UNIVERSITÉ DE LILLE
POLITIQUE DE SÉCURITÉ DU SYSTÈME D'INFORMATION ET PROTECTION DES DONNÉES PERSONNELLES

SÉCURITÉ DES ÉQUIPEMENTS INFORMATIQUES CONTENANT DES DONNÉES EN CAS DE CHANGEMENT D'AFFECTATION
V20190710-SSI/EC

Problématique

les données stockées dans les équipements informatiques changeant d'affectation ne doivent pas pouvoir être lues par le nouveau bénéficiaire si celui-ci n'a pas le « droit d'en connaître ».

Définitions

Données : données professionnelles sensibles ou non + données personnelles d'un ou plusieurs usagers

Données sensibles : de manière générale, données dont la divulgation, l'altération ou l'indisponibilité aurait des conséquences importantes, graves ou mortelles pour l'Etablissement ou pour les usagers (cf. https://ssi.univ-lille.fr/sites/ssi.univ-lille.fr/files/ssi/universite_de_lille-ssi-sensibilite_des_donnees.pdf)

En cas d'absence de classification interne, on appellera « données sensibles » les « données personnelles sensibles » au sens de la CNIL (cf. https://www.cnil.fr/fr/definition/donnee-sensible) ou les données considérées comme telles au sens de la Protection du Potentiel Scientifique et Technique de l'Etat (PPST)

*Dispositif de stockag*e (liste non exhaustive) : disque dur interne ou externe de technologie mécanique (HD) ou électronique (SSD), mémoire flash (Clef USB, SD, CompactFlash, …), smartphone avec mémoire intégrée, CD-ROM, bandes magnétiques

Equipement informatique contenant des données (liste non exhaustive) : ordinateur fixe ou portable, serveur, imprimante multi-fonction, baie de stockage partagée, smartphone, dispositif d'acquisition de données médicales, système d'enregistrement audio ou vidéo

Changement d'affectation : transfert interne, don, vente, mise au rebut, destruction

Règles de sécurité (extraites du référentiel de sécurité « Politique de Sécurité des Systèmes d'Information de l'Etat » -PSSIE-)

EXP-MIS-REB (mise au rebut) : lorsqu'une ressource informatique est amenée à quitter définitivement l'entité, les données présentes sur les disques durs ou la mémoire intégrée doivent être effacées de manière sécurisée. L'effacement des données sensibles doit s'appuyer sur des

produits qualifiés, ou respecter des procédures établies en concertation avec l'ANSSI.

EXP-REAFFECT (réaffectation de matériels informatiques) : une procédure de gestion des postes et supports dans le cadre de départs de personnel ou de réaffectations à de nouveaux utilisateurs doit être mise en place et validée par le RSSI. Elle doit définir les conditions de recours à un effacement des données.

EXP-CI-EFFAC (effacement de support) : le reconditionnement et la réutilisation des disques durs pour un autre usage (ex : réattribution d'une machine/serveur) ne sont autorisés qu'après une opération d'effacement sécurisé des données.

EXP-CI-DESTR (destruction de support) : la fin de vie d'un support ou d'un matériel embarquant un support de stockage (imprimante, routeur, commutateur…) doit s'accompagner d'une opération de destruction avant remise au constructeur.

EXP-MAINT-EXT (maintenance externe) : les données non chiffrées doivent être effacées avant l'envoi en maintenance externe de toute ressource informatique. Les opérations de chiffrement doivent faire appel à des produits qualifiés. L'effacement des données sensibles doit s'appuyer sur des produits qualifiés, ou respecter des procédures établies en concertation avec l'ANSSI.

PDT-REAFFECT (réaffectation du poste de travail) : une procédure SSI définit les règles concernant le traitement à appliquer aux informations ayant été stockées ou manipulées sur les postes réaffectés.

PDT-SUPPR-PART (suppression des données sur les postes partagés) : les données présentes sur les postes partagés (portable de prêt, par exemple) doivent être supprimées entre deux utilisations, dès lors que les utilisateurs ne disposent pas du même besoin d'en connaître.

Mesures adaptées à l'Université de Lille

Si le dispositif de stockage est chiffré selon une méthode standard et si le mot de passe de déverrouillage n'est pas trivial, le dispositif peut être réaffecté sans précaution supplémentaire.

Si le dispositif de stockage n'est pas chiffré, celui-ci doit être (au choix) :

1) soit effacé entièrement (par réécriture de la totalité de l'espace de stockage) ou réinitialisé quand il n'y a pas d'autre possibilité (cas des smartphones),

2) soit rendu définitivement inutilisable,

3) soit extrait de l'équipement, pour être réaffecté à un poste de travail ayant les mêmes exigences de sécurité, ou pour être conservé en lieu sécurisé (à éviter, principalement à cause du risque de vol).

Précaution 1 : assurer la disponibilité des documents
Dans tous les cas, il convient de vérifier que l'effacement ne supprime pas l'unique version d'un document utile. Pour un équipement individuel, on demandera à l'ancien bénéficiaire de vérifier que ses données professionnelles sont correctement stockées sur un serveur et de faire le nécessaire pour ses données privées.

Précaution 2 : respecter la « loi Archives »
En cas de suppression d'une source unique d'un document, il convient de se rapprocher du Service des Archives, afin de vérifier la durée d'utilité administrative (DUA) et le sort final des données et, le cas échéant, pour réaliser un bordereau d'élimination réglementaire.

La procédure pour l'élimination des archives est disponible sur l'intranet : https://intranet.univ-lille.fr/finances/finances-informations-generales/

Précaution 3 : préférer détruire plutôt qu'effacer les données sensibles :
Si les données stockées étaient sensibles au sens de la PPST ou au sens de la CNIL (cf. https://ssi.univ-lille.fr/sites/ssi.univ-lille.fr/files/ssi/universite_de_lille-ssi-sensibilite_des_donnees.pdf), il faudrait théoriquement effacer ces données à l'aide d'un matériel ou d'un logiciel qualifié par l'ANSSI (Agence Nationale de la SSI) ; étant donné le coût et le temps nécessaires à cette tâche d'effacement hautement sécurisé, il est préférable de rendre définitivement inutilisables les dispositifs de stockage concernés ou de les réaffecter à un poste de travail ayant les mêmes exigences de sécurité.

Informations techniques

Un simple formatage de disque ou suppression de fichiers est insuffisant pour effacer des données.

L'effacement complet d'un disque dur mécanique nécessite des logiciels spécifiques permettant de réécrire des données aléatoires ou nulles sur toute la surface du disque ("zero-write", "random writes").

L'effacement complet d'un dispositif de stockage de type « FLASH » (clef USB, disque « SSD ») nécessite d'utiliser un logiciel spécifiquement fourni par le fabricant.

Exemples d'outils pour effacer les disques durs mécaniques : Seagate Seatools, Western Digital Data Lifeguard, Samsung HUtil, HGST Windows Drive Fitness Test, ou un logiciel dédié tel Blancoo (certifié effacement hautement sécurisé par l'ANSSI).

Exemples d'outils pour effacer les disques SSD ou les mémoires flash : Intel Solid State Toolbox, Corsair SSD Toolbox, SanDisk SSD,Toolbox, Samsung Magician Software, OCZ Toolbox.