

Bonnes pratiques

Sécurité des Systèmes d'Information

- Généralités
- Mots de passe
- Station de travail
- Clef USB
- ACSSI
- Mails
- Internet
- Données personnelles et documents sensibles
- Ordinateur personnel
- Les 10 commandements Cyberprotection de la DGSIC

- Avoir signé l'attestation de reconnaissance de responsabilité (ARR) concernant l'engagement INDIVIDUEL de responsabilité au bon usage des systèmes d'information ;
- Avoir pris connaissance de l'instruction ministérielle n°2003/DEF/DGSIC du 20 novembre 2008 portant code de bon usage des systèmes d'information et de communication du ministère de la défense ;
- Avoir la fiche REFLEXE avec les coordonnées de son CSSI ou OSSI.

Si utilisation de ISPT :

- Avoir signé la charte ISPT_STC-IA régissant les services de navigation sur Internet depuis le poste de travail Intradef.

Généralités sur la bonne conduite de l'utilisateur MINDEF

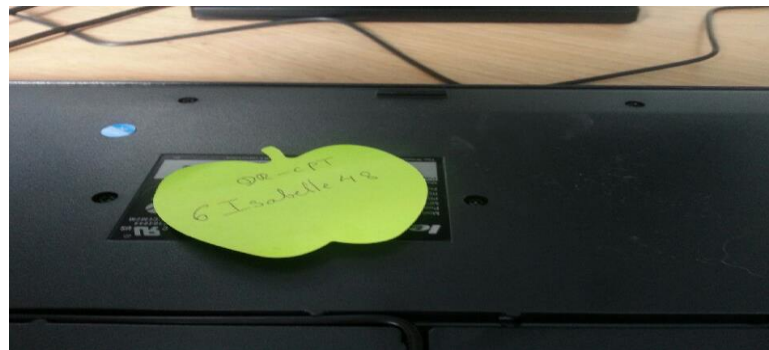
- Choisir des mots de passe sûrs, ne pas les divulguer et les changer régulièrement ;
- Respecter les droits accordés et protéger son poste de travail et ses données ;
- Respecter la confidentialité des données et des communications ;
- Verrouiller ou arrêter son poste de travail ;
- Ne pas utiliser d'équipement personnel pour exercer son activité professionnelle.

Généralités sur la bonne conduite de l'utilisateur MINDEF

- L'usage des clef USB personnelle est interdite : on ne met pas de données privées sur sa clef professionnelle ;
- Ne pas modifier la configuration d'un équipement ou de son poste de travail (pas d'essai de crack de logiciel, par exemple) ;
- Ne pas tenter de manipulations hasardeuses ou tester des mesures de sécurité ;
- Être vigilant et rendre compte de toute anomalie ou incident à son CSSI ou OSSI pour qu'il établisse un retour d'expérience (RETEX) à l'OSSI du SGA.

Mauvaises pratiques sur les mots de passe

- Pas de mot de passe : Données accessibles facilement modifiables, voire effaçables ;
- Mot de passe simpliste : (ex : prénom des enfants, date de naissance, etc.), il peut être retrouvé rapidement, soit par déduction, soit par un logiciel de crackage de mot de passe ;
- Mot de passe noté sur un pense-bête et collé sur l'écran ou sous le clavier : Absence totale de sécurité.



Bonnes pratiques sur les mots de passe

- Retenir une phrase simple :


Prendre les initiales des mots (alterner minuscules, majuscules, chiffres et caractères spéciaux) :

- 5*8=KaRentE
- LTEedl8 pour "La Tour Eiffel est dans le 8ème"
- Utiliser un mot de passe différent :
 - pour la connexion à Intradef,
 - à Internet,
 - chez soi (différents pour les mails et les comptes sur sites de VPC).
- **Ne pas les laisser accessibles à un tiers.**

Mauvaises pratiques sur les stations de travail

- L'utilisateur s'absente de son bureau en laissant sa session ouverte
- A la reprise, pas de mot de passe demandé : possibilité de modification, divulgation, ou suppression des données ;
- Il oublie sa clé USB branchée sur le poste : risque de vol de la clé et/ou des données qu'elle contient.

Bonnes pratiques sur les stations de travail

- Verrouiller la station de travail (raccourci clavier :  + L) ;
- Retirer les clés USB, dès que celles-ci ne sont plus utilisées y compris lors d'une absence momentanée

Mauvaises pratiques sur les clefs USB

- Stocker tous ses documents sur clé USB : en cas de perte ou de vol, risque de divulgation de données sensibles et perte du travail ;
- Laisser trainer sa clef USB ;
- Accepter volontiers les clés USB «cadeau» : présence possible de logiciels d'aspiration de données ;
- Utiliser aussi bien des clés USB «personnelles» que des «professionnelles» sur n'importe quel ordinateur : multiplication des risques de transmission de virus et d'informations sensibles sur un réseau non sécurisé.

Bonnes pratiques sur les clefs USB

- Effacer toutes les données inutiles des clés USB ;
- Utiliser exclusivement des clés « professionnelles » sur les réseaux MINDEF et ne pas les brancher sur des ordinateurs personnels ;
- Ne pas accepter de clé USB « cadeau ».

Mauvaises pratiques sur les ACSSI

ACSSI : Est dénommé Article Contrôlé de la Sécurité des Systèmes d'Information tout document, logiciel ou matériel, qui par son intégrité ou sa confidentialité contribue à la sécurité d'un système d'information. Ce sont : Carte ISIS, Carte CD, CD-ROM CD ou SD, Documents CD ou SD, THEOREM (ACSSI CD) et GLOBULL, clef RCI (ACSSI DR).

- Laissez trainer des documents CD ou SD (papier) ou CD-ROM CD ou SD sur son bureau ;
- Mettre les cartes ISIS ou CD dans son sac personnel ou dans veste ;
- Lire du Confidentiel Défense sur un poste Intradef ;
- Lire du Secret Défense sur un poste Intradef.

Bonnes pratiques sur les ACSSI

- Rangement dans le coffre de sûreté ou armoire forte de tous les ACSSI CD après utilisation :
 - Carte ISIS, Carte RECRU, Carte CD, CD-ROM CD ou SD, Documents CD ou SD, TEOREM.
- Pour les ACSSI DR (GLOBULL et clef RCI), il est très fortement recommandé de les ranger dans le coffre de sûreté également ;
- Utiliser un poste Confidentiel Défense pour lire un CD-ROM CD ;
- Utiliser un poste Secret Défense pour lire un CD-ROM SD.

Mauvaises pratiques sur les mails

- Ouvrir sans regarder l'expéditeur qu'il soit connu ou non ;
- Ouvrir les pièces jointes et cliquer sur les liens d'un mail sans se méfier : risque de propagation de virus et de récupération de données ;
- Envoyer des documents sans protection et sur n'importe quel réseau : possibilité d'interception du mail et donc des documents ;
- Donner son adresse mail professionnelle sur INTERNET : l'adresse mail peut être récupérée, piégée et servir à envoyer des logiciels malveillants ;
- Utiliser son adresse mail professionnelle comme une adresse personnelle pour effectuer des commandes sur des sites de VPC ou des petites annonces.

Bonnes pratiques sur les mails

- Etre vigilant avec ses mails :
 - vérifier que l'expéditeur est connu,
 - faire preuve de prudence en cliquant sur les liens et en ouvrant les pièces jointes,
 - ne pas faire circuler, les rumeurs, chaînes,
- Ne communiquer son adresse mail professionnelle qu'à des personnes de confiance ;
- Utiliser des moyens de transmission adaptés à la sensibilité de l'information.

Mauvaises pratiques sur INTERNET

- Naviguer sur INTERNET sans prendre de précautions (sites peu fréquentables ou non réputés, liens non sûrs, etc...) : risque de piégeage du navigateur et d'introduire des logiciels malveillants sur son poste ;
- Etre très bavard et parler de ses activités professionnelles sur les réseaux sociaux (photos, commentaires, CV) :
 - Mise en danger de sa personne et de ses collègues ce qui peut amener du chantage, espionnage, terrorisme),
 - Atteinte à l'image de marque du ministère de la Défense.
- S'exprimer sans retenue (opinion politique, religieuse, professionnelle, personnelle, etc...) : donne des informations pouvant intéresser le renseignement adverse ou toute personne mal intentionnée ;
- Se croire invincible.

Bonnes pratiques sur INTERNET

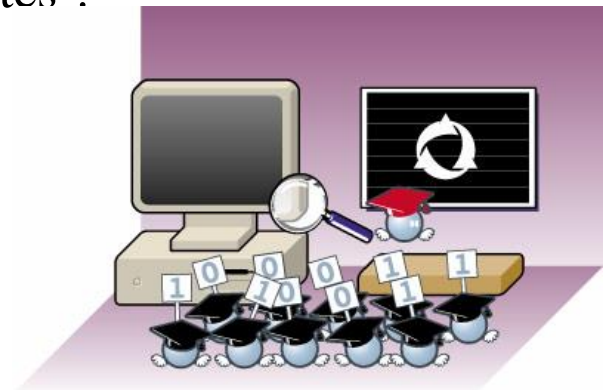
- Naviguer sur des sites connus et fiables ;
- Ne pas cliquer sur des liens sans rapport avec le site (publicité, site de rencontre, site X) ;
- Sur les réseaux sociaux :
 - respecter la discrétion professionnelle et le devoir de réserve,
 - ☐ s'assurer de l'identité du correspondant avant tout échange,
 - ☐ bien réfléchir avant de publier (photos, vidéos, commentaires, etc...).
- L'oubli numérique est difficile même après suppression du compte ou des données ;
- RAPPEL : l'envoi, le dépôt et le traitement de documents sensibles sont INTERDIT sur INTERNET.

Rappel sur l'usage des médias sociaux : le guide des médias sociaux édité par la DICOD sur ww.defense.gouv.fr .

Focus sur les informations personnelles

Avant toute publication ou divulgation d'informations notamment sur Internet, nous devons nous poser des questions fondamentales:

- Les informations que je veux publier sont-elles sensibles, y compris dans les photos et les vidéos ?
- Ai-je le droit de les publier sans porter tort à autrui ?
- Est-ce que j'ai envie qu'elles soient vues par tous et soient encore visibles dans 10 ans?
- Quelles pourraient être les conséquences si elles venaient d'être connues de tous, y compris des terroristes ?



Focus sur les documents sensibles

- Pas de transmission sur Internet de documents sensibles portant les mentions Diffusion Restreinte, Spécial France, Confidentiel médical, Confidentiel Personnel ou Confidentiel Industrie ;
- Pas de Confidentiel Défense, ni Secret Défense sur Internet ;
- L'envoi par Internet d'un document sensible non classifié de défense ne peut se faire que s'il est chiffré avec le logiciel ACID Cryptofiler.

Conseils de base pour son ordinateur personnel

- Choisir un anti-virus robuste, un antivirus à jour, un pare-feu personnel, un anti-spam, un anti espion ;
- Maintenir son système et ses logiciels à jour par les correctifs critiques mis à disposition par les éditeurs ;
- Ne pas exécuter de programmes de provenance inconnue, aller sur des sites réputés « sûrs » ;
- Ne pas donner son e-mail perso à tout-va ou créer un e-mail « poubelle » pour recevoir les news letters, publicités etc ;
- Ne pas ouvrir d'e-mails de provenance inconnue, les mettre directement à la poubelle ;
- Etre méfiant à la réception des courriers de loterie, de relance de banque, d'EDF, ...

Avec un ordinateur portable personnel

- Dispositif anti-vol du portable ;
- Activer la mise en veille automatique (10mn) ;
- Banaliser et renommer vos répertoires privés et sensibles ;
- Chiffrer les informations sensibles non classifiées ;
- Protéger la connexion Internet par mot de passe solide ;
- Utiliser un antivirus à jour, un pare-feu personnel, un anti-spam, un anti espion ;
- Utiliser un système d'exploitation et des logiciels bureautiques à jour ;
- Porter une attention particulière dans les aéroports, les hôtels, aux frontières... ;
- Attention aux vols de données à distance, au WIFI des hôtels.

Rappel : le passeport de conseil aux voyageurs sur
http://www.ssi.gouv.fr/uploads/IMG/pdf/passeport_voyageurs_anssi.pdf

A retenir

10 commandements de la CYBERPROTECTION DGSIC

N°1

Passez les supports amovibles par le sas antivirus ou le point d'insertion des données (PID) du réseau concerné et ne connectez pas de supports personnels sur un ordinateur professionnel.



(3) Je privilège l'usage d'une station antivirus

N°2

Effacez toutes les données inutiles de vos clés USB

La clé USB n'est pas un outil de stockage.



(10) Les données sont effacées du support dès qu'elles n'ont plus de raison d'y être

N°3

Informez immédiatement de tout comportement anormal votre correspondant SSI qui contactera les organismes compétents et vous guidera dans les actions à mener



② Je préviens mon DSSI en cas de problème



N°4

Naviguez prudemment sur Internet



① J'applique mon devoir de réserve sur les réseaux sociaux

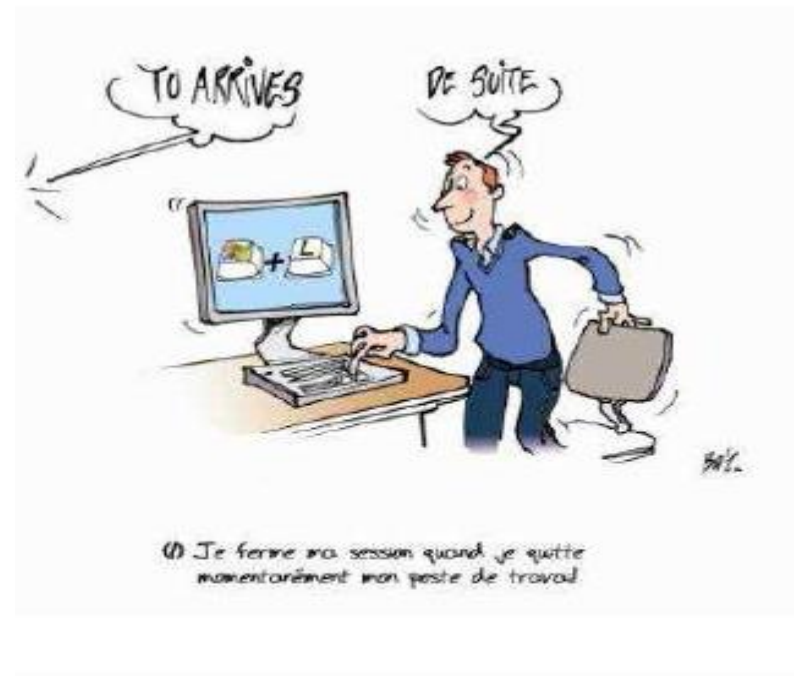
N°5

Utilisez des mots de passe véritablement robustes et secrets, ne les laissez pas accessibles



N°6

Verrouillez votre session de travail lorsque vous quittez momentanément votre poste de travail



N°7

Ne communiquez votre adresse mail professionnelle qu'à des personnes de confiance



N°8

Soyez vigilant avec les mails que vous recevez.



(2) Je suis vigilant sur l'objet et l'expéditeur des mails que je reçois

Vérifier l'expéditeur, cliquez avec prudence sur les liens et ouvrez avec discernement les pièces jointes



(3) Je reste prudent avant d'ouvrir une pièce jointe ou de cliquer sur un lien

N°9

Adaptez les moyens de transmission en fonction de la sensibilité des informations



⑨ J'adapte le moyen de transmission en fonction de la sensibilité de l'information

N°10

Ne cherchez pas à contourner la politique de sécurité



⑩ J'ai une attitude responsable et proactive vis-à-vis de la SSI