Charte de bons usages informatiques

syncerus

Charte de bons usages informatiques

Version	Date	Dernière modification	Rédacteur	Valideur

01. Contexte

« Description du contexte et des enjeux de l'entreprise »

02. Objectifs de la charte

La pérennité et le développement de l'entreprise profitent à l'ensemble de ses collaborateurs en leur offrant une sécurité de l'emploi, des perspectives d'évolution en partageant l'esprit de responsabilité incarné par l'entreprise familiale.

L'intégrité et l'agilité du Système d'Information et des informations qu'il contient dépendent principalement :

- Des bons usages des utilisateurs du Système d'Information
- De lignes managériales responsabilisées et engagées dans l'application de ces bons usages
- De la mise en œuvre de moyens de maîtrise efficaces en minimisant les contraintes sur les utilisateurs

La présente CHARTE DES BONS USAGES INFORMATIQUES vise à formaliser l'ENGAGEMENT commun tripartie entre les Utilisateurs du SI, les Manageurs, la Fonction Systèmes d'Information.

syncerus

Utilisateurs	Manager / Chaîne de direction	DSI
Organisation de la maîtrise et de l'agilité des Systèmes d'information		
• Je consulte le Service informatique et/ou mon manager pour l'ensemble de mes interrogations relatives à l'utilisation ou à l'évolution du S.I. • Je suis conscient que les mesures de maîtrise dans l'entreprise sont importantes afin de garantir la pérennité de l'activité. • Je suis responsable de la justesse des données que je saisis.	**Manager :** • Je fais remonter les besoins des projets d'évolution du S.I. au CoDir pour arbitrage. **Codir :** • J'attribue les ressources matérielles et humaines nécessaires à l'évolution du SI. • Je tranche et valide les besoins en fonction des objectifs stratégiques.	Je mets en œuvre et pilote une approche de la maîtrise et d'agilité des Systèmes d'Information. • Je suis support des autres Directions et émet des recommandations lorsque je suis sollicité. • Je formalise les règles d'évolution du SI en fonction de l'évolution de l'entreprise que je mets à disposition des responsables métier.
Sécurité de l'environnement de travail		
• J'ai conscience du fait que le poste de travail est maitrisé au mieux pour les besoins de sécurité de l'entreprise. • En cas de besoin, je contacte le Service Informatique pour l'installation d'un nouveau logiciel. • Je suis conscient qu'une certaine traçabilité de mes usages est effectuée uniquement à des fins de maîtrise du S.I. et notamment pour permettre d'identifier les attaques informatiques « intelligentes ». • A partir de mes équipements personnels, je m'efforce de ne pas télécharger de données de l'entreprise de sorte à en garantir la sécurité.	• J'ai la charge de vérifier que mes collaborateurs observent les règles de sécurité informatique de l'Entreprise • J'assure l'interface entre les besoins utilisateurs et les règles de sécurité. Je fais suis décideur et responsable des éventuelles exceptions de sécurité nécessaires au bon fonctionnement de mon service.	• Je m'efforce d'être facilitateur dans l'accompagnement des nouveaux besoins et de ne pas bloquer les usages nécessaires au bon fonctionnement des métiers. **Accès aux S.I. depuis des terminaux maîtrisés par l'entreprise :** l'ensemble des terminaux fournis par le groupe (ordinateurs, tablettes, smartphones…) sont munis de systèmes permettant d'en assurer la maîtrise et notamment : journalisation de l'activité, antivirus, chiffrement ou suppression des données à distance, mises à jour, gestion des droits utilisateurs, … La limitation des droits utilisateurs est mesurée afin de limiter les contraintes utilisateurs tout en assurer un niveau maîtrise efficace. **Accès aux S.I. depuis des terminaux non maîtrisés par l'entreprise :** j'accède depuis un système de bureau à distance sécurisé.

syncerus

Utilisateurs	Manager / Chaîne de direction	DSI
Évolution des outils numériques		
• Je m'efforce de consulter le service informatique pour obtenir une analyse technique des outils avant de les commander et de les exploiter. • Je suis conscient qu'en utilisant des outils non validés par l'équipe informatique, je crée directement des vulnérabilités et je mets en danger l'entreprise. De plus, en cas de commande avant validation par l'équipe informatique je coupe toute capacité de négociation avec le fournisseur.	• Je formalise et centralise les nouveaux besoins pour les soumettre à la DSI. • Je porte ma demande au Codir pour arbitrage budget et priorité. • Je suis responsable de l'évolution des usages et des nouveaux projets dans mon service. Ainsi, je me dois de veiller à ce que mes collaborateurs consultent l'équipe informatique dans le cadre de l'évolution de leurs outils.	• Je qualifie le niveau de sécurité et d'interopérabilité de l'ensemble des outils informatiques à venir. • J'audite les outils sélectionnés par les métiers avant leur commande pour identifier les meilleures possibilités d'intégration et de sécurisation. • Je conseille les utilisateurs sans remettre en cause leurs besoins. • Je vise à ce que l'ensemble des accords avec les fournisseurs et partenaires comportent un volet / interopérabilité des données.
Gestion des habilitations & authentification		
• Je m'efforce de ne pas copier mes mots de passe en dehors du coffre-fort sécurisé mis à ma disposition. • Je choisis un mot de passe que je suis le seul à pouvoir deviner. • J'informe mon manager de tous accès ou comportement qui me semble anormal.	• Je suis responsable des habilitations que j'attribue à mes équipes et des identifiants/mots de passe que je communique. • Je suis responsable du suivi des évolutions des habilitations en fonction de l'évolution de l'activité de mon équipe. • Je ne fournis pas de moyens d'authentification ou d'accès à des outils autres que les comptes génériques prévus à cet effet.	• Je mets à disposition des managers les mécanismes nécessaires à la gestion des habilitations : processus d'arrivée/sorties/évolution des utilisateurs, profils applicatifs (utilisateur, administrateur, ...), etc. • Je mets à disposition des utilisateurs un coffre-fort de mots de passes qui permet de sécuriser les mots de passe de l'entreprise. • Je mets en place une politique de sécurité des mots de passe qui permet un niveau de sécurité minimal. • Je fais attention à ce que les comptes génériques aient des droits limités : Les comptes génériques font l'objet d'une approbation séparée, appropriée et d'un contrôle permanent pour faciliter le travail des agents de Production et de Logistique.

Utilisateurs	Manager / Chaîne de direction	DSI
Manipulation des informations de l'entreprise		
• Je m'efforce d'utiliser les outils de stockage et de partage d'information mis à disposition par l'entreprise : adresse email, Teams et OneDrive. • Je suis conscient que faire sortir les informations de l'entreprise sur des médias non maîtrisés (clés USB, drives Google, iCloud, Dropbox, …, OneDrive personnel, WeTransfer, boite mail personnelle, etc.) est une faute professionnelle, en particulier pour les informations explicitement classifiées en usage interne ou confidentiel. • Je comprends que mes extractions de données et mes transferts d'informations peuvent être tracés et que des alertes automatisées permettront de remonter les écarts d'utilisation à la Direction de l'entreprise. • J'inscris le niveau de classification dans l'ensemble des documents produits.	• Étant responsable des droits affectés à mon équipe, je vérifie au moins annuellement l'ensemble des droits qui leurs sont affectés. • Je définie la classification des informations produites ou manipulées par mon équipe : • **Confidentiel :** groupe de personnes désignées uniquement ; • **Interne :** seul le personnel et les partenaires munis d'un accord de confidentialité peuvent accéder à l'information • **Public :** l'information est destinée à être communiquée à l'extérieur de l'entreprise • **Contient des données personnelles :** l'information doit être inscrite dans le registre des traitements des données à caractère personnel qui en détermine leur utilisation (RGPD). • Je vérifie que le niveau de confidentialité est mentionné dans les documents produits.	• J'applique une surveillance à l'accès et l'utilisations de données sensibles (RH, bancaires, clients, …). • J'alerte les managers sur d'éventuelles incohérences de droits qui pourraient être détectées. • Une cartographie et une classification des informations est mise en œuvre.
Gestion des besoins et problématiques du quotidien		
• Je comprends que pour répondre de façon efficace, professionnelle et organisée à l'ensemble des sollicitations de l'Entreprise, le Service Informatique ne peut pas prendre en charge immédiatement l'ensemble de mes propres sollicitations. • Je m'efforce de respecter le processus de sollicitation du point de contact unique et de planification du traitement de ma requête sans contacter individuellement le personnel de service informatique.	• En cas de besoin ou problématiques bloquantes, j'appuie la requête de mon collaborateur pour la faire passer en priorité.	• Je m'engage à réagir aux besoins exprimés et à corriger rapidement les dysfonctionnements constatés et ainsi éviter que les utilisateurs aient recours à des solutions de contournement (Shadow IT). • Je mets en place un point de contact unique, joignable par téléphone, mail ou en présentiel qui aura pour fonction de prendre en charge les sollicitations, de les formaliser et de planifier leur prise en charge.

4. Annexe

4.1. Exigences Règlementaires

Les entreprises comme les Hommes sont soumis à des exigences réglementaires qui régissent les relations entre individus et entités. Elles sont là pour expliquer, protéger, dissuader voire sanctionner.

Les entreprises sont soumises à nombreuses responsabilités qu'elles doivent assumer (notamment RSE). Ces responsabilités sont portées par des hommes/femmes dans le cadre de leur rôle professionnel. Prendre connaissance des enjeux et failles permet d'adopter une nouvelle vision et réflexes pour la sécurité de tous.

Cela s'applique à toutes actions réalisées dans l'entreprise par les collaborateurs mais également par les externes (prestataires, intérimaires…) ayant accès aux locaux, applications, données du groupe Mais ces bonnes pratiques permettent de se protéger également de manière individuelle dans la sphère privée.

Adoptez les bons réflexes c'est vous protégez, vous et votre entreprise.

Les bonnes pratiques relèvent principalement du bon sens à condition de prendre conscience de l'importance de la sécurité de l'information.

Cas pratiques :

- Vous êtes responsables des données que vous stockées :
On s'introduit sur votre ordinateur et on y dépose des images illicites ou données compromettantes dont vous ne soupçonnez pas l'existence. Vous êtes au sens de la loi responsable.

- Vous cliquez sur un lien qui a permis qu'on récupère votre mot de passe ce qui a permis de subtiliser des données de l'entreprise (cf. Phishing). Toute l'entreprise est en arrêt pendant des jours. Vous êtes responsable.

- Vous avez prêté vos accès à un collègue qui a fait une erreur et à supprimer par mégarde des fichiers sans possibilité de les restaurer. Vous êtes responsable.

4.2. Responsabilité sociale des entreprises - RSE

Rse : ISO 26 000

Les différents thèmes de responsabilité de l'entreprise selon l'ISO 26 000 sont :

- La gouvernance de l'organisation (compromise par une fuite de donnée ou attaque)
- Les droits humains
- Les relations et conditions de travail
- L'environnement
- Les bonnes pratiques des affaires
- La protection des consommateurs
- La contribution au développement local

Importance de la donnée dans le Système d'Information

La donnée est la propriété de l'entreprise. Son utilisation, sa transmission ou sa destruction est soumise aux règles de l'entreprise mais elle est également soumise à des lois.

Sécurité

Désigne l'ensemble des éléments mis en place pour garantir l'accès restreints aux données aux seuls destinataires de celle-ci. « Le niveau de sécurité d'un S.I. est déterminé par son maillon le plus faible »

Confidentialité

La donnée d'entreprise est soumise au secret professionnel. Une donnée livrée à des tiers sans contrôle peut faire l'objet d'espionnage industriel et provoquer une concurrence déloyale.

Le RGPD (Règlement Général sur la Protection des Données du 23 mai 2018) régit les règles d'exploitation des données personnelles. A ce titre, il impose notamment à déterminer l'objet de détention ou la durée de conservation pour les données.

Ne sous-estimez pas l'ingéniosité de l'exploitation d'une donnée.

Le personnel employé par l'entreprise à quelque titre que ce soit est tenu de garder une discrétion absolue sur tout ce qui a trait aux secrets et procédés de fabrication et d'une manière générale sur toutes les opérations dont il aurait connaissance dans l'exercice de ses fonctions, sous réserve de l'exercice du droit d'expression légalement organisé. A ce titre, l'employé ne doit pas stocker de document interne de l'entreprise sur un espace non sécurisé ou sur un support externe à l'entreprise.

Les données de votre entreprise ne doivent pas être stockées hors des espaces sécurisés prévus à cet effet (ex. : sur votre C:\ dans mes documents, bureau etc.).

Disponibilité

La donnée pour être exploitable doit être partagée dans l'ensemble de l'entreprise pour devenir un levier de performance efficace. Si tout le monde partage la même vision dans l'entreprise alors, les efforts pourront allez dans la même direction.

Intégrité

La donnée doit être fiable pour être exploitée. L'altération de la donnée par un tiers est plus difficile à détecter que sa suppression.
Par exemple le remplacement ou la falsification d'un RIB fournisseur au profit d'un tiers malveillant.