

Annexe au CCTP :

Sécurité

La sécurité constitue un attendu important du marché.

Le titulaire devra notamment se soumettre aux exigences de sécurité que pourrait exiger le ministère ou l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information).

Le service fourni doit satisfaire aux principes de mise en œuvre et aux exigences techniques suivantes :

Principes de mise en œuvre

- Obligation de compte-rendu : tout incident, même mineur, doit faire l'objet sans délai d'un compte-rendu, distinguant les éléments de preuve factuels, des éléments d'interprétation, les actions correctives ou préventives mises en œuvre (court/moyen et long terme),
- Obligation du suivi et d'information du ministère sur les vulnérabilités des composants logiciels installés,
- Gestion documentée de la politique de mise en place ou non des patches de mises à jour, au regard des incidences sur les applications,
- Obligation de niveau de protection : les moyens de protection doivent être mis en place pour toutes les attaques estimées possibles, même si elles paraissent improbables.

Le titulaire doit mettre en œuvre un processus d'amélioration continu de la sécurité de ses applicatifs. Ce processus doit être présenté selon les 4 étapes de la méthode de gestion de la qualité PDCA (*Plan-Do-Check-Act*) :

- phase de préparation ;
- phase de réalisation ;
- phase de vérification : préciser la fréquence ainsi que le périmètre technique et organisationnel des audits réalisés en interne par les équipes du titulaire ou par une société tierce ;
- phase d'ajustement (mesures correctives suite aux insuffisances constatées lors de la vérification.

Exigences techniques minimales

- Mise à jour des composants logiciels : Le titulaire doit faire évoluer son socle applicatif et en déployer la mise à jour pour corriger les problèmes de sécurité et pour garantir l'utilisation d'une version maintenue des composants logiciels (cette mise à jour est réalisée gratuitement sur les environnements du ministère).
- Protection des mots de passe : aucun mot de passe réutilisable ne doit être autorisé même sur le réseau protégé derrière le second routeur, aucun mot de passe par défaut ou faible ne doit être laissé sur un système, les mots de passe doivent être stockés de manière chiffrés etc. ,
- Il est strictement interdit au titulaire ou à ses éventuels sous-traitants travaillant pour le ministère, sauf après accord explicite du ministère, d'utiliser les services Google (Gmail etc.) et plus généralement tout autre service externe d'échange, de travail ou de communication externe à leur entreprise et fournis par un tiers en mode web.

Les exigences listées ci-dessus sont les exigences minimales et ne constituent pas la liste exhaustive des recommandations de sécurité que le titulaire doit mettre en œuvre. Le titulaire est responsable de la mise en œuvre de ces exigences au regard de l'état de l'art.

Les contenus multimédias étant utilisés pour la communication habituelle du ministère et en cas de crise, le non respect des exigences de sécurité peut avoir des impacts sur l'image du ministère ou de personnalités, ou encore avoir un effet sur la gestion d'une crise si les procédures *ad hoc* ne sont pas respectées.

Le ministère se réserve la faculté, après en avoir informé le titulaire de réaliser ou de faire réaliser par un organisme indépendant des audits ou tests de sécurité permettant au ministère d'évaluer le respect par le titulaire de ses obligations en matière de sécurité du système d'information.

Ces audits donneront lieu à une injonction de correction par le titulaire des défauts constatés et / ou de mise en conformité avec les obligations contractuelles.

Localisation des données

L'ensemble des lieux d'hébergement (site principal, site(s) de secours, de sauvegarde, etc.) doivent répondre d'une part aux exigences de sécurité du ministère, et d'autre part aux obligations légales et réglementaires, notamment loi du 6 janvier 1978 modifiée, relative à la protection des données à caractère personnel. Il en va de même des sites de télémaintenance s'ils peuvent accéder aux données.

Certains types d'infogérance ne permettent pas de localiser avec certitude les données hébergées.

En Europe, le cadre juridique de protection des données à caractère personnel s'appuie sur le principe suivant : il doit être possible de constater à tout moment la localisation des données (principe de territorialité).

L'impossibilité de localiser les données dans les nuages publics pose le problème de la compétence des

juridictions et du droit applicable.

Le titulaire devra donc communiquer dans sa réponse la liste de tous les lieux de stockage de données (site d'hébergement principal, site(s) de secours, etc.). A défaut (cette disposition n'ayant pas la préférence du ministère), si la faisabilité technique de cette exigence peut s'avérer délicate dans le cadre d'architectures distribuées, il sera demandé au titulaire d'être en mesure de localiser, *a posteriori*, et non en permanence, le lieu de stockage des données, en particulier suite à un incident.

Authentification OpenID Connect

Le ministère a mis en œuvre un référentiel d'identification de ses agents : il s'agit de l'annuaire LDAP de messagerie nommé "Agricoll".

L'authentification couplée à ce référentiel s'effectue au travers d'un système de SSO (Single Sign On) basé sur le protocole OIDC nommé EAP.

La solution retenue permettra l'utilisation de ce système SSO pour l'authentification des utilisateurs back-office.
