

Exigences de sécurité pour les échanges par courriel

CONSULTATION N° : 73260099

Intitulé : PRESTATIONS DE SERVICE DE BROyage ET
DE SENSIBILISATION A LA GESTION DES DECHETS
VERTS DES HABITANTS



Contenu

1. Objet	3
2. Mesures de sécurité des ressources humaines	3
3. Mesures de sécurité du poste de travail	3
4. Mesures de sécurité de la messagerie	3

1. Objet

Le présent document décrit les dispositions que le titulaire doit mettre en œuvre pour répondre aux exigences de sécurité de la Métropole Aix-Marseille-Provence lors de ses échanges par courriel.

Le titulaire notifie à la Métropole tout incident de sécurité dans un délai maximum de 24 heures calendaires après en avoir pris connaissance et par courrier électronique à l'adresse **rssi@ampmetropole.fr**. Cette notification est accompagnée de toute documentation utile afin de permettre à la Métropole de s'en prémunir.

2. Mesures de sécurité des ressources humaines

La gestion des ressources humaines participant à la réalisation des prestations doit permettre de garantir la sécurité des données de la Métropole.

Des plans de formation et des plans de sensibilisation aux mesures de sécurité sont mis en place à l'attention du personnel du titulaire et, quand cela est pertinent, des sous-traitants. De plus, le personnel et les sous-traitants reçoivent régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leurs fonctions.

3. Mesures de sécurité du poste de travail

L'installation des postes utilisés dans le cadre du projet respecte les bonnes pratiques de sécurisation. Le titulaire doit être en capacité de nous transmettre la liste des pratiques qu'il a mises en œuvre.

Une solution contre les codes malveillants est déployée sur chaque poste du périmètre projet du titulaire.

Les mises à jour de sécurité du système d'exploitation et des applications sont réalisées tous les mois.

Les postes de travail se verrouillent automatiquement au bout de dix minutes d'inactivité.

Une solution de pare-feu est activée sur les postes de travail, solution qui autorise les flux nécessaires au titulaire.

4. Mesures de sécurité de la messagerie

Chaque utilisateur a un compte de messagerie unique et personnelle.

La politique de mots de passe est conforme aux recommandations de la CNIL. Le mot de passe doit être renouvelé tous les ans.

L'authentification à facteurs multiples est active pour les connexions à la messagerie.

Les utilisateurs sont sensibilisés pour lutter contre l'hameçonnage tous les ans.

La messagerie est maintenue à jour contre les vulnérabilités de sécurité informatique.

Le domaine de messagerie intègre les configurations de sécurité afin d'éviter son usurpation et une potentielle utilisation illicite de celui-ci (paramètres DMARC, DKIM et SPF en mode rejet).

Si le titulaire renvoie vers son site internet dans le cadre d'un échange par courriel, les flux entre l'utilisateur et le site Internet du titulaire sont chiffrés par le protocole TLS en version minimale 1.2. Un bandeau de consentement pour les cookies et autres traceurs non nécessaires au service est proposé à la première connexion en page d'accueil. L'accès aux outils et interfaces d'administration du site Internet est restreint aux seules personnes habilitées. Le site Internet est maintenu à jour contre les vulnérabilités de sécurité informatique et audité tous les ans. En cas de vulnérabilités détectées, le titulaire procède aux correctifs.