

SSI Sensibilisation à la sécurité de l'information**

Prérequis	Connaissances de base en informatique
Compétence opérationnelle	Etre capable de comprendre les dangers liés à l'utilisation de l'informatique et de s'en protéger :
Objectifs d'apprentissage	<ul style="list-style-type: none"> ◆ en gérant ses mots de passe de manière à protéger l'accès aux données ; ◆ en maîtrisant les règles de bonne conduite de la messagerie électronique ; ◆ en appliquant les règles de bonne conduite pour limiter les risques liés à Internet ; ◆ en connaissant les aspects juridiques liés à l'utilisation du système d'information ainsi que les règles de bonne conduite à tenir ; ◆ en protégeant les unités informatiques mobiles pour conjuguer mobilité et sécurité ; ◆ en utilisant les réseaux sociaux à bon escient ; ◆ en expliquant quelques notions fondamentales de la sécurité de l'information.
Durée d'apprentissage	40 heures dont 20 heures de cours et 20 heures de travail personnel.

SSI Indicateurs

Objectifs d'apprentissage	Pondérations et Indicateurs
<p>Gérer ses mots de passe de manière à protéger l'accès aux données.</p>	<p style="text-align: right;"><i>Pondération des indicateurs : A : essentiel B : important C : complémentaire</i></p> <ul style="list-style-type: none"> A Il connaît les règles de bonne conduite en matière de mot de passe. (I001) C Il connaît l'utilité d'un mot de passe. (I002) C Il connaît les risques en cas d'usurpation de mot de passe. (I003) C Il différencie les bons mots de passe des mauvais (il peut citer des exemples de bons et de mauvais mots de passe). (I004) B Il applique les règles qui permettent de se souvenir d'un "bon" mot de passe (mot de passe facile à retenir et difficile à découvrir). (I005) C Il compose des mots de passe avec un mélange de chiffres, de lettres et de caractères spéciaux. (I006) B Il change les mots de passe attribués par défaut. (I007) B Il change fréquemment ses mots de passe (mot de passe du système d'exploitation, mot de passe Web, etc.) (I008) B Il sait dans quels cas il peut partager un mot de passe. (I009) B Il sait comment gérer les mots de passe Web (tout navigateur confondu). (I010) C Sur Internet, il utilise des mots de passe de qualité pour accéder à des applications sensibles (e-commerce / e-banking). (I011) B Il sait comment gérer ses mots de passe dans les forums. (I012) B Il utilise un coffre-fort à mot de passe pour gérer ses mots de passe. (I013)
<p>Maîtriser les règles de bonne conduite de la messagerie électronique.</p>	<ul style="list-style-type: none"> A Il connaît les règles de bonne conduite en matière de messagerie électronique. (I014) C Il connaît les règles de rédaction d'un e-mail. (I015) B Il connaît les principaux risques liés au courrier électronique (risques d'usurpation des adresses e-mail, liens externes contenus dans les e-mail, phishing, hoax, etc.). (I016) B Il gère, avec précaution, les fichiers joints aux e-mails. (I017) C Il utilise un logiciel de chiffrement lorsqu'il doit envoyer des informations confidentielles par e-mail. (I018) B Il gère, avec prudence, les e-mails qui demandent des informations personnelles. (I019) B Il n'envoie pas de courriers électroniques en chaîne. (I020) C Il gère les courriers indésirables. (I021) B Il connaît les principes à respecter dans les avis d'absence (gestion des e-mails en cas d'absence). (I022) B Il signale que son e-mail est privé ou confidentiel. (I023) B Il se désinscrit d'une newsletter. (I024)

SSI Indicateurs

Objectifs d'apprentissage	Pondérations et Indicateurs
	<p>B Il utilise à bon escient les fonctions "copie" et "copie cachée". (I025)</p>
<p>Appliquer les règles de bonne conduite pour limiter les risques liés à Internet.</p>	<p>A Il connaît les règles de bonne conduite sur Internet. (I026)</p> <p>B Il quitte correctement les applications Web sensibles (par les menus de déconnexion). (I027)</p> <p>B Il n'utilise pas les options "Se souvenir de moi" ou "Rester connecté" (I028)</p> <p>B Il vérifie les mises à jour des logiciels de sécurité installés sur son poste. (I029)</p> <p>B Il reconnaît une page Web sécurisée. (I030)</p> <p>B Il réagit correctement en cas de fraude. (I031)</p> <p>C Il connaît les dangers des forums et des blogs. (I032)</p> <p>C Il connaît les dangers du chat. (I033)</p> <p>B Il connaît les principes à appliquer lors du téléchargement. (I034)</p> <p>C Il sait pourquoi le téléchargement est risqué. (I035)</p> <p>B Il sait quelles sont les traces laissées sur son ordinateur par la navigation sur Internet. (I036)</p> <p>B Il évite la saisie semi-automatique. (I037)</p> <p>C Il connaît les composants Internet potentiellement dangereux. (I038)</p> <p>C Il désactive les composants potentiellement dangereux. (I039)</p> <p>C Il utilise la navigation privée. (I040)</p> <p>B Il utilise un bloqueur de fenêtres publicitaires intempestives. (I041)</p>
<p>Connaître les aspects juridiques liés à l'utilisation du système d'information ainsi que les règles de bonne conduite à tenir.</p>	<p>A Il connaît les règles de bonne conduite en matière de protection des données. (I042)</p> <p>B Il sait ce qu'est une donnée sensible selon la loi fédérale sur la protection des données (LPD). (I043)</p> <p>C Il connaît le but de la loi fédérale sur la protection des données (LPD). (I044)</p> <p>C Il connaît le but du règlement général sur la protection des données (RGPD). (I045)</p> <p>B Il sait quelles données doivent être protégées (en entreprise et en privé). (I046)</p> <p>C Il connaît les infractions spécifiques à la sécurité du système d'information (quelle législation s'applique à un acte illicite, quelles sanctions en cas d'infraction). (I047)</p> <p>B Il connaît la législation propre à Internet (utilisation abusive de photos, téléchargement d'oeuvres sans le consentement de leur auteur, utilisation de logiciels sans licence, protection des marques, utilisation de copies privées, etc.). (I048)</p>

SSI Indicateurs

Objectifs d'apprentissage	Pondérations et Indicateurs
	<p style="text-align: right;"><i>Pondération des indicateurs : A : essentiel B : important C : complémentaire</i></p> <p>B Il connaît la réglementation qui s'applique aux e-mails (envoi en masse d'e-mails, etc.). (I049)</p> <p>B Il respecte les règles en matière de propriété intellectuelle (utilisation des ressources informatiques dans le cadre légitime de son activité, utilisation de tout support numérique permettant la conservation des données, etc.). (I050)</p> <p>C Il sait quelles données Internet peuvent être utilisées en fonction de leurs droits respectifs. (I051)</p> <p>C Il surveille ses impressions. (I052)</p> <p>B Il surveille ses communications. (I053)</p> <p>C Il classe les données selon les règles émises par son entreprise. (I054)</p> <p>C Il sait qui peut surveiller ses accès à Internet. (I055)</p> <p>B Il protège la transmission d'information sensible lors de l'envoi de fichiers. (I056)</p>
<p>Protéger les unités informatiques mobiles pour conjuguer mobilité et sécurité.</p>	<p>A Il connaît les règles de bonne conduite en matière de mobilité. (I057)</p> <p>B Il connaît les solutions pour faire face aux dangers de l'informatique mobile. (I058)</p> <p>B Il connaît les dangers liés à l'informatique mobile. (I059)</p> <p>B Il connaît les principaux équipements de l'informatique mobile. (I060)</p> <p>C Il sait qui porte la responsabilité des informations emportées sur des équipements mobiles. (I061)</p> <p>B Il protège l'accès aux informations qui se trouvent sur les équipements mobiles. (I062)</p> <p>B Il ne stocke aucune donnée confidentielle sur les équipements mobiles sans les chiffrer. (I063)</p> <p>B Il protège les supports amovibles contre les logiciels malveillants. (I064)</p> <p>B Il utilise les périphériques USB en toute sécurité. (I065)</p> <p>B Il nettoie le contenu de sa clé USB. (I066)</p> <p>B Il bloque l'accès à sa clé USB. (I067)</p> <p>C Il connaît les risques de vol d'information associés aux périphériques USB. (I068)</p> <p>B Il contrôle le contenu d'un support amovible à l'aide de l'antivirus. (I069)</p> <p>B Il protège le contenu de son smartphone. (I070)</p> <p>C Il connaît les dangers des smartphones. (I071)</p> <p>B Il utilise des accès à distance sécurisés. (I072)</p> <p>C Il identifie une application mobile (app) fiable. (I073)</p>

SSI Indicateurs

Objectifs d'apprentissage	Pondérations et Indicateurs
	C Il connaît l'utilité et le fonctionnement d'un VPN (réseau privé virtuel). (I074)
Utiliser les réseaux sociaux à bon escient.	<p>A Il connaît les règles de bonne conduite en matière de réseau social. (I075)</p> <p>C Il sait ce qu'est un réseau social (site de socialisation). (I076)</p> <p>C Il connaît les réseaux sociaux les plus connus (Facebook, LinkedIn, Twitter, etc.). (I077)</p> <p>B Il connaît les dangers liés aux réseaux sociaux. (I078)</p> <p>C Il sait en quoi les sites de socialisation portent atteinte à la vie privée. (I079)</p> <p>C Il sait que la diffusion de données personnelles sur les sites de socialisation accroît les risques de spam. (I080)</p> <p>B Il configure correctement les paramètres des réseaux sociaux auxquels il est abonné. (I081)</p> <p>B Il connaît les recommandations lors de la création d'un compte sur un réseau social. (I082)</p> <p>B Il règle les paramètres de confidentialité dans un réseau social. (I083)</p> <p>C Il modifie la protection par défaut. (I084)</p> <p>C Il gère ses coordonnées dans un réseau social. (I085)</p> <p>C Il protège sa vie privée sur un réseau social (il ne publie pas ses données personnelles comme sa date de naissance, son mot de passe, etc.). (I086)</p> <p>C Il ne publie pas d'informations qui pourraient lui nuire sur le plan professionnel. (I087)</p> <p>C Il gère ses albums photos dans un réseau social. (I088)</p> <p>C Il bloque des personnes indésirables sur un réseau social. (I089)</p> <p>B Il contrôle la publication de certaines actualités. (I090)</p>
Expliquer quelques notions fondamentales de la sécurité de l'information.	<p>A Il connaît les règles de bonne conduite en matière de sécurité de l'information. (I091)</p> <p>B Il sait ce qu'est la sécurité de l'information. (I092)</p> <p>B Il connaît les principaux objectifs de la sécurité informatique (confidentialité, intégrité, disponibilité, authenticité). (I093)</p> <p>C Il connaît la typologie des risques informatiques (humains, organisationnels, matériels, etc.). (I094)</p> <p>B Il sait ce qu'est une faille de sécurité. (I095)</p> <p>C Il connaît les conséquences d'une faille de sécurité. (I096)</p> <p>B Il verrouille son poste de travail. (I097)</p> <p>B Il reconnaît les signes d'infection d'un ordinateur par un virus. (I098)</p> <p>C Il sait comment agir si son PC est infecté par un virus provenant d'un site Web ou d'un e-mail. (I099)</p>

SSI Indicateurs

Objectifs d'apprentissage	Pondérations et Indicateurs
	<p style="text-align: right;"><i>Pondération des indicateurs : A : essentiel B : important C : complémentaire</i></p> <p>B Il respecte la configuration mise en place sur son ordinateur. (I100)</p> <p>C Il connaît les différents moyens de protection mis en place dans la plupart des entreprises. (I101)</p> <p>A Il met régulièrement à jour son antivirus et les logiciels utilisés. (I102)</p> <p>B Il s'assure que les informations sensibles échangées avec des collègues ne sont accessibles qu'aux personnes autorisées. (I103)</p> <p>B Il sait comment les droits d'accès sont gérés en entreprise. (I104)</p> <p>C Il connaît le rôle du pare-feu. (I105)</p> <p>B Il distingue les différents types de logiciels malicieux (virus, vers, cheval de Troie, etc.). (I106)</p> <p>B Il connaît différents types d'attaques (flux de données, attaque DDOS, ingénierie sociale, malware, etc). (I107)</p> <p>B Il connaît différentes méthodes d'escroquerie (phishing, hoax, etc.). (I108)</p> <p>B Il connaît les procédés de manipulation sociale pour obtenir des informations. (I109)</p> <p>B Il connaît les risques inhérents à l'utilisation des connexions sans fil (WiFi, bluetooth, infrarouge, etc.). (I110)</p> <p>B Il applique les consignes de sauvegarde dictées par l'entreprise. (I111)</p> <p>B Il connaît les dangers liés à l'utilisation d'un poste en libre accès. (I112)</p> <p>B Il connaît les dangers liés à l'utilisation d'une connexion Internet non sécurisée. (I113)</p>