MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

Service du haut fonctionnaire de défense et de sécurité

Secrétariat général
SDS
Affaire suivie par :
Christophe Peyrel
HFADS
Tél : 01 55 55 87 00
Mél : christophe.peyrel@education.gouv.fr

110 rue de Grenelle
75357 Paris SP 07

Paris, le 20 DEC. 2022

La secrétaire générale
Haut fonctionnaire de défense et de sécurité

à

Mesdames et Messieurs les présidents d'université et d'établissements de recherche

Objet : mesures de sécurité relatives aux données numériques sensibles

Le vol récent d'ordinateur d'un personnel d'un établissement contenant des informations sensibles et stratégiques, m'amène à demander de renforcer les mesures de protection des informations physiques et virtuelles qui sont appliquées au sein des laboratoires en zones à régime restrictifs (ZRR) afin de protéger le potentiel scientifique et technique de la Nation (PPST) et à tous les autres cas sensibles qui ne sont pas ou ne peuvent pas être protégés par des ZRR.

En effet certains personnels des établissements publics détiennent ou manipulent des données stratégiques ou sensibles dont la captation ou la compromission pourrait nuire gravement à l'établissement, aux intérêts de l'Etat, et aux intérêts de partenaires extérieurs (publics ou privés) avec lesquels des collaborations stratégiques sont nouées. Les risques de captation d'informations sensibles sont souvent renforcés par le caractère fréquemment nomade de l'exercice des fonctions des personnels.

Aussi je souhaite que les personnels occupant dans vos établissements, des fonctions sensibles ou stratégiques au regard de la PPST, telles que celles de directeur ou vice-président en charge de la valorisation et de l'innovation, de la recherche, des partenariats, ou des relations internationales, et les chercheurs travaillant en ZRR, soient sensibilisés à la sécurité numérique et que les mesures de précautions et de bon sens ci-dessous énumérées, soient respectées dans les meilleurs délais. Il s'agit des mesures suivantes :

Lors des déplacements, s'agissant des téléphones et ordinateurs professionnels :

- Ne jamais laisser les matériels en dehors de la surveillance du détenteur dans les lieux publics (incluant les salons et séminaires professionnels) ;
- Ne jamais laisser le matériel dans une voiture ou dans un train sans une surveillance permanente ;
- Utiliser un filtre de confidentialité sur l'écran d'ordinateur pour éviter toute indiscrétion et captation visuelle d'information ;
- Et d'une manière générale, essayer autant que possible de limiter le déplacement des moyens numériques contenant des informations très sensibles.

Au domicile ou à l'hôtel :

- Lorsque le matériel n'est pas utilisé, l'éteindre complétement (un ordinateur en veille est plus vulnérable) et le ranger le de manière sécurisée et hors de vue ; dans la mesure du possible, une mise sous clé du matériel est recommandée (coffre d'hôtel, placard fermant à clé à domicile) ;
- Conservez le téléphone au plus près de soi et en toute circonstance (y compris la nuit) ;
- Fermer toujours les fenêtres et portes du lieu où est utilisé ou rangé le matériel ;

- Pendant la journée, si le matériel se retrouve sans surveillance de manière ponctuelle, verrouiller la session et le sécuriser, si possible, avec un système de sécurité tel q'un câble antivol à clé ;

En complément pour les déplacements nationaux et européens :

- S'assurer auprès du service informatique qu'un mécanisme de protection par chiffrement des disques durs est actif sur l'ordinateur et, le cas échéant, sur les clés USB ou disques amovibles professionnels;
- Stocker les fichiers très sensibles (de type « diffusion restreinte »[1] ou confidentiel entreprise), dans des containers chiffrés disposant d'un visa de sécurité de l'ANSSI (ACID ou ZED) ;
- Sécuriser au maximum le téléphone portable en utilisant une modalité de verrouillage robuste (code PIN suffisamment complexe ou données biométriques) et s'assurer que le chiffrement des données du téléphone est actif ;

Les responsables de la sécurité des systèmes d'information (RSSI) et directeurs des systèmes d'information (DSI) des établissements et opérateurs peuvent également s'appuyer sur le guide de l'ANSSI traitant du nomadisme numérique[2].

Pour les déplacements à **l'étranger hors Europe** :

- Ne pas emporter l'ordinateur professionnel habituel (comportant les informations sensibles, **même si elles sont chiffrées**) mais dédier un ordinateur aux missions à l'étranger ne contenant que des fichiers non sensibles et les contenus strictement nécessaires au déplacement ;
- De même éviter autant que possible d'emporter le téléphone portable professionnel habituel mais utiliser un téléphone portable non sensible ;

L'ANSSI a élaboré un guide de conseils aux voyageurs, à consulter avant tout déplacement à l'étranger[3].

Ces précautions ne sont pas anodines. Certains pays sont susceptibles de demander les identifiants d'accès aux équipements numériques (dont les clés des moyens de chiffrement) et peuvent parfois réaliser des copies numériques de disques durs au moment de l'entrée ou de la sortie du territoire.

Enfin et pour mémoire, les **informations relevant du secret de la défense nationale** au sens de l'instruction générale interministérielle sur la protection du secret de la défense nationale (IGI 1300) ne sont pas concernées par ces préconisations car elles **ne peuvent en aucun cas être stockées dans des équipements ou moyens numériques qui n'ont pas été agréés[4] pour cet usage.**

Si malgré leur vigilance, ces personnels constataient le moindre incident, il convient sans délai de signaler l'évènement (ou une suspicion d'évènement) au service informatique et au fonctionnaire de sécurité et de défense de l'établissement, puis de réaliser un dépôt de plainte si l'incident est avéré.

Je vous remercie de veiller au respect de ces consignes qui sont toutes issues de cas déjà constatés de vols de données.

Les fonctionnaires de sécurité et de défense (FSD) des établissements des établissements des établissements y seront sensibilisés par les services du haut fonctionnaire de défense et de sécurité qui restent à votre entière disposition pour répondre à vos questions.

Marie-Anne LEVEQUE

Copie : Mesdames et Messieurs les recteurs de région académique
Mesdames et Messieurs les recteurs délégués ESRI

---

[1] Une entité qui met en œuvre un SI traitant des informations « Diffusion Restreinte » (DR) doit se conformer à la réglementation applicable, c'est-à-dire à la date de rédaction de cette note, à l'instruction interministérielle n°901/SGDSN/ANSSI relative à la protection des systèmes d'information sensibles (II 901)
[2] https://www.ssi.gouv.fr/uploads/2018/10/guide_nomadisme_anssi_pa_054_v1.pdf
[3] https://www.ssi.gouv.fr/uploads/IMG/pdf/passeport_voyageurs_anssi.pdf
[4] L'ANSSI est l'unique autorité d'homologation pour les moyens et SI relevant de l'IGI 1300