

Activité 1

Compétences du référentiel

Gérer le patrimoine informatique

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

1- L'utilisateur Martin a enfreint une règle de la charte car d'après l'article 4, 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.

2- Théodore a enfreint les règles de la charte car il ne peut en aucun cas essayer de pénétrer le système informatique comme le démontre les Article 7 et Article 8;
Article 7 : 7.1 : le contrôle des activités est automatisé (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.)

Article 8 : 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 à 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.

3- Clément a enfreint les règles de la charte informatique de l'entreprise car il n'est en aucun cas autorisé de divulguer ces identifiants de connexions, comme le montre **l'article 4 de la charte : 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. **Et l'article 4.3** : 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.

4- Anouk n'est pas en règle car il a oublié de verrouiller sa session avant de quitter son poste (**Article 4, 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). De plus Léo, ne devrait pas sans l'accord de Anouk devoir utiliser sa session ni sa boîte mail. On peut s'appuyer sur **l'article 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.

5- Djibril ne peut pas et n'a pas le droit d'installer de jeu sur son ordinateur de travail car il est sur son lieu de travail et non personnel; comme le montre **les articles 4.6 et 4.7**, **l'article 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. et **l'article 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...).

6- Arthur n'a pas respecter les conditions d'utilisation de la charte informatique (**article 4.6** : 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).

7- Jules et son collègues sont tous les deux en non-respect des règles d'utilisation de la charte informatique, car le collègue de Jules aurait dû verrouiller sa session avant de quitter son poste (**Article 4.4** : L'utilisateur doit veiller à verrouiller sa session dès lors qu'il quitte son poste de travail, même de manière temporaire), et pour Jules (**Article 4.5** : 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).

8- Véronique n'a pas respectée les règles d'utilisation de la charte informatique en laissant un document confidentiel sur le photocopieur (**Article 4.1** : 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. Et **l'article 4.2** : 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).