université PARIS-SACLAY

Politique de Sécurité des Systèmes d'Information opérationnelle de l'unité – Préconisation de l'Université Paris- Saclay à adapter suivant le contexte en accord avec le RSSI de l'Université Paris-Saclay et du/des RSSIs des EPSTs associés

1. Politique, organisation, gouvernance

L'unité de recherche UMR 8079 suit la Politique de Sécurité des Systèmes d'Information (PSSI) proposée par les établissements de tutelle, se basant elles-mêmes sur la PSSI-Etat (PSSI-E).

2. Ressources humaines

Une charte d'application de la politique Sécurité des Systèmes d'Information (SSI), récapitulant les mesures pratiques d'utilisation sécurisée des ressources informatiques et élaborée sous le pilotage de la chaîne fonctionnelle SSI de l'Université Paris-Saclay, est communiquée à l'ensemble des agents de l'unité. Cette charte doit être opposable juridiquement et, si possible, intégrée au règlement intérieur de l'unité. Le personnel non permanent (stagiaires, intérimaires, prestataires…) est informé de ses devoirs dans le cadre de son usage des SI de l'unité.

Les Chargés SSI (CSSI) locaux doivent être spécifiquement formés à la SSI. Les administrateurs des SI doivent être régulièrement sensibilisés aux devoirs liés à leur fonction, et doivent veiller à respecter ces exigences dans le cadre de leurs activités quotidiennes.
Toutes les personnes manipulant des informations sensibles doivent le faire avec une attention et une probité particulière, dans le respect des textes en vigueur. Les sanctions éventuelles s'appliquant aux cas de négligence ou de malveillance leur sont rappelées.
Chaque utilisateur doit être régulièrement informé des exigences de sécurité le concernant, et motivé à leur respect. Il doit être formé à l'utilisation des outils de travail conformément aux règles SSI.
Une procédure permettant de gérer les arrivées, les mutations et les départs des collaborateurs dans les SI doit être formalisée, et appliquée strictement.
Les règles de la PSSI opérationnelle s'appliquent à tout personnel permanent, ou non, utilisateur d'un SI de l'unité.

3. Gestion des biens

L'unité établit et maintient à jour un inventaire des ressources informatiques sous sa responsabilité, en s'appuyant le cas échéant sur un outillage adapté. Cet inventaire est tenu à disposition des tutelles de la chaîne SSI en cas de besoin de coordination opérationnelle.
Ainsi un tableau d'inventaire est mis en place et maintenu à jour concernant les postes informatiques et serveurs, leur identification et de leurs utilisateurs.
L'historique des biens inventoriés doit être conservé, dans le respect de la législation.

Une base de données de configuration des SI sera constituée, dans la mesure du possible, maintenue à jour et tenue à disposition du RSSI.

L'utilisateur doit protéger les informations qu'il est amené à manipuler dans le cadre de ses fonctions, selon

leur sensibilité estimée au sein de l'unité, tout au long de leur cycle de vie, depuis la création du brouillon jusqu'à son éventuelle destruction.

4. Intégration de la SSI dans le cycle de vie des systèmes d'information

Un SI traitant soit de données personnelles soit offrant un accès personnalisé à un large public doit faire l'objet d'une homologation de sa sécurité par la chaîne SSI des tutelles quand cela est nécessaire.
Les mesures de protection doivent être gérés dynamiquement au long de la vie du SI, de sa conception et jusqu'à son retrait de service. La SSI se traite au quotidien par des pratiques d'hygiène informatique.

Des procédures écrites définissent les actes élémentaires du maintien en condition de sécurité lors des phases de conception, évolution ou retrait d'un système. Un tableau de bord SSI est mis en place et tenu à jour. Il fournit au RSSI et aux autorités une vision générale du niveau de sécurité et de son évolution, rendant ainsi plus efficace le pilotage de la SSI.

Toute prestation dans le domaine des SI est encadrée par des clauses de sécurité. Elles spécifient les mesures SSI que le prestataire doit respecter dans le cadre de ses activités. Un maintien d'un niveau de sécurité au cours du temps se fera par contrôles réguliers. Toute opération d'externalisation s'appuie sur une analyse de risques préalable, de façon à formaliser des objectifs de sécurité et définir des mesures adaptées, cette analyse servira au contrat établi avec le prestataire.

L'hébergement des données sensibles sur le territoire national est obligatoire, sauf accord du HFDS, et dérogation dûment motivée.

Tout contrat d'hébergement détaille les dispositions mises en œuvre pour prendre en compte la SSI. Ce sont notamment les mesures prises pour assurer le maintien en condition de sécurité des systèmes et permettre une gestion de crise efficace (conditions d'accès aux journaux, mise en place d'astreintes, etc.).

5. Sécurité physique

5.1 Sécurité physique des locaux abritant les SI

Un découpage des sites en zones physiques de sécurité doit être effectué, en liaison avec le RSSI, les CSSI et les services en charge de l'infrastructure physique. Pour chaque zone de sécurité, des critères précis d'autorisation d'accès sont établis.
Tout accès réseau installé dans une zone d'accueil du public doit être filtré ou isolé du reste du réseau informatique de l'entité.
Le traitement d'informations sensibles au sein des zones d'accueil est interdit.
L'accès aux locaux techniques abritant des équipements d'alimentation et de distribution d'énergie, ou des équipements de réseau et de téléphonie, doit être physiquement protégé.
Il convient, dans la mesure du possible, de protéger le câblage réseau contre les dommages et les interceptions des communications qu'ils transmettent.

5.2 Sécurité physique des centres informatiques

Un découpage du centre informatique en zones physiques de sécurité doit être effectué, en liaison avec le RSSI et les services en charge de la sécurité et des moyens généraux. Des règles doivent fixer les conditions d'accès à ces différentes zones.
Dans le cas où un tiers gère tout ou partie des locaux du centre informatique, une convention de service, définissant les responsabilités mutuelles en matière de sécurité, doit être établie entre ce tiers et l'entité.
L'accès aux salles informatiques est autorisé uniquement au personnel du centre informatique, aux personnes habilitées ou aux visiteurs accompagnés. Dans la mesure du possible ces accès doivent reposer

sur un dispositif de contrôle d'accès physique. Ce dispositif doit s'appuyer sur des produits qualifiés, lorsqu'ils sont disponibles, et bénéficier d'un maintien en condition de sécurité rigoureux. La délivrance des moyens d'accès physique doit respecter un processus formel permettant de s'assurer de l'identité de la personne, s'appuyant sur le processus d'arrivée et de départ du personnel. Le personnel autre que celui explicitement autorisé et habilité, mais néanmoins appelé à intervenir dans les zones sensibles (entretien ou réparation des bâtiments, des équipements non informatiques, nettoyage, visiteurs...), intervient systématiquement et impérativement sous surveillance permanente.
Une traçabilité des accès des visiteurs externes, aux zones informatiques restreintes doit être mise en place. Ces traces sont alors conservées un an, dans le respect des textes protégeant les données personnelles.
L'alimentation secteur des équipements devra être conforme aux règles de l'art, de façon à se prémunir des atteintes à la sécurité des personnes et équipements liées à un défaut électrique.
Un dispositif de climatisation dimensionné en fonction des besoins énergétiques du système informatique doit être installé. Des procédures de réaction en cas de panne, connues du personnel, doivent être élaborées et vérifiées annuellement.
Ces dispositions visent à prévenir toute surchauffe des équipements, pouvant engendrer une perte du service voire une détérioration du matériel.
L'installation de matériel de protection contre le feu est obligatoire. Des procédures de réaction à un incendie sont définies et régulièrement testées. Les salles techniques doivent être propres. Aucun carton, papier, ou autre source potentielle de départ de feu ne doit être entreposé dans ces locaux.
Une étude sur les risques dus aux voies d'eau doit être réalisée. Cette étude doit notamment prendre en compte le risque de fuite sur un collecteur d'eau douce.

6. Sécurité des réseaux

6.1 Sécurité des réseaux nationaux

Seuls les équipements gérés et configurés par les équipes informatiques habilitées peuvent être connectés au réseau local d'une entité. Pour les équipements non-maîtrisés (postes prévus par les invités, visiteurs, etc.), un réseau spécifique (invité ou collaborateurs) sera prévu.
Toute interconnexion entre les réseaux locaux d'une entité et un réseau externe (réseau d'un tiers, Internet, etc.) doit être réalisée via les infrastructures de la tutelle hébergeant l'unité.

Les accès à Internet passent obligatoirement à travers les passerelles de la tutelle hébergeant l'unité. Dès lors que des informations sensibles doivent transiter sur des réseaux non maîtrisés, il convient de les protéger spécifiquement par chiffrement adapté.

6.2 Sécurité des réseaux locaux

Par analogie avec le cloisonnement physique d'un bâtiment, le SI doit être segmenté selon des zones présentant chacune un niveau de sécurité homogène.
L'interconnexion au niveau local de réseaux locaux d'une entité n'est possible que si la proximité géographique le justifie et sous réserve de la mise en place de connexions dédiées à cet effet, et de passerelles sécurisées et validées par le RSSI.
Dans le cas où une entité partage des locaux (bureaux ou locaux techniques) avec des entités externes, des mesures de cloisonnement des ressources informatiques doivent être mises en place. Si le cloisonnement n'est pas physique, les mesures prises doivent être validées par le ou les RSSI concernés.
En cas d'accueil d'entreprises en partenariat dans les locaux, l'utilisation d'un type de réseau différent sera envisagée et proposée (réseau « invité » ou « réseau dédié »).

6.3 Accès spécifiques

Les accès spécifiques à Internet nécessitant des droits particuliers pour un usage métier ne peuvent être

mis en place que sur dérogation dûment justifiée (ex : certains VPN, Visioconférence…).

6.4 Sécurité des réseaux sans fil

Le déploiement technique du réseau sans fil tient du périmètre exclusif de l'entité gérant le SI de l'Université Paris-Saclay, la DSI. Avant tout nouveau déploiement de réseau WiFi, une analyse de risque se fera par collaboration entre l'unité (direction, équipe informatique) et la DSI, et les recommandations des tutelles SSI seront suivies.
D'une manière générale le déploiement de réseau sans fil, par un ou des usagers, à l'intérieur de l'unité est interdit.

6.5 Sécurisation des mécanismes de commutation et de routage

La configuration, la gestion des équipements de commutation, le routage et la gestion de leur sécurité sont faites par la DSI de l'Université Paris-Saclay qui gère la mise en œuvre du réseau informatique de l'Université Paris-Saclay.

7. Architecture des SI

D'une manière générale, l'architecture des SI est conçue de façon à satisfaire l'ensemble des besoins en disponibilité, confidentialité, traçabilité et intégrité. Le principe de défense en profondeur doit être respecté, notamment d'environnements de sécurité en zone d'hébergement, de machines virtuelles ou physiques dédiées, de réseaux locaux virtuels (VLAN) appropriés, d'un filtrage strict des flux applicatifs et d'administration.
Le réseau de stockage/sauvegarde pour les besoins des centres informatiques repose, si possible, sur une architecture dédiée à cet effet.

8. Exploitation des SI

Ce paragraphe concerne les postes de travail fixes ou mobiles, les systèmes serveur et tous les autres systèmes (imprimantes, autres dispositifs en réseau, etc.).

8.1 Protection des informations sensibles

Les informations identifiées comme sensibles doivent faire l'objet de mesures précises pour garantir leur confidentialité et leur intégrité (ex : chiffrement poste et/ou dossiers, sauvegarde).

8.2 Sécurité des ressources informatiques

Seules les interventions majeures (ex : le changement d'un système d'exploitation (OS), d'une version majeure à une autre, le rajout d'OS en boot multiple ou en émulation avec une autre adresse IP) sur les systèmes sont consignées dans un tableau de bord SSI.
Sur les serveurs, en plus, le changement de versions majeures des composants essentiels en fonctions des services fournis (ex : version majeure de Samba sur serveur de fichiers, version 2.2 à 2.4 d'Apache sur serveur web majeur, etc.) seront indiquées dans le tableau de bord SSI.

La configuration standard des systèmes doit faire l'objet d'une installation consolidée, la procédure généraliste documentée succinctement mais précisément avec maintien à jour des évolutions dans le temps.

8.3 Gestion des autorisations et contrôle d'accès logique aux ressources

L'accès aux ressources non-publiques (poste de travail, partage réseau, site web collaboratif, etc.) doit se faire avec une authentification individuelle de l'utilisateur. Toute action d'autorisation d'accès d'un utilisateur à une ressource des SI doit se faire selon les règles établies dans l'unité, en s'appuyant sur les arrivées/départs du personnel.
Ainsi, la période de validité des accès et leur étendue (email, wifi, site intranet labo) en fonction du type de poste (membre permanent du laboratoire, stagiaire, visiteur, …) est établie selon des règles de base par défaut et les particularités aménagées selon les indications des responsables d'équipe et de la direction (modification durée, accès à des services spécifiques selon besoin, par exemple machines calcul, accès réseau par VPN, etc.).

Les informations d'authentification sont considérées comme des données sensibles et leur conservation ne se fait pas en clair mais elles sont chiffrées en conséquence (recommandations ANSSI). Chaque compte est créé avec un mot de passe aléatoire unique.

L'utilisation des certificats électroniques doit respecter les règles du Référentiel Général de Sécurité (RGS). Les certificats personnels ou non présents sur les postes ou serveurs sont des données sensibles, la protection contre le vol doit être mise en œuvre et documentée. L'obtention des certificats personnels ou autres se base sur les mécanismes mis à disposition par les tutelles.

Des méthodes de contrôle d'utilisation de mots de passe de qualité, lors de leur création, (longueur minimale, non-utilisation de mots de dictionnaire, utilisation minuscules/majuscules avec chiffres et/ou caractères spéciaux) doivent être mis en place sur les serveurs mais aussi sur les postes quand c'est possible ou le niveau de criticité du poste l'impose (gestion financière et personnel, gestion projets sensibles, etc.).

Les utilisateurs doivent avoir des mots de passe différents sur différents types de service (compte professionnel, comptes personnels, …) afin de limiter le risque en cas de fuite ou piratage sur un des services.

Pour les identifiants d'administration des serveurs ou postes critiques, des identifiants d'administration et les clés de chiffrage des disques/dossiers seront déposés sous séquestre en enveloppe scellée dans le coffre-fort ou armoire blindée de la direction.

Les personnes habilitées à administrer certains postes utilisés dans le travail scientifique (utilisateurs, ordinateur de commande/contrôle des expériences) peuvent être désignées par les R.E. (responsables d'équipe), selon les besoins spécifiques des équipes. Leur noms et machines en charge doivent être tenus à jour dans un tableau succinct en annexe à l'inventaire.
Chaque administrateur dispose de son propre mot de passe pour l'administration, et ne doit en aucun cas le communiquer.
Lors du départ d'un administrateur disposant de privilèges sur des composantes du SI, ses comptes d'administration doivent être clôturés et tous les mots de passe d'éventuels comptes de gestion partagés dont il avait connaissance doivent être changés.

8.4 Exploitation sécurisée des ressources informatiques

Les utilisateurs n'ont pas droit d'administration sauf exception dûment motivée et validée par le RSSI. Pour les postes, elle peut se faire par des administrateurs (cf. 8.3.), validation R.E.
Seul le personnel des métiers informatiques administre les serveurs généraux de l'unité, leur nom et étendue sont consignés sur une fiche SSI. L'accès aux outils d'administration s'effectue selon une désignation écrite dans le tableau de bord SSI. Les connexions doivent se faire par des protocoles sécurisés.

Étant donné les besoins des manipulations sur les postes utilisées pour la recherche, des personnes pouvant les gérer sont désignées selon besoin (cf. 8.3).
Pour les outils d'administration (interfaces), les noms des administrateurs et des interfaces auxquelles ils ont accès sont spécifiés dans un tableau de bord SSI. Ils sont validés par la direction. L'administration se fait

par protocole sécurisé (à défaut d'un réseau spécifique pour les salles machines).

Les données non chiffrées doivent être effacées avant l'envoi en maintenance externe de toute ressource informatique. Les opérations de chiffrement et les outils d'effacement doivent faire appel à des produits qualifiés (recommandés par les tutelles et approuvées par l'unité).

Lorsqu'une ressource informatique est amenée à quitter définitivement l'entité, les données (chiffrées ou non) présentes sur les disques durs ou la mémoire intégrée doivent être effacées de manière sécurisée. L'effacement des données et la sécurisation de l'espace libre doit s'appuyer sur des produits qualifiés (recommandés par les tutelles et approuvées par l'unité).

Tous les postes devant subir une réaffectation ou une mise au rebut doivent être traitées en accord avec le responsable du parc (sous son conseil ou par lui, selon ce qu'il préconise).

Tous les postes clients ou serveurs, doivent être équipés d'un logiciel de protection contre les codes malveillants (« antivirus »). Il s'agit de ceux préconisés par les tutelles et approuvés par le service informatique de l'unité.
Les mises à jour des bases antivirales et des moteurs d'antivirus doivent être déployées automatiquement sur les serveurs et les postes de travail par un dispositif mis en œuvre par le service informatique de l'unité (commun ou autonome selon les cas).
Les journaux d'événements de l'antivirus des serveurs doivent être conservés selon la réglementation en vigueur les concernant.

L'utilisateur d'un poste ne doit en aucun cas porter atteinte au fonctionnement du logiciel de protection (ex : désactiver les mises à jour, désactiver l'antivirus, etc.).
Des conseils pour un changement de configuration du navigateur web doivent être donnés par le service informatique lorsqu'on est averti d'un danger particulier (par exemple désactiver un nouveau service d'un navigateur comme Firefox qui serait compromettant, un système de recherche douteux, etc.).

Une politique de mises à jour des correctifs des OS et des logiciels le nécessitant (suite Office, navigateur…) doit être définie par le service gestionnaire du parc ; en principe les mises à jour de sécurité doivent être activées pour se faire automatiquement.
L'utilisateur d'un poste de travail ou d'expérimentation ne doit en aucun cas modifier le comportement du système de mise à jour de l'OS présent sur le poste et des logiciels. S'il n'y a pas de système de mises à jour automatique (ex : certains OS type Linux) l'administrateur du système doit les faire manuellement et de façon régulière.

Pour les cas des postes avec un OS obsolète (plus de mises à jour existantes), mais pour lesquelles il n'est pas possible de les migrer car ils gèrent un équipement matériel spécifique ou des programmes de commande bien particuliers, une isolation réseau (filtrage strict) doit être envisagée (à définir en collaboration avec la DSI), de même lorsque un antivirus actuel ne peut plus opérer sur un tel poste. La limitation d'une possible contamination par échanges par clé USB doit être prévue.

Les systèmes sont pourvus d'un mécanisme de journalisation des éventements de sécurité, ce système doit rester actif et pourra être analysé sur demande en cas d'incident.
Une politique de gestion des journaux d'événements des serveurs (sécurité, accès aux services, etc.) doit exister ainsi qu'une possibilité de les garder de manière sûre en cas de compromission quand c'est nécessaire (ex : centralisation journaux web ou accès externes). Ils doivent être conservés conformément à la législation en vigueur (actuellement 12 mois glissantes sauf autre contrainte particulière) et doivent pouvoir être fournies rapidement aux tutelles SSI en cas d'incident de sécurité le nécessitant. Des outils d'analyse statistique et de report d'alarme doivent être envisagées quand nécessaire (ex : très grand nombre de tentatives de connexion échouées par minute).

8.5 Défense des systèmes d'information

Les administrateurs des serveurs doivent analyser les journaux en vue de la détection des phénomènes techniques et de sécurité anormale. La détection des anomalies des flux réseau incombent à la DSI qui gère le réseau de l'Université Paris-Saclay.
Les postes informatiques sont fournis à l'utilisateur par l'unité et sont configurés et gérés par elle (à travers le service informatique gérant le parc). La connexion et l'utilisation d'équipement non maîtrisés, non administrés et non mis à jour par l'unité est interdite sur les réseaux restreints (hors réseau « invité »). Si des procédures spécifiques pour les collaborateurs sont nécessaires, elles seront établies par les équipes informatiques avec la direction et une fiche SSI établie et transmise au RSSI pour approbation.

Tout utilisateur (y compris invité) doit avoir un système antivirus à jour et opérant.

Pour les supports de données amovibles ou les équipements portables il est recommandé de chiffrer les données. Pour les données sensibles cela est obligatoire et les stockages amovibles doivent être stockés dans un meuble fermant à clé.

Toute perte ou vol de matériel (poste, stockage) doit être impérativement déclarée aux RSSI (Université Paris-Saclay et CNRS) et transmis au plus vite via le CSSI.

Pour les réaffectations, mises au rebut ou envoi en réparation à un tiers, la procédure de gestion des données des postes (effacement sécurisé) en vigueur dans l'unité doit obligatoirement être respectée.

Les usages possibles des équipements nomades pour le traitement des informations sensibles (ex : emails de travail incluant les échanges sur les projets sensibles) doit être établi par l'unité en accord avec les RSSI des tutelles. Pour accéder au réseau de l'unité, les utilisateurs doivent obligatoirement utiliser les portails et méthodes mises en place en accord avec la DSI (les accès VPN gérés par la DSI).

En cas de besoin éventuel concernant impression d'informations sensibles que la direction signalerait, une procédure spécifique sera définie en interne pour les machines envisagées (ex : récupération de la sortie d'impression après saisie d'un code).

8.6 Exploitation des centres informatiques (serveurs)

Les systèmes d'exploitation déployés doivent faire l'objet d'un support valide de la part d'un éditeur ou d'un prestataire de service. Seuls les services et applications nécessaires sont installés.
Les échanges de fichiers entre applications doivent privilégier les protocoles sécurisés (SSL/TLS, FTPS).
De façon à garantir un niveau de sécurité satisfaisant face aux attaques informatiques, des mécanismes de filtrage et de cloisonnement doivent être mis en œuvre.

Le service de noms de domaine utilise les serveurs de l'Université Paris-Saclay.
Afin d'assurer une cohérence dans les échanges entre applications ainsi qu'une traçabilité pertinente des événements techniques et de sécurité, les centres d'exploitation emploient une référence de temps commune (service NTP, Network Time Protocol). Il repose sur le service offert par la DSI.

Un cloisonnement entre les flux de supervision (remontée d'informations) et les flux d'administration (commandes, mises à jour) doit être mis en place.
L'accès aux supports informatiques amovibles fait l'objet d'un traitement adapté, plus particulièrement lorsqu'ils ont été utilisés pour mémoriser de l'information sensible ou lorsqu'ils sont utilisés pour des opérations d'exploitation. Une destruction adaptée sera faite avant mise au déchet.

Dans un centre informatique, le contrôle physique des accès réseaux, l'attribution des adresses IP, le filtrage des informations et l'usage de dispositifs spécifiques (machines virtuelles, cartes d'administration à distance, etc.) font l'objet de procédures sécurisées.

9. Sécurité du poste de travail

Les postes de travail sont configurés et gérés par l'équipe locale de l'unité en charge de la gestion du parc.

La configuration typique est définie dans un document succinct mais complet SSI. (ex : désactiver la recherche et l'exécution automatique lors de l'introduction d'un média (clé USB, DVD), interdiction du partage de connexion réseau ou du mode ad-hoc, etc).

Les boîtiers d'unités centrales sont de préférence verrouillés par cadenas. Les plus petites doivent être attachées par câble antivol. Les postes portables sont munis systématiquement d'un câble antivol et les utilisateurs sensibilisés à l'utiliser.

Les utilisateurs ne doivent pas travailler avec des comptes « administrateur » et le principe du « moindre privilège » s'appliquera. L'accès au compte « administrateur local » se limite aux personnes du service informatique en charge et en cas de besoin pour les postes utilisées à la recherche aux personnes désignées dans les équipes et notées dans un tableau SSI et tenu à jour.

Des partages réseau de travail sont mis à disposition des équipes et services et leur utilisation est encouragée. Pour certains services critiques (comme la gestion, les achats, la SSI), leur utilisation est convenue avec la direction. Une solution de sauvegarde chiffrée des données de travail sera proposée aux utilisateurs.

Les accès au SI de l'entité par les postes nomades doivent passer par les solutions mises en place par la DSI.
Les informations stockées sur les postes nomades doivent se limiter au strict nécessaire. Les informations sensibles doivent être chiffrées par une solution adoptée par l'unité.

Les possibilités d'usage dangereux des interfaces réseaux (filaire, wifi, Bluetooth, 3G) doivent être limités par les administrateurs et recensées dans un document SSI (ex : partage connexion wifi interdite, partages interdits, etc.).

La mise en place de services serveur est interdite (sauf accord exceptionnel des équipes informatique et de la direction) ex : (s)ftp, web, services DHCP, DNS, etc.

Les appareils réseaux comme copieurs multifonction, imprimantes, onduleurs, interfaces de gestion doivent avoir le mot de passe usine changé dès leur mise en place.

Les utilisateurs doivent utiliser un code personnel pour les postes téléphoniques, notamment pour la messagerie si c'est possible techniquement.

Dans le cas des terminaux téléphoniques GSM à usage professionnel, les conseils de l'équipe informatique doivent être suivis pour la protection physique (ex : pas de « root»-age, pas d'usage applications non absolument nécessaires, des réglages des paramètres de sécurité, un verrouillage par code ou schéma, ne pas désactiver le code pin/sim, etc.).
Un outil de vérification régulière de la conformité des postes pourra être prévu au sein de l'unité, dès que les tutelles les proposeront.
Il est convenu que la prise à distance d'écran (active ou passive) des postes de travail (fixes ou mobiles) n'est pas autorisée dans l'unité.

10. Sécurité du développement des systèmes

La SSI est à prendre en compte lors des développements de logiciels et systèmes concernant les accès publiques aux ressources (ex : application web, formulaire...). Le service à l'origine du développement a

l'obligation de suivre les recommandations existantes et de documenter leur implémentation par écrit. Sont exclus de cette catégorie les logiciels de calcul et de pilotage d'appareillage, à usage interne.
Les développements web en particulier doivent suivre les « règles de bonnes pratiques » et recommandation en vigueur (ex : méthodes de sécurisation des moteurs PHP, des propriétés par défaut des dossiers, etc.).

En cas d'appel à un sous-traitant, le respect des normes de développement sécurisées, le suivi de leur application, la production d'une documentation spécifique expliquant les choix d'implémentation (ex : codage et gestion de l'authentification, gestion des droits, chiffrement, etc.) et l'obligation du prestataire de corriger dans un temps raisonnable les erreurs, défauts, vulnérabilités qui lui seront remontées seront prévus par contrat. Il faut prévoir de demander aux prestataires la fourniture des sources dans les contrats chaque fois que cela est possible.
La diffusion des informations sur les logiciels ou composantes utilisées doit être limitée pour ne pas aider un attaquant (ex : désactiver l'affichage par défaut sur le web de la version de PHP ou du serveur web, version du CMS, etc.).

11. Traitement des incidents

Il est nécessaire de partager l'information (alertes, incidents, remises en état) dans la chaîne SSI dans le respect des règles de prudence.
La chaîne fonctionnelle SSI est informée par la chaîne opérationnelle de tout incident de sécurité, même dans le cas où il est apparemment mineur mais dont l'impact est susceptible de dépasser le SI de l'entité.
On doit tenir à jour un historique clair à propos de chaque incident et des suites lies à son éventuelle escalade.
Le signalement des incidents (ou possibilités d'incident) ainsi que l'évolution des événements doivent être communiqués de suite au CSSI de l'unité afin qu'il tienne informé à son tour la chaîne SSI.

12. Continuité d'activité

Un PCA (Plan de Continuité d'Activité) des SI est à établir entre les équipes informatiques et la direction pour les systèmes SI vitaux au fonctionnement de l'unité, en recensant ensemble les parties essentielles du SI à prendre en compte et les modalités d'y parvenir. Ce plan est à faire figurer dans les documents SSI de l'unité et sera transmis au RSSI. Ce plan doit permettre, dans un premier temps, de maintenir en mode dégradé les activités critiques, puis de récupérer et de restaurer toutes les fonctionnalités du système d'information.
Le CSSI s'assure de la bonne mise en œuvre des dispositions prévues dans le PCA des SI. Il organise des exercices afin de tester le PCA.

Les équipes informatiques mettent en œuvre les dispositifs techniques et les procédures opérationnelles contribuant à la continuité des SI, en assurent la supervision au quotidien et la maintenance dans le temps.
Les sauvegardes de données ne doivent pas être soumises aux mêmes risques de sinistres que les données sauvegardées. Elles doivent être traitées de manière à garantir leur confidentialité et leur intégrité.