**Annexe 2**
**Bonnes pratiques applicables à la conception de sujets d'examens sur informatique**

La prise en compte de la sécurité doit se faire de façon globale pour qu'elle soit efficace. Ce document traite de la sécurisation de premier niveau des ordinateurs et de leur utilisation, ainsi que des points de vigilance particuliers liés à la manipulation des documents sensibles que sont les sujets et propositions de sujet d'examens.
Les différents niveaux de sécurisation sont :
- les actions de sécurisation d'un ordinateur (sécurisation du moyen) ;
- les bonnes pratiques d'utilisation (sécurisation de l'utilisation du moyen) ;
- les actions de protection des données sensibles (sécurisation de l'utilisation du moyen dans un contexte métier spécifique).

**Ces actions et pratiques sont génériques et ne se substituent pas aux chartes ou consignes locales.**

## 1. Les actions de sécurisation d'un ordinateur

### Sécurisation liée aux logiciels et configurations :

- mise à jour du système d'exploitation et des logiciels utilisés (ne pas utiliser de logiciel sans avoir souscrit à une licence qui permet d'obtenir les mises à jour) ;
- utilisation d'un antivirus à jour (base de signatures et version logiciel) configuré pour scanner les fichiers impliqués dans les actions de l'utilisateur (ouverture d'une clé USB, copie de fichier etc. ) ;
- activer la fonctionnalité de pare-feu du système et ne pas autoriser les demandes d'exceptions proposées par le logiciel sans les avoir étudiées ;
- n'utiliser que des logiciels dont l'origine est fiable (site de l'éditeur ou d'un distributeur officiel) et s'assurer que la maintenance est prévue (proscrire les téléchargements de sources non maitrisées et les fichiers transmis par partage, clé USB ou messagerie) ;
- activer le verrouillage automatique nécessitant le mot de passe pour déverrouiller ;
- utiliser au quotidien des comptes utilisateurs aux droits restreints.

### Protection physique :

- ne pas laisser un ordinateur portable sans surveillance (par exemple, dans le train) ;
- l'accrocher à un point fixe à l'aide de moyens appropriés.

## 2. Les bonnes pratiques d'utilisation

- Ne pas partager son mot de passe : il est garant de l'identité et donc de la responsabilité et n'est pas un simple contrôle d'accès.
- Utiliser des mots de passe faciles à retenir et difficiles à deviner : au moins 9 (mais la préconisation est parfois d'utiliser au moins 12 caractères) caractères mélangeant les lettres, chiffres et caractères spéciaux, basés sur une méthode permettant de s'en souvenir. cf.http://www.ssi.gouv.fr/guide/mot-de-passe/).
- Avoir un mot de passe différent pour chaque usage (en ligne, intranet, système...) : si l'un d'entre eux est compromis, les autres accès seront préservés.
- S'assurer de la confidentialité de la saisie des mots de passe : il faut éviter qu'un tiers ne voit la saisie, et ne pas le noter sur un support en libre accès.
- Ne jamais divulguer son mot de passe, et plus généralement, d'informations sans s'assurer de l'interlocuteur, de son identité et de la justification de sa demande : un administrateur n'a pas besoin de mot de passe.
- Utiliser avec prudence le courriel et la messagerie instantanée et préférer les messageries professionnelles.
- Naviguer sur Internet avec prudence : favoriser les sites connus et n'autoriser, si possible, l'exécution des scripts qu'à la demande.

- Effectuer des sauvegardes régulières et vérifier la restauration des informations : penser aux sauvegardes différentielles et complètes.
- Contrôler la diffusion d'informations personnelles : tout ce qui transite par Internet restera sur Internet.
- Remonter les incidents et les dysfonctionnements : un incident de sécurité est souvent détecté à la suite d'un dysfonctionnement constaté par un utilisateur.

## 3. Les actions de protection des sujets

- Ne pas multiplier les copies des documents et avoir conscience de leur emplacement (sur supports physiques ou par envoi mail).
- Enregistrer les documents dans des espaces sécurisés (cf. précisions sur les espaces sécurisés ci-dessous).
- Travailler directement depuis les espaces sécurisés : éditer les documents sans les recopier dans des espaces non sécurisés.
- Se méfier des sauvegardes automatiques : vérifier les configurations des logiciels utilisés.
- Marquer les documents dès leur création, dans le contenu et le nom du fichier.
- Effectuer des recherches de ces marquages et de mots clés pour vérifier les documents sensibles présents sur un ordinateur.
- Faire des sauvegardes au même niveau de sécurité : le chiffrement limite les accès aux données. Si les sauvegardes sont stockées dans un lieu sécurisé, par exemple dans un coffre, l'absence de chiffrement peut être envisagée.
- Effacer les documents de façon sécurisée (cf. compléments techniques ci-dessous).
- Effacer les supports physiques (cf. compléments techniques ci-dessous).
- Manipulation des versions papiers :
    - imprimer avec prudence : les documents imprimés à distance sont parfois pris par erreur par une tierce personne ;
    - transport des documents : les documents sensibles doivent être transportés dans une enveloppe fermée portant la mention de sensibilité et les contacts et l'adresse à laquelle la retourner en cas de perte ;
    - apposer un marquage visible : les documents doivent comporter le niveau de sensibilité afin que le lecteur sache quelles mesures adopter ;
    - détruire les documents sensibles : les documents sensibles doivent être physiquement détruits et non pas jetés.

## 4. Précisions sur les espaces sécurisés

Dans ce document, on appelle « espace sécurisé », une zone chiffrée avec un contrôle par mot de passe ou moyen cryptographique. Cette zone peut être un fichier, un conteneur logique avec plusieurs fichiers, une partition ou un support physique complet (disque, clé USB etc.) avec un chiffrement logiciel ou matériel. Le chiffrement peut être intégré aux systèmes d'exploitation afin d'associer le déchiffrement à l'identification de l'utilisateur et lui rendre cette opération transparente.
Attention, lors de l'utilisation de chiffrement, il convient de gérer le risque de perte des moyens de déchiffrement.

Il existe de nombreuses solutions possibles. Il conviendra de les tester au préalable sur des aspects techniques, mais aussi pratiques. Il conviendra de choisir des solutions homogènes, en adéquation avec les recommandations locales.

Plus d'informations sur le chiffrement sont disponibles sur le site du pôle SSI, dans la section publications techniques.

## Compléments techniques

Effacement des supports de stockage de masse :
http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-medias-amovibles/effacement-des-supports-de-stockage-de-masse.html

Les solutions de chiffrement de disque
https://ssi.in.orion.education.fr/index.php/Les-solutions-de-chiffrement-d/440/0/

Liste des produits certifiés CSPN par l'ANSSI
http://www.ssi.gouv.fr/administration/produits-certifies/cspn/produits-certifies-cspn/
Liste des produits qualifiés par l'ANSSI
http://www.ssi.gouv.fr/administration/qualifications/produits-recommandes-par-lanssi/les-produits/

Les 10 commandements de la sécurité sur l'internet par l'ANSSI (avec une fiche explicative pour chaque)
http://www.ssi.gouv.fr/particulier/precautions-elementaires/dix-regles-de-base/