NOM : Prénom :	La charte informatique	Durée : 01h00

Présentation du contexte

Rostand NetInfo est une entreprise au service du numérique, elle assure depuis janvier 2019 la vente de solution informatique auprès de ces clients. Les principales solutions sont l'infogérance serveurs, le service utilisateur, le cloud computing, le travail collaboratif et la sécurité informatique. Ces clients sont principalement des PME mais aussi des grandes entreprises.

En 2020, l'entreprise a lancé le travail à distance afin d'améliorer le quotidien des salariés et pour répondre aux besoins des clients malgré la crise sanitaire.

La société Rostand NetInfo a de fortes contraintes pour la vente de ces services. En effet, pour rassurer ces clients. L'entreprise doit mettre en place une charte informatique.

Vous travaillez par équipe de deux. Vous aurez pour mission d'assister l'entreprise dans la mission suivante :

- Réaliser une charte informatique en adéquation avec les besoins de l'entreprise ;

Le système informatique, architecturé comporte actuellement :

- 10 postes clients lourds et 60 postes clients légers destinés à se déplacer en clientèle et liés au travail à distance ;
- 10 serveurs ;
- 70 utilisateurs.

Vous vous appuierez sur les dossiers documentaires mis à votre disposition.

NOM : Prénom :	La charte informatique	Durée : 01h00

Annexes

Évaluer le niveau de sécurité des données personnelles de votre organisme

Avez-vous pensé à ?

Fiche		Mesure	
1	Sensibiliser les utilisateurs	Informez et sensibilisez les personnes manipulant les données	☐
		Rédigez une charte informatique et lui donner une force contraignante	☐
2	Authentifier les utilisateurs	Définissez un identifiant (*login*) unique à chaque utilisateur	☐
		Adoptez une politique de mot de passe utilisateur conforme à nos recommandations	☐
		Obligez l'utilisateur à changer son mot de passe après réinitialisation	☐
		Limitez le nombre de tentatives d'accès à un compte	☐
3	Gérer les habilitations	Définissez des profils d'habilitation	☐
		Supprimez les permissions d'accès obsolètes	☐
		Réaliser une revue annuelle des habilitations	☐
4	Tracer les accès et gérer les incidents	Prévoyez un système de journalisation	☐
		Informez les utilisateurs de la mise en place du système de journalisation	☐
		Protégez les équipements de journalisation et les informations journalisées	☐
		Prévoyez les procédures pour les notifications de violation de données à caractère personnel	☐
5	Sécuriser les postes de travail	Prévoyez une procédure de verrouillage automatique de session	☐
		Utilisez des antivirus régulièrement mis à jour	☐
		Installez un « pare-feu » (*firewall*) logiciel	☐
		Recueillez l'accord de l'utilisateur avant toute intervention sur son poste	☐
6	Sécuriser l'informatique mobile	Prévoyez des moyens de chiffrement des équipements mobiles	☐
		Faites des sauvegardes ou synchronisations régulières des données	☐
		Exigez un secret pour le déverrouillage des smartphones	☐
7	Protéger le réseau informatique interne	Limitez les flux réseau au strict nécessaire	☐
		Sécurisez les accès distants des appareils informatiques nomades par VPN	☐
		Mettez en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi	☐

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

8	Sécuriser les serveurs	Limitez l'accès aux outils et interfaces d'administration aux seules personnes habilitées	☐

NOM : Prénom :	La charte informatique	Durée : 01h00

		Installez sans délai les mises à jour critiques	□
		Assurez une disponibilité des données	□
9	Sécuriser les sites web	Utilisez le protocole TLS et vérifiez sa mise en œuvre	□
		Vérifiez qu'aucun mot de passe ou identifiant ne passe dans les url	□
		Contrôlez que les entrées des utilisateurs correspondent à ce qui est attendu	□
		Mettez un bandeau de consentement pour les *cookies* non nécessaires au service	□
10	Sauvegarder et prévoir la continuité d'activité	Effectuez des sauvegardes régulières	□
		Stockez les supports de sauvegarde dans un endroit sûr	□
		Prévoyez des moyens de sécurité pour le convoyage des sauvegardes	□
		Prévoyez et testez régulièrement la continuité d'activité	□
11	Archiver de manière sécurisée	Mettez en œuvre des modalités d'accès spécifiques aux données archivées	□
		Détruisez les archives obsolètes de manière sécurisée	□
12	Encadrer la maintenance et la destruction des données	Enregistrez les interventions de maintenance dans une main courante	□
		Encadrez par un responsable de l'organisme les interventions par des tiers	□
		Effacez les données de tout matériel avant sa mise au rebut	□
13	Gérer la sous-traitance	Prévoyez une clause spécifique dans les contrats des sous-traitants	□
		Prévoyez les conditions de restitution et de destruction des données	□
		Assurez-vous de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)	□
14	Sécuriser les échanges avec d'autres organismes	Chiffrez les données avant leur envoi	□
		Assurez-vous qu'il s'agit du bon destinataire	□
		Transmettez le secret lors d'un envoi distinct et via un canal différent	□
15	Protéger les locaux	Restreignez les accès aux locaux au moyen de portes verrouillées	□
		Installez des alarmes anti-intrusion et vérifiez-les périodiquement	□
16	Encadrer les développements informatiques	Proposez des paramètres respectueux de la vie privée aux utilisateurs finaux	□
		Évitez les zones de commentaires ou encadrez-les strictement	□
		Testez sur des données fictives ou anonymisées	□
17	Utiliser des fonctions cryptographiques	Utilisez des algorithmes, des logiciels et des bibliothèques reconnues	□
		Conservez les secrets et les clés cryptographiques de manière sécurisée	□

NOM : Prénom :	La charte informatique	Durée : 01h00

Charte informatique de l'entreprise Rostand NetInfo

PREAMBULE

L'entreprise Rostand NetInfo 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
- Divers réseaux clients

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

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

Article 1 : Utilisateurs concernés

La présente charte s'applique à l'ensemble des utilisateurs du système d'information dont notamment :

- 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
- téléphones
- réseau informatique (serveurs, routeurs et connectique)
- photocopieurs
- logiciels
- données informatisées
- messagerie
- …

Aux fins d'assurer la sécurité informatique du SI, tout matériel connecté au SI de 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 elle peut limiter l'accès à certaines ressources.

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.

4.1 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.

4.2 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

4.3 Verrouillage de sa session

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

4.4 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.

4.5 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 : Modalités d'utilisation des ressources informatiques

Note : décrire ici les modalités d'usage normal des ressources informatiques mises à disposition des utilisateurs - par exemple leur poste de travail, les différentes applications utilisées, la téléphonie mobile, etc

Article 6 : 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.

Article 7 : Email

Chaque employé peut disposer d'une adresse email pour l'exercice de ses missions.

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

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.

Article 8 : Sanctions

Les manquements aux règles édictées par la présente charte peuvent engager la responsabilité de l'utilisateur et entraîner des sanctions à son encontre (limitation d'usage du SI, sanctions disciplinaires.

Article 9 : Information et entrée en vigueur

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

Elle entre en vigueur au 01/10/2022