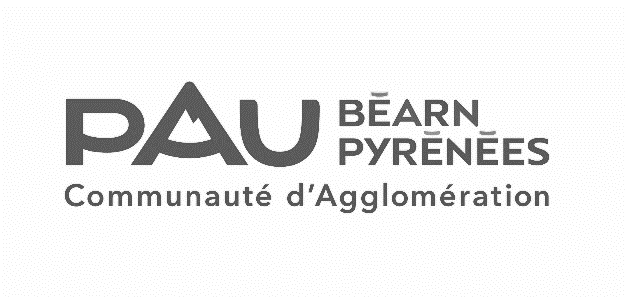
|  |
| --- |
| **DOCUMENT D'AIDE A LA REPONSE TECHNIQUE CYBERSECURITE** |



**CA PAU BEARN PYRENEES**

Hôtel de France

2B Place Royale

BP 547

64010 PAU CEDEX

**TABLE DES MATIERES**

I. Sensibiliser et former 3

II. Connaitre le système d’information 3

III. Authentifier et contrôler les accès 3

IV. Sécuriser les postes 4

V. Sécuriser le réseau 4

VI. Sécuriser l’administration 5

VII. Gérer le nomadisme 5

VIII. Maintenir à jour le système d’information 6

IX. Superviser, auditer, réagir 6

X. Pour aller plus loin 6

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Règles relatives au guide d’hygiène informatique de l’ANSSI, en relation avec l’annexe CCSC** | **Réponses apportées par le candidat** | **Catégorie 5 : répond aux exigences avec beaucoup d’avantages particuliers** | **Catégorie 4 : répond aux exigences avec un minium d’avantages particuliers** | **Catégorie 3 : répond aux exigences sans avantage particulier** | **Catégorie 2 : ne répond que partiellement aux exigences** | **Catégorie 1 : ne répond pas aux exigences** | **Catégorie 0 : réponse non fournie** |
| Sensibiliser et former | | | | | | | |
| 1. Former les équipes opérationnelles à la sécurité des systèmes d’information |  |  |  |  |  |  |  |
| 1. Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique |  |  |  |  |  |  |  |
| 1. Maîtriser les risques de l’infogérance |  |  |  |  |  |  |  |
| Connaitre le système d’information | | | | | | | |
| 1. Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau |  |  |  |  |  |  |  |
| 1. Disposer d’un inventaire exhaustif des comptes privilégiés et le maintenir à jour |  |  |  |  |  |  |  |
| 1. Organiser les procédures d’arrivée, de départ et de changement de fonction des utilisateurs |  |  |  |  |  |  |  |
| 1. Autoriser la connexion au réseau de l’entité aux seuls équipements maîtrisés |  |  |  |  |  |  |  |
| Authentifier et contrôler les accès | | | | | | | |
| 1. Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/ administrateur |  |  |  |  |  |  |  |
| 1. Attribuer les bons droits sur les ressources sensibles du système d’information |  |  |  |  |  |  |  |
| 1. Définir et vérifier des règles de choix et de dimensionnement des mots de passe |  |  |  |  |  |  |  |
| 1. Protéger les mots de passe stockés sur les systèmes |  |  |  |  |  |  |  |
| 1. Changer les éléments d’authentification par défaut sur les équipements et services |  |  |  |  |  |  |  |
| 1. Privilégier lorsque c’est possible une authentification forte |  |  |  |  |  |  |  |
| Sécuriser les postes | | | | | | | |
| 1. Mettre en place un niveau de sécurité minimal sur l’ensemble du parc informatique |  |  |  |  |  |  |  |
| 1. Se protéger des menaces relatives à l’utilisation de supports amovibles |  |  |  |  |  |  |  |
| 1. Utiliser un outil de gestion centralisée afin d’homogénéiser les politiques de sécurité |  |  |  |  |  |  |  |
| 1. Activer et configurer le pare-feu local des postes de travail |  |  |  |  |  |  |  |
| 1. Chiffrer les données sensibles transmises par voie Internet |  |  |  |  |  |  |  |
| Sécuriser le réseau | | | | | | | |
| 1. Segmenter le réseau et mettre en place un cloisonnement entre ces zones |  |  |  |  |  |  |  |
| 1. S’assurer de la sécurité des réseaux d’accès Wi-Fi et de la séparation des usages |  |  |  |  |  |  |  |
| 1. Utiliser des protocoles sécurisés dès qu’ils existent |  |  |  |  |  |  |  |
| 1. Mettre en place une passerelle d’accès sécurisé à Internet |  |  |  |  |  |  |  |
| 1. Cloisonner les services visibles depuis Internet du reste du système d’information |  |  |  |  |  |  |  |
| 1. Protéger sa messagerie professionnelle |  |  |  |  |  |  |  |
| 1. Sécuriser les interconnexions réseau dédiées avec les partenaires |  |  |  |  |  |  |  |
| 1. Contrôler et protéger l’accès aux salles serveurs et aux locaux techniques |  |  |  |  |  |  |  |
| Sécuriser l’administration | | | | | | | |
| 1. Interdire l’accès à Internet depuis les postes ou serveurs utilisés pour l’administration du système d’information |  |  |  |  |  |  |  |
| 1. Utiliser un réseau dédié et cloisonné pour l’administration du système d’information |  |  |  |  |  |  |  |
| 1. Limiter au strict besoin opérationnel les droits d’administration sur les postes de travail |  |  |  |  |  |  |  |
| Gérer le nomadisme | | | | | | | |
| 1. Prendre des mesures de sécurisation physique des terminaux nomades |  |  |  |  |  |  |  |
| 1. Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable |  |  |  |  |  |  |  |
| 1. Sécuriser la connexion réseau des postes utilisés en situation de nomadisme |  |  |  |  |  |  |  |
| 1. Adopter des politiques de sécurité dédiées aux terminaux mobiles |  |  |  |  |  |  |  |
| Maintenir à jour le système d’information | | | | | | | |
| 1. Définir une politique de mise à jour des composants du système d’information |  |  |  |  |  |  |  |
| 1. Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles |  |  |  |  |  |  |  |
| Superviser, auditer, réagir | | | | | | | |
| 1. Activer et configurer les journaux des composants les plus importants |  |  |  |  |  |  |  |
| 1. Définir et appliquer une politique de sauvegarde des composants critiques |  |  |  |  |  |  |  |
| 1. Procéder à des contrôles et audits de sécurité réguliers puis appliquer les actions correctives associées |  |  |  |  |  |  |  |
| 1. Désigner un référent en sécurité des systèmes d’information et le faire connaître auprès du personnel |  |  |  |  |  |  |  |
| 1. Définir une procédure de gestion des incidents de sécurité |  |  |  |  |  |  |  |
| Pour aller plus loin | | | | | | | |
| 1. Mener une analyse de risques formelle |  |  |  |  |  |  |  |
| 1. Privilégier l’usage de produits et de services qualifiés par l’ANSSI |  |  |  |  |  |  |  |

**L’absence de réponse n’entrainera pas de rejet de l’offre. La qualité de la réponse peut toutefois être prise en compte en cas de pondération précisée dans le règlement de consultation.**

**La conformité aux règles ci-dessus, se base sur les livrables qui sont précisés dans le cahier des charges et/ou la gestion de la sécurité informatique du titulaire et de ses sous-traitant le cas échéant.**

**Références des règles détaillées : Guide v.2 sur https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/**