Paris, le 30 NOV. 2018

A l'attention de
Mesdames et Messieurs
les directrices et directeurs d'unité

Le Directeur général délégué
aux ressources

www.cnrs.fr

Campus Gérard-Mégie
3, rue Michel-Ange
75794 Paris cedex 16

T. 01 44 96 48 40
F. 01 44 96 53 80

Objet : Chiffrement des ordinateurs et protection des smartphones professionnels

Des incidents graves intervenus récemment obligent à rappeler l'impératif de procéder au chiffrage des ordinateurs de votre laboratoire à très bref délai.

- Il s'agit d'une obligation, s'inscrivant dans la politique de sécurité des systèmes d'information de l'Etat.
- Il s'agit d'une nécessité pour protéger les travaux de recherche. En effet, le CNRS est confronté à une recrudescence de vols ou pertes d'ordinateurs.
- Avec le règlement général de protection des données (RGPD), et la sensibilité attachée aux données personnelles, il s'agit d'une exigence légitime pour tous ceux dont les données sont confiées au CNRS.

Les conséquences en cas de vol ou de perte d'ordinateur, si celui-ci n'est pas chiffré, sont très concrètes et peuvent se révéler extrêmement dommageables :

- concernant les données personnelles, une atteinte grave peut être portée au respect de la vie privée ;
- concernant les données relevant du patrimoine scientifique et technologique (PPST), des intérêts liés à la Défense peuvent être affectés ;
- dans le cas de projets en collaboration avec des tiers, notamment du secteur économique, le projet de recherche peut être interrompu ou le dépôt de titres de propriété compromis ;
- dans tous les cas, l'atteinte à l'image du CNRS peut être très problématique.

Le chiffrement des disques durs des ordinateurs doit être réalisé pour limiter ces risques. Quelle que soit la plateforme logicielle utilisée (Windows, MacOS, Linux), les systèmes modernes disposent tous de la capacité native à chiffrer entièrement un disque dur, sans affecter l'utilisation quotidienne de l'ordinateur.

Lorsqu'un *smartphone* est utilisé à des fins professionnelles et que des données du CNRS (messagerie électronique par exemple) y sont stockées, la même consigne de sécurité s'applique. Là encore, cette fonction est native sur tous les systèmes récents. Elle s'accompagne nécessairement de l'activation d'un code de verrouillage robuste (8 caractères minimum).

En tant que directeur d'unité, il vous appartient de veiller à la bonne mise en œuvre de ces mesures de protection des données au sein de votre unité. **Il vous est demandé que l'ensemble du parc des ordinateurs de votre unité, quelle que soit l'origine du financement, soit chiffré pour le 31 janvier 2019, ainsi que les smartphones.** Les délégations régionales informent de cette démarche les partenaires académiques du CNRS.

Les opérations nécessaires sont techniquement simples et rapides : vous trouverez en annexe un mode d'emploi. Naturellement, vous pouvez aussi vous appuyer sur les administrateurs système et réseau des unités, les services informatiques des délégations régionales et les chargés de sécurité des systèmes d'information.

Compte tenu des précédents rappels sur ce sujet sensible, des vérifications seront opérées de manière aléatoire à partir du 1er février 2019 et des responsabilités pourront être recherchées en cas de violation de ces obligations qui s'imposent à tous.

Votre concours est indispensable à la mise en œuvre de ces mesures élémentaires de protection, dans l'intérêt de chaque agent et de la science. Je vous en remercie par avance.

Pour le Président-directeur général
et par délégation
Le directeur général délégué aux ressources

Christophe Coudroy

Plusieurs dizaines d'ordinateurs, de smartphones déclarés volés ou perdus tous les ans au CNRS ...

Des données de la recherche, des données à caractère personnel ou liées à votre vie privée irrémédiablement perdues ! Pas pour tout le monde ?

Protéger ses données contre la perte ou le vol ?

C'est très simple. Une action en deux temps

1. Sauvegarder

Régulièrement, mais pas n'importe où... Assurez-vous d'avoir toujours accès à vos sauvegardes, et de pouvoir les restaurer au besoin.

2. Chiffrer

Vous trouverez dans ce guide des éléments concrets de mise en œuvre du chiffrement sur vos équipements. C'est simple, efficace et sans risques.

« Avant de prendre sa retraite, le directeur du renseignement américain, James Clapper, a dit que j'avais accéléré l'adoption du chiffrement de 7 ans [avec mes révélations]. Pour lui, c'était une insulte, mais je l'ai pris comme une sorte de compliment. »

- Edward Snowden, 2017

Des questions techniques ? Des problèmes de mise en œuvre ?

Prenez contact avec votre Chargé de SSI dans votre unité ou votre délégation.

Direction des Systèmes d'Information

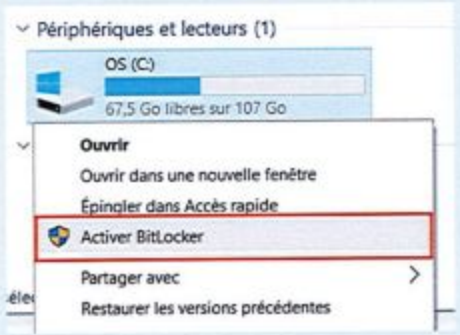
Département Sécurité des SI

CHIFFREMENT DES TERMINAUX

Vademecum

Je travaille sous Microsoft Windows

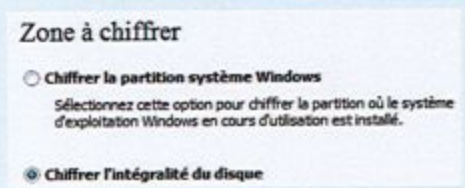
A. J'utilise BitLocker intégré au système d'exploitation de mon PC...



Dans mon explorateur de fichiers, je fais un clic droit sur mon disque système (C:) et je choisis « *Activer Bitlocker* ».
Je sauvegarde ma clé de récupération sous forme d'un fichier PDF sur une clé USB, que je conserve sous clé.

B. ...ou j'utilise VeraCrypt, outil open-source de chiffrement « full disk »

J'installe et je lance le logiciel VeraCrypt [https://www.veracrypt.fr]. Je sélectionne les menus suivants. **Je sauvegarde le disque de récupération sous forme de fichier ZIP sur une clé USB**, que je conserve sous clé.



Je travaille sous Apple Mac OS X

J'utilise FileVault intégré au système d'exploitation de mon ordinateur Apple

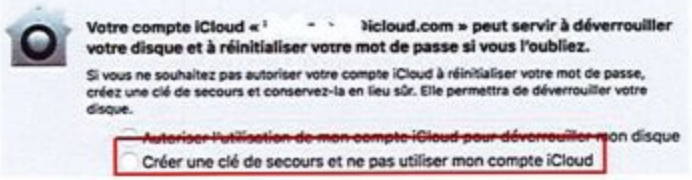
Je clique sur le menu Pomme > *Préférences Système*, puis sur *Sécurité et confidentialité*.

Je clique sur l'onglet *FileVault*.

Je clique sur le cadenas puis je saisis un nom et un mot de passe d'administrateur.

Je clique enfin sur *Activer FileVault*.

ATTENTION: En aucun cas je ne sauvegarde la clé de récupération sur mon compte iCloud! Je la sauvegarde sur une clé USB, que je conserve sous clé.



Je travaille sous Linux (Fedora, Debian...)

Lors de l'installation de mon système, je choisis l'option de chiffrement de mes données.

Et sur mon smartphone ?

Les systèmes d'exploitation d'Apple (iOS) ou de Google (Android) permettent d'activer très simplement un chiffrement de l'ensemble des données. Faites un tour dans les options de sécurité de votre téléphone.