Activité 1 : Respect des règles d'utilisation

Durée : 1h00

Compétences du référentiel

Gérer le patrimoine informatique

- Vérifier le respect des règles d'utilisation des ressources numériques

Objectifs

Etudier et comprendre une charte informatique.

Vous disposez en annexe de la charte informatique en vigueur dans l'entreprise Tartempion. Pour chaque situation décrite, vous indiquerez si l'utilisateur a enfreint une règle de la charte et/ou la loi. Justifier vos réponses, en précisant notamment l'article de la charte ou l'article de loi concerné.

1. Martin s'est rendu dans le bureau de son responsable afin de lui poser une question. Il a laissé sa session connectée puisqu'il en a pour 5 minutes.

2. Théodore, pour prouver ses compétences informatiques, a essayé sans succès de pénétrer le système informatique de l'entreprise.

3. Clément est en congé. Il a malheureusement oublié d'effectuer une correction importante dans un fichier sur lequel il travaille. Il contacte son stagiaire, lui fournit ses identifiants de connexion et lui demande d'effectuer la correction.

4. Anouk s'éloigne quelques instants de son poste pour aider un collègue bloqué sur un problème. Léo s'installe devant son ordinateur (resté connecté) et envoie un courrier électronique (au nom d'Anouk) à un autre collègue.

5. Djibril a acheté un super jeu dont il a fait une copie avant de l'installer sur son ordinateur de bureau

6. Arthur a utilisé une clé USB personnelle pour transférer un document sur son poste. Malheureusement, sa clé USB contient un virus. Il a infecté son poste.

7. Jules s'est installé sur le poste d'un collègue qui s'est absenté temporairement et a réussi à accéder à une application sensible avec le compte de celui-ci, alors qu'il ne dispose pas des habilitations nécessaires. Il a supprimé volontairement des données pour nuire à son collègue.

8. Véronique a laissé trainer sur le photocopieur un document relatif à un projet ultra confidentiel sur lequel elle travaille.

ANNEXE : Charte informatique de l'entreprise

Préambule

L'entreprise TARTEMPION met à disposition de ses utilisateurs un système d'information (SI) et des moyens informatiques nécessaires à l'exécution de ses missions et de ses activités.

Celui-ci comprend :

- un réseau informatique
- un réseau téléphonique

Dans le cadre de leurs fonctions, les utilisateurs sont conduits à utiliser les ressources informatiques mises à leur disposition par l'entreprise.

L'utilisation du système d'information et de communication doit être effectuée exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte.

Dans un objectif de transparence, la présente charte définit les règles dans lesquelles ces ressources peuvent être utilisées.

Article 1 : Utilisateurs concernés

Sauf mention contraire, la présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication de l'entreprise, quel que soit leur statut :

- les dirigeants et mandataires sociaux
- les salariés
- les intérimaires
- les stagiaires
- les employés de sociétés prestataires
- les visiteurs occasionnels

Il appartient aux salariés de l'organisation de s'assurer de faire accepter la présente charte à toute personne à laquelle ils permettraient l'accès au SI.

Article 2 : Périmètre du système d'information

Le système d'information est composé des ressources suivantes :

- ordinateurs (fixes ou portables)
- téléphones,assistants personnels
- périphériques
- réseau informatique (serveurs, routeurs et connectique)
- photocopieurs
- logiciels
- fichiers, données et bases de données
- messagerie
- intranet, extranet
- abonnements à des services interactifs
- …

Aux fins d'assurer la sécurité informatique du SI, tout matériel connecté réseau de l'entreprise ou contenant des informations à caractère professionnel concernant l'entreprise, y compris le matériel personnel des utilisateurs indiqués à l'article 1, est régi par la présente charte.

Article 3 : Règles générales d'utilisation

Le SI doit être utilisé à des fins professionnelles, conformes aux objectifs de l'organisation, sauf exception prévue par les présentes, ou par la loi.

Les utilisateurs ne peuvent en aucun cas utiliser le SI de l'organisation pour se livrer à des activités concurrentes, et/ou susceptibles de porter préjudice à l'organisation de quelque manière que ce soit.

Article 4 : sécurité informatique

L'entreprise met en œuvre une série de moyens pour assurer la sécurité de son système d'information et des données traitées, en particulier des données personnelles.

A ce titre, l'accès à certains éléments du système d'information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiants, mots de passe)

4.1 Principe général de responsabilité et obligation de prudence

L'utilisateur est responsable des ressources informatiques qui lui sont confiées dans le cadre de ses missions, et doit concourir à leur protection, notamment en faisant preuve de prudence. L'utilisateur doit s'assurer d'utiliser les ressources informatiques mises à sa disposition de manière raisonnable, conformément à ses missions.

4.2 Obligation générale de confidentialité

L'utilisateur s'engage à préserver la confidentialité des informations, et en particulier des données personnelles, traitées sur le SI de l'organisation.

Il s'engage à prendre toutes les précautions utiles pour éviter que ne soient divulguées de son fait, ou du fait de personnes dont il a la responsabilité, ces informations confidentielles.

4.3 Mot de passe

L'accès aux SI ou aux ressources informatiques mises à disposition est protégé par mot de passe individuel. Ce mot de passe doit être gardé confidentiel par l'utilisateur afin de permettre le contrôle de l'activité de chacun. Le mot de passe doit être mémorisé et ne doit pas être écrit sous quelque forme que ce soit. Il ne doit pas être transmis ou confié à un tiers ou être rendu accessible. Le login et le mot de passe doivent être saisis lors de chaque accès au système d'information.

Le mot de passe doit se conformer à la politique de mot de passe édictée conformément aux prescriptions de la CNIL relativement à la protection des données personnelles et notamment :

- être composé de plus de 12 caractères ;
- ces caractères doivent être une combinaison de caractères alphanumériques de chiffres,
- de majuscules,
- de minuscules,
- et de caractères spéciaux

4.4 Verrouillage de sa session

L'utilisateur doit veiller à verrouiller sa session dès lors qu'il quitte son poste de travail, même de manière temporaire.

4.5 Installation de logiciels

L'utilisateur ne doit pas installer, copier, modifier ou détruire de logiciels sur son poste informatique sans l'accord du service informatique en raison notamment du risque de virus informatiques.

4.6 Utilisation de matériel n'appartenant pas à l'entreprise

En cas d'accès au système d'information avec du matériel n'appartenant pas à l'entreprise (assistants personnels, supports amovibles, …), il appartient à l'utilisateur de veiller à la sécurité du matériel utilisé et à son innocuité.

4.7 Copie de données informatiques

L'utilisateur doit respecter les procédures définies par l'organisme afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant les règles de sécurité, afin d'éviter la perte de données (ex : vol de clé usb, perte d'un ordinateur portable contenant d'importantes quantités d'informations confidentielles…).

Article 5 : Accès à Internet

L'accès à l'Internet est autorisé au travers du SI, toutefois, pour des raisons de sécurité l'accès à certains sites peut être limité.

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, blogs, sites est interdite OU autorisée, sous réserve d'autorisation préalable du service Communication. Un tel mode d'expression est susceptible d'engager la responsabilité de l'entreprise, une vigilance renforcée des utilisateurs est donc indispensable.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts de l'entreprise, y compris sur Internet.

Article 6 : Messagerie électronique

La messagerie électronique est un moyen d'amélioration de la communication au sein des entreprises et avec les tiers. Chaque salarié dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique attribuée par le service informatique.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les salariés sont invités à informer le service informatique des dysfonctionnements qu'ils constatent dans le dispositif de filtrage.

6.1 Conseils généraux

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier manuscrit et peut rapidement être communiqué à des tiers. Il convient de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale de l'entreprise et/ou de l'utilisateur

Avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités. Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

En cas d'envoi à une liste de diffusion, il est important de vérifier la liste des abonnés à celle-ci.

La vigilance des utilisateurs doit redoubler en présence d'informations à caractère confidentiel. Les messages doivent dans ce cas être cryptés, conformément aux recommandations du service informatique.

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent comporter aucun élément illicite, tel que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire

6.2 Utilisation personnelle de la messagerie

Par principe, tous les messages envoyés ou reçus sont présumés être envoyés à titre professionnel.

Les utilisateurs sont invités, dans la mesure du possible, à utiliser leur messagerie personnelle via un client en ligne pour l'envoi de message à caractère personnel.

Par exception, les utilisateurs peuvent utiliser la messagerie à des fins personnelles, dans les limites posées par la loi. Les messages personnels doivent alors porter la mention “PRIVE” dans l’objet et être classés dans un répertoire “PRIVE” dans la messagerie, pour les messages reçus.

6.3 Limites techniques

Pour des raisons techniques, l'envoi de messages électroniques n'est possible, directement, que vers un nombre limité de destinataires, fixé par service informatique. Cette limite est susceptible d'être levée temporairement ou définitivement sur demande adressée au service informatique par la hiérarchie.

Les messages électroniques sont conservés pendant une durée de 3 mois. Passé ce délai, ils sont automatiquement archivés. Si le salarié souhaite conserver des messages au-delà de ce délai, il lui appartient d'en prendre copie.

Article 7 : Contrôle des activités

7.1 Contrôles automatisés

Le système d'information et de communication s'appuie sur des fichiers journaux (" logs "), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'entreprise, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au système d'information.

Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication. Sont notamment surveillées et conservées les données relatives :

- À l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications suppression de fichiers ;
- Aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites web ou le téléchargement de fichiers.

L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

7.2 Procédure de contrôle manuel

En cas de dysfonctionnement constaté par le service informatique, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs.

Lorsque le contrôle porte sur les fichiers d'un utilisateur et sauf risque ou événement particulier, le service informatique ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé (en visio).

Le contenu des messages à caractère personnel des utilisateurs (tels que définis à l'article 6 des présentes), ne peut en aucun cas être contrôlé par le service informatique.

Article 8 : Sanctions

Les manquements aux règles et mesures de sécurité édictées par la présente charte peuvent engager la responsabilité de l'utilisateur et entraîner des sanctions à son encontre (limitation ou suspension d'usage de tout ou partie du SI, sanctions disciplinaires proportionnées la gravité des faits concernés).

Dès lors qu'une sanction disciplinaire est susceptible d'être prononcée à l'encontre d'un salarié, celui-ci est informé dans un bref délai des faits qui lui sont reprochés, sauf risque ou événement particulier.

Article 9 : Information des salariés

La présente charte est ajoutée en annexe du règlement intérieur et communiquée individuellement à chaque employé.

Le service informatique est à la disposition des salariés pour leur fournir toute information concernant l'utilisation des NTIC. Il informe les utilisateurs régulièrement sur l'évolution des limites techniques du système d'information et sur les menaces susceptibles de peser sur sa sécurité.

La présente charte et l'ensemble des règles techniques sont disponibles sur l'intranet de l'entreprise.

Des opérations de communication internes seront organisées, de manière régulière, afin d'informer les salariés sur les pratiques d'utilisation des NTIC recommandées.

Article 10 : Entrée en vigueur

La présente charte est applicable à compter du **12 juin 2018**.

Elle a été adoptée après information et consultation des délégués du personnel et du comité d'hygiène et de sécurité.