Université de Relizane

Bureau Stratégie du Numérique

Charte Informatique

Table des matières

Introduction

Cette charte informatique a pour but de définir les règles et les bonnes pratiques pour l'utilisation du matériel informatique au sein de l'université de Relizane. Cette charte s'applique à tous les étudiants, enseignants, personnels administratifs et techniques qui utilisent les ressources informatiques de l'université.

- **Utilisation du matériel informatique**

Le matériel informatique de l'université est destiné à un usage professionnel et académique. Tout usage personnel est interdit. Les utilisateurs doivent respecter les normes de sécurité et de confidentialité pour éviter toute violation des données ou des informations sensibles.

- **Sécurité et confidentialité**

Tous les utilisateurs doivent prendre des mesures raisonnables pour protéger les ressources informatiques de l'université contre les accès non autorisés, les pertes, les vols, les dommages et les utilisations abusives. Les utilisateurs doivent utiliser des mots de passe forts, ne pas divulguer les informations de connexion et verrouiller les ordinateurs lorsqu'ils ne sont pas utilisés.

- **Logiciels et licences**

Les utilisateurs doivent respecter les termes et les conditions des licences de logiciel et ne pas copier, installer ou utiliser des logiciels non autorisés. Tout logiciel acheté par l'université est la propriété de l'université et ne peut être utilisé que conformément aux politiques et aux directives de l'université.

- **Internet et messagerie électronique**

L'accès à Internet et l'utilisation de la messagerie électronique sont autorisés pour un usage professionnel et académique. Toutefois, les utilisateurs doivent éviter d'accéder à des contenus illicites ou inappropriés, ou d'envoyer des messages inappropriés ou non autorisés. Les utilisateurs ne doivent pas télécharger ou installer de logiciels malveillants ou des virus.

- **Réseaux et équipements**

Les utilisateurs ne doivent pas modifier ou altérer les équipements informatiques ou les réseaux de l'université. Tout équipement apporté de l'extérieur doit être inspecté et approuvé par les services informatiques de l'université avant d'être connecté au réseau de l'université.

- **Responsabilité**

Tous les utilisateurs sont responsables de leur comportement en matière d'utilisation des ressources informatiques de l'université. Tout comportement inapproprié ou non autorisé sera

considéré comme une violation de cette charte et pourra entraîner des sanctions disciplinaires ou pénales.

- **Système de surveillance**

L'université de Relizane se réserve le droit de surveiller l'utilisation des ressources informatiques par les utilisateurs de l'université à des fins de sécurité, de conformité aux politiques et aux lois, et pour garantir la disponibilité et l'intégrité des systèmes informatiques. Les moyens de surveillance peuvent inclure, mais ne sont pas limités à :

Enregistrement des journaux d'accès : Les serveurs et les systèmes de l'université peuvent enregistrer les informations sur l'accès et l'utilisation des ressources informatiques, y compris les adresses IP, les horodatages, les sites web visités, les applications utilisées et les fichiers accédés.

Surveillance de la messagerie électronique : L'université se réserve le droit de surveiller les messages électroniques envoyés ou reçus via les systèmes de messagerie électronique de l'université pour garantir la sécurité des utilisateurs et des ressources informatiques.

Surveillance de l'activité du réseau : L'université peut surveiller l'activité du réseau pour identifier les comportements malveillants ou inappropriés, y compris les attaques de réseau, les abus de bande passante et les téléchargements illégaux de fichiers.

Surveillance vidéo : Des caméras de surveillance peuvent être utilisées pour surveiller les zones publiques et sensibles de l'université pour garantir la sécurité et prévenir les activités illégales ou inappropriées.

L'université s'engage à respecter la vie privée des utilisateurs dans la mesure du possible tout en assurant la sécurité des ressources informatiques. Toutes les données recueillies dans le cadre de la surveillance sont traitées conformément aux lois et réglementations applicables. Les utilisateurs sont invités à signaler tout comportement suspect ou toute violation de cette charte à l'université.

- **L'accès à distance**

L'utilisation de l'accès à distance est soumise aux politiques et procédures suivantes :

Sécurité de l'accès : Les utilisateurs doivent s'authentifier avant de pouvoir accéder à distance aux ressources informatiques de l'université. Les identifiants de connexion, les mots de passe et les autres informations d'authentification ne doivent être divulgués à personne.

Protection des données : Les utilisateurs doivent prendre toutes les mesures nécessaires pour protéger les données confidentielles ou sensibles lors de l'accès à distance. Les données ne doivent pas être stockées sur des ordinateurs personnels ou des appareils mobiles sans autorisation préalable.

Utilisation des réseaux : Les utilisateurs ne doivent pas utiliser de réseaux publics ou non sécurisés pour accéder à distance aux ressources informatiques de l'université. L'utilisation d'un réseau privé virtuel (VPN) est recommandée pour garantir la sécurité des données.

Déconnexion : Les utilisateurs doivent se déconnecter des ressources informatiques de l'université à la fin de chaque session d'accès à distance. Les sessions inactives seront automatiquement déconnectées après une période déterminée par l'université.

Signalement d'incidents : Les utilisateurs sont tenus de signaler immédiatement tout incident de sécurité ou toute violation de la politique de sécurité de l'université à l'équipe de sécurité informatique de l'université.

L'université se réserve le droit de restreindre ou de révoquer l'accès à distance en cas de violation de cette politique ou de tout autre comportement inapproprié ou dangereux. Les utilisateurs sont responsables de leur comportement lors de l'accès à distance et peuvent être tenus responsables de toute violation de la politique de sécurité de l'université.

- **Une politique de gestion de crise.**

En cas d'incident de sécurité ou de violation de la politique de sécurité, l'université mettra en œuvre les procédures suivantes pour gérer la crise :

Signalement de l'incident : Tout incident de sécurité ou violation de la politique de sécurité doit être signalé immédiatement à l'équipe de sécurité informatique de l'université.

Evaluation de la gravité de l'incident : L'équipe de sécurité informatique de l'université évaluera la gravité de l'incident et déterminera l'étendue des dommages potentiels.

Déploiement de mesures d'atténuation : L'équipe de sécurité informatique de l'université déploiera des mesures d'atténuation pour minimiser les dommages causés par l'incident.

Enquête sur l'incident : L'équipe de sécurité informatique de l'université mènera une enquête sur l'incident pour déterminer la cause et les circonstances de l'incident.

Correction des vulnérabilités : L'équipe de sécurité informatique de l'université corrigera toutes les vulnérabilités découvertes lors de l'enquête pour éviter que l'incident ne se reproduise.

Notification des parties prenantes : Si l'incident affecte les parties prenantes de l'université, telles que les employés, les étudiants, les fournisseurs ou les clients, l'université les informera immédiatement de l'incident.

Communication externe : L'université communiquera avec les autorités compétentes, telles que les forces de l'ordre ou les organismes de réglementation, si l'incident implique une violation de la loi.

Rétablissement des services : L'équipe de sécurité informatique de l'université travaillera pour rétablir les services affectés dès que possible.

L'université se réserve le droit de prendre toutes les mesures nécessaires pour gérer une crise de sécurité, y compris la restriction ou la révocation de l'accès aux ressources informatiques de l'université. Les utilisateurs sont tenus de coopérer pleinement avec l'université dans la gestion de toute crise de sécurité.

- **Les sanctions**

Toute violation de la politique de sécurité de l'université est passible de sanctions. Les sanctions peuvent inclure, mais ne sont pas limitées à :

Avertissement : Dans certains cas, l'université peut choisir d'émettre un avertissement à l'utilisateur pour une première violation mineure de la politique de sécurité.

Suspension de l'accès : Si l'utilisateur viole de manière répétée la politique de sécurité de l'université, l'université peut suspendre son accès aux ressources informatiques de l'université pour une période déterminée.

Révocation de l'accès : Dans les cas les plus graves, l'université peut révoquer complètement l'accès de l'utilisateur aux ressources informatiques de l'université.

Responsabilité pénale : Si l'utilisateur commet une violation de la politique de sécurité qui constitue une infraction pénale, l'université peut coopérer avec les autorités compétentes pour poursuivre l'utilisateur en justice.

L'université se réserve le droit de déterminer les sanctions appropriées en fonction de la gravité de la violation de la politique de sécurité. Les sanctions peuvent être appliquées de manière progressive en fonction de la fréquence et de la gravité des violations commises par l'utilisateur.

Il est important que tous les utilisateurs comprennent les conséquences potentielles d'une violation de la politique de sécurité de l'université et prennent des mesures pour éviter toute violation de la politique de sécurité.

Conclusion

Cette charte informatique est destinée à aider les utilisateurs à utiliser les ressources informatiques de l'université de manière responsable et sûre. Les utilisateurs doivent respecter les règles énoncées dans cette charte afin de garantir la sécurité et la confidentialité des données et des informations de l'université.