CHARTE DE BON USAGE DU SYSTEME D'INFORMATION DE L'AP-HP

Annexe 3 : Glossaire

Mai 2015

Annexe 3 : Glossaire

Archivage : Action de recueillir, de classer et de conserver des documents à des fins de consultation ultérieure

Authentifiant : Attribut permettant de vérifier que l'accédant qui souhaite se connecter à un système est bien celui qu'il prétend être. Il s'agit généralement d'un mot de passe.

Bien : Élément unitaire (logiciel, matériel, service) pour lequel s'applique les règles de bon usage du Système d'Information.

Cheval de Troie : *TROJAN* en anglais. Programme malveillant qui se masque en un programme favorable. Sa particularité par rapport à d'autres codes malveillants est qu'il ne se multiplie pas. Il peut notamment offrir à un attaquant :

- Un accès complet au système
- Des informations de types mots de passe ou adresse de messagerie
- La liste de toutes les actions exercées par l'utilisateur

Chiffrement (appelé aussi improprement "cryptage") : Moyen à utiliser pour préserver la confidentialité des informations sous forme électronique. Le contenu d'un message, d'un document, est alors rendu illisible pour quiconque ne possède pas la clé permettant de le déchiffrer.

CNIL : Commission Nationale de l'Informatique et des Libertés. Autorité administrative indépendante chargée de veiller au respect de la vie privée et des libertés dans le monde numérique.

Code PIN : Numéro d'identification personnel composé de plusieurs chiffres permettant d'authentifier le propriétaire d'une ressource (téléphone portable, carte de paiement, etc.)

Compte : Ensemble des éléments d'une connexion à une ressource, permettant à son titulaire d'utiliser ladite ressource. Il s'agit généralement d'un identifiant, d'un authentifiant, et des droits associés.

Confidentialité : Un des critères de sécurité permettant de s'assurer que l'information ne soit accessible qu'aux personnes autorisées à y accéder.

Contrôle d'accès : Fonctionnalité de sécurité visant à autoriser l'accès à un bien ou un traitement en fonction de l'identifiant et l'authentifiant fournis et des droits associés.

Disponibilité : Un des critères de sécurité, aptitude d'une fonction à rendre le service attendu en temps voulu et dans les conditions d'usage prévues.

Droits d'accès : Ensemble de droits accordés sur une ressource, permettant d'effectuer des actions sur celle-ci (création, consultation, modification, suppression).

Fraude informatique : Toute conduite qui implique la manipulation d'un ordinateur ou des informations informatiques, quelle que soit la méthode utilisée, dans le but d'obtenir de façon malhonnête de l'information, de l'argent, des biens ou tout autre avantage, ou dans l'intention de nuire (ex : captation ou suppression d'informations, copie pirate de logiciels ; accès, entrave ou altération d'un traitement automatisé des informations…)

Gestion Technique centralisée ou GTC est un mode de supervision par système d'automate centralisé, gérant un très grand nombre de paramètres et de fonctions différentes, à partir des données envoyées par des capteurs au sein de grandes structures.

Habilitation : Attribution à un utilisateur de droits d'accès à des biens informatiques par une entité autorisée.

Identifiant : *Login* en anglais. Attribut unique permettant à une personne de s'identifier à un système. Il s'agit, à titre d'illustration, du code APH pour les agents. Il est généralement associé à un authentifiant.

Incidents de sécurité : on appelle incident de sécurité du Système d'Information tout événement affectant ou pouvant affecter la disponibilité, l'intégrité, la confidentialité ou la traçabilité du Système d'Information de l'AP-HP. Il peut s'agir de vol d'information, de corruption de données, ou d'infection virale d'un poste de travail par exemple.

Informations à caractère personnel : Toute information relative à une personne physique identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres (art. 2 de la loi du 6 janvier 1978 modifiée en août 2004).

Intégrité : Un des critères de sécurité, garantie de l'exactitude, de la fiabilité et de l'exhaustivité des informations et des méthodes de traitement.

Nom de domaine ou adresse URL : Correspond à l'adresse d'un site Internet. Il est composé deux parties : le nom du site et un suffixe tel que « .fr », « .org », etc.

Annexe 3 : Glossaire

Pare-feu : *Firewall* en anglais. Outil matériel ou logiciel permettant de définir les typologies de communications autorisées sur un réseau.

Partenaire : Entité externe qui intervient en liaison avec l'AP-HP sur un domaine donné (exemple : les associations).

Pourriel : Le pourriel (SPAM) est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.

Responsable de la Sécurité du Système d'Information (RSSI) : Il assure la gouvernance et le pilotage de la sécurité à l'échelle de son entité en identifiant les risques, porte les projets de sécurité, et apporte un support concernant les problématiques de sécurité. Le rôle des RSSI est défini dans la Politique Générale de Sécurité du SI de l'AP-HP.

Sous-traitant : Entités ou organismes externes en relation contractuelle avec l'AP-HP. Le sous-traitant travaille à la demande et sous le contrôle de l'AP-HP.

Spam : cf. pourriel

Support SI : Service à contacter pour toute question relative au Système d'Information. Il peut s'agir du support SI des Groupes Hospitaliers, des sites ou des CCS pour tout ce qui concerne les applications.

Système d'Information : ensemble organisé de ressources (données, procédures, matériels, logiciels, personnels, etc.) permettant d'acquérir, traiter, stocker, diffuser ou détruire les informations utilisées par les entités dans leurs métiers, et ceci quel que soit le support des informations.

Tiers : Entités ou organismes externes en relation contractuelle avec l'AP-HP. Sont ainsi considérés comme des tiers : les prestataires, les intérimaires, les partenaires…

Traçabilité : critère de sécurité qui garantit le suivi des actions des utilisateurs lors de l'utilisation ou de l'accès aux ressources matérielles ou informatiques.

Utilisateur : Désigne toute personne susceptible de pouvoir accéder au SI de l'AP-HP. Sauf mention contraire, désigne également les administrateurs, les exploitants et les prestataires externes intervenant sur le SI.

Ver : Programme autonome dont la vocation première est de se répliquer. Il intègre ses propres fonctions de réplication et d'infection. Il peut ainsi se transmettre en tant que pièce jointe à un courrier électronique (« mass-mailer »), ou se propager *via* le réseau.

VPN ou Virtual Private Network : Il s'agit d'un réseau privé virtuel mis en place par les organismes souhaitant interconnecter leur réseau à celui d'un organisme tiers. Le VPN peut être considéré comme une extension du réseau permettant de préserver le niveau de sécurité de celui-ci.

Virus : Programme hostile susceptible d'infecter les fichiers, de saturer les réseaux. Il peut en résulter des dysfonctionnements divers : par exemple l'effacement du disque dur, la suppression ou la compromission de fichiers.

WIFI : Ensemble de protocoles de communication sans fils permettant de faire communiquer plusieurs équipements informatiques.