Cybersécurité

Liste des « best practices »

Edition 2025

label qualité uspf genève

1. PARE-FEU ET ANTIVIRUS

Détails
Installer des logiciels antivirus, antispam et configurer un pare-feu pour protéger les systèmes contre les logiciels malveillants et les menaces en ligne.

Exemple(s)
1. Configuration des services fournis par le pare-feu : IPS - IDS - Reverse-Proxy – GeoIP.
2. Mise en place d'un EDR (end point) et vérification des mises à jour régulières.

2. SAUVEGARDES RÉGULIÈRES

Détails
Mettre en place des sauvegardes régulières des données importantes. Stocker ces sauvegardes hors site pour éviter toute perte de données en cas de problème.

Exemple(s)
Test régulier des sauvegardes (au moins d'une VM).

3. MISES À JOUR RÉGULIÈRES

Détails
S'assurer que les systèmes d'exploitation, les logiciels et les antivirus soient régulièrement mis à jour pour combler les failles de sécurité connues.

Exemple(s)
Surveillance des sources de MAJ proposées par les fournisseurs afin de les déployer dès que possible. Mise à jour des drivers des périphériques.

4. GESTION DES ACCÈS ET SEGMENTATION RÉSEAU

Détails
Limiter l'accès aux informations sensibles uniquement aux personnes qui en ont besoin. Réviser et révoquer les accès lorsque nécessaire.

Exemple(s)
1. Mise en place d'une matrice de flux réseau (VLAN, SWITCH, etc…). Au minimum : le réseau WIFI public ségrégué du LAN + accès externes.
2. Gestion des accès la plus implicite possible.

5. GESTION DES MOTS DE PASSE

Détails
Encourager l'utilisation de mots de passe forts et la mise en place d'une politique de gestion des mots de passe.

Exemple(s)
Eviter de stocker les mots de passe dans les navigateurs sans chiffrer l'accès à cette base de mots de passe.

6. EXTERNALISATION DE LA SÉCURITÉ

Détails
Si les ressources internes sont limitées, envisager de faire appel à un prestataire de services de sécurité informatique pour une surveillance et une gestion continue de la cybersécurité. Effectuer des audits internes et externes au minimum tous les 5 ans et une première fois lorsque l'on met en place le "label". Suivi des actions correctives.

Exemple(s)
Mise en place d'une hiérarchie de niveaux de responsabilité.

7. PARTAGE D'INFORMATIONS

Détails
Encourager les adhérents à signaler tout incident de sécurité ou comportement suspect à l'Association pour une réaction rapide.

Exemple(s)
Consignation de ces informations afin d'améliorer le niveau de la détection ciblée.

8. SENSIBILISATION À LA SÉCURITÉ

Détails
1. Organiser des sessions de sensibilisation à la sécurité informatique.
2. Sensibiliser aux risques liés à la cybersécurité, aux pratiques de sécurité de base et à la gestion des mots de passe. Formation et campagne de phishing. (Intégrer une sensibilisation fraude, cyber, nLPD au sein de la formation IMMOBASE).

Exemple(s)
Campagne de sensibilisation régulière (sous forme de quizz par exemple).

9. AUTHENTIFICATION À DEUX FACTEURS (2FA)

Détails
Activer l'authentification à deux facteurs partout où cela est possible pour renforcer la sécurité des comptes.

Exemple(s)
Microsoft Authenticator (par exemple).

10. SURVEILLANCE DES ACTIVITÉS

Détails
Mettre en place un contrôle d'accès physique dans les locaux.

Exemple(s)
Installer un système d’alarme.

11. POLITIQUE DE TÉLÉTRAVAIL SÉCURISÉ

Détails
Si le télétravail est pratiqué, mettre en place des politiques de sécurité appropriées pour les employés-ées travaillant à distance.

Exemple(s)
1. Double authentification.
2. Limitation des accès par pays.

12. RÉDACTION D’UNE POLITIQUE DE SÉCURITÉ

Détails
Élaborer une politique de sécurité informatique simple, mais claire, et s'assurer que tous les collaborateurs-trices la comprennent et la respectent.

Exemple(s)
Création, mise en place et amélioration régulière de la charte informatique ainsi que du règlement interne.

13. INVENTAIRE PRÉCIS

Détails
Rester à jour par rapport à l'intégralité des actifs matériels.

Exemple(s)
Mise en place d'un outil d'inventaire

14. RÉPONSE À INCIDENT

Détails
Se prémunir à l'aide d'un plan d'actions formalisé dans un document PDF en cas d'attaque.

Exemple(s)
1. Responsables : qui - quoi - quand - comment, dans quel délai, etc.

15. SURVEILLANCE DES MISES À JOUR DE SÉCURITÉ

Détails
Rester informé des dernières vulnérabilités et des correctifs de sécurité en s'abonnant aux bulletins d'informations et aux alertes de sécurité. (cf. boite noire SUPRA)

Exemple(s)
Intégration d'un SOC (Security Operations Center).

16. CONFIGURATION DES PROTOCOLES DES DOMAINES

Détails
Configurer et gérer des méthodes d'authentification du courrier électronique et noms de domaines DMARC, DKIM et SPF.

ATTESTATION « BEST PRACTICES » CYBERSÉCURITÉ

Annexe 1

au 31 décembre 2025

La régie _____ atteste par la présente avoir mis en œuvre les pratiques recommandées et définies en matière de cybersécurité, selon la liste des « best practices », édition 2025, qui sont les suivantes :

Veuillez cocher ce qui convient.

- ☐ pare-feu et antivirus
- ☐ sauvegardes régulières
- ☐ mises à jour régulières
- ☐ gestion des accès et segmentation réseau
- ☐ gestion des mots de passe
- ☐ externalisation de la sécurité
- ☐ partage d'informations
- ☐ sensibilisation à la sécurité
- ☐ authentification à deux facteurs (2FA)
- ☐ surveillance des activités
- ☐ politique de télétravail sécurisé
- ☐ rédaction d'une politique de sécurité
- ☐ inventaire précis
- ☐ réponse à incident
- ☐ surveillance des mises à jour de sécurité
- ☐ configuration des protocoles des domaines

Le présent document est partie intégrante du Label Qualité de l'USPI Genève.

Le membre certifie que les informations contenues dans la présente sont conformes à la réalité. L'USPI Genève se réserve le droit de procéder à un contrôle. Sur demande, la régie doit pouvoir démontrer concrètement les mesures qui ont été entreprises.

Date _____ Signature _____