des exigences organisationnelles et techniques suivantes :

A- Exigences organisationnelles

Objectifs de sécurité de l'information

1. *Le contractant doit s'assurer que le partenaire a défini des objectifs de sécurité de l'information. Les objectifs doivent être révisés si des changements importants surviennent dans le projet. Le contractant doit documenter l'approbation formelle des objectifs de sécurité de l'information par le partenaire.*

Rôles et responsabilités

2. *Le contractant doit établir et diriger un comité de la sécurité de l'information qui doit inclure les représentants de la GIZ, le partenaire et le contractant. Le comité de sécurité de l'information doit se réunir régulièrement pour examiner les risques liés à la mise en œuvre du système et prendre des décisions sur les mesures d'atténuation. Toutes les réunions du comité de sécurité de l'information doivent être documentées par le contractant.*
3. *Le contractant doit identifier, analyser et évaluer le risque de sécurité de l'information. Le résultat de l'évaluation des risques de sécurité de l'information doit être rapporté au comité de sécurité de l'information et le plan de traitement des risques correspondant doit être documenté par le contractant.*
4. *La responsabilité du risque incombe au partenaire de la GIZ. Ce dernier est chargé de surveiller et de contrôler le risque et de veiller à ce qu'il soit atténué en temps opportun. Le partenaire a l'autorité de prendre des décisions sur les mesures d'atténuation des risques identifiés. Il est également responsable des résultats qui découlent ces mesures.*

Séparation des attributions

5. *L'octroi de droits d'accès erronés, inadéquats ou obsolètes dans le système d'information doit être évité. Par conséquent, le contractant doit établir un processus empêchant une seule et même personne d'approuver, attribuer, modifier et supprimer les droits d'accès dans le système d'information. Si cela devait être le cas, le contractant devrait obtenir l'accord formel du partenaire et devra le documenter.*

Sécurité de l'information dans la gestion de projet

6. *Le contractant devra proposer une méthodologie de gestion de projet qui démontre la prise en compte des présentes exigences de sécurité de l'information et la documentation de la conformité durant l'exécution du projet.*

Inventaire des actifs et responsabilités

7. *Le partenaire est le propriétaire du système d'information et il lui revient la responsabilité de s'assurer que seules les personnes autorisées ont accès et que le système d'information est géré de manière à protéger sa disponibilité, la confidentialité et l'intégrité des informations traitées.*
8. *Le contractant doit tenir un inventaire des actifs qui comprend tous les actifs qui composent le système d'information ainsi que les responsables d'actifs correspondants. Le contractant doit s'assurer que ces responsabilités sont approuvées par chaque responsable d'actif. Le contractant doit tenir l'inventaire des actifs à jour et le réviser régulièrement au besoin.*

Accord sur le niveau de service du contractant

9. *Le contractant doit convenir avec le partenaire d'un accord de niveau de service (SLA). Celui-ci doit documenter les attentes de niveau services que le contractant est tenu de respecter lors de l'assistance technique et de la maintenance du système d'information.*

B- Exigences techniques**Hébergement**

1. *L'application devra être hébergée dans le centre de données du partenaire ou dans un autre centre avec l'accord du partenaire ; les exigences techniques en matière de sécurité doivent être coordonnées avec le service informatique du partenaire.*

Framework

2. *Les informations sur le Framework utilisé ne doivent pas être incluses dans le code source des pages Web générées.*

Environnement de travail

3. *Le contractant veillera à mettre en place des environnements distincts pour le développement, les tests et la mise en production de l'application.*

Pare-feu & Antivirus

4. *Un pare-feu doit être installé en amont du serveur. Un logiciel antivirus à jour doit être utilisé sur le serveur et configuré en conséquence pour les mises à jour automatiques.*

Séparation de l'application et des données

5. *Une séparation entre l'application et les données doit être prévue, c'est-à-dire qu'un serveur d'application et un serveur distinct pour la base de données et le stockage des fichiers doivent être fournis, avec une communication via un pare-feu.*

Fichiers journaux

6. Un fichier journal doit être mis en place, dans lequel au moins les connexions et déconnexions de tous les utilisateurs et les actions telles que les mises à jour, les sauvegardes, les téléchargements et les chargements, les modifications des données de compte et des autorisations, ainsi que toutes les actions et événements liés à la sécurité doivent être enregistrés et documentés.

Codes et messages d'erreur du système

7. Les messages d'erreur générés par l'application (notamment la gestion des exceptions/exceptions) ne doivent fournir aucune information permettant de tirer des conclusions sur l'architecture ou les logiciels/versions de logiciels utilisés.

SQL Injection

8. Le système doit être renforcé contre les injections SQL. Cela concerne en particulier la validation, le filtrage et le nettoyage des entrées utilisateur.

Cross-Site-Scripting

9. Le système doit être protégé contre le Cross Site Scripting (XSS) côté client.

Politique de mot de passe

10. Une politique de mots de passe doit être définie avec le partenaire et mise en œuvre par le contractant. Les mots de passe ne doivent pas être stockés en texte clair. Les mots de passe ne peuvent être stockés que sous forme de valeurs de hachage.

Rôle et concept d'autorisation

11. Un concept de rôle et d'autorisation doit être mis en œuvre, qui inclut et distingue les rôles d'administrateur système (autorisation complète sur l'ensemble du système), d'administrateur fonctionnel (gestion des comptes utilisateur) et l'utilisateur final.

Téléchargement de fichier

12. Lors du téléchargement de fichiers, des filtres de fichiers appropriés doivent être prévus afin qu'aucun fichier avec un contenu exécutable (scripts, programmes ou codes SQL) ne puisse être téléchargé et exécuté.

Sauvegarde et restauration

13. Les sauvegardes régulières de l'ensemble du système doivent être effectuées par le contractant. Le contractant devra s'assurer de vérifier l'utilisabilité des restaurations. La sauvegarde peut être stockée sur le serveur, mais une copie doit toujours être stockée hors ligne pour éviter toute perte due à des attaques de pirates informatiques. Les intervalles de sauvegarde doivent être définis en accord avec le partenaire.