Document du SMI
Nature du document :

Identification

QUASPASDD220005

Nom du FDR : SMI

HYGIENE INFORMATIQUE POUR LES CONTRATS DE L'ANDRA

Ind.	Date	Historique des derniers indices applicables
A	26/10/2022	Création du document

1. Introduction

Toute délivrance de prestations et/ou de fournitures à l'Andra implique l'emploi de moyens numériques, exposant les deux parties à des risques de cybersécurité.

L'objet du présent document est de définir les exigences **minimales** de l'Andra en matière de sécurité informatique que le Titulaire s'engage à mettre en œuvre, à respecter et à maintenir dans le temps en vue de garantir la protection des systèmes d'information de l'Andra.

Ces exigences sont inspirées du Guide des bonnes pratiques de l'informatique publié conjointement par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et la Confédération des Petites et Moyennes Entreprises (CPME). Elles permettent de limiter une grande partie des risques liés à l'usage de l'informatique.

https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf

Le présent document, à vocation générale, ne tient pas compte des éventuelles dispositions particulières à respecter impérativement dans le cadre spécifique des marchés à clause de sécurité.

2. Exigences minimales adressées aux prestataires, applicables au sein de leur entreprise et pour les services délivrés à l'Andra

2.1 Connaissez vos utilisateurs et prestataires

✓ Réservez l'accès à vos systèmes informatiques aux personnels de l'entreprise et aux prestataires dûment identifiés

✓ Limitez l'utilisation de comptes avec privilège d'administration aux personnels des services informatiques et aux intervenants de support et maintenance

✓ Pour les autres personnes, n'ouvrez que des comptes de type utilisateur, dépourvus de privilèges permettant de modifier le fonctionnement des systèmes

✓ Limitez strictement les comptes anonymes et génériques ; chaque utilisateur doit être identifié nommément

✓ Vérifiez régulièrement que les droits octroyés à chacun sur les systèmes d'information sont appliqués au plus juste et surtout qu'ils sont révoqués lors du départ de la personne

2.2 Sécurisez les comptes et mots de passe

✓ Attribuez des comptes nominatifs pour tous les accès à votre informatique, administrateurs et prestataires informatiques inclus

✓ Imposez des règles de choix, de dimensionnement (longueur) et de durée de vie des mots de passe permettant de garantir une authentification forte

✓ Modifiez toujours les éléments d'authentification (identifiants, mots de passe) définis par défaut sur les équipements (imprimantes, serveurs, box, équipements réseaux…)

✓ Interdisez la conservation des mots de passe dans des fichiers non chiffrés ou sur des post-it

✓ Sensibilisez les collaborateurs au fait qu'ils ne doivent pas préenregistrer leurs mots de passe dans les navigateurs

2.3 Maintenez à jour les équipements et logiciels informatiques

✓ S'il existe un service informatique au sein de votre structure, chargez-le de la mise à jour des équipements, des systèmes d'exploitation et des logiciels

✓ S'il n'en existe pas, imposez à vos utilisateurs de faire cette démarche :

- Configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement
- Téléchargez les correctifs de sécurité disponibles sur les sites Internet officiels des éditeurs

✓ N'autorisez l'installation des logiciels qu'aux informaticiens internes ou prestataires

2.4 Faites des sauvegardes

✓ Réalisez des sauvegardes régulières de vos données (chaque jour ou chaque semaine)

✓ Protégez les supports amovibles d'accès illégitimes et conservez-en régulièrement un exemplaire hors site pour faire face à un sinistre majeur

✓ En cas de sauvegarde de données/documents sur internet, prenez en compte les risques sur la confidentialité des données et leur localisation (le RGPD restreint l'exportation de données à caractère personnel hors de l'UE)

✓ Assurez-vous de pouvoir récupérer les données si vous changez de fournisseurs

2.5 Maîtrisez votre périmètre informatique

✓ Quelle que soit la nature des réseaux utilisés (Internet, Wi-Fi, réseau local Ethernet), assurez-vous de garantir la protection des accès par une restriction des connexions au moyen d'équipements identifiés et autorisés (ordinateurs, smartphones, imprimantes, etc.)

✓ Dans la mesure du possible, réalisez un enregistrement des connexions en vue de détecter les anomalies, au moins *a posteriori*

✓ Établissez un inventaire des équipements informatiques de toute nature et tenez-le à jour au fur et à mesure des changements

2.6 Conciliez mobilité et sécurité

✓ Sur tous les équipements mobiles (ordinateur portable, smartphone), ne conservez que les données nécessaires au déplacement ou à la mission

✓ N'enregistrez pas sur l'appareil les mots de passe, les identifiants bancaires, les codes PIN de moyens de paiement

✓ Veillez à utiliser des filtres de confidentialité sur les écrans

✓ N'autorisez la connexion qu'à des réseaux de confiance, évitez les réseaux wi-fi ouverts au public

✓ Équipez les équipements mobiles d'un système de chiffrement automatique du disque

2.7 Sécurisez votre messagerie électronique

✓ Filtrez vos messages entrants contre les virus et le spam

✓ Sensibilisez tous vos utilisateurs à un emploi prudent de la messagerie, face aux risques de phishing et de rançongiciel

✓ N'employez pas la messagerie pour conserver vos données

✓ Encadrez et limitez les usages de la messagerie de l'entreprise à des fins personnelles

2.8 Sécurisez vos approvisionnements informatiques

✓ Faites l'acquisition de matériels informatiques et de logiciels auprès de sources fiables

✓ Assurez-vous de détenir les licences officielles des logiciels

✓ N'installez jamais un logiciel depuis une clé USB si vous n'en connaissez pas l'origine

✓ Désactivez l'ouverture automatique des documents et fichiers téléchargés et lancez une analyse antivirus avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue

2.9 Séparez les usages professionnels et personnels

✓ Privilégiez l'emploi d'équipements distincts pour les usages personnels et professionnels

- Ne faites pas suivre les messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles
- N'hébergez pas de données professionnelles sur vos équipements personnels (clé USB, téléphone, etc.) ou sur des moyens personnels de stockage en ligne
- Encadrez ou interdisez la connexion de supports amovibles personnels (clés USB, disques durs externes, etc.) aux ordinateurs de l'entreprise.

✓ N'employez pas les mêmes mots de passe pour vos outils personnels et professionnels

2.10 Protégez les informations et identités

✓ Assurez-vous de la présence d'un logiciel anti-virus sur vos équipements, serveurs et postes de travail, et de sa mise à jour quotidienne

✓ Sur internet, soyez vigilant vis-à-vis des formulaires que vous êtes amenés à remplir :

- Ne transmettez que les informations strictement nécessaires
- Décochez les cases qui autoriseraient le site à conserver ou à partager vos données
- Ne donnez accès qu'à un minimum d'informations personnelles et professionnelles sur les réseaux sociaux, et soyez vigilant lors de vos interactions avec les autres utilisateurs
- Vérifiez régulièrement les paramètres de sécurité et de confidentialité des services et applications en ligne, ces derniers peuvent changer sans que vous en ayez été prévenus
- Ne confiez pas d'informations confidentielles de votre entreprise à des services en ligne sur internet, sans avoir signé au préalable avec le fournisseur un contrat qui vous donne des assurances de sécurité et de protection juridique