Septembre 2025

LIVRET DE SECURITE INFORMATIQUE

Document à usage strictement interne, ne pas diffuser.

INSTITUT DE RECHERCHE INTERDISCIPLINAIRE SUR LES ENJEUX SOCIAUX

PDF

Léo Tertrais-Flamand (RSSI)

Table des matières

Ordinateurs professionnels et personnels : quelle différence en matière de sécurité ? 3
Chiffrement des ordinateurs et téléphones 4
Chiffrement des stockages externes 6
Utiliser des services conseillés 7
Services interdits et alternatives autorisées 8
Stockage et partage de fichiers 9
Gestion des mots de passe 11
Messagerie 13
Internet et confidentialité : VPN 14
Partir en mission à l'étranger 15
Procédure en cas d'incident 16
IA génératives 17
Transcrire des fichiers audios avec Whisper via Humanum 18

Ordinateurs professionnels et personnels : quelle différence en matière de sécurité ?

En principe, les chercheurs et personnels devraient disposer d'ordinateurs professionnels, fournis et configurés par les services informatiques des tutelles. Ces machines respectent pour partie les normes de sécurité attendues, mais ne sont pas toujours configurés correctement ou mis à jour régulièrement.

La majorité des agents du laboratoire utilisent aussi – voire uniquement – leurs appareils personnels pour travailler.

⚠️ À partir du moment où un ordinateur ou un téléphone personnel contient des données ou des comptes liés à vos recherches, il doit être considéré comme un appareil professionnel. Cela signifie qu'il doit se conformer aux règles définies par la Politique de sécurité des systèmes d'information (PSSI) du laboratoire et donc de s'aligner sur les bonnes pratiques que ce livret balise.

👉 Activez les mises à jour automatiques de l'ordinateur, du téléphone et des logiciels principaux (navigateur, antivirus, suites bureautiques). Évitez d'utiliser des systèmes obsolètes : Windows 10 ou vieux macOS qui ne reçoivent plus de correctifs de sécurité.

Chiffrement des ordinateurs et téléphones

Pourquoi ?

Le chiffrement est le seul moyen de protéger vos données en cas de perte, vol ou saisie d'un appareil. Sans chiffrement, n'importe qui peut accéder directement aux fichiers du disque dur. Avec chiffrement, les données sont illisibles sans la clé de déverrouillage.

C'est une mesure invisible au quotidien, mais essentielle pour protéger vos travaux de recherche et vos informations personnelles.

Comment faire ?

⚠️ **Avant tout, sauvegardez vos données.**

Le chiffrement modifie la structure du disque. En cas de coupure ou de bug pendant l'opération (très rare, mais possible), les données peuvent devenir inaccessibles.

Faites une copie temporaire complète de vos fichiers importants (sur un disque externe ou sur un drive).

Windows 11

- Vérifier : ouvrir Explorateur de fichiers → "Ce PC". Si un cadenas apparaît sur l'icône du disque, il est déjà chiffré.
- Sinon : clic droit sur le disque → Gérer BitLocker → Activer BitLocker.

- Sauvegarder la clé de récupération dans un fichier. Transmettre la clé à votre direction d'unité via un canal sécurisé et la conserver dans un endroit sûr.
- Choisir l'option : Chiffrer l'intégralité du disque.

⚠️ **Limitations :**

Windows 10 est en passe de devenir obsolète, il faut dès que possible faire le changement vers Windows 11.

BitLocker n'est pas disponible sur toutes les éditions de Windows 11. Sur les versions **"**Familiale", le chiffrement est limité et nécessite un compte Microsoft connecté. Pour un chiffrement complet, il est fortement recommandé de passer à une version Windows 11 Pro.

macOS (FileVault)

1. Menu → Réglages Système → Sécurité et confidentialité → onglet FileVault.
2. Cliquer sur le cadenas (mot de passe administrateur).
3. Cliquer sur Activer FileVault.
4. Choisir Créer une clé de restauration (ne pas utiliser iCloud).

- Transmettre la clé à la direction de l'unité via un canal sécurisé et la conserver dans un gestionnaire de mot de passe.

Android (smartphone)

- Le chiffrement est activé par défaut sur les versions récentes.
- La structure des paramètres varie en fonction des constructeurs de téléphone, vérifiez ce qu'il en est pour votre modèle en cherchant sur internet.

iOS (iPhone/iPad)

- Le chiffrement est activé automatiquement dès qu'un code de verrouillage est défini.
- Vérifier : Réglages → Face ID/Touch ID et code → définir un code si nécessaire.

Chiffrement des stockages externes

Pourquoi ?

Les supports externes (clés USB, disques durs portables, SSD) sont particulièrement vulnérables : ils s'égarent facilement et sont souvent utilisés en mission. Sans chiffrement, toute personne qui les trouve peut lire directement vos données.

Comment faire ?

⚠️ Toujours sauvegarder vos données avant activation. Le chiffrement réécrit la structure du support et un incident rare peut rendre les données inaccessibles.

Windows 11 Pro et macOS (solution native)

- Windows 11 Pro : utilisez BitLocker To Go (clic droit → Activer BitLocker).
- macOS : clic droit sur le disque → Chiffrer "Nom du disque" → choisir un mot de passe robuste.

Si vous n'avez pas BitLocker ou que vous souhaitez une compatibilité entre différents OS

Utilisez VeraCrypt, logiciel libre et gratuit, disponible pour Windows, macOS et Linux.

Installation et création d'un volume chiffré :

Télécharger et installer VeraCrypt depuis https://veracrypt.fr. Brancher le disque externe ou la clé USB. Ouvrir VeraCrypt et cliquer sur *Create Volume*. Choisir « Encrypt a non-system partition/drive » (chiffrement d'un disque externe). Sélectionner le disque à chiffrer. Définir l'algorithme par défaut (AES) et un mot de passe robuste. Lancer le formatage et attendre la fin du chiffrement.

Utilisation :

Pour ouvrir le disque, lancer VeraCrypt, choisir une lettre de lecteur libre (ex. : « Z: »), sélectionner le volume chiffré puis cliquer sur *Mount*. Entrer le mot de passe → le disque apparaît dans l'explorateur comme un disque classique.

Utiliser des services conseillés

Pourquoi ?

Les grands acteurs du numérique (Google, Apple, Facebook/Meta, Amazon, Microsoft – dits *GAFAM*) proposent des outils pratiques et gratuits, mais leur modèle économique repose largement sur la collecte et l'exploitation des données. Utiliser ces services pour vos recherches comporte donc un risque : vos données (ou métadonnées) peuvent être stockées sur des serveurs hors d'Europe, exploitées à des fins commerciales et soumises à des législations étrangères (comme le *Cloud Act* aux États-Unis).

Le Règlement général sur la protection des données (RGPD) et les Politiques de sécurité des systèmes d'information (PSSI), en vigueur à différents niveaux (État, tutelles, laboratoire), proscrivent l'usage de services numériques stockant les données hors du territoire national. Il est donc nécessaire de privilégier les alternatives institutionnelles et/ou libres, qui assurent une meilleure protection des données.

Comment ?

Les services spécifiques mentionnés dans les différentes sections de ce livret s'inscrivent dans une suite plus large d'outils numériques (visioconférence, espaces de travail collaboratifs, messagerie, agenda, transfert de fichiers lourds, sondages, mise en ligne de contenus…) proposés dans divers annuaires de services. Vous y trouverez des solutions couvrant la plupart de vos besoins :

- Offre de services numériques du CNRS
- La Suite numérique de l'Etat
- Espace numérique de travail (ENT) de votre établissement de rattachement
- Huma-Num
- Framalibre

Services interdits et alternatives autorisées

Usage	Exemples de services interdits	Alternatives autorisées
Stockage et partage de fichier via un Cloud	Dropbox, iCloud, Google Drive…	CNRS SDrive ; Resana ; Sharedoc de Huma-num
Envoi de gros fichiers	WeTransfert	Renater Filesender (jusqu'à 100Go) ; France Transfert (jusqu'à 20Go)
Visioconférence	Skype, Teams, Google Meet…	Webinaire de l'Etat ; Zoom CNRS (pour les contenus non-sensibles)
Sondage	Doodle	Renater Evento ; FramaForms
Messagerie instantanée	WhatsApp, Messenger…	Tchap ; Signal
Gestionnaire de mots de passe	Gestionnaires de mots de passe navigateurs (Firefox, Chrome…) ou externes (NordPass, ProtonPass…)	Keepass, Macpass
Edition de texte participative	Google doc	Resana ; FramaPads (pour le contenu non-sensible)
Edition de tableur participative	Google Calc	Grist ; FramaCalc (pour le contenu non-sensible)

Stockage et partage de fichiers

Pourquoi ?

Les espaces de stockage institutionnels permettent de sauvegarder vos documents de travail et de les partager facilement. Ils garantissent également le respect des règles de sécurité et de confidentialité imposées par les tutelles, contrairement aux services privés (Google Drive, One Drive, Dropbox…).

👉 Pour vos projets collectifs, il est préférable d'utiliser des dossiers partagés que d'envoyer des documents individuellement par mail ou via des clés USB non chiffrées.

Comment faire ?

Sdrive (CNRS)

Chaque agent dispose par défaut de 100 Go. Vous pouvez y déposer vos fichiers, créer des espaces de travail partagés et accéder à vos données depuis n'importe où. L'accès se fait via votre compte CNRS (Janus) et l'interface web https://sdrive.cnrs.fr.

En installant le logiciel Nextcloud sur votre ordinateur, Sdrive se présente comme un simple dossier local : tout fichier que vous y placez est automatiquement synchronisé avec le serveur, sauvegardé en ligne et accessible depuis vos autres appareils.

- Téléchargez et installer le client Nextcloud https://nextcloud.com/fr/installer/) correspondant à votre système (Windows, macOS, Linux, Android ou iOS).
- À la première ouverture, entrez l'adresse de serveur : https://sdrive.cnrs.fr.
- Authentifiez-vous avec vos identifiants CNRS (Janus).
- Choisissez les dossiers locaux que vous souhaitez synchroniser.

Resana (La suite numérique)

Plateforme collaborative interministérielle qui permet de partager des documents et de travailler en équipe. L'accès se fait avec vos identifiants professionnels sur https://resana.numerique.gouv.fr

France Transfert (La suite numérique)

Alternative à *WeTransfer* pour l'envoi de fichiers volumineux, proposée par l'État : https://francetransfert.numerique.gouv.fr/upload.

ShareDocs (Huma-Num)

Solution de stockage sécurisée dédiée aux sciences humaines et sociales, adaptée aux projets collectifs : https://www.huma-num.fr/.

Utiliser le service Sharedocs nécessite de poser une demande d'espace de stockage. L'acceptation de la demande peut prendre quelques jours.

De la même manière que pour *Sdrive*, vous pouvez configurer votre espace *Sharedocs* pour qu'il se présente comme un dossier local :

- Connectez vous sur votre navigateur à votre compte Sharedocs sur Huma-Num
- Ajouter un compte sur *Nextcloud* (si non installé voir ci-dessus) en ajoutant l'adresse de serveur : https://sharedocs.huma-num.fr/ puis suivre la procédure.

Gestion des mots de passe

Pourquoi ?

Réutiliser un même mot de passe ou les stocker dans un fichier texte expose à des risques importants. Un gestionnaire de mots de passe vous permet de créer et de conserver des mots de passe complexes et uniques pour chaque service, sans avoir à les mémoriser.

Choisissez un outil adapté à vos usages, mais évitez absolument la réutilisation de mots de passe.

👉 Ne prêtez jamais vos identifiants institutionnels à un collègue. Si vous devez exceptionnellement transmettre un accès, faites-le uniquement de façon sécurisée : via un lien temporaire et sécurisé généré par votre gestionnaire de mots de passe, ou par téléphone, jamais par mail ou messagerie instantanée. Changez ensuite immédiatement le mot de passe.

⚠️ Activez la double authentification (2FA) si elle est proposée. La 2FA ajoute une seconde barrière de sécurité en plus de votre mot de passe : soit un code temporaire envoyé par SMS ou mail ; soit une application d'authentification (Authy, FreeOTP…) générant un code à usage unique. Même si votre mot de passe est compromis, un attaquant ne pourra pas se connecter sans ce second facteur. Activez toujours cette option dès qu'elle est disponible.

Comment faire ?

KeePass (Windows) ou MacPass (Mac)

KeePass/MacPass est recommandé par le CNRS : il est gratuit, open source et fonctionne sans connexion à un service externe.

Téléchargez KeePass depuis https://keepass.info/download.html. Créez une nouvelle base de mots de passe (.kdbx) et définissez un mot de passe maître robuste (c'est le seul à retenir). Ajoutez vos entrées (une fiche compile : identifiant, mot de passe et éventuellement le lien du site internet concerné)

- Lors d'une nouvelle inscription à un service ou en cas de changement de mot de passe, laissez KeePass générer des mots de passe aléatoires.

- Stockez la base dans votre Sdrive pour la synchroniser sur plusieurs appareils. Sur mobile, utilisez KeePassDX (Android) ou KeePassium (iOS) que vous pouvez également synchroniser.
- Vous pouvez configurer votre gestionnaire de mot de passe pour remplir automatiquement vos identifiants lorsque vous souhaitez vous connecter à un service. Vous trouverez des tutoriels pour Keepass (https://keeform.org/) et MacPass (https://github.com/MacPass/MacPass/wiki/Autotype)

Gestionnaire intégré au navigateur ou au système d'exploitation

Votre navigateur (Chrome, Firefox, Safari…) ou votre système d'exploitation (macOS) proposent d'enregistrer vos mots de passe automatiquement. Ce n'est pas une solution satisfaisante, mais cela reste préférable à l'absence de protection. Si vous utilisez cette option, activez impérativement un mot de passe maître ou l'équivalent (« mot de passe principal » sous Firefox, trousseau protégé sous macOS/iOS) et évitez de synchronisez vos mots de passe pour les conserver uniquement en local.

Carnet physique ou document numérique

Si vous persistez à utiliser un carnet physique ou document numérique dans lequel vous consignez vos identifiants, adoptez au minimum un système de notation partielle. Plutôt que d'inscrire le mot de passe dans son entièreté, p. ex. « Motdepasse2025 », préférez : « Mot*********25 ».

Messagerie

Pourquoi ?

Votre adresse mail professionnelle est un identifiant central : elle donne accès à vos services institutionnels. Si elle est compromise, c'est l'ensemble de votre environnement de travail qui est exposé.

Comment faire ?

Utilisez systématiquement votre adresse institutionnelle pour vos activités professionnelles. Évitez d'utiliser une boîte personnelle (Gmail, Yahoo, etc.) pour transférer ou stocker des données liées à vos activités professionnelles.

Si vous n'avez pas d'autre choix que d'utiliser une adresse personnelle, privilégiez des services offrant un chiffrement de bout en bout (par exemple ProtonMail, Tutanota).

Pour les discussions instantanées ou groupes de travail, privilégiez des solutions sécurisées proposés par les services mentionnés dans la section « Utiliser des services conseillés ».

Ne communiquez jamais vos identifiants par mail, même si le message semble provenir de votre tutelle : il peut s'agir de phishing.

Vérifiez toujours les liens contenus dans les mails : passez la souris dessus pour voir l'URL réelle.

Évitez d'ouvrir les pièces jointes provenant d'expéditeurs inconnus.

Internet et confidentialité : VPN

👉 Utilisez un navigateur à jour (Firefox, Chrome). Limitez les extensions de navigateur au strict nécessaire (certaines collectent vos données). Activez le blocage natif des traqueurs et cookies tiers (des navigateurs comme Firefox le font sans ajouts d'extensions comme uBlock Origin ou Privacy Badger).

Pourquoi ?

Un VPN (réseau privé virtuel) crée un tunnel chiffré entre votre appareil et Internet. Cela permet de sécuriser vos connexions sur les réseaux Wi-Fi publics ou inconnus (cafés, hôtels, transports), de masquer vos échanges à d'éventuels intermédiaires (fournisseur d'accès, administrateur réseau local), et de contourner certaines restrictions d'accès lors de déplacements à l'étranger.

En pratique, le CNRS ne propose pas encore de service VPN centralisé. Mais certaines tutelles, comme l'Université Paris XIII, mettent à disposition leur propre solution. Lorsque c'est possible, il est fortement conseillé d'utiliser le VPN de votre établissement.

Activez toujours le VPN sur un réseau Wi-Fi public ou partagé. Vérifiez que l'icône du VPN apparaît bien dans la barre d'état avant de commencer à travailler. Lors de missions à l'étranger, démarrez systématiquement le VPN avant de réinstaller ou consulter vos données de recherche.

Comment faire ?

VPN proposé par votre tutelle

Consultez la documentation de votre établissement ou contactez le service informatique pour connaître le logiciel recommandé. Installez le client officiel. Connectez-vous avec vos identifiants institutionnels. Activez la connexion avant toute utilisation d'Internet sur un réseau public.

Si aucun VPN institutionnel n'est proposé

Vous pouvez recourir à une solution tierce (par exemple ProtonVPN ou NordVPN). Elles offrent une bonne sécurité, à condition de choisir un fournisseur réputé, transparent sur sa politique de confidentialité et certifié « no-log ».

Partir en mission à l’étranger

Pourquoi ?

Les déplacements internationaux exposent vos appareils et données à des risques accrus : vol, saisie, inspection, mais aussi espionnage ou altération technique. Certains pays imposent même de déverrouiller vos appareils à la frontière. Pour éviter toute compromission, il est recommandé de voyager avec du matériel « propre », chiffré, et de ne transporter aucune donnée sensible directement sur vos appareils

Comment faire ?

Avant le départ

Minimisez le nombre d’appareils emportés.

Déposez vos données sensibles dans un espace institutionnel sécurisé (Sdrive, Resana, ShareDocs) et supprimez-les temporairement de vos appareils.

Vérifiez la législation du pays de destination : dans certains États, l’entrée avec un appareil chiffré est interdite ou soumise à autorisation ; le non-respect de cette règle peut conduire à la saisie du matériel.

Demandez si possible un ordinateur et un téléphone de prêt, vides et déjà chiffrés (ou non chiffré si la législation le demande).

Pendant le trajet et le séjour

Gardez vos équipements près de vous ou sous clé, y compris dans les hôtels et bureaux.

Méfiez-vous des réseaux non maîtrisés, activez toujours un VPN avant de vous connecter.

Éteignez/verrouillez vos appareils lorsqu’ils ne sont pas utilisés.

En cas de saisie ou inspection par les autorités, coopérez mais signalez immédiatement l’incident au CNRS.

Ne connectez pas de supports offerts ou douteux (ex. clés USB).

⚠ La biométrie est pratique mais risquée : elle peut être imposée physiquement et parfois légalement exigée, contrairement au mot de passe mieux protégé. Préférez un mot de passe long et robuste, et désactivez la biométrie avant un voyage ou en contexte à risque.

Procédure en cas d’incident

Pourquoi ?

Un incident informatique (infection, piratage, vol d’équipement, comportement suspect d’un compte ou d’un appareil) doit toujours être pris au sérieux. Même si les conséquences paraissent limitées, un signalement rapide permet de contenir la menace.

Comment faire ?

Limiter la portée

Ne paniquez pas, mais réagissez immédiatement. Isolez l’appareil concerné en coupant sa connexion réseau (Wi-Fi, câble) sans l’éteindre : cela conserve les traces utiles à l’analyse.

Évaluer la gravité

Notez les éléments visibles : combien d’appareils ou d’utilisateurs touchés, quel type de données concernées, le caractère sensible ou non des informations.

Déclarer l’incident

Prévenez rapidement votre d’unité, le RSSI régional (dr01-rssi@cnrs.fr ou +33 6 17 49 72 30) et les tutelles concernées.

En cas de contexte extra-métropolitain : contactez l’ambassade de France locale, le numéro de crise CNRS (+33 1 45 20 02 51) et l’adresse fsd.incident@cnrs.fr.

Préparer la suite

Restez disponible pour les analyses complémentaires. Préparez-vous à modifier vos mots de passe. Conservez les informations clés : nom de la machine, adresse IP si affichée, identifiant utilisateur, ce que vous faisiez au moment de l’incident.

IA génératives

Pourquoi ?

Les outils d'intelligence artificielle générative (ChatGPT, Copilot, Gemini…) peuvent rendre de nombreux services (résumés, brouillons, codes, traductions rapides). Mais les données que vous leur transmettez (textes, extraits d'archives, données personnelles, résultats non publiés) peuvent être enregistrées, analysées et réutilisées par l'éditeur du service. Les serveurs sont souvent situés hors d'Europe, donc soumis à d'autres législations que le RGPD. Rien ne garantit la confidentialité ou la destruction des informations envoyées.

Comment faire ?

N'utilisez pas ces outils pour traiter des données sensibles ou inédites de recherche. Si vous souhaitez quand même vous en servir, limitez-vous à des contenus publics, anonymisés ou sans importance stratégique et préférez des modèles open source et souverains (Mistral, Bloom, Llama 3 en local via LM Studio ou Ollama).

Transcrire des fichiers audios avec Whisper via Humanum

Pourquoi ?

La transcription automatique permet de gagner beaucoup de temps dans l'exploitation de vos entretiens, réunions ou séminaires.
Le service Whisper est accessible via la plateforme Humanum, une infrastructure publique française de recherche qui respecte les normes de protection des données.

Contrairement aux services commerciaux, vos enregistrements ne servent pas à entraîner de nouveaux modèles : ils sont uniquement traités pour produire une transcription.

👉 Connectez votre espace Sharedocs en local (cf. section « Stockage et partage de fichiers ») pour gérer plus facilement vos retranscriptions.

Comment faire ?

- Créer un compte sur Humanum avec votre adresse institutionnelle.
- Se connecter à ShareDocs (le cloud Humanum).
- Demander un espace de stockage. L'acceptation de la demande peut prendre quelques jours.
- Une fois l'accès accordé, ouvrir le dossier : hnTools_watchFolder → SpeechToText → Whisper.
- Choisir le modèle (du moins précis *small* au plus précis *large*) et la langue. Déposer votre fichier audio (formats acceptés : .wav, .mp3, .m4a).
- La transcription est lancée : vous recevrez un mail quand le traitement est terminé.
- Récupérez votre transcription dans ShareDocs (fichier .txt) et supprimez les fichiers de la plateforme après avoir terminé.

Ce guide rassemble les consignes pratiques et les procédures minimales à appliquer pour sécuriser les postes de travail, les données de recherche et les déplacements professionnels.

Ces recommandations s'inscrivent dans le cadre de la PSSI de l'IRIS.

Ce livret a été rédigé par Léo Tertrais-Flamand dans le cadre d'une mission temporaire. En cas de question le concernant, contactez en priorité le responsable de la sécurité des systèmes d'information actuel de l'IRIS, Issa Cissé (issa.cisse@ehess.fr).

Document à usage strictement interne.

Ce guide décrit les routines et procédures de sécurité spécifiques au laboratoire. Il ne doit pas être diffusé en dehors de l'unité.

Les thèmes abordés :

- Chiffrement des ordinateurs et téléphones
- Stockage et partage de fichiers
- Chiffrement des stockages externes
- Gestion des mots de passe
- Messagerie
- Internet et confidentialité : VPN
- Partir en mission à l'étranger
- Procédure en cas d'incident
- IA générative
- Transcrire des fichiers audios avec Whisper via Huma-num