Réglementation du service informatique

L'association OREMIS lutte contre le harcèlement scolaire, le cyberharcèlement, et soutient les élèves à besoins spécifiques. Cette réglementation du service informatique définit les règles et responsabilités nécessaires pour assurer un fonctionnement sécurisé et en accord avec les valeurs de l'association. Tous les membres du service informatique doivent lire, comprendre et respecter cette réglementation afin de contribuer efficacement aux objectifs d'OREMIS, dans un esprit de collaboration et de respect des normes de sécurité.

1. Dispositions Générales

I.1.1 Tous les sites web et outils numériques sont la propriété de l'association OREMIS et protégés par les droits d'auteur. Toute tentative de décompilation, d'exploitation, de piratage ou toute autre activité visant à accéder à du matériel ou des zones restreintes/encryptées est strictement interdite.

Les utilisateurs qui découvrent une faille de sécurité dans les logiciels d'OREMIS sont encouragés à la signaler au service informatique pour résoudre le problème. L'exploitation ou la divulgation de cette faille à des tiers est interdite. Si de telles activités sont détectées et/ou non signalées aux instances appropriées (par exemple, le service informatique ou les services d'infrastructure), une sanction appropriée (telle qu'une suspension) peut être imposée par le Conseil Exécutif.

2. Rôles et responsabilités

Directeurs délégués

I.2.1.1 Le DDIN/DDAIN est responsable de la supervision globale du service informatique. Il coordonne les activités entre les différentes équipes, assure le respect des normes de sécurité et veille à la bonne gestion des ressources. Il est également chargé de la communication avec les autres départements de

l'association, assurant une collaboration efficace et une intégration fluide des solutions technologiques.

Développeurs web

I.2.2.1 Les développeurs web sont responsables de la création, de la maintenance et de la sécurité des sites web et des outils numériques de l'association. Ils doivent s'assurer que toutes les applications respectent les standards de sécurité, sont conformes au RGPD et répondent aux besoins des utilisateurs internes et externes.

Gestionnaires documentaire

I.2.3.1 L'équipe de documentation est chargée de produire, de maintenir et de mettre à jour les guides, manuels et autres documents nécessaires pour l'association OREMIS. Elle est également chargée de la mise à jour régulière du wiki interne de notre association.

Administrateurs des infrastructures

I.2.4.1 Les administrateurs des infrastructures sont responsables de la gestion, de la sécurité et de la maintenance des serveurs, des bases de données et des réseaux de l'association. Ils doivent garantir la disponibilité, la résilience et l'intégrité des systèmes informatiques, en effectuant des sauvegardes régulières et en surveillant l'ensemble des infrastructures.

DevOps

I.2.5.1 Les DevOps sont responsables de l'automatisation des processus, du déploiement continu et de l'intégration des systèmes. Ils veillent à l'optimisation des flux de travail, à la réduction des temps d'arrêt et à l'amélioration continue des performances des systèmes informatiques.

3. Procédures et conformité

Sécurité des systèmes

I.3.1.1 Tous les membres du service informatique doivent suivre les procédures de sécurité établies pour protéger les données et les systèmes d'OREMIS contre les accès non autorisés, les piratages, et autres menaces.

I.3.1.2 Les incidents de sécurité doivent être signalés immédiatement au DDIN/DDAIN ainsi qu'au conseil exécutif et les mesures correctives doivent être prises sans délai.

Gestion des accès

I.3.2.1 Les identifiants d'accès aux systèmes doivent être attribués de manière rigoureuse, en assurant que chaque membre dispose des permissions nécessaires pour accomplir ses tâches.

I.3.2.2 Les identifiants doivent être changés régulièrement et immédiatement en cas de départ ou de changement de poste d'un membre du service.

Sauvegardes et Maintenance

I.3.3.1 Des sauvegardes régulières des systèmes et des données doivent être effectuées, au moins une fois par trimestre, pour garantir la continuité des services en cas de panne ou de cyberattaque.

I.3.3.2 Les administrateurs des infrastructures sont responsables de la mise en œuvre et de la vérification des sauvegardes, ainsi que de la maintenance préventive des systèmes.

I.3.3.3 Toute opération susceptible de provoquer ou de risquer de provoquer des dysfonctionnements systèmes doit être soumise au conseil exécutif pour approbation au moins 72 heures avant sa mise en œuvre.

4. Respect de la réglementation et responsabilité pénale

I.4.1 Tous les membres du service informatique d'OREMIS doivent lire, comprendre et se conformer à cette réglementation. Toute violation des règles établies pourra entraîner des mesures disciplinaires.

I.4.2 Le chef de service Informatique a la responsabilité de veiller à ce que toutes les procédures de sécurité et de conformité soient scrupuleusement suivies, et de signaler immédiatement toute infraction ou risque potentiel au conseil exécutif.

I.4.3 En cas de manquement aux obligations définies dans cette réglementation, les responsabilités pénale et civile des bénévoles et du chef de service Informatique peuvent être engagées.

I.4.4 Les membres du service informatique, y compris le chef de service, doivent être conscients que toute négligence, omission ou action délibérée susceptible de compromettre la sécurité des systèmes ou de causer des dommages peut entraîner des sanctions pénales, conformément à la législation en vigueur.

Annexes

Abus de confiance (Article 314-1 du Code pénal)
Cette infraction consiste à détourner, au préjudice d'autrui, des fonds, valeurs ou tout autre bien (données, serveurs informatique) qui vous a été remis dans le cadre de votre mission. Les bénévoles doivent manipuler les ressources de l'association avec intégrité et dans le respect des objectifs définis.

Atteinte aux systèmes de traitement automatisé de données (Articles 323-1 à 323-8 du Code pénal)
Cette série d'articles vise à protéger les systèmes informatiques contre toute intrusion, altération, ou sabotage. Il est strictement interdit de nuire au bon fonctionnement des systèmes informatiques de l'association ou de tenter de le faire.

Détournement de données personnelles (Articles 226-16 à 226-24 du Code pénal)
Ces articles concernent la protection des données personnelles. Il est interdit de collecter, utiliser ou divulguer des données personnelles sans autorisation. Les bénévoles doivent respecter la confidentialité des données traitées au sein de l'association.

Mise en danger de la vie d'autrui (Article 223-1 du Code pénal)
Cette infraction concerne toute action ou omission qui crée un risque immédiat de mort ou de blessure pour autrui. En informatique, cela peut inclure des actes comme la manipulation dangereuse des systèmes de sécurité, pouvant avoir des conséquences graves sur la vie des personnes.

Responsabilité pénale des dirigeants (Article 121-2 du Code pénal)
Cet article prévoit que les dirigeants d'une association peuvent être tenus responsables pénalement des infractions commises par l'association. Les bénévoles doivent être conscients que leurs actions peuvent engager la responsabilité des dirigeants (DDIN/DDAIN, DEXI, CA) de l'association.

Adopté par le conseil d'administration en sa séance du 21 10 2024.