Charte définissant les conditions d'utilisation des ressources informatiques et d'accès aux réseaux numériques mis à disposition par le CNRS, dite

Charte informatique

La présente Charte informatique a pour objet d'encadrer les droits et obligations des Utilisateurs lorsqu'ils utilisent des Ressources informatiques ou des accès à des Réseaux numériques mis à disposition par le CNRS.

Elle répond à la préoccupation du CNRS de protéger les informations qui constituent son patrimoine immatériel contre toute altération, volontaire ou accidentelle, de leur confidentialité, intégrité ou disponibilité, et participe à la protection de son image et de ses intérêts légitimes. Toute altération est en effet susceptible d'avoir des impacts importants (humains, financiers, juridiques, d'image, environnementaux, atteinte au fonctionnement de l'organisme ou au potentiel scientifique et technique).

Le CNRS met en œuvre les mesures techniques et organisationnelles pour assurer la sécurité des Ressources informatiques et des accès aux Réseaux numériques mis à disposition des Utilisateurs.

Les Utilisateurs respectent les termes de la présente Charte informatique, ainsi que la réglementation générale, et celle plus spécifique relative à la sécurité des systèmes d'information (SSI) telle que susvisée dans la décision portant approbation de la Charte informatique, de la Politique générale de sécurité de l'information (PGSI) du CNRS et en complément de la PSSI opérationnelle en vigueur dans l'Entité.

L'Utilisateur est responsable de la sécurité des Ressources informatiques mises à disposition par le CNRS pour l'usage qu'il en fait. Il s'appuie sur le Chargé de la sécurité des systèmes d'information (CSSI) de l'Entité ou le Responsable de la sécurité des systèmes d'information en délégation régionale (RSSI-DR) pour l'aider et répondre à ses questions. Il leur signale, ainsi qu'à son responsable hiérarchique, tout incident, dysfonctionnement ou événement anormal. Lorsque des données personnelles sont concernées, il signale également l'incident au délégué à la protection des données (DPD) compétent. La Coordination Nationale pour la SSI (CNSSI) sous la direction du RSSI National (RSSI-N) gère les relations avec la tutelle, les partenaires de niveau national et les agences de l'État. Elle anime la chaîne fonctionnelle SSI de l'établissement.

Table des matières

I. Définitions

Administrateur : Personnel technique (Administrateur Systèmes et Réseaux (ASR), technicien informatique…) ou fonctionnel (maître d'ouvrage d'une application, administrateur de droits d'accès...) qui dispose pour l'exercice de ses fonctions d'accès particuliers aux systèmes d'information du CNRS, lui conférant des privilèges élevés et des accès larges aux systèmes et/ou aux données, conformément à la fiche de poste ou à la mission spécifique dont il est investi.

Chiffrement des données : Transformation mathématique des données pour les rendre illisibles aux personnes n'ayant pas le droit d'en connaître, permettant ainsi d'assurer la confidentialité, l'intégrité et l'authenticité des données et de leur producteur, ainsi qu'une protection contre les conséquences d'un vol ou d'une fuite de ces données. Le déchiffrement nécessite la saisie d'un code secret connu de l'Utilisateur seul.

CNSSI : Coordination nationale pour la sécurité des systèmes d'information (cnssi@cnrs.fr) ; direction en charge de la définition et de l'appui à la mise en œuvre d'une politique de sécurité des systèmes d'information de l'établissement et de la conformité aux réglementations du domaine.

CSSI : Le chargé de la SSI pour l'Entité.

Délégué à la protection des données (DPD ou DPO) : En charge de la conformité au RGPD des traitements de données à caractère personnel mis en œuvre par l'établissement et ses Entités (pour le CNRS : dpd.demandes@dpd-cnrs.fr).

Entité(s) : Toutes les entités créées par le CNRS pour l'accomplissement de ses missions, notamment les unités dont le CNRS est tutelle, les services et directions administratives.

Équipements informatiques : Tout dispositif mis à disposition de l'Utilisateur pour le stockage ou le traitement de données numériques, tels que les ordinateurs portables, postes de travail, écrans, supports de stockage externes (disques ou bandes magnétiques ou optiques, mémoires flash, lecteurs USB, etc.), smartphones, tablettes, dispositifs d'authentification, etc.

Réseaux numériques : Ensemble des réseaux de communication électronique auxquels les Utilisateurs accèdent, qu'il s'agisse de réseaux locaux à l'Entité ou externes, incluant l'usage des ressources Internet.

RSSI-DR : Responsable SSI en délégation régionale ; le représentant régional de la SSI en délégation, membre de la chaîne fonctionnelle SSI, rattaché hiérarchiquement au délégué régional et fonctionnellement à la CNSSI.

Ressources informatiques : Ensemble des moyens informatiques de stockage, de traitement et de transfert des données numériques (Équipements informatiques, systèmes d'information, serveurs informatiques, applications, sites web, accès internet, réseaux, etc.) mis à disposition par le CNRS à l'Utilisateur dans le cadre de ses activités depuis l'Entité ou à distance.

Utilisateur(s) : Agent(s) des Entités ainsi que les personnes physiques ou morales hébergées ou accueillies dans l'Entité et les visiteurs ou prestataires, qui ont accès aux Ressources informatiques mises à disposition par le CNRS.

II. Cadre réglementaire applicable

Outre les textes encadrant la politique de sécurité des systèmes d'information[1], l'Utilisateur est également tenu dans le cadre de son utilisation des Ressources informatiques ou des accès à des Réseaux numériques mis à disposition par le CNRS, de respecter l'ensemble des réglementations suivantes (non exhaustif) :

- Les obligations déontologiques mentionnées aux articles L121-1 à L121-11 du code général de la fonction publique ;
- Les dispositions relatives à la protection du potentiel scientifique et technique de la Nation (PPST) (notamment les articles 413-7, 413-8 et R. 413-1 et suivants du code pénal, le décret n°2011-1425 du 2 novembre 2011 et l'arrêté du 3 juillet 2012 modifié relatif à la PPST de la Nation) ;
- La loi du 29 juillet 1881 modifiée sur la liberté de la presse : l'Utilisateur ne diffuse pas d'informations constituant des atteintes à la personnalité (diffamation, injure, provocation à la discrimination et la haine raciale, négationnisme) ;
- Les dispositions relatives au respect de la vie privée (article 9 du code civil) et au secret professionnel (article L121-6 du code général de la fonction publique et articles 226-13 et 226-14 du code pénal) ;
- La réglementation relative au traitement des données à caractère personnel, notamment la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (loi Informatique et Libertés) ainsi que le Règlement général de protection des données (RGPD) du 27 avril 2016 ;
- Les dispositions du code de la propriété intellectuelle ;
- Les dispositions relatives aux atteintes aux systèmes de traitement automatisé de données (article 323-1 à 323-8 du code pénal) ;
- Le Règlement (UE) 2022/2065 du 19 octobre 2022 relatif à un marché unique des services numériques modifiant la directive 2000/31/CE (« Règlement sur les services numériques » ou « DSA » (*Digital Services Act)*), qui fixe un ensemble de règles pour responsabiliser les plateformes numériques et lutter contre la diffusion de contenus illicites ou préjudiciables ou de produits illégaux ;
- La loi n°2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique.

Les manquements aux dispositions susvisées peuvent être assortis de sanctions pénales et/ou disciplinaires.

[1] Voir à ce sujet : https://securite-si.cnrs.fr/pssi/

III. Protection des Équipements informatiques

L'Utilisateur assure la protection des Équipements informatiques mis à sa disposition :

- les Équipements informatiques avec support de stockage (poste de travail, ordinateur portable, smartphone, tablette, support de stockage externe, etc.) font l'objet de mesures de Chiffrement des données et de protection contre les logiciels malveillants, conformes à la PSSI de l'Entité en vigueur, avec l'appui du CSSI et de l'équipe informatique de son Entité ;
- il n'introduit pas de supports de stockage externes de données (disques ou bandes magnétiques ou optiques, mémoires flash, lecteurs USB, etc.) sans respecter les dispositions de la PSSI de l'Entité et prend les précautions nécessaires pour s'assurer de leur innocuité, avec l'appui du CSSI et de l'équipe informatique de son Entité ;
- en cas d'absence, même momentanée, il verrouille ou ferme toutes les sessions en cours sur son poste de travail. Il arrête son poste de travail en fin de journée ou en cas d'absence ;
- il utilise les moyens de protection fournis (câble antivol, rangement dans un tiroir ou une armoire fermant à clé, etc.) pour protéger l'accès physique aux équipements mobiles et les informations qu'ils renferment contre le vol ;
- il signale immédiatement au CSSI ou au RSSI de la délégation régionale et/ou de l'autre tutelle, et à son responsable hiérarchique, toute perte, tout vol ou toute compromission suspectée ou avérée d'un Équipement informatique mis à sa disposition, ou encore tout dysfonctionnement dans les correctifs de sécurité ou mises à jour des applications. En cas de suspicion de violation de données personnelles, il signale également l'incident au DPD compétent.

En cas de vol d'un Équipement informatique dont le CNRS est propriétaire, la compétence pour déposer une plainte revient au CNRS en application de la circulaire pénale[2].

IV. Protection des moyens d'authentification et conditions d'utilisation des droits d'accès aux systèmes d'information

L'Utilisateur est responsable de l'utilisation des systèmes d'information qui est réalisée avec ses moyens d'authentification et droits d'accès.

a) Protection des moyens d'authentification

L'Utilisateur assure la protection des moyens d'authentification qui lui ont été attribués ou qu'il a générés (badges, mots de passe, clés privées liées aux certificats, dispositifs d'authentification renforcée etc.) :

- il ne les communique jamais à un tiers, y compris à son responsable hiérarchique et à l'équipe chargée des systèmes d'information de son Entité ou en délégation régionale ;

[2] Circulaire n°CIR192121DAJ du 30 août 2019 relative à la mise en œuvre de poursuites pénales par le CNRS.

- il applique les règles de complexité[3] et de renouvellement en vigueur selon le moyen d'authentification utilisé ;
- il modifie ou demande le renouvellement de ses moyens d'authentification dès lors qu'il en suspecte la divulgation ; il en informe immédiatement le CSSI de l'unité, ou le RSSI-DR ainsi que son responsable hiérarchique ;
- il garantit l'accès à ses données professionnelles, notamment dans le cadre de la politique de recouvrement[4] de données mise en œuvre au sein de l'Entité.

L'Utilisateur ne fait pas usage des moyens d'authentification d'une tierce personne. De la même façon, il n'essaie pas de masquer sa propre identité lors de ses accès au système d'information.

b) Conditions d'utilisation des droits d'accès aux systèmes d'information et réseaux

L'Utilisateur ne fait usage de ses droits d'accès que pour accéder à des informations ou des services nécessaires à l'exercice des missions qui lui ont été confiées et pour lesquels il est autorisé.

Il ne porte pas atteinte au fonctionnement des systèmes d'information et réseaux, aux mesures de protection mises en œuvre, ni à leurs fonctionnalités.

A ce titre :

- il n'est pas autorisé à accéder et il ne tente pas d'accéder à des Ressources informatiques pour lesquelles il n'a pas reçu d'habilitation explicite ;
- il informe l'Administrateur de toute évolution de ses fonctions nécessitant une modification de ses droits d'accès ;
- il ne connecte pas aux réseaux locaux de l'Entité– quelle que soit la nature de ces réseaux (filaires ou non filaires) – des matériels autres que ceux confiés ou autorisés par l'Entité ;
- il n'installe pas, ne télécharge pas ou n'utilise pas, sur le matériel de l'Entité ou sur du matériel personnel utilisé à des fins professionnelles, des logiciels dont les droits de licence n'ont pas été acquittés, ou provenant de sites illégaux ou interdits par l'Entité ;
- il n'utilise pas les licences logicielles acquises par le CNRS sur des équipements personnels, ou autres que ceux confiés par l'Entité ;
- conformément aux dispositions de l'article 323-3-1 du code pénal, l'Utilisateur n'est pas autorisé à utiliser des logiciels ou tout autre moyen destinés à tester, contourner ou pénétrer la sécurité des Ressources informatiques du CNRS, sauf si ses fonctions le nécessitent (CSSI, RSSI-DR, RSSI-N) et ce, dans le respect de l'éthique professionnelle et après information préalable de sa hiérarchie.

Les accès aux systèmes d'information d'une unité protégée (ZRR) font l'objet d'une autorisation préalable conformément à la réglementation applicable et dont les modalités sont définies dans le règlement intérieur.

[3] https://sesame.cnrs.fr/secure/CHANGE_PASSWORD

[4] Le recouvrement est le dispositif de secours permettant à une personne habilitée d'accéder à des données lorsque le mécanisme principal n'est plus utilisable (perte de mot de passe par exemple).

c) Interdiction d'utiliser des services numériques gratuits

Le CNRS proscrit l'usage de services en ligne gratuits (ou proposés à vil prix) qu'il n'aurait pas validés au préalable pour le stockage, le traitement et la diffusion d'informations professionnelles, qu'il s'agisse de travail collaboratif, visioconférence, traitement de données, d'intelligence artificielle, d'aide à la conception de documents, etc., à partir des Ressources informatiques mises à disposition par le CNRS.

En effet, l'utilisation de ces services présente des risques importants pour la confidentialité des données transmises et l'intégrité des systèmes qui s'y connectent (publicités intégrées captant et monétisant les données personnelles, analyse des données confiées et revente à des tiers, accès par des pays étrangers aux données de leurs utilisateurs, etc.).

Seule l'utilisation des outils et applications mis à disposition par le CNRS ou une co-tutelle, ou explicitement autorisés par ceux-ci, est autorisée[5].

d) Finalité d'utilisation des Ressources informatiques

Si une utilisation résiduelle privée peut être tolérée, il est rappelé que l'usage des Ressources informatiques mises à disposition par le CNRS est présumé avoir un caractère professionnel.

L'Utilisateur n'est pas autorisé à utiliser ses coordonnées professionnelles, en particulier son adresse électronique ou autre identifiant, sur des services sans lien avec son activité professionnelle. En contrevenant à cette consigne, il facilite la préparation de cyber-attaques et peut engendrer des atteintes à la réputation du CNRS.

Par ailleurs, certains sites web ou applications malveillants profitent de failles logicielles pour récupérer les données présentes sur le poste de travail. D'autres sites mettent à disposition des logiciels qui, sous une apparence anodine, ou dissimulés dans d'autres, peuvent prendre le contrôle de l'ordinateur et transmettre son contenu au pirate à l'insu de l'Utilisateur.

Par conséquent, l'Utilisateur :

- ne doit pas se connecter à des sites suspects[6] ;
- ne peut pas télécharger ou installer des logiciels qui n'ont pas été validés par l'Entité;
- n'opère les sauvegardes de données, les partages d'information, les échanges collaboratifs, que sur des dispositifs validés et mis à disposition par le CNRS ou une co-tutelle et dont la sécurité a été attestée par l'établissement (via, par exemple, une homologation de sécurité) ;
- chiffre au moyen des outils fournis par l'établissement les données confidentielles qui seraient amenées à être stockées sur des sites tiers ou transmises via des messageries non sécurisées.

[5] Se référer à : https://magelan.cnrs.fr, https://securite-si.cnrs.fr, https://intranet.cnrs.fr/Cnrs_pratique/si/Pages/default.aspx
[6] Sites affichant des informations manifestement illégales, trompeuses, tentant d'abuser de la crédulité des internautes.

V. Protection des informations contenues dans les Ressources informatiques

L'Utilisateur est informé des risques pour lui ou pour l'établissement, liés à son utilisation des Ressources informatiques mises à sa disposition dans le cadre de son activité professionnelle.

Ces risques sont principalement :

- la divulgation de données à caractère personnel au sens du RGPD et de la loi Informatique et Libertés ;
- le vol ou la corruption d'informations produites, traitées ou connues par l'Utilisateur, laissées accessibles par négligence ou erreur, ou divulguées par l'Utilisateur lui-même ;
- la perte de données scientifiques ou administratives ;
- l'abus ou le détournement des accès aux applications et services auxquels l'Utilisateur a accès, en particulier après le vol des identifiants personnels de l'Utilisateur ;
- l'utilisation illégale de certaines informations accessibles sur Internet (images, photos, etc.) en violation des droits de propriété intellectuelle. ;
- l'interruption préjudiciable du fonctionnement des Ressources informatiques par l'action malveillante, maladroite ou inopportune d'un tiers.

Par sa vigilance, son comportement rigoureux et responsable, l'Utilisateur contribue pleinement à la maîtrise de ces risques, protégeant l'établissement ainsi que lui-même.

Il respecte les mesures de conservation des données professionnelles définies au sein de l'Entité, en conformité notamment avec le code du patrimoine et en lien avec le correspondant archive.

Lorsque ses données ne font pas l'objet de sauvegardes automatiques mises en place par l'Entité dont il relève, l'Utilisateur met en œuvre le système de sauvegarde manuel préconisé par son Entité.

A noter : un système d'information sensible traite d'informations dont la divulgation à des personnes non autorisées, l'altération ou l'indisponibilité sont de nature à porter atteinte aux intérêts des personnes concernées par ces données, au bon fonctionnement du service, et plus globalement aux missions et intérêts de l'établissement et/ou de ses partenaires et/ou à la PPST.

La transmission de données sensibles relevant de l'instruction interministérielle n°901 du 28 janvier 2015 (données sensibles non classifiées de défense) ou de l'instruction interministérielle n°1300 du 9 août 2021 (données relevant du secret de la défense nationale) est interdite sauf en utilisant des solutions techniques qualifiées par l'ANSSI.

Ainsi, l'Utilisateur protège les informations qu'il est amené à manipuler dans le cadre de ses fonctions, selon leur sensibilité.

Lorsqu'il crée un contenu numérique, l'Utilisateur détermine son niveau de sensibilité et applique les règles permettant de garantir sa protection durant tout son cycle de vie (marquage, stockage, transmission, impression,

suppression, etc.). Il applique les règles de marquage et de diffusion des informations définies dans la PSSI (et à défaut dans la PSSI du CNRS[7], règles PDI-1 et PDI-2).

Lorsque les données qu'il traite sont à caractère personnel, il respecte la réglementation relative à la protection des données personnelles, notamment le RGPD et la loi Informatique et Libertés, en lien avec le directeur d'unité et le DPD compétent.

VI. Protection des correspondances numériques

L'Utilisateur assure la protection de ses correspondances numériques (courriels, visioconférence, réseaux sociaux, forums de discussion, messagerie instantanée, partage de documents, diffusion d'enregistrements, voix, images, vidéos, etc.).

Le CSSI ou le RSSI-DR apporte son soutien à l'Utilisateur pour la mise en œuvre de l'ensemble des mesures suivantes.

a) Adresse de courrier électronique et boîte aux lettres associée

Le CNRS met à la disposition de l'Utilisateur, s'il est agent du CNRS, une boîte aux lettres professionnelle nominative dans le domaine de messagerie « cnrs.fr », lui permettant d'émettre et de recevoir des messages électroniques. L'utilisation de cette adresse de courrier électronique nominative se fait sous la responsabilité de l'Utilisateur.

L'Utilisateur dont l'employeur n'est pas le CNRS utilise l'adresse de courrier électronique fournie par son employeur conformément aux règles qu'il a édictées.

L'Utilisateur n'est pas autorisé à utiliser une messagerie personnelle pour transmettre des messages à caractère professionnel, ou accéder aux systèmes d'information du CNRS (par exemple en tant qu'identifiant Janus).

Par principe, tout message envoyé ou reçu depuis la messagerie professionnelle mise à disposition des agents par l'administration qui les emploie est présumé revêtir un caractère professionnel.

Ainsi, les messages à caractère professionnel des agents du CNRS sont accessibles par le CNRS sans qu'il soit nécessaire d'obtenir l'accord préalable de l'agent, ni que ce dernier soit présent.

Sous réserve de respecter la procédure idoine et les messages identifiés comme « *privés* », il peut s'avérer nécessaire pour le CNRS d'accéder à la messagerie professionnelle d'un de ses agents (en cas de départ ou d'absence prolongée par exemple)[8].

[7] https://securite-si.cnrs.fr/pssi/

[8] Note DAJ « Cadre juridique applicable et procédure d'accès à la messagerie professionnelle d'un agent CNRS » du 25 octobre 2023.

b) Contenu des correspondances numériques

Lors de ses échanges numériques écrits ou oraux (courriels, visioconférence, réseaux sociaux, forums de discussion, messagerie instantanée, partage de documents, diffusion d'enregistrements, voix, images, vidéos, etc.), l'Utilisateur doit respecter la réglementation applicable, notamment le droit pénal (interdisant notamment le chantage ou les menaces, les messages malveillants et le harcèlement), les lois mémorielles[9] et la loi du 29 juillet 1881 sur la liberté de la presse, ainsi que les obligations déontologiques encadrées par le code général de la fonction publique[10].

Ainsi, tout Utilisateur est tenu de veiller à ne publier aucun contenu :

- faisant l'apologie d'idéologies fascistes, xénophobes, racistes ou sectaires ;
- injurieux ou diffamatoire au sens de l'article 29 de la loi du 29 juillet 1881 ;
- portant atteinte à des droits de propriété intellectuelle appartenant à des tiers ;
- à caractère insultant, humiliant ou portant atteinte à la vie privée, à l'image d'un tiers ou à la présomption d'innocence au sens des articles 9 et 9-1 du code civil ;
- à caractère pédopornographique ;
- susceptible de constituer une publicité directe ou indirecte illicite ;
- provoquant à la commission d'infractions ou faisant l'apologie d'infractions au sens de l'article 24 de la loi du 29 juillet 1881 ;
- contestant les crimes contre l'humanité et autres crimes visés à l'article 24 bis de la même loi ;
- susceptible de porter atteinte à l'ordre public, au respect de la personne humaine ou de sa dignité, à l'égalité entre les femmes et les hommes, à la protection des mineurs ;
- encourageant, contenant ou provoquant à la discrimination, l'injure, la haine ou la violence à l'égard d'une personne ou d'un groupe de personnes, notamment en raison de leur origine, ou de leur appartenance ou non à une ethnie, une nation, une race ou une religion, de leur handicap, de leurs préférences sexuelles ou de toute autre différence ;
- faisant l'apologie ou la négation ou la remise en question des crimes de guerre et/ou contre l'humanité ;
- encourageant la commission de crimes et délits ou le commerce et la consommation de substances illicites, la prostitution, le terrorisme, les agressions sexuelles, le vol, le suicide, la violence, les

[9] Il s'agit des lois suivantes :
- Loi du 13 juillet 1990 tendant à réprimer tout acte raciste, antisémite ou xénophobe qui crée le délit de négation du génocide des juifs ;
- Loi du 29 janvier 2001 relative à la reconnaissance du génocide arménien de 1915 ;
- Loi du 21 mai 2001 tendant à la reconnaissance de la traite et de l'esclavage en tant que crime contre l'humanité ;
- Loi du 23 février 2005 portant reconnaissance de la Nation et contribution nationale en faveur des Français rapatriés.

[10] Articles L121-1 et suivants.

dégradations et détériorations volontaires dangereuses pour les personnes, les atteintes à l'autorité de la Justice.

L'Utilisateur respecte notamment la circulaire relative aux conditions d'utilisation des réseaux sociaux au CNRS[11] et la charte de l'expression publique des scientifiques du CNRS[12].

En cas de manquement, l'Utilisateur s'expose à des poursuites pénales et/ou disciplinaires.

L'hébergeur du service, lorsqu'il reçoit une notification de contenus manifestement illicites, doit procéder au retrait de ces contenus, conformément à l'article 6 du Règlement sur les services numériques.

Par ailleurs, les informations échangées par voie électronique avec des tiers portent, sur le plan juridique, une valeur probante et peuvent former un contrat sous certaines conditions.

L'Utilisateur doit, en conséquence, être prudent sur la nature des informations qu'il échange par voie électronique, au même titre que pour les courriers traditionnels.

c) Publication d'informations sur les sites institutionnels

Toute publication d'information sur les sites internet ou réseaux institutionnels ou l'intranet de l'Entité est réalisée sous la responsabilité du responsable de publication, conformément au règlement intérieur de l'Entité et à la circulaire relative aux conditions d'utilisation des réseaux sociaux au CNRS susvisée. En cas de publication de contenus illicites, l'Utilisateur expose le CNRS et engage la responsabilité de ce dernier.

Aucune publication d'information à caractère privé non professionnelle, ou création de pages privées non professionnelles sur les sites institutionnels, l'intranet de l'Entité, ou via les Ressources informatiques de l'Entité n'est autorisée, sauf disposition particulière décidée au sein de l'Entité et autorisation des tutelles.

d) Visioconférence et messagerie instantanée

L'usage des services de visioconférence est encadré par des consignes[13] de l'établissement que l'Utilisateur s'engage à respecter. Les outils préconisés sont les seuls pouvant être utilisés pour des échanges professionnels. En particulier, l'Utilisateur, en lien avec le CSSI, privilégie les outils de visioconférence indiqués en fonction de la sensibilité de ses échanges.

Il est rappelé que l'enregistrement des audio/visioconférences est possible uniquement après accord explicite et tracé (écrit ou oral enregistré) de tous les participants à la conférence. Ces enregistrements doivent être conservés uniquement pour leur durée d'utilité administrative, de manière à garantir leur confidentialité, et détruits à l'issue du délai autorisé et dans les conditions fixées par le code du patrimoine.

[11] https://docutiles.cnrs.fr/docutiles/documents/21186
[12] https://www.cnrs.fr/sites/default/files/news/2025-07/Guide%20de%20l%27expression%20publique%20des%20scientifiques%20du%20CNRS_WEB.pdf
[13] https://intranet.cnrs.fr/Cnrs_pratique/si/pratique/Pages/Outils-communication.aspx

e) Vigilance sur les informations reçues

L'Utilisateur fait preuve de vigilance et d'esprit critique vis-à-vis des informations reçues par voie numérique (désinformation, virus informatique, tentative d'escroquerie, chaînes, …). En particulier, la plus grande vigilance est attendue concernant les messages semblant émaner d'autorités administratives, financières, judiciaires, ou de personnalités connues. Il en est de même pour les informations reçues sous forme de fichiers audio ou vidéo qui peuvent avoir été générés par des intelligences artificielles (ex : *deep fakes*[14]). Tout doute doit amener l'Utilisateur à en informer son responsable hiérarchique et à contacter l'équipe informatique de l'Entité pour avis.

VII. Usage des technologies d'intelligence artificielle

Sauf dérogation[15], dans le cadre des activités professionnelles, l'usage par les agents CNRS et les directeurs d'Entité d'outils d'IA générative généralistes « grand public », accessibles gratuitement ou de manière payante, autres que l'agent conversationnel en IA générative interne au CNRS[16], est proscrit.

VIII. Télétravail

En situation de télétravail, l'Utilisateur respecte, outre la présente Charte informatique, les instructions du directeur de l'Entité, et les consignes listées dans le guide opérationnel du télétravailleur[17]. Il s'assure de la protection des informations qu'il traite dans cette situation où les risques liés à la confidentialité des données sont accrus.

Les accès aux Ressources informatiques de l'Entité sont réalisés exclusivement au moyen des accès VPN (réseau privé virtuel) fournis par l'Entité.

IX. En mission

L'Utilisateur en mission s'expose à des risques accrus de perte et de vol des équipements confiés, mais aussi de perte de confidentialité des données qu'il emmène avec lui (y compris en cas de consultation par les services de police/justice étrangers par exemple). Il minimise donc cette quantité de données au strict nécessaire et adopte une posture de vigilance accrue sur ses équipements pendant la durée de la mission.

En amont de la mission, il prend attache avec l'équipe informatique de l'Entité pour connaître et appliquer les consignes spécifiques. En tout état de cause, il est recommandé d'appliquer strictement les consignes de l'ANSSI[18].

[14] Technique basée sur l'intelligence artificielle, qui permet de créer des trucages ultraréalistes (ou *hypertrucages*) d'images, de vidéos et de sons, à des fins de fraude, de désinformation et de cyberharcèlement.
[15] En cours de définition
[16] https://emmy.cnrs.fr/files/Conditions_utilisation_emmy.pdf
[17] https://intranet.cnrs.fr/Cnrs_pratique/recruter/temps/Documents/Teletravail_guide_operationnel_2023_2.pdf
[18] passeport_voyageurs_anssi.pdf

X. Vie privée et ressources informatiques personnelles

a) Vie privée résiduelle

Les Ressources informatiques (poste de travail, serveurs, applications, services numériques, messagerie, accès internet, téléphone, etc.) fournies à l'Utilisateur, par le CNRS ou une co-tutelle sont réservées à l'exercice de son activité professionnelle.

Un usage personnel de ces Ressources informatiques est toutefois toléré à condition :

- qu'il reste de courte durée pendant les heures de travail ;
- qu'il n'affecte pas l'usage professionnel ;
- qu'il ne mette pas en danger le bon fonctionnement et les mesures de sécurité en vigueur sur les Ressources informatiques ;
- qu'il ne soit pas réalisé dans un but lucratif ;
- qu'il n'enfreigne pas la réglementation et les dispositions internes.

Tout message clairement identifié comme étant personnel (par exemple, avec l'indication « Privé » en objet), ou classé dans un répertoire « Privé », se voit conférer la nature d'une correspondance privée protégée par le droit au respect de la vie privée.

Les messages privés ne peuvent être consultés par l'employeur qu'en présence de l'agent et avec son autorisation expresse.

L'Utilisateur procède au stockage de ses données à caractère privé (fichiers, documents, etc.) dans un espace de données prévu explicitement à cet effet ou en mentionnant le caractère privé sur la ressource utilisée. Les données à caractère professionnel ne doivent pas être rangées dans cet espace privé. Ce dernier ne doit occuper qu'une part mineure des Ressources informatiques allouées. La protection, la migration et la sauvegarde régulière des données à caractère privé incombent à l'Utilisateur.

b) Ressources informatiques personnelles

L'usage de ressources informatiques personnelles (ordinateurs, smartphones, lecteurs USB, disques durs externes, tablettes, accès à des services externes, etc. achetés sur des crédits personnels) dans le cadre professionnel, bien que découragé, reste une possibilité que le directeur de l'Entité peut autoriser explicitement, individuellement, ponctuellement et à titre dérogatoire dans son Entité, à condition d'en encadrer l'usage dans le respect de la politique de sécurité de l'Entité.

Il est rappelé que, dans les unités impactées par le dispositif de Zone à Régime Restrictif (ZRR), l'usage des équipements personnels est interdit.

Lorsque des ressources informatiques personnelles sont utilisées pour accéder aux systèmes d'information du CNRS, elles ne doivent pas remettre en cause ou affaiblir les politiques de sécurité en vigueur dans les Entités par une protection insuffisante ou une utilisation inappropriée.

L'Utilisateur protège les équipements personnels qu'il utilise pour accéder, à distance ou à partir du réseau local d'une Entité, aux systèmes d'information du CNRS ou stocker des données professionnelles en respectant les mêmes mesures de sécurité que pour les Équipements informatiques professionnels. En particulier, il s'assure :

- d'une protection antivirale efficace,
- de la mise à jour de tous les correctifs logiciels sur ces équipements,
- de l'absence de stockage d'identifiants professionnels sur l'équipement personnel.

Il est accompagné au besoin par l'équipe informatique de l'Entité pour cette mise en œuvre.

XI. Gestion des départs

Les données professionnelles restent à la disposition de l'employeur. Les mesures de conservation des données professionnelles sont définies au sein de l'Entité, conformément au code du patrimoine et en lien avec les correspondants archives.

Avant son départ, l'Utilisateur s'assure, en lien avec son supérieur hiérarchique, que l'Entité a un accès effectif aux données professionnelles dont il dispose.

L'Utilisateur est responsable de son espace de données à caractère privé et il lui appartient de le détruire au moment de son départ. En cas de circonstances exceptionnelles (départ impromptu ou décès), le CNRS ne conserve les espaces de données à caractère privé présents sur les Ressources informatiques fournies par le CNRS que pendant une période de 3 mois maximum (délai permettant à l'Utilisateur ou ses ayants droit de récupérer les informations qui s'y trouvent).

En cas de décès, il revient au supérieur hiérarchique de l'agent concerné, en qualité de responsable de traitement, de vérifier si celui-ci a, de son vivant, défini des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès. En l'absence de telles directives, les héritiers qui justifient de leur identité (copie de pièce d'identité et justificatif du lien de parenté) ont la possibilité d'exercer certains droits prévus par l'article 85 de la loi Informatique et Libertés. La décision de communiquer les données s'apprécie le cas échéant en opportunité.

XII. Protection des données à caractère personnel

Dans le cadre de ses activités, l'Utilisateur peut être amené à traiter des données à caractère personnel.

Il s'engage à se conformer à la règlementation relative à la protection des données personnelles, ainsi qu'à la procédure mise en œuvre par les tutelles en la matière et à la PSSI opérationnelle en vigueur dans l'Entité. Il procède notamment à l'inscription du traitement dans le registre dédié de sa structure de rattachement. A cette fin, il prend contact avec le DPD compétent.

XIII. Respect de la propriété intellectuelle

L'Utilisateur ne reproduit pas, ne télécharge pas, ne copie pas, ne diffuse pas, ne modifie pas ni n'utilise de logiciels, bases de données, pages web, images, vidéos, photographies ou autres créations protégées par le droit de la propriété intellectuelle, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

XIV. Traçabilité des activités de l'Utilisateur

La réglementation impose au CNRS de garder un historique des accès à ses systèmes d'information réalisés par les Utilisateurs[19]. Le CNRS a donc mis en place une journalisation de ces accès, conformément aux règles énoncées dans la PGSI et conforme à la réglementation relative à la protection des données personnelles.

L'Administrateur a accès aux traces générées par l'Utilisateur lors de ses accès sur l'ensemble des Ressources informatiques mises à sa disposition par le CNRS ainsi que sur les réseaux locaux et distants. Ces traces (appelées également « fichiers de journalisation » ou « journaux ») sont conservées 12 mois au maximum.

Les Administrateurs peuvent, en cas de dysfonctionnement technique, d'intrusion ou de tentative d'attaque sur les systèmes informatiques, utiliser ces traces pour tenter de retrouver l'origine de l'incident et en atténuer les conséquences.

Le CNRS met en œuvre des logiciels de protection des Équipements informatiques contre les logiciels et actions malveillants, qui assurent une surveillance en temps réel de l'activité de ces Équipements informatiques. En cas de détection de comportement suspect des Équipements informatiques, le logiciel de protection peut être amené à suspendre la connexion ou l'activité des Équipements informatiques. Ces logiciels collectent également des informations sur le comportement des Équipements informatiques et leur utilisation en conformité avec la réglementation en vigueur[20].

XV. Dispositions spécifiques aux personnels à privilèges élevés sur le système d'information

a) Prérogatives de l'Administrateur

En application des consignes qui lui ont été transmises, l'Administrateur peut prendre toute disposition nécessaire afin d'assurer le bon fonctionnement et la sécurité des Ressources informatiques dans son périmètre de responsabilité établi dans sa fiche de poste ou sa lettre de mission. En particulier, il peut, dans le respect de la déontologie et de la réglementation :

▪ isoler, suspendre ou reconfigurer des comptes utilisateurs, équipements ou applications informatiques pouvant compromettre la sécurité du système d'information ; lorsque la situation l'exige, il demande l'autorisation de son supérieur hiérarchique et informe dans tous les cas le CSSI ou le RSSI-DR ;

▪ procéder à des vérifications techniques sur les fichiers et bases de données, la messagerie, les connexions à Internet, les fichiers de journalisation, etc. afin de déceler toute anomalie ou incident de sécurité qui pourrait porter atteinte au bon fonctionnement et à la sécurité des systèmes d'information dans les activités d'administration et d'assistance ;

[19] Décret n° 2021-1362 du 20 octobre 2021 relatif à la conservation des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, pris en application du II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, qui impose aux fournisseurs d'hébergement et aux fournisseurs d'accès internet de conserver les données d'identification pour les connexions à leurs services et l'article L.34-1 du Code des postes et des communications électroniques (CPCE) qui impose une obligation de conservation de ces données

[20] Traitement de données personnelles inscrit au registre du CNRS sous numéro 2-25229.

▪ traiter (détection, analyse, éradication, filtrage, etc.) ou s'assurer du traitement de tout flux informatique présentant des risques de sécurité (par exemple : virus, intrusion, utilisation d'un logiciel interdit ou potentiellement dangereux, etc.). Sur la base de données statistiques, l'Administrateur peut alerter le RSSI-DR de toute utilisation de Ressources informatiques qui apparaîtrait comme non conforme à la présente Charte informatique ou à la PSSI.

L'Administrateur qui détourne le motif de son habilitation à d'autres fins commet une atteinte aux systèmes de traitement automatisé de données, et s'expose à des poursuites disciplinaires et/ou pénales.

b) Obligations de l'Administrateur

L'Administrateur observe strictement les règles de sécurité et les limites fixées à ses interventions :

▪ il observe les règles de sécurité en vigueur visant notamment à protéger l'utilisation des comptes et des droits privilégiés qui lui ont été attribués ; il veille notamment à la protection des postes de travail à partir desquels il exerce ses fonctions et à la gestion des identifiants et des moyens d'authentification des comptes privilégiés. Il est rappelé que les accès confiés à un Administrateur sont confidentiels et incessibles ;

▪ il limite ses actions aux Ressources informatiques dont il a la charge et dans le respect de la finalité de sa mission ; par ailleurs, il ne modifie les configurations et les droits d'accès que dans les cas préalablement définis ;

▪ il ne reçoit pas de consignes d'une personne non habilitée et fait remonter auprès de son supérieur hiérarchique direct mentionné dans sa fiche de poste et au RSSI-DR toute requête lui paraissant inappropriée ou contraire à la réglementation ; en cas de requête qui lui semblerait non appropriée présentée par sa hiérarchie, il expose à celle-ci les raisons de son opposition ; si cette requête est maintenue, il prévient le RSSI-DR ou le RSSI-N.

En outre :

▪ les contrôles réalisés doivent être faits non seulement en toute transparence mais aussi de manière proportionnée et adaptée à la finalité dont est informé préalablement l'Utilisateur ;

▪ il s'efforce d'éviter tout conflit pouvant exister entre ses intérêts personnels et ceux du service ; il informe sa hiérarchie de tout conflit d'intérêts dans lequel il pourrait être impliqué pouvant altérer l'efficacité de sa mission ;

▪ il documente ses actions et interventions afin de garantir le bon fonctionnement et la continuité du service ;

▪ il coopère avec le RSSI-DR ; il est tenu de suivre les procédures préalablement définies.

L'Administrateur est soumis à une obligation de confidentialité dans le cadre de sa mission. C'est pourquoi :

▪ les permissions d'administration attribuées à un Administrateur ne sont utilisées que pour mener à bien les tâches qui lui sont confiées ;

▪ les outils mis à sa disposition ne sont utilisés que dans un but professionnel d'administration, supervision, exploitation, maintenance ou assistance ;

▪ l'Administrateur prend connaissance des informations à caractère professionnel contenues dans les systèmes d'information ou donne accès à celles-ci seulement dans le cadre de ses fonctions et/ou sur demande explicite de son responsable ou, en son absence, du RSSI-DR (un résumé succinct de l'action sera consigné) ;

▪ il ne peut prendre connaissance ou tenter de prendre connaissance du contenu des répertoires, fichiers ou messages explicitement désignés comme privés qu'en présence de l'agent et avec son autorisation expresse, en cas d'urgence justifiée ou de nécessité vis-à-vis de la réglementation et de la sécurité des systèmes d'information ;

▪ en cas d'assistance, il ne prend en main, à distance, le poste de travail d'un Utilisateur qu'avec l'autorisation explicite de ce dernier et ne se connecte qu'aux seules ressources nécessaires à l'accomplissement de sa mission ;

▪ les devoirs de réserve et de respect du secret professionnel lui imposent l'interdiction de faire état publiquement ou à un tiers non habilité du détail de ses missions ou de ses fonctions.