MINISTÈRE
DE L'ACTION
ET DES COMPTES
PUBLICS

Liberté
Égalité
Fraternité

Centre Interministériel de
Services Informatiques relatifs
aux Ressources Humaines

Processus de sécurité dans les ressources humaines

Charte informatique du CISIRH

Table des matières

ARTICLE 1 : Préambule 10
ARTICLE 2 : Définitions 10
2.1 Ressources informatiques 10
2.1 Services numériques 10
2.2 Utilisateurs 10
2.3 Administrateurs 10
ARTICLE 3 : Champs d'application 11
ARTICLE 4 : Droits et devoirs des utilisateurs 12
4.1 Gestion des accès au système d'information et de communication 12
4.2 Utilisation des ressources 12
4.3 Privilèges et droits « administrateurs » 13
4.4 Règles générales de sécurité 13
4.5 Gestion des authentifiants informatiques 13
4.6 Mise en œuvre d'outils ayant un impact sur la sécurité du SI 14
4.7 Devoir de rendre compte 15
4.8 Raccordement des équipements informatiques 15
4.9 Sécurité des données professionnelles 16
4.10 Utilisation des ressources numériques du CISIRH en externe 17
4.11 Vol ou perte d'équipements informatiques ou téléphoniques 19
4.12 Gestion et utilisation des supports amovible 19
4.13 Connexion aux réseaux sans fil 19
4.14 Obligation de formation 19
4.15 Départ ou mutation d'un utilisateur 20
ARTICLE 5 : Droits et devoirs des administrateurs du Système d'Information 20
5.1 Devoir de réserve des administrateurs 20
5.2 Devoir d'information, de conseil et d'alerte 20
5.3 Devoir de respect de la vie privée des utilisateurs 21

5.4 Gestion des traces dans le système d'information et de communication..... 21
5.5 Gestion des sauvegardes des données des utilisateurs..... 21
5.6 Gestion des accès d'un équipement informatique ou téléphonique 21
5.7 Droits de configuration des équipements 21
5.8 Maintenance 22
ARTICLE 6 : Respect de la propriété intellectuelle.....22
6.1 Reproduction ou décompilation de logiciels.....22
6.2 Installation de contenus numériques soumis aux copyrights, droits d'auteur ou gestion des droits numériques (DRM) 22
6.3 Logiciels professionnels installés sur un équipement privé 22
6.4 Archivage des ressources documentaires 23
ARTICLE 7 : Respect de la confidentialité des informations.....23
7.1 Droits d'accès aux informations 23
7.2 Hébergement des informations.....23
7.3 Interception des communications entre tiers 23
7.4 Respect des engagements de confidentialité avec un tiers 23
7.5 Traitement des données à caractère personnel 23
7.6 Continuité de service 24
7.7 Confidentialité des données 24
ARTICLE 8 : Relations avec les sites distants et les autres sites informatiques 24
8.1 Connexion à un site distant.....24
8.2 Fonctionnement intègre du système d'information 25
8.3 Partage d'information avec un site distant 25
ARTICLE 9 : Échanges électroniques.....25
9.1 Devoir de réserve 25
9.2 ègles de savoir-vivre.....25
9.3 Responsabilité de l'utilisateur relative au contenu des échanges 25
9.4 Intégrité des échanges électroniques 26
9.5 Messagerie instantanée 26

ARTICLE 10 : Télétravail 26
ARTICLE 11 : Évolution de la charte.....26
ARTICLE 12 : Sanctions applicables 26

Documents applicables

Type du document	Origine	Nom du document	Date
Norme internationale	Organisation internationale de normalisation ISO et Commission Electrotechnique Internationale IEC	ISO/CEI 27001 :2022 – Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences	2022
Norme internationale	Organisation internationale de normalisation ISO et Commission Electrotechnique Internationale CEI	ISO/CEI 27701 – Techniques de sécurité – Extension d'ISO/IEC 27001 et ISO/CEI 27002 au management de la protection de la vie privée – Exigences et lignes directrices	Publiée en avril 2021
PSSI	CISIRH	Politique de Sécurité des Systèmes d'Information du CISIRH	2022
PGSSI	Ministère de l'Economie et des Finances	Arrêté du 13 décembre 2023 portant approbation de la politique ministérielle de sécurité numérique des ministères économiques et financiers	13 décembre 2023
Charte	Ministère de l'Economie et des Finances	Charte ministérielle d'utilisation des outils numériques	Publiée en février 2018

Un document applicable comprend des exigences auxquelles le CISIRH doit se conformer. Il peut s'agir de dispositions législatives ou contractuelles ainsi que des stipulations réglementaires ou des règles normatives.

Documents de référence

Type du document	Origine	Nom du document	Date
Norme internationale	Organisation internationale de normalisation ISO et Commission Electrotechnique Internationale IEC	ISO/CEI 27002 - Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information	2022

Un document de référence apporte des renseignements ou des enseignements pouvant intégrer des recommandations sans portée obligatoire.

Terminologie

Acronyme	Signification
ISO	Organisation internationale de normalisation
CEI	Commission Electrotechnique Internationale
CGU	Conditions générales d'utilisation
DRM	*Digital rights management* Gestion des droits numériques ayant pour objectif de contrôler l'utilisation qui est faite des œuvres numériques par leur cryptage
HFDS	Haut-fonctionnaire de défense et de sécurité
HTTP	*Hypertext Transfer Protocol* Protocole de communication client-serveur développé pour le Web
SMSI	Système de Management de la Sécurité de l'Information
SNUM	Service du numérique des ministères économiques et financiers
SSI	Sécurité des Systèmes d'Information
RSSI	Responsable de la Sécurité des Systèmes d'Information du CISIRH
PSSI	Politique de sécurité des systèmes d'information

Acronyme	Signification
PSSI-E	Politique de sécurité des systèmes d'information de l'Etat
VPN	*Virtual private network* Réseau privé virtuel
RGPD	Règlement général sur la protection des données
SNUM	Service du numérique du Secrétariat Général des Ministères économiques et financiers
LAB	Laboratoire d'innovation du CISIRH

Terme	Définition
Cookie	Témoin de connexion défini par le protocole de communication HTTP comme étant un court texte envoyé par un serveur à un client

ARTICLE 1 : Préambule

La présente charte, rédigée dans le cadre de la réglementation propre à l'Administration française et au Centre Interministériel de Systèmes Informatiques relatifs aux Ressources Humaines (CISIRH), définit les règles d'usage et de sécurité que le CISIRH et l'utilisateur s'engagent à respecter. Elle précise notamment les droits et devoirs de chacun. Elle découle de la charte ministérielle[1].

ARTICLE 2 : Définitions

2.1 Ressources informatiques

Le terme « ressources informatiques » désigne l'ensemble du matériel (équipements informatiques, multimédias, téléphoniques, de stockage, d'archivage, de gestion…), les logiciels accessibles en interne ou en externe via le réseau du CISIRH ainsi que les données du CISIRH et les données collectées ou confiées au CISIRH.

Les équipements tiers, notamment personnels, utilisés sur le système d'information du CISIRH dans le respect des consignes de sécurité en vigueur, deviennent pour le temps de l'usage une ressource informatique du CISIRH et sont donc soumis à cette présente charte.

2.1 Services numériques

Les « services numériques » correspondent à l'ensemble des outils et applications (d'échange, de collaboration, …) utilisant des ressources informatiques internes ou externes du CISIRH.

2.2 Utilisateurs

Les personnes utilisant le système d'information du CISIRH, les ressources informatiques s'y rapportant et les services numériques sont appelées « utilisateurs ».

2.3 Administrateurs

Les « administrateurs » sont les utilisateurs chargés officiellement (lettre de mission, fiche de poste, contrat de travail, contrat de prestation…) du bon fonctionnement et de la sécurité de ressources informatiques faisant partie du système d'information du CISIRH. Ainsi, ils jouissent de droits étendus du fait de leur fonction et non de leur position hiérarchique. Il s'agit des utilisateurs ayant des droits d'administration sur leur poste de travail (du réseau SNUM ou du réseau CISIRH).

Ils sont généralement membres du service en charge des systèmes d'information du CISIRH.

[1] Charte Ministérielle sur le site du Haut-fonctionnaire de défense et de sécurité (HFDS)

Les « administrateurs systèmes et réseaux » sont en charge de l'installation, du maintien et de la gestion des « équipements techniques ». Ils sont responsables du bon fonctionnement des infrastructures informatiques placées sous leur responsabilité.

Les « administrateurs applicatifs » sont en charge des activités d'exploitation liées aux applications et logiciels du CISIRH ainsi que de la gestion des données. Ils sont responsables du bon fonctionnement des applications et logiciels placés sous leur responsabilité.

De plus, dans le cadre du Lab du CISIRH, par dérogation, un utilisateur peut jouir de droits et privilèges étendus sur son poste de travail. Il possède des droits d'administrateur local, c'est-à-dire, qu'il peut modifier la configuration de son poste de travail.

ARTICLE 3 : Champs d'application

Les présentes dispositions s'appliquent à l'ensemble des utilisateurs :

- ✓ personnel du CISIRH (y compris les stagiaires et apprentis)
- ✓ personnel travaillant ou accueillis dans les locaux
- ✓ de manière générale, à l'ensemble des personnes physiques présentes sur le site du CISIRH ou ayant accès aux systèmes d'information sous la responsabilité du CISIRH (visiteurs, stagiaires, intervenants, personnels d'autres organismes ou administrations, prestataires, invités, membres d'associations, bénévoles…) en présentiel ou à distance.

Le système d'information couvert par la charte comprend les ressources informatiques et numériques mises en place par le CISIRH ou mises à sa disposition par le service du numérique (SNUM) des ministères économiques et financiers. Sont notamment concernées les solutions s'adressant aux partenaires du CISIRH ainsi que les applications internes, notamment pour la gestion documentaire ou les demandes de changement.

Tout agissement contraire aux dispositions de la présente charte peut entrainer une suspension temporaire ou définitive des droits d'accès au système d'information et de communication, et est passible, selon la gravité des faits, de sanctions disciplinaires, civiles ou pénales.

ARTICLE 4 : Droits et devoirs des utilisateurs

4.1 Gestion des accès au système d'information et de communication

L'utilisation des ressources informatiques au CISIRH est soumise à autorisation préalable, concrétisée par l'ouverture d'un compte ou le droit de connecter un équipement informatique ou téléphonique sur le réseau du CISIRH.

Cette autorisation est strictement personnelle et correspond à des privilèges en rapport avec l'activité de l'utilisateur. Elle ne peut donc en aucun cas être cédée à un tiers, même temporairement. Les actions effectuées avec une autorisation d'accès sont imputables à l'utilisateur détenteur de cette autorisation. Un utilisateur ne doit pas utiliser de comptes autres que ceux pour lesquels il a reçu une autorisation. Il doit s'abstenir de toute tentative de s'approprier ou de déchiffrer le mot de passe d'un autre utilisateur. L'utilisateur ne doit pas s'éloigner d'un équipement informatique ou téléphonique mobile sans s'être préalablement déconnecté de sa session ou l'avoir verrouillée.

Si une menace avérée ou une suspicion de menace pèse sur le système d'information, après avis du RSSI (responsable de la sécurité des systèmes d'information), le CISIRH se réserve le droit de retirer à tout moment cette autorisation, et ce, sans préavis. L'administrateur informera l'utilisateur impacté par tout moyen (mail, minimessage transmis par téléphone, etc.) permettant une traçabilité.

Enfin, cette autorisation prend fin lors de la cessation de l'activité de l'utilisateur et elle est réexaminée lors de toute modification d'activité (changement de service, changement de catégorie d'utilisateur). Le bureau des affaires générales notifie à l'administrateur le départ d'un utilisateur dans le cadre du circuit de départ. Le paragraphe 4.14 précise les dispositions applicables en cas de départ ou mutation d'un utilisateur.

4.2 Utilisation des ressources

L'utilisation du système d'information et de communication est limitée à des activités légitimes de développement informatique, d'exploitation, et à toute activité administrative de gestion et de support liée à ces activités.

Ces moyens de communication et de traitement de l'information (ressources informatiques, téléphoniques, etc.) ne peuvent être utilisés pour une finalité extérieure au CISIRH, sauf autorisation préalable formalisée par une personne ayant autorité pour engager le CISIRH.

Tout utilisateur s'engage à utiliser correctement les ressources mises à sa disposition (mémoire à ne pas saturer, espace disque, bande passante des réseaux,

imprimantes…). Ainsi le renvoi automatique des messages parvenant dans une boîte-aux-lettres est interdit. Plutôt que transmettre un document en pièce jointe à un courriel, il est recommandé de communiquer son emplacement dans une ressource partagée ou une base documentaire.

Dans le cadre de l'utilisation d'Internet, seuls les services Internet présentant un lien direct et nécessaire avec l'activité professionnelle ont vocation à être consultés.

Les restrictions sur les accès internet peuvent être partiellement ou totalement levées, après autorisation du Responsable de la Sécurité des Systèmes d'Information du CISIRH, dans le cas où les besoins métiers des utilisateurs pourraient le justifier.

Conformément à la charte ministérielle, une consultation d'Internet pour un motif privé est tolérée (courriels personnels, recherches hors contexte professionnel, etc.) si elle s'inscrit dans le cadre de la présente charte, si elle est ponctuelle et brève, si le contenu consulté n'est pas contraire à l'ordre public et aux bonnes mœurs et enfin si cette consultation n'interfère pas outre mesure avec les missions confiées à l'utilisateur.

4.3 Privilèges et droits « administrateurs »

Par dérogation à la politique de sécurité des systèmes d'information de l'Etat (PSSI-E), l'utilisateur est autorisé, sur demande dument justifiée, à jouir des droits et privilèges administrateurs locaux sur les postes de travail. A ce titre, ils sont soumis aux dispositions de l'article 5.

Le RSSI maintient une liste des utilisateurs possédant des privilèges et droits administrateurs.

4.4 Règles générales de sécurité

Chaque utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques du CISIRH. A ce titre, il se doit, à son niveau, de contribuer à la sécurité du système d'information afin de ne pas constituer lui-même un élément de faiblesse pour le système d'information du CISIRH.

4.5 Gestion des authentifiants informatiques

Tout utilisateur doit choisir des mots de passe sûrs respectant à minima les recommandations ci-dessous :

- ✓ Pour un utilisateur, le mot de passe doit contenir :
  - au moins 16 caractères ;

- au moins une majuscule (A-Z);
- au moins une minuscule (a-z);
- au moins un chiffre (0-9);
- au moins un caractère spécial

✓ Pour un administrateur (compte nominatif ou compte de service/technique), le mot de passe doit contenir :

- au moins 20 caractères ;
- au moins une majuscule (A-Z);
- au moins une minuscule (a-z);
- au moins un chiffre (0-9);
- au moins un caractère spécial.

Un renouvellement de ces mots de passe est demandé sur avec une périodicité d'un an pour les mots de passe administrateurs et une périodicité de trois ans pour les mots de passe utilisateurs.

L'administrateur (ou le RSSI) peut en tester la robustesse.

Ces mots de passe doivent être gardés secrets :

- ✓ ils ne doivent pas être écrits
- ✓ ils ne doivent pas être enregistrés dans des systèmes externes au CISIRH (exemple : synchronisation des mots de passe via un navigateur).
- ✓ l'utilisation d'un coffre-fort de mot de passe est obligatoire[2]
- ✓ ils ne doivent en aucun cas être communiqués à des tiers

À la demande des administrateurs (ou du RSSI), ils doivent être changés.

4.6 Mise en œuvre d'outils ayant un impact sur la sécurité du SI

L'utilisation ou le développement de programmes informatiques ou la mise en œuvre de technologies mettant sciemment en cause la sécurité du système d'information et de communication du CISIRH ou des réseaux nationaux ou internationaux, sont strictement interdits.

En particulier, l'utilisateur ne peut arguer d'une intention pédagogique ou démonstrative pour être exonéré des sanctions disciplinaires ou des éventuelles poursuites que le CISIRH ou l'autorité judiciaire seraient en droit d'engager.

[2] Keepass est l'outil du SNUM dédié à cette fonction. Il est installé par défaut sur les postes bureautiques – Guide d'utilisation

4.7 Devoir de rendre compte

Un utilisateur doit signaler toute violation, tentative de violation ou soupçon de violation du système d'information et de communication dans les délais les plus brefs à son responsable hiérarchique. Il doit également en informer le Responsable de la Sécurité des Systèmes d'Information (RSSI) du CISIRH, ainsi que :

- La permanence Cybersécurité Centrale Bercy s'il s'agit d'un poste de travail standard,
- L'administrateur CISIRH s'il s'agit d'un poste de travail spécifique.

Ces dispositions s'appliquent, par exemple, en cas de comportement anormal du poste de travail après avoir cliqué sur une pièce jointe. La fiche réflexe cybersécurité Poste de travail précise comment détecter un comportement anormal, réagir au plus vite puis rédiger une chronologie des événements.

Cette fiche réflexe est disponible sur l'intranet des ministères économiques et financiers.

L'utilisateur s'engage à ne pas exploiter les éventuelles failles de sécurité, anomalies de fonctionnement, ou défauts de configuration.

L'administrateur peut prendre la responsabilité de ne pas apporter de correction, si la correction n'est pas disponible ou est considérée comme induisant d'autres problèmes, après avoir informé le RSSI.

4.8 Raccordement des équipements informatiques

L'utilisateur ne doit pas connecter à son poste de travail ou au réseau du CISIRH d'équipements informatiques ou téléphoniques sans autorisation du responsable de la sécurité du système d'information et de communication (mail du chef d'équipe à l'adresse rssi.cisirh@finances.gouv.fr).

L'utilisation de moyens de communication et de traitement de l'information personnels à finalité professionnel est interdite sauf dans les cas autorisés par le CISIRH.

Conformément à la présente charte, l'administrateur (ou le RSSI) se réserve le droit de bloquer à tout instant, tout équipement ne respectant pas cette règle.

L'utilisateur a le devoir de protéger les équipements qu'il raccorde au système d'information et de communication du CISIRH, ou de s'assurer que ceux-ci le sont (antivirus dont les signatures virales sont à jour, mises à jour de sécurité, etc.).

A la demande du RSSI, l'utilisateur doit pouvoir prouver qu'il se conforme à cette obligation.

4.9 Sécurité des données professionnelles

L'utilisateur doit veiller à la sécurité de ses données professionnelles, y compris son courrier électronique, en termes de confidentialité, intégrité et disponibilité. Cela implique de s'assurer qu'une sauvegarde est effectuée à une fréquence adaptée au besoin métier et que leur lieu de stockage est pérenne.

Sauf contrainte particulière (matériel incompatible, législation propre à un pays), le chiffrement est obligatoire dans le cas d'usage d'informatique nomade (ordinateurs portables, téléphone mobiles, clefs USB, disques externes, et tout support de stockage amovible de manière générale) et tout export sur un support amovible, en particulier clé USB est interdit.

Le CISIRH propose une solution de conteneur sécurisé Zed![3] permettant l'échange de fichier de manière sécurisée par la création d'une archive chiffrée.

L'utilisation de services grand public comme les solutions de stockage dans le « nuage » (cloud) ou de partage en ligne est interdit. Le paragraphe 9.5 fixe les règles applicables aux messageries instantanées.

Les documents et les actifs bénéficient d'un marquage suivant la politique de gestion documentaire du CISIRH. Le marquage constitue une indication donnée par le propriétaire à l'attention de chaque utilisateur destinataire pour l'informer du niveau de confidentialité de l'information transmise. En l'absence de marquage, préciser que par défaut, l'information communiquée par courriel est publique ou bien interne.

Le transfert de courriers électroniques de la messagerie professionnelle vers une autre messagerie est interdit.

Le timbre suivant est ajouté à la signature des utilisateurs :

« Ce message électronique et tous les fichiers attachés sont confidentiels et destinés exclusivement à l'usage de la personne à laquelle ils sont adressés.

Si vous n'êtes pas le destinataire de ce message, merci d'avertir ou de le retourner à son émetteur et de détruire ce message électronique et tous les fichiers attachés de votre système informatique. »

[3] Utilisation sécurisée de Zed!

En l'absence de logiciel automatique de marquage, chaque utilisateur doit manuellement indiquer le niveau de classification : C1 - Non protégé, C2 - Confidentiel ou C3 - Restreint dans le timbre de signature de ses courriers électroniques.

Pour simplifier cette démarche, il est recommandé de créer une signature type, puis de dupliquer cette signature en modifiant uniquement le niveau de classification.

Les utilisateurs doivent sélectionner la signature adaptée en fonction du contenu du message et de ses destinataires, avant l'envoi.

Voici un exemple de signature :

C2 - Confidentiel

[Prénom][Nom]
[Rôle/Fonction]
Centre Interministériel de Services Informatiques relatifs aux Ressources Humaines
« Le CISIRH, garant de l'ADN des progiciels RH et des bonnes pratiques métiers »
41, boulevard Vincent Auriol, 75013 PARIS
[Téléphone]
[Adresse mail]
www.economie.gouv.fr/cisirh

Ce message électronique et tous les fichiers attachés sont confidentiels et destinés exclusivement à l'usage de la personne à laquelle ils sont adressés.
Si vous n'êtes pas le destinataire de ce message, merci d'avertir ou de le retourner à son émetteur et de détruire ce message électronique et tous les fichiers attachés de votre système informatique.

4.10 Utilisation des ressources numériques du CISIRH en externe

Par principe, il est interdit de sortir le matériel ainsi que les données sensibles (dont les données caractère personnel traitées par le CISIRH) de l'Administration du territoire national sauf accord formel du Directeur du CISIRH.

Dans ce dernier cas les dispositions suivantes s'appliquent.

En cas de déplacement dans un pays dont la législation interdit le chiffrement de données, ou oblige les utilisateurs à remettre leurs mots de passe ou clefs de chiffrement aux autorités locales, les utilisateurs doivent se conformer aux lois, ne pas importer de matériels chiffrés, et ne pas transporter de données sensibles dont les données à caractère personnel.

L'usage de services externes (exemples : espace disques, messagerie, bureautique) et les serveurs de données (exemples : Web, FTP, RDP) ne présentant pas de garantie contractuelle de confidentialité, intégrité ou disponibilité est déconseillé. Avant de faire usage de tels services, l'utilisateur doit s'assurer de l'absence de données que leur sensibilité ne rend pas éligibles à ces services (ex : données personnelles, secret industriel, etc.). En cas de mobilité ou de télétravail, l'usage de la solution de VPN proposée par le SNUM est obligatoire.

Lors de départ en mission, notamment à l'étranger, les utilisateurs doivent prendre connaissance des conseils aux voyageurs édictés par l'ANSSI (utiliser des matériels dédiés, sans données sensibles, sans données contraires aux législations locales) :

- ✓ **Avant le voyage :**
  - Relire les règles du CISIRH en matière de SSI
  - Prendre connaissance de la législation locale
  - Utiliser du matériel dédié (ne contenant pas d'information et ne pas transporter de données confidentielles)
  - Sauvegarder ses données et laisser la sauvegarde en lieu sûr (en cas de vol ou de perte de matériel)
  - Utiliser un filtre sur l'écran
- ✓ **Pendant le voyage :**
  - Garder le matériel avec soi
  - Utiliser des mots de passe forts
  - Utiliser le chiffrement
  - Informer le CISIRH en cas de perte ou de vol
  - Ne pas utiliser les équipements offerts (clés USB notamment)
  - Ne pas se connecter à des postes qui ne sont pas de confiance
  - Ne pas charger ses équipements sur les bornes libre-service

- ✓ **Après le voyage :**
  - Récupérer les données recueillies durant le voyage via une messagerie puis les effacer de l'équipement
  - Changer les mots de passe
  - Faire analyser ses équipements

4.11 Vol ou perte d'équipements informatiques ou téléphoniques

En cas de vol ou de perte, l'utilisateur prévient le plus rapidement son supérieur hiérarchique ainsi que l'administrateur, le support du SNUM (« 88000 »), et le RSSI du CISIRH qui prendront les mesures appropriées.

Un dépôt de plainte doit être fait par l'utilisateur qui communiquera la copie du récépissé à l'administrateur et au RSSI.

Il convient de notifier le vol ou la perte même en cas de restitution ou de recouvrement du matériel.

4.12 Gestion et utilisation des supports amovible

L'usage des supports amovibles (clés USB, disques externes) est encadré par les règles exposés ci-dessous. En effet, les supports amovibles représentent une menace potentielle.

Les règles ci-dessous s'appliquent :

- ✓ Utilisation exclusive de supports amovibles fournis par le CISIRH : il est interdit d'utiliser des dispositifs personnels pour importer ou exporter des données ;
- ✓ Le transfert de données depuis un support amovible est autorisé uniquement si le dispositif a été décontaminé préalablement par la station blanche du CISIRH ;
- ✓ Il est interdit d'exporter des données via un support amovible, même ceux fournis par le CISIRH. Tout manquement à ces règles engage la responsabilité de l'agent ;
- ✓ Pour faciliter la sauvegarde des données professionnelles, le CISIRH offre des alternatives sécurisées : une ressource partagée (BALIDFS) et un cloud sécurisé (OODRIVE). De plus, l'outil LINA permet une sauvegarde centralisée des documents jusqu'à 60 Go par agent.

4.13 Connexion aux réseaux sans fil

L'utilisateur ne doit pas utiliser de réseaux sans fil ouverts (ex : point d'accès WIFI partagés entre plusieurs utilisateurs). Néanmoins, il peut utiliser un partage de connexion issu d'un ordiphone professionnel ou personnel.

4.14 Obligation de formation

Est obligatoire la participation aux sessions de sensibilisation à la Sécurité des Systèmes d'Information et au fonctionnement d'un Système de Management de la Sécurité de l'Information du CISIRH.

4.15 Départ ou mutation d'un utilisateur

Lorsqu'un utilisateur cesse son activité au CISIRH en cas de départ ou de mutation, il doit laisser ses données professionnelles à disposition du CISIRH et de son ancien bureau. Par ailleurs, l'utilisateur est responsable avant son départ de la destruction de ses données privées.

Avant son départ et même en cas de mutation un utilisateur doit restituer au bureau des affaires générales l'ensemble des équipements et les moyens d'accès qui lui avaient été attribués pour permettre d'exercer son activité professionnelle.

ARTICLE 5 : Droits et devoirs des administrateurs du Système d'Information

5.1 Devoir de réserve des administrateurs

L'administrateur est soumis dans l'exercice de sa fonction à un devoir de réserve et de confidentialité.

Pour assurer le bon fonctionnement et la sécurité du système d'information et de communication, il peut procéder aux investigations nécessaires (recherche de traces dans les journaux, audit d'un poste de travail, vérification des accès…).

Pour répondre à une réquisition judiciaire, la hiérarchie pourra demander aux administrateurs de communiquer les informations obtenues dans l'exercice de leurs fonctions et entrant dans l'objet de la réquisition.

5.2 Devoir d'information, de conseil et d'alerte

L'administrateur s'engage à informer la Direction du CISIRH des modalités et éventuelles difficultés de mise en œuvre de la politique de sécurité des systèmes d'information et/ou des différentes politiques et procédures.

L'administrateur informe d'urgence son autorité hiérarchique et le RSSI du CISIRH de toute alerte technique et de toute situation d'urgence rencontrée relatives au système d'information.

L'administrateur s'engage à une obligation générale de conseil, d'information, de recommandation, d'alerte et de mise en garde auprès de la Direction du CISIRH et des utilisateurs.

En outre, l'administrateur assure une veille générale du système d'information et informe le RSSI du CISIRH de tout événement relatif à la sécurité de l'information. Cette notion concerne le dysfonctionnement qu'il pourrait constater ou de toute information relative à la sécurité. Les incidents de sécurité font l'objet d'une procédure dédiée que l'administrateur doit appliquer.

5.3 Devoir de respect de la vie privée des utilisateurs

L'administrateur peut explorer l'ensemble des fichiers, répertoires, courriels et de manière générale, toutes les données d'un utilisateur à l'exception des éléments indiqués comme « privé » (ex : l'objet d'un courriel est « PRIVE », un répertoire est intitulé « Usage privé », etc.).

L'accès aux données personnelles (mention « privée » comme développé précédemment) ne peut se faire qu'en présence de l'utilisateur directement concerné. Seul fait exception à cette règle le cas d'une réquisition de l'autorité judiciaire. Dans ce cas, l'administrateur est autorisé à accéder aux données personnelles d'un utilisateur concerné par cette enquête, sans le consentement de celui-ci.

5.4 Gestion des traces dans le système d'information et de communication

L'administrateur assure l'enregistrement et la gestion des traces et journaux d'événements du système d'information et de communication. Il duplique et assure pendant la durée légale de conservation prévue, la sauvegarde et la conservation des traces et des journaux d'événements.

5.5 Gestion des sauvegardes des données des utilisateurs

L'administrateur peut réaliser la sauvegarde et l'archivage de certains serveurs à risques, y compris ceux hébergeant les données des utilisateurs et le courrier électronique, afin d'assurer la continuité d'activité du système d'information et de communication.

5.6 Gestion des accès d'un équipement informatique ou téléphonique

Le CISIRH peut interdire tout flux informatique (web, courriel, transfert de fichiers, téléphonie, vidéo, etc.), ainsi que tout équipement informatique ou téléphonique présentant des risques pour la sécurité (virus, rançongiciel, cheval de Troie, etc.), ou en infraction avec la réglementation en vigueur.

L'administrateur ainsi que le RSSI du CISIRH peuvent procéder à toute recherche préventive de faille sur les équipements informatiques ou téléphoniques, privés ou non, raccordés au système d'information et de communication. Il peut déconnecter, physiquement ou logiquement, une machine en cas de suspicion.

5.7 Droits de configuration des équipements

En cas d'infection virale ou de panne sur un équipement informatique ou téléphonique, l'administrateur pourra reconfigurer ce matériel dans un état « sortie d'usine » au détriment des données présentes localement.

L'utilisateur reconnait le droit à l'administrateur de réaliser cette tâche, même si elle se fait au détriment des données présentes localement sur son matériel.

5.8 Maintenance

Pour effectuer la maintenance corrective, curative ou évolutive, le CISIRH se réserve la possibilité de réaliser des interventions (le plus souvent à distance) sur les ressources matérielles et logicielles mises à la disposition des utilisateurs.

Toute situation bloquante pour le système ou générant une difficulté technique, pourra conduire à l'isolement du poste voire à la suppression des éléments en cause et éventuellement, la suspension du compte informatique.

Avant toute prise en main à distance, l'administrateur informe au préalable, et en toute transparence, l'utilisateur concerné et recueille l'accord de celui-ci.

L'administrateur s'interdit d'utiliser ces outils pour exercer un contrôle de l'activité des utilisateurs et, en tout état de cause, les utilisera dans les strictes limites de ses missions. L'administrateur s'engage ainsi à n'accéder qu'aux données nécessaires à l'accomplissement de ses missions et à en assurer la confidentialité.

ARTICLE 6 : Respect de la propriété intellectuelle

6.1 Reproduction ou décompilation de logiciels

La reproduction des logiciels commerciaux autre que pour l'établissement d'une copie de sauvegarde est interdite.

La décompilation de logiciels propriétaires est interdite.

6.2 Installation de contenus numériques soumis aux copyrights, droits d'auteur ou gestion des droits numériques (DRM)

Il est interdit d'installer sur le système d'information et de communication du CISIRH ou tout matériel connecté à ce SI un logiciel, une police de caractères ou tout autre fichier en violation des droits d'auteur, copyrights, DRM et licences associées.

Les licences des logiciels (commerciaux ou libres) doivent naturellement être respectées.

6.3 Logiciels professionnels installés sur un équipement privé

Les logiciels professionnels mis à disposition par le CISIRH sur des équipements informatiques ou téléphoniques personnels doivent être supprimés lors du départ du CISIRH.

6.4 Archivage des ressources documentaires

L'usage des ressources documentaires doit être conforme à la politique de gestion documentaire du CISIRH.

Le téléchargement massif et systématique de ressources documentaires par l'intermédiaire d'un robot ou de tout autre logiciel est interdit.

ARTICLE 7 : Respect de la confidentialité des informations

7.1 Droits d'accès aux informations

Tout utilisateur est responsable, pour ses fichiers et répertoires, des droits de lecture et de modification qu'il donne aux autres utilisateurs. Il est cependant interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas correctement protégées. En conséquence, l'utilisateur ne doit pas tenter de lire, copier, divulguer, modifier les fichiers d'un autre utilisateur sans y avoir été explicitement autorisé.

7.2 Hébergement des informations

L'utilisateur doit utiliser les serveurs de partage de fichiers ou de gestion documentaire du CISIRH et de ses partenaires, ainsi que ceux d'un hébergeur validé par le RSSI.

L'usage d'autres hébergements distants est interdit.

7.3 Interception des communications entre tiers

L'utilisateur ne doit pas tenter d'intercepter des communications entre tiers.

7.4 Respect des engagements de confidentialité avec un tiers

L'utilisateur est tenu de prendre les mesures de protection des données garantissant le respect des engagements de confidentialité pris par le CISIRH vis-à-vis des partenaires du CISIRH. Ces engagements sont détaillés dans les conventions de service et dans la politique de gestion de la relation avec les tiers du CISIRH.

Elles sont disponibles sur demande auprès de rssi.cisirh@finances.gouv.fr.

7.5 Traitement des données à caractère personnel

Tout traitement de données nominatives doit respecter le Règlement Général sur la Protection des Données (RGPD). Le délégué à la protection des données doit être informé de tout projet de traitement de données nominatives sur le système d'information et de communication du CISIRH, afin d'accompagner le responsable du traitement dans la mise en conformité avec le RGPD.

Les droits d'accès, de rectification, de suppression, de limitation et de portabilité sont exercés auprès du délégué à la protection des données à cette adresse : dpo.cisirh@finances.gouv.fr.

Pour tous renseignements sur la protection des données personnelles, il est possible de contacter le délégué à la protection des données à cette adresse : dpo.cisirh@finances.gouv.fr.

7.6 Continuité de service

En cas d'absence d'un utilisateur, toute mesure indispensable à la continuité du service peut être mise en œuvre qui ne contredise pas les règles décrites dans la présente charte et dans la Politique de sécurité des systèmes d'information (PSSI) du CISIRH, comme par exemple, le transfert de dossiers, de droits d'accès temporaires ou permanents à des personnes ayant le besoin d'en connaître, et comportant les éventuelles habilitations requises.

7.7 Confidentialité des données

L'utilisateur doit être extrêmement vigilant vis-à-vis des données considérées comme confidentielles (données à caractère personnel et informations techniques).

En particulier, il ne doit pas transporter ou déposer sans protection (telle qu'un chiffrement) des données sensibles dont les données à caractère personnel sur des supports ou services non fiabilisés. L'accès à des données sensibles est interdit depuis des postes ou des réseaux externes à l'administration.

Le partage de données depuis un poste de travail est interdit (l'utilisateur doit partager ses données via un serveur de fichiers ou un serveur de gestion documentaire autorisés par le responsable de la sécurité du système d'information et de communication du CISIRH, ou encore la messagerie ou les services de collaboration du CISIRH).

Lors de consultations d'informations sensibles, l'utilisateur doit être vigilant quant aux traces laissées : historique de navigateurs, mots de passe, mémoires caches, témoins de connexion (« cookies »), etc.

ARTICLE 8 : Relations avec les sites distants et les autres sites informatiques

8.1 Connexion à un site distant

Tout VPN (réseau privé virtuel) ou chiffrement réseau mis en œuvre dans un but illégitime ou a fortiori illégal sont interdits.

8.2 Fonctionnement intègre du système d'information

Il est interdit de se livrer depuis des ressources informatiques appartenant au CISIRH ou étant connectées aux réseaux informatiques du CISIRH à des actes mettant sciemment en péril la sécurité ou le fonctionnement du système d'information, locaux ou distants, et des réseaux de télécommunications ou nuire à l'image du CISIRH.

8.3 Partage d'information avec un site distant

L'utilisateur doit être vigilant lors de toute saisie d'informations personnelles sur Internet, notamment avec la multiplication des courriers d'hameçonnage (phishing).

Le CISIRH ne pourra être tenu responsable des dommages subis lors de telles divulgations d'informations.

L'administrateur (ou le RSSI) se réserve le droit de bloquer les accès d'un utilisateur victime d'hameçonnage à des fins de protection du système d'information et de communication et d'audit, et ce pour toute la durée qu'il estime nécessaire.

Le RSSI peut organiser des simulations d'attaque de type hameçonnage sur tout ou partie des utilisateurs dans un but uniquement pédagogique et de sensibilisation. Les résultats de cette simulation sont confidentiels.

ARTICLE 9 : Échanges électroniques

9.1 Devoir de réserve

Dans ses échanges, nul ne peut s'exprimer au nom du CISIRH ou engager le CISIRH sans y avoir été dûment autorisé, ou sans que les fonctions qu'il exerce le prévoient.

9.2 ègles de savoir-vivre

Chacun doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques (mails, chats, réseaux sociaux, etc.). De plus, l'utilisateur doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

9.3 Responsabilité de l'utilisateur relative au contenu des échanges

Compte tenu de la valeur juridique d'un courriel, chacun doit être vigilant sur son contenu et s'assurer de sa conservation (un an minimum). Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles 1174 à 1177 du code civil. L'utilisateur doit en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

9.4 Intégrité des échanges électroniques

Il est rappelé qu'aucune garantie de bonne transmission et de délai d'acheminement ne peut être apportée aux courriels qui sont émis ou réexpédiés hors du CISIRH, du fait même du fonctionnement d'Internet.

9.5 Messagerie instantanée

Les applications de messagerie instantanée sont devenues des outils de travail à part entière.

Le CISIRH utilise le service TCHAP (tchap.gouv.fr), proposé par la Direction interministérielle du numérique. L'utilisation d'autres applications et à fortiori l'utilisation des applications « grand public » (WhatsApp, Messenger, SMS) est interdite dans un contexte professionnel.

ARTICLE 10 : Télétravail

Le décret n° 2016-151 du 11 février 2016 relatif aux conditions et modalités de mise en œuvre du télétravail dans la fonction publique et la magistrature modifié stipule que le télétravail désigne toute forme d'organisation du travail dans laquelle les fonctions qui auraient pu être exercées par un agent dans les locaux où il est affecté sont réalisées hors de ces locaux en utilisant les technologies de l'information et de la communication

Une note de service du 20 septembre 2021 cadre les modalités de télétravail au CISIRH dans le respect des directives ministérielles et notamment de l'accord collectif ministériel sur le télétravail.

A l'instar des autres modes de travail, l'utilisation de matériel professionnel est obligatoire dans les conditions fixées par la présente charte.

ARTICLE 11 : Évolution de la charte

Cette charte est consultable sur l'Intranet du CISIRH, et elle est susceptible de modifications en fonction des évolutions techniques et réglementaires, des usages et de l'organisation du CISIRH. Seule la dernière version française fait foi.

ARTICLE 12 : Sanctions applicables

Tout utilisateur n'ayant pas respecté les dispositions de la présente charte est passible de poursuites, disciplinaires, civiles ou pénales.