SI – Charte d'utilisation du système d'information

1. Objet

Cette charte s'adresse à l'ensemble des collaborateurs ORES (internes et externes) qui interagissent avec le système d'information d'ORES, informatique (ordinateurs, tablettes, applications, …) ou papier (courrier, contrat, archives, ...). Elle a pour objectif d'informer le collaborateur de ses responsabilités dans les comportements appropriés à adopter à l'égard de la Sécurité de l'Information.

L'ensemble des règles énoncées ci-dessous sont issues des différents documents de gouvernance de la sécurité de l'information (disponibles sur le portail dédié).

2. Domaine d'application

Bien qu'ils ne soient pas soumis aux règles découlant du contrat de travail ni à l'autorité patronale d'ORES, les collaborateurs externes travaillant pour ORES (consultants, intérimaires, étudiants et stagiaires) sont également tenus de se conformer aux standards de sécurité édictés par ORES. Ils en seront dument informés soit directement par ORES, soit par le biais de la société qui les emploie ou par le MSP (Managed Service Provider) d'ORES lorsqu'il s'agit de contrats de services. Les règles édictées dans ce document sont à interpréter à la lumière de cet avertissement.

3. Notes de version et diffusion

VERSION : N° v 1.1 du 19/09/2024
MISE EN APPLICATION : 19/09/2024
DERNIÈRE RÉVISION MAJEURE OU PÉRIODIQUE : 30/04/2024

NOTES DE MISE À JOUR : Référence à la Notice Utilisateur Comment transférer l'information
POUR MISE EN APPLICATION : Information Security Office
POUR INFORMATION : Tout ORES
MOTS CLÉS : Règles, charte, usage, manipulation, signalement, classification, transfert, marquage, incidents, badges, visiteurs, perte, vol, équipement

	NOMS	DATE - SIGNATURE
RÉDACTEUR	Julien MAQUINAY Bruno GUILLAUME	
RESPONSABLE D'ACTIVITÉS	Pierre GERODEZ	
RESPONSABLE DU PROCESSUS	Stéphane BALDINO	
CONFORMITÉ QUALITÉ IT	Axelle GILON	

TABLE DES MATIÈRES

4. Règles concernant l'utilisation du matériel informatique

4.1. Bon usage des équipements informatiques

CUSI-1. Le collaborateur **DOIT** utiliser les équipements informatiques et les logiciels mis à sa disposition par ORES à des fins professionnelles.

CUSI-2. Le collaborateur **DOIT** les utiliser en personne prudente et raisonnable.

CUSI-3. Le collaborateur ne **PEUT PAS** les utiliser pour des activités non autorisées telles que les jeux ou la consultation de contenu d'éthique discutable.

CUSI-4. Le collaborateur **NE PEUT PAS** envoyer automatiquement des courriels à son adresse privée (notamment en activant un « *forward* » automatique des courriels entrants), même pendant ses périodes d'absence (vacances, incapacité de travail, etc.).

CUSI-5. Le collaborateur **NE PEUT PAS** installer sur son ordinateur des logiciels qui n'ont pas été préalablement approuvés par ORES.

4.2. Précautions contre le vol et la dégradation

CUSI-6. Le collaborateur **DOIT** prendre toutes les précautions nécessaires pour éviter le vol et la dégradation des équipements informatiques qui lui ont été confiés, en particulier en dehors des sites ORES.

CUSI-7. En conséquence, le collaborateur

a. **NE PEUT PAS** laisser son ordinateur sans surveillance dans sa voiture
b. **DOIT** rester vigilant dans les transports en commun
c. **NE PEUT PAS** manger ou boire au-dessus de son ordinateur portable

4.3. Signalement des pertes et vols

CUSI-8. En cas de perte ou de vol de matériel, le collaborateur **DOIT** en informer immédiatement la Direction Informatique.

CUSI-9. En cas de vol le collaborateur **DOIT** également déclarer le vol à la police.

4.4. Sécurité des sessions et des applications

CUSI-10. Le collaborateur **DOIT** verrouiller sa session dès que son ordinateur est laissé sans surveillance.

CUSI-11. Le collaborateur **DOIT** également veiller à se déconnecter des applications qu'il n'utilise plus.

4.5. Sécurisation des supports d'information

CUSI-12. Le collaborateur **DOIT** veiller à sécuriser les supports d'information qu'il utilise, tels que les documents imprimés et les clés USB.

CUSI-13. Il **DOIT** limiter au maximum l'usage de ce genre de supports.

CUSI-14. Il **DOIT** ranger les documents papiers sensibles dans des armoires fermées à clé.

CUSI-15. Il **DOIT** sécuriser l'accès aux informations stockées sur les clés USB, disques durs externes et cartes mémoire via un mécanisme d'authentification et de chiffrement (basé sur la connaissance d'un secret).

CUSI-16. Au besoin, il **DOIT** effectuer une destruction partielle ou complète du support d'information pour rendre l'information inaccessible (déchiqueteuse à papier, formatage du support amovible, réinitialisation d'usine, etc.).

4.6. RESPECT DES DISPOSITIFS DE SÉCURITÉ

CUSI-17. Le collaborateur **NE PEUT PAS** entraver le bon fonctionnement des dispositifs de sécurité mis en place par ORES tels les antivirus, les VPN, les mécanismes d'authentification et de contrôle d'accès, le filtrage des flux de navigation internet, le blocage de l'installation de logiciels non standard,…

5. Règles concernant la manipulation de l'information

5.1. PROTECTION DE L'INFORMATION

CUSI-18. Le collaborateur **DOIT** manipuler et protéger l'information à laquelle il accède en fonction de son niveau de confidentialité (C1-Public, C2-Interne, C3-Restreint, C4-Confidentiel).

CUSI-19. Il **DOIT** donc notamment

a. S'assurer que les bonnes permissions ont été spécifiées sur les dossiers partagés
b. Partager les informations sensibles uniquement avec les personnes habilitées
c. Effacer les annotations sur les tableaux et les « flip charts » en fin de réunions

5.2. PRINCIPE DU BUREAU PROPRE

CUSI-20. Le collaborateur **NE PEUT PAS** laisser traîner des documents sensibles sur son bureau, sur une imprimante ou dans des armoires non sécurisées. Ceci s'applique également aux clés USB et autres supports de stockage externes.

5.3. STOCKAGE SÉCURISÉ DES ARCHIVES

CUSI-21. Le collaborateur **DOIT** stocker de manière sécurisée ses archives, qu'elles soient papier, électroniques ou sous forme de courriels.

5.4. TRANSFERT DE L'INFORMATION

CUSI-22. Pour transférer de l'information à l'intérieur ou à l'extérieur de l'entreprise, le collaborateur **DOIT** faire usage des outils informatiques mis à disposition par ORES et respecter les règles décrites dans la notice dédiée consultable sur le portail de sécurité de l'information des membres du personnel.

CUSI-23. Il **DOIT** donc éviter l'usage de services tels Google Drive, Dropbox, WeTransfer, etc.

CUSI-24. En cas de doute sur la bonne manière de transférer de l'information, le collaborateur **DOIT** s'adresser à sa hiérarchie.

5.5. MARQUAGE DES DOCUMENTS

CUSI-25. Lors de la création de documents, le collaborateur **DOIT** les marquer en fonction du niveau de confidentialité des informations qu'ils contiennent (« C1-Public », « C2-Interne », « C3-Restreint » ou « C4-Confidentiel »).

CUSI-26. À cette fin les modèles de documents et les pictogrammes confidentialité mis à disposition par le service Communication **DOIVENT** être utilisés.

.

5.6. ÉLIMINATION DE L'INFORMATION INUTILE

CUSI-27. Le collaborateur **DOIT** effacer ou détruire toute information devenue inutile ou obsolète. Cela s'applique aux documents papier, aux fichiers électroniques et aux courriels.

CUSI-28. Il **DOIT** veiller à vider régulièrement la corbeille de son ordinateur et appliquer les procédures de destruction appropriées pour les supports physiques.

6. Règles concernant la notification d'événements préjudiciables à la sécurité de l'information

6.1. SIGNALEMENT DES ÉVÉNEMENTS SUSPECTS

CUSI-29. Le collaborateur **DOIT** signaler tout événement suspect pouvant potentiellement affecter la sécurité du système d'information d'ORES en créant un incident de sécurité via l'application **Easy IT**.

CUSI-30. Il **DOIT** donc notamment

a. Signaler toute personne qui s'introduirait de manière suspecte dans un bâtiment ORES en contournant les dispositifs de sécurité tels que portails, badges, réception, clés, codes, etc. (ces événements suspects liés à la sécurité physique peuvent également faire l'objet d'une création de « ticket patrimoine »).
b. Signaler toute tentative d'ingénierie sociale dont il aurait fait l'objet (par exemple, s'il est contacté via les réseaux sociaux pour obtenir des informations sensibles concernant ORES).

6.2. SIGNALEMENT DES FAILLES DE SÉCURITÉ

CUSI-31. Le collaborateur **DOIT** signaler toute suspicion ou observation d'une faille de sécurité (vulnérabilité) au sein du système d'information d'ORES en créant un incident de sécurité via l'application **Easy IT** (il peut s'agir de toute anomalie relative à la sécurité observée sur son ordinateur ou sur le réseau informatique, comme un antivirus désactivé ou non mis à jour, des droits d'accès excessifs, etc.)

CUSI-32. Si la faille de sécurité observée concerne des données à caractère personnel, le collaborateur **DOIT** le mentionner au moment de la création de l'incident de sécurité afin que le Data Protection Officer (DPO) soit immédiatement mis au courant (impact RGPD).

6.3. SIGNALEMENT DES TENTATIVES D'HAMEÇONNAGE (PHISHING)

CUSI-33. Le collaborateur **DOIT** signaler toute tentative d'hameçonnage au moyen du bouton « Signaler le message » dans le client de messagerie électronique (MS Outlook) pour tout courriel qu'il suspecte comme étant illégitime.

7. Règles concernant la sécurité physique

7.1. USAGE DU BADGE D'ACCÈS

CUSI-34. Le collaborateur **DOIT** veiller à garder sur lui en permanence son badge d'accès et il **DOIT** restreindre son emploi à un usage strictement personnel.

CUSI-35. Le collaborateur **NE PEUT PAS**

a. Laisser traîner son badge sur son bureau
b. Prêter son badge
c. Utiliser son badge pour faire entrer quelqu'un d'autre

7.2. ACCOMPAGNEMENT DES VISITEURS D'UN JOUR

CUSI-36. Lorsqu'il reçoit un « visiteur d'un jour », le collaborateur **DOIT** accompagner ce visiteur en permanence durant sa présence sur site.

CUSI-37. Pour les sites d'ORES disposant d'un accueil physique ou virtuel, le collaborateur **DOIT** également s'assurer que son visiteur porte de manière visible un badge d'identification

8. Règles concernant le contrôle d'accès

8.1. PRINCIPE DE BASE

CUSI-38. Un compte utilisateur permettant l'accès au système d'information est strictement personnel. Toute action effectuée avec ce compte sera donc directement imputable au collaborateur à qui ce compte a été attribué.

8.2. CONFIDENTIALITÉ DES INFORMATIONS D'AUTHENTIFICATION

CUSI-39. Le collaborateur **DOIT** prendre toutes les mesures nécessaires pour conserver secrètes ses informations d'authentification (codes PIN, identifiants, mots de passe).

CUSI-40. Il **DOIT** donc notamment

a. Privilégier l'usage d'une application de gestion de mots de passe
b. Ne pas conserver ses identifiants sur un post-it, dans un cahier ou dans un fichier non protégé (Word, Excel, Notepad, etc.)
c. Ne jamais communiquer ses mots de passe avec autrui (pas même un collègue)

8.3. DIFFÉRENCIATION DES MOTS DE PASSE

CUSI-41. Le collaborateur **DOIT** toujours veiller à utiliser des mots de passe distincts dans la sphère professionnelle et dans la sphère privée.

8.4. PRINCIPE DU "BESOIN DE CONNAÎTRE"

CUSI-42. Un collaborateur ne peut consulter une information que si cela est strictement nécessaire à l'exercice de sa mission. Disposer de droits d'accès à une information est donc une condition nécessaire **mais pas suffisante** pour accéder à cette information. Concrètement un collaborateur ne **DOIT** pas consulter d'informations sur des employés, des clients, des partenaires quand ces informations ne sont pas nécessaires pour réaliser son travail (par exemple, messagerie de collègues, dates de naissance, numéro de registre national, numéro de compte en banque, adresse privée, données du voisin, etc.).

9. Documents associés

IT-021-D01 Directive de la Sécurité de l'Information **[Ref 0]**