

# Comment chiffrer son disque dur?

3





## Pourquoi ce guide ?

Dans le cadre professionnel ou le cadre personnel, vous conservez sur votre ordinateur des documents qui peuvent contenir des informations confidentielles ou des données à caractère personnel qui ne doivent pas être accessibles à tous.

En cas de vol ou de perte, le chiffrement du disque dur est une solution qui va permettre de rendre inaccessibles les données qui y sont contenues et d'empêcher un tiers mal intentionné d'en avoir l'usage.



L'objectif de ce guide est de vous proposer des moyens de chiffrement sur votre ordinateur et sur vos supports de stockage amovibles.

# Le chiffrement, c'est quoi ?

C'est un procédé de cryptographie permettant de rendre impossible la compréhension d'un document à toute personne qui ne possède pas la clé de déchiffrement.

## **Cela permet d'assurer :**

- La confidentialité : les documents sont protégés des lectures non désirées.
- L'authenticité : l'origine du document est sûre.
- L'intégrité : le document n'a pas été modifié.

## **Pourquoi chiffrer ?**

### **1. Protéger le contenu d'un disque dur**

Les ordinateurs sont des outils qui sont malheureusement facilement perdus ou volés.

Chiffrer le disque dur de son ordinateur rend illisible le contenu à toute personne qui ne dispose pas du mot de passe de la session utilisateur. Sans ce mot de passe, la seule solution pour réutiliser un disque dur chiffré sera de le reformater pour le réinitialiser et cette opération supprimera les informations y figurant.

Il est indispensable de paramétrer le verrouillage automatique de votre appareil en cas d'inactivité. Sans cette précaution élémentaire, la session en cours restant ouverte, le chiffrement de votre disque dur serait sans effet sur la sécurité de vos données.

### **Attention au cloud !**

Lorsque vous conservez des documents personnels et/ou sensibles sur un cloud, la confidentialité des données n'est pas garantie !

Sauf si :

- les données sont chiffrées,
- vous maîtrisez le lieu géographique de stockage des données du cloud (ex : serveur de l'université ou du CNRS).

## 2. Limiter le risque de violation des données personnelles

Le chiffrement est une mesure de sécurité efficace contre les « violations de données personnelles » visées par le règlement général de protection des données (RGPD, art. 33). Le chiffrement préservera les intérêts des personnes (usagers, membres du personnel) dont les données personnelles figurent sur le support chiffré.

### **Et si je perds (ou on me dérobe) un PC contenant des données personnelles mais dont le DD n'est pas chiffré ?**

Dans tous les cas, la disparition du matériel devra être portée le plus vite possible à la connaissance du délégué à la protection des données ([dpo@univ-lille.fr](mailto:dpo@univ-lille.fr)).

L'existence d'un risque avéré pour la (ou les) personne(s) dont les données personnelles seraient exposées devra faire l'objet d'une notification à la CNIL (RGPD, art. 33).

Si ce risque est élevé (usurpation d'identité, accès des données de santé p. ex.), une communication devra être réalisée auprès de la (ou les) personne(s) lésées exposant : la nature de la violation, le nom et les coordonnées du délégué à la protection des données de l'Université, ses conséquences probables et les mesures prises ou proposées pour y remédier (RGPD, art. 34).

# Comment chiffrer ?

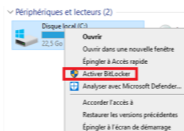
Il faut ici distinguer 2 choses :

- Le chiffrement de l'intégralité du ou des disques de votre ordinateur.
- Le chiffrement d'un périphérique extérieur (clés USB, disque dur externe...) ou d'une partie d'un disque dur.

## Chiffrement de l'intégralité du (ou des) disque(s) de votre ordinateur

### 1. Sous Windows

Vous pouvez utiliser BitLocker, ce logiciel est directement intégré à Windows<sup>1</sup>. Dans l'explorateur de fichier, je fais un clic droit sur mon disque local (c:) et je choisis « Activer Bitlocker ».



### Attention :

Pensez bien à sauvegarder votre clé de récupération et à la mettre en lieu sûr en cas de problème.

1. Si vous utilisez une version familiale de Windows, Bitlocker n'est pas disponible, dans ce cas reportez vous plus loin à la procédure d'installation de VeraCrypt.

En cas de doute sur le chiffrement du disque dur d'un ordinateur géré par la Direction générale déléguée au numérique de l'Université de Lille, il est recommandé de vous rapprocher du service assistance de proximité en déposant un ticket via GLPI, accessible depuis votre ENT.

## 2. Sous Mac OS

Vous pouvez utiliser FileVault, ce logiciel est directement intégré dans toutes les versions de Mac OS.

Choisissez le menu Pomme  > Réglages système.

- cliquer sur « confidentialité et sécurité » dans la barre latérale
- faites défiler vers le bas jusqu'à la section FileVault à droite, puis cliquez sur « activer ou désactiver ».

### Attention :

Pensez bien à sauvegarder votre clé de secours et à la mettre en lieu sûr en cas de problème.

## 3. Sous Linux

Le chiffrement du disque dur d'un PC utilisant d'un système d'exploitation Linux doit être réalisé lors de l'installation de celui-ci. À défaut, le chiffrement ne pourra être réalisé qu'en ayant recours à une application comme VeraCrypt (voir plus loin la procédure d'installation).

## Chiffrement d'une partie du disque dur interne ou d'un périphérique externe (disque dur externe, clé USB..)

VeraCrypt est un des logiciels de chiffrement, libre et gratuit, préconisé par la CNIL<sup>2</sup>. Plutôt que de chiffrer vos documents un par un, ce logiciel va permettre de chiffrer une zone (ou conteneur) du disque dur de votre ordinateur ou d'un support de stockage externe.

### 1. Installer VeraCrypt

#### étape 1

Télécharger le logiciel VeraCrypt sur  
[veracrypt.fr/en/Downloads.html](https://veracrypt.fr/en/Downloads.html)



#### étape 2

Installer VeraCrypt selon  
votre système d'exploitation



#### étape 3

Créer le volume chiffré  
voir tutoriel de la CNIL sur Youtube  
[youtube.com/watch?v=fMpzmkzAliE](https://youtube.com/watch?v=fMpzmkzAliE)



## 2. À chaque utilisation de VeraCrypt



Lancer VeraCrypt.



Sélectionner un volume disponible et ouvrir le conteneur (fichier) chiffré.



Monter le disque codé en saisissant le mot de passe et le code PIN.



Utiliser votre nouveau lecteur comme un disque classique.



Démonter votre volume et fermer VeraCrypt en fin d'utilisation.



Une question relative aux données personnelles ?  
Contactez le délégué à la protection des données :

*[dpo@univ-lille.fr](mailto:dpo@univ-lille.fr)*

La page intranet :

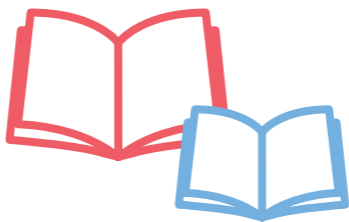
*[ent.univ-lille.fr/ulille/environnement-de-travail/donnees-personnelles](http://ent.univ-lille.fr/ulille/environnement-de-travail/donnees-personnelles)*

Une question relative à la sécurité ?  
Contactez les responsables de la sécurité des systèmes  
d'information :

*[rssi@univ-lille.fr](mailto:rssi@univ-lille.fr)*

Le site :

*[ssi.univ-lille.fr](http://ssi.univ-lille.fr)*



## Déjà paru

- 1** Loi informatique et liberté : suis-je concerné-e ?
- 2** Le règlement général sur la protection des données : ce qui change
- 3** Comment chiffrer son disque dur ?
- 4** Guide du directeur de thèse ou de mémoire
- 5** Phishing : quelques conseils pour ne pas se faire piéger
- 6** La lettre d'information du projet de recherche
- 7** Réaliser une enquête anonyme
- 8** Organiser et nommer ses documents numériques







