BULLETIN OFFICIEL DES ARMÉES

Édition Chronologique

PARTIE PERMANENTE
Administration Centrale

INSTRUCTION N° 560/DEF/DCSSA/EPG/ECX
relative à la mise en œuvre de la sécurité informatique dans le service de santé des armées.

Du *27 août 1998*

DIRECTION CENTRALE DU SERVICE DE SANTÉ DES ARMÉES : *sous-direction études, planification, gestion ; bureau études générales, réglementation et contentieux.*

INSTRUCTION N° 560/DEF/DCSSA/EPG/ECX relative à la mise en œuvre de la sécurité informatique dans le service de santé des armées.

Du 27 août 1998 NOR D E

F G 9 8 5 4 0 7 7 J

Références :

Articles 226-13, 323-1 à 323-7 et 413-9 à 413-12 du code pénal. du 1er janvier 1999
Loi 78-17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (BOC, p. 4161) modifiée.
Instruction technique 230 /DEF/DCSSA/ETG du 30 décembre 1980 relative au secret professionnel médical dans les armées (BOC, p. 4925) modifiée.
Instruction n° 4418/DEF du 6 juillet 1981 relative à l'organisation de la sécurité informatique au sein du ministère de la défense (BOC, p. 4129).
Instruction n° 175/DEF/EMA/OL/2 - 237/DEF/DCSSA/ETG du 26 janvier 1982 relative au secret professionnel médical dans les armées (BOC, p. 832).
Instruction n° 605/DEF/DCSSA/EPG/ECX du 27 octobre 1993 relative à l'informatique et aux systèmes d'information et de communication dans le service de santé des armées (BOC, p. 5547).

Pièce(s) Jointe(s) :

Onze annexes.

Modifié par :

Erratum du 7 août 2012 (BOC N° 2 du 11 janvier 2013, texte 3).

Classement dans l'édition méthodique : BOEM 160.4.3, 620-0.1.5

Référence de publication : BOC, p. 3920.

SOMMAIRE

Préambule.

TITRE PREMIER. L'ORGANISATION DE LA SÉCURITÉ INFORMATIQUE.

Article premier. L'organisation de la sécurité informatique centralisée.

Article 2. L'organisation de la sécurité informatique dans les établissements.

TITRE II. LES MODALITÉS DE LA SÉCURITÉ INFORMATIQUE.

Article 3. Mesures de sécurité physique.

Article 4. Mesures de contrôle du personnel.

Article 5. Mesures de protection des données.

TITRE III. PROCÉDES D'ÉVALUATION DE LA SÉCURITÉ INFORMATIQUE.

Article 6. La traçabilité.

Article 7. Le schéma directeur de sécurité informatique.

ANNEXE(S)

ANNEXE I. CHARTE DE L'UTILISATEUR.

ANNEXE I BIS. ARTICLES 226-13, 323-1 A 323-7 ET 413-9 A 413-12 DU CODE PÉNAL.

ANNEXE II. MODÈLE DE NOTE D'INFORMATION POUR LES HOPITAUX DES ARMÉES.

ANNEXE III. MODÈLE DE FICHE D'INFORMATIONÀ APPOSER DANS LES SALLES D'ATTENTE DES CABINETS MÉDICAUX NON HOSPITALIERS ADAPTÉ DU TEXTE PROPOSÉ PAR LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS.

ANNEXE IV. RECOMMANDATIONS MINIMALESDE LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS SUR LES MESURES DE SÉCURITÉ LOGIQUE À ADOPTER POUR APPLICATIONS DE DONNÉES MÉDICALES FONCTIONNANT EN RÉSEAU.

ANNEXE V. CADRE GÉNÉRAL DU RAPPORT ANNUEL DE SÉCURITÉ INFORMATIQUE.

ANNEXE VI. CRITÈRES À RETENIR POUR LE CHOIX D'UNE SALLE INFORMATIQUE.

ANNEXE VII. MESURES À APPLIQUER EN MATIÈRE DE PROTECTION DES ÉLÉMENTS DU RESEAU, EN PARTICULIER DES COMPOSANTS ACTIFS.

ANNEXE VIII. MESURES A APPLIQUER EN MATIÈRE DE SAUVEGARDE DES DONNÉES.

ANNEXE IX. ÉVALUATION DES RISQUES D'ORIGINE HUMAINE.

ANNEXE X. PROCÉDURES DE TRANSFERTÀ METTRE EN ŒUVRE LORS DE LA MISE À JOUR DE PROGRAMMES OU DE DONNÉES DEPUIS LE SITE CENTRAL (CETIMA).

ANNEXE XI. FICHES SPECIFIQUES AUX HOPITAUX DES ARMEES.

Préambule.

Le développement croissant des moyens informatiques de toutes natures au sein des organismes du service de santé des armées et leur utilisation de plus en plus répandue sont la source de problèmes nouveaux et complexes en matière de protection des informations et des matériels.

Dans un tel contexte, la sécurité informatique a pour objet de préserver les informations transmises, conservées et traitées dans les systèmes informatiques de toute tentative de destruction, de falsification, de détournement ou d'utilisation frauduleuse et de s'opposer aux tentatives d'altération du fonctionnement normal des applications et des systèmes supports.

Volet particulier de la sécurité générale du service de santé des armées, elle relève de la responsabilité du commandement à tous les échelons et doit être prise en considération dès le stade de la conception des systèmes informatiques.

La sécurité informatique concerne tous les organismes du service mettant en œuvre des systèmes informatiques, les centres de traitement de l'information du service et leurs équipements d'extrémités, les responsables fonctionnels (maîtres d'ouvrage) et les réalisateurs (maîtres d'œuvre) d'applications et de programmes informatiques, ainsi que les voies et réseaux de télécommunications qui relient entre eux les organismes et personnels du service.

Elle s'applique à l'ensemble des éléments du système d'information, c'est-à-dire aux procédés destinés à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information (applications informatiques, ordinateurs, micro-ordinateurs portables, imprimantes, centraux et postes téléphoniques, serveurs, réseaux, télécopieurs, photocopieurs, minitel, ondes hertziennes et tout autre système de communication de données).

Elle s'applique aux informations ne relevant pas du secret défense, mais dont la destruction, la falsification, le détournement ou l'utilisation frauduleuse porterait atteinte aux intérêts du service, à son patrimoine scientifique et technique, ou à la vie privée ou professionnelle des individus qui font appel à lui. Elle concerne notamment les données relevant de la mention de protection « confidentiel spécifique » (données médicales, de gestion de personnel, de fournisseurs, etc.) mais aussi, par extension, toutes les applications informatiques du service traitant directement ou indirectement des informations nominatives.

Dans cette perspective, la présente instruction expose dans un premier temps les règles d'organisation de la sécurité informatique au sein du service de santé des armées (titre Ier), avant d'aborder dans un second temps les règles relatives à ses modalités concrètes (titre II) et d'examiner enfin quels en sont les principaux procédés d'évaluation (titre III).

TITRE PREMIER.
L'ORGANISATION DE LA SÉCURITÉ INFORMATIQUE.

Article premier.
L'organisation de la sécurité informatique centralisée.

I. ***LA COMMISSION DE L'INFORMATIQUE, DES SYSTEMES D'INFORMATION ET DE COMMUNICATION.***

Présidée par le directeur adjoint du service de santé des armées et composée :

- des sous-directeurs de la direction centrale du service de santé des armées (*DCSSA*) ;

- du chef de bureau systèmes d'information et de communication ;

- du commandant du centre de traitement des informations médicales des armées ;- de tout membre du personnel dont le président juge la participation opportune.

La commission de l'informatique, des systèmes d'information et de communication (*CISIC*) est chargée d'examiner les questions de sécurité informatique.

A cet effet, chacune de ses séances comporte un volet sécurité informatique et un volet sécurité des réseaux. Elle formule toutes propositions utiles qui sont soumises à la décision du directeur central du service de santé des armées.

II. ***LE BUREAU DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.***

Le bureau des systèmes d'information et de communication (*BSIC*) est chargé du contrôle de l'exécution des décisions en matière de sécurité informatique et de sécurité des réseaux prises par le directeur central du service de santé des armées sur proposition de la *CISIC*.

Lors de chaque séance de la *CISIC*, sur la base des rapports annuels transmis par les établissements du service, le *BSIC* rend compte des événements et contrôles survenus depuis la précédente séance, fait la synthèse de l'évaluation des risques, évalue les besoins en formation et propose toute mesure nécessaire en matière de sécurité informatique et de sécurité des réseaux.

III. ***LE CENTRE DE TRAITEMENT DES INFORMATIONS MÉDICALES DES ARMÉES.***

Le centre de traitement des informations médicales des armées (*CeTIMA*) exerce les missions ci-après définies sous le contrôle de la *DCSSA*.

Le *CeTIMA* est chargé de la mise en œuvre et de l'exploitation des moyens de liaison entre les différents établissements du service. Il peut être amené, sur décision de la *DCSSA*, à prendre en charge les accès vers d'autres réseaux des secteurs défense, publics ou parapublics (réseau santé social).

Dans le cadre du réseau spécifique au service de santé, il a la charge des lignes de transport et des équipements d'extrémité des réseaux inter-établissements. Il veille à assurer la sécurité spécifique de ces dispositifs de liaison, des données qui y transitent et de leur sauvegarde.

Il met en œuvre des dispositifs permettant de surveiller en permanence le fonctionnement des installations et d'apporter par télémaintenance, en cas de besoin, son aide technique aux établissements demandeurs.

Il assure, en liaison avec les organismes spécialisés des armées, une veille technologique des différents dispositifs de sécurité disponibles sur le marché, procède à leur évaluation et en rend compte à la *DCSSA*.

Lorsqu'il est chargé de la diffusion par télédistribution de logiciels du commerce et de ceux issus de développements, il utilise des procédures agréées en liaison avec les établissements destinataires, que ceux-ci soient ou non en connexion permanente avec le centre.

Lorsqu'il assure des opérations de télémaintenance sur ces logiciels à la demande des établissements ou sur avis motivé du *BSIC*, son personnel doit respecter les mêmes règles de confidentialité et de sécurité que les utilisateurs tels que définis à l'article 2, I, 3o. Ce personnel ne peut intervenir à distance qu'après avoir averti le responsable local concerné, avoir obtenu son accord et pris avec lui les mesures nécessaires.

Article 2.

L'organisation de la sécurité informatique dans les établissements.

I. ***RÈGLES D'ORGANISATION APPLICABLES À TOUS LES ÉTABLISSEMENTS.***

1. ***Le responsable local de la sécurité informatique.***

L'adjoint au chef d'établissement, nommé responsable local, est chargé de la sécurité informatique au sein de l'établissement. Pour l'accomplissement de ses missions, il est aidé des chefs de service, du correspondant local de sécurité informatique et des techniciens assurant le support des équipements et des applications. Il rend compte de ses actions au chef d'établissement et en obtient approbation.

Il fixe, conformément aux textes généraux en vigueur en la matière, les règles locales appropriées au contexte particulier de l'établissement (missions, applications, matériel…) ; il prend les mesures nécessaires au respect des règles de sécurité des systèmes d'information, veille à leur application et signale au chef d'établissement les manquements éventuellement constatés.

En application des décisions de la *DCSSA*, il initie et organise toutes les actions de conseil et de formation en matière de sécurité des systèmes d'information auprès des utilisateurs. Il adapte à chaque catégorie de personnel la formation relative aux procédures de sécurité et à leurs évolutions, modifications ou suppressions. Une attention toute particulière est portée à la formation du correspondant local de sécurité.

Il est chargé de l'information du personnel ainsi que, dans les hôpitaux des armées et les services médicaux d'unité, de celle des patients conformément aux directives de la commission nationale de l'informatique et des libertés.

Il définit la politique locale en matière de sauvegardes.

Il octroie et gère les droits d'accès aux diverses ressources informatiques de l'établissement. Dans les établissements hospitaliers, il octroie et gère ces droits d'accès en tenant compte des directives émises par le comité d'éthique et des expérimentations cliniques de l'établissement ; il transmet, temporairement et jusqu'à la mise en place d'une nouvelle architecture, la grille d'habilitation validée par ledit comité au *CeTIMA* pour exploitation.

Après approbation par le chef d'établissement, il transmet à la *DCSSA* (*BSIC*) le rapport annuel élaboré par le correspondant local de sécurité informatique. Cette transmission doit intervenir dans les délais compatibles avec les dates retenues pour les réunions de la *CISIC*.

2. ***Le correspondant local de sécurité informatique.***

Le correspondant local de sécurité informatique est désigné, après approbation de la *DCSSA*, par le chef de l'établissement en fonction de ses compétences techniques.

Il évalue les menaces et risques qui pèsent sur les informations, les équipements et les réseaux de l'établissement, adapte les mesures qui lui paraissent nécessaires et en rend compte au responsable local.

Il constitue le dossier de sécurité informatique de l'établissement et est chargé de sa tenue à jour et de sa conservation dans une zone protégée, sous le contrôle du responsable local. Il tient également les registres de maintenance et de dépannage et les registres relatifs aux sauvegardes du système d'information.

Il consulte régulièrement les journaux ou « mouchards » des différentes transactions effectuées dans les systèmes informatiques et en fait la synthèse pour le responsable local.

Annuellement, il rédige à l'attention du responsable local un rapport de sécurité informatique qui comporte une partie « sécurité informatique » et une partie « sécurité des réseaux ».

3. ***Les utilisateurs.***

Les utilisateurs sont les membres du personnel de l'établissement susceptibles d'utiliser les éléments du système d'information tels que définis en préambule.

Avant d'avoir le droit d'accéder aux ressources informatiques, tout utilisateur doit prendre connaissance des règles de sécurité informatique en vigueur dans l'établissement et signe la charte correspondante.

Chaque utilisateur veille à la bonne utilisation du matériel qui lui est confié et des données qu'il peut être amené à manipuler au travers des outils informatiques ; il veille à la mise à jour de son mot de passe ou de sa carte d'accès ; il veille à la protection des supports magnétiques amovibles de sauvegarde locale et à la diffusion des différents documents qu'il peut produire depuis son poste de travail.

En cas d'absence inopinée ou en présence d'un personnel non habilité, il fait en sorte que les informations affichées sur l'écran ne soient pas visibles. En dehors des heures ouvrables, son bureau doit être net de tout document, les portes fermées et les corbeilles à papier exemptes de tout document confidentiel.

Il tient le répertoire exact de la composition de sa configuration sur le plan du matériel et des logiciels (type d'équipement, numéro de série, nombre et nature des moyens de connexions extérieures) à destination du correspondant local de sécurité ; cet inventaire peut être une copie de celui fait par la cellule spécialisée de l'établissement. Il ne doit pas introduire dans sa configuration des données ou programmes étrangers à l'exécution de ses tâches habituelles.

Il lui est interdit, lorsqu'il dispose d'un poste de travail relié au réseau de l'établissement de se connecter à des réseaux externes à l'organisme sans autorisation écrite du responsable local. La connexion d'un poste isolé relève d'une autorisation identique. Il lui est interdit d'effectuer des copies des logiciels bureautiques ou d'exploitation, mis en place par l'organisme.

Lors des opérations de maintenance, tant matérielles que logicielles, il doit veiller à ce que les données confidentielles ne soient pas accessibles aux intervenants et en tout état de cause s'assurer qu'un personnel qualifié de l'établissement soit en permanence présent lors de ces opérations.

4. ***Le personnel technique.***

Le personnel technique est une catégorie particulière d'utilisateurs tels que le responsable d'exploitation, l'administrateur système, le gestionnaire de réseau, les administrateurs et programmeurs des applications informatiques.

Le personnel technique veille au bon fonctionnement technique des postes de travail, du réseau, des serveurs de fichiers, de communication, d'impression qui y sont connectés.

Pour les configurations collectives (serveurs divers, supports des systèmes gestionnaires de base de données…) et les équipements du réseau commun de l'établissement, il est chargé de l'exécution régulière des sauvegardes des données communes.

En tant qu'utilisateur, il est astreint aux mêmes contraintes de sécurité informatique que le reste du personnel de l'établissement.

Il signale au correspondant local de sécurité, en fonction des relevés pratiqués sur les différents postes de travail lors de ses interventions, l'existence éventuelle des logiciels non autorisés qui y seraient implantés.

Il tient à jour en permanence l'inventaire des équipements, dispositifs réseaux et logiciels installés sur toutes les configurations de l'établissement. L'utilisation de logiciels spécialisés de télésurveillance locale est organisée et tracée conformément à la réglementation spécifique en la matière (journal des accès).

Il rend compte régulièrement de ses actions et constatations au correspondant local de sécurité.

II. ***RÈGLES PARTICULIÈRES APPLICABLES A CERTAINS ÉTABLISSEMENTS.***

Le *CeTIMA*, le centre de recherches du service de santé (*CRSSA*), le service de radio-protection du service de santé (*SPRA*) et tous établissements du service de santé des armées qui sont amenés à traiter des informations classifiées, appliquent les directives générales du ministère de la défense dans ce domaine.

Ils sont tenus de désigner un officier de sécurité informatique chargé :

- d'établir et tenir à jour le dossier de sécurité informatique de l'établissement ;

- de participer et de préparer le travail de la commission d'homologation des centres informatiques du ministère de la défense ;

- d'évaluer en permanence les variations des risques et de déterminer les mesures à prendre pour y faire face.

Lorsqu'ils supervisent ou procèdent à des développements en tant que maîtres d'œuvre, ils doivent proposer aux maîtres d'ouvrage toutes les mesures qui pourront permettre d'assurer le fonctionnement en toute sécurité des applications en cours de réalisation afin de faciliter ultérieurement les tâches des utilisateurs dans le domaine de la sécurité informatique.

TITRE II.
LES MODALITÉS DE LA SÉCURITÉ INFORMATIQUE.

La sécurité informatique comprend trois objectifs essentiels qui sont la disponibilité, la confidentialité et l'intégrité du système et qui doivent être intégrés dès la phase d'achat et/ou de conception des éléments d'un système d'information et plus particulièrement en matière d'applications informatiques.

La disponibilité est l'aptitude du système à remplir une fonction dans des conditions définies d'horaires, de délais et de performance. Elle représente la continuité du service. A cet effet, la duplication du matériel sensible doit, dans toute la mesure du possible, être réalisée.

La confidentialité est la caractéristique du système d'information permettant l'accès à ses données aux seules personnes dûment autorisées. Sa mise en œuvre est réalisée grâce aux deux moyens que sont le contrôle d'accès et le chiffrement. Le contrôle d'accès comprend un ensemble de procédures d'identification, d'authentification et d'habilitation portant sur des utilisateurs, des matériels et des logiciels. Le chiffrement a pour but de rendre les données inintelligibles à toute personne ne possédant pas une clé convenue d'avance.

L'intégrité est la caractéristique qui garantit que les données n'ont pas subi d'altération et qu'elles ont conservé toute leur pertinence. Dans cette perspective, les sauvegardes permettent de pallier aux risques d'altération des données dont l'origine peut résider dans des erreurs de saisie, des malversations, des problèmes de logiciels, de matériels ou de réseaux.

La poursuite de ces objectifs se concrétise par des mesures de sécurité physique, des mesures de contrôle du personnel et enfin des mesures de protection des données.

Article 3.
Mesures de sécurité physique.

I. ***LOCAUX.***

Outre les moyens de protection contre les risques d'incendie, de survoltage, de variation de l'intensité du courant, des températures extrêmes, des fumées, de l'électricité statique…, les systèmes traitant des informations confidentielles doivent respecter les consignes suivantes :

- pendant l'absence du personnel, les locaux où se trouvent les postes de travail doivent être fermés à clé ; dans l'impossibilité, le poste de travail inutilisé au-delà d'une durée définie par le responsable local doit être mis hors tension ;

- les différentes clés des locaux ou des armoires à protéger doivent être tenues dans un endroit lui-même protégé, accessible aux seules personnes autorisées. Toute sortie de clé doit être contrôlée et les personnes autorisées doivent être désignées par le responsable local ;

- les locaux de plus grande vulnérabilité doivent être contrôlés par un système anti-intrusion et éventuellement équipés d'un système d'alarme ;

- les alarmes doivent être régulièrement vérifiées et testées, un rythme mensuel est souhaitable, un procès-verbal consignera les constatations ;

- les procédures de mise en et hors service des dispositifs d'alarme doivent être définies et connues d'un nombre restreint de personnes ;

- les procédures de réaction à une alarme (arrêt et remise en service, intervention, réparation, information du correspondant local de sécurité…) doivent être définies et régulièrement testées ;

- pour limiter les risques de compromission par rayonnement ou conduction parasites des informations confidentielles, il convient d'utiliser des matériels respectant les normes de compatibilité électromagnétique en vigueur et de les installer selon leurs recommandations spécifiques. Les postes de travail, les unités de traitement, les terminaux connectés ou non, les imprimantes doivent notamment être situés le plus loin possible des lieux ouverts au public.

II. ***EMPLACEMENTS.***

Les emplacements où sont installés les postes de travail, ceux des serveurs de communication et de fichiers et ceux où sont conservés les supports de données et de programmes doivent être différents et séparés.

Ces différentes zones doivent être protégées en fonction de la confidentialité des données et de la valeur stratégique des matériels et des applications (serveurs, supports de sauvegarde et autres éléments-clés du réseau tels que modems, répartiteurs, routeurs…).

III. ***MATÉRIEL.***

Tous les éléments matériels du système d'information doivent être identifiés et cette identification doit être unique. Tous les fichiers d'informations confidentielles doivent être répertoriés. Un inventaire complet des éléments du système d'information doit être réalisé une fois par an ; si un matériel a disparu, le correspondant local de sécurité en est immédiatement averti.

1. ***Installation, branchement.***

L'installation, le branchement et la première mise en route de l'équipement s'effectuent en présence du correspondant local de sécurité.

Les imprimantes et les unités centrales peuvent être pourvues de scellés placés de façon telle qu'une intervention physique soit immédiatement apparente.

Afin d'éviter le vol, les claviers peuvent être verrouillés en cas de non-utilisation, les postes de travail peuvent être fixés à la table et la mise sous tension verrouillée. Certains micro-ordinateurs peuvent être équipés de cadenas incorporés afin d'éviter une ouverture du boîtier de l'unité centrale. Ces mesures prennent davantage d'importance si un disque non amovible est utilisé.

Les écrans des postes de travail doivent, dans la mesure du possible, être disposés de telle sorte qu'ils ne puissent être vus par des personnes non habilitées. En particulier, il convient d'éviter que les écrans soient positionnés face à une fenêtre ou une porte. En la présence de personnes non habilitées, les écrans sont effacés, mis en veille ou éteints.

2. ***Maintenance et dépannage.***

La maintenance préventive est une opération qui doit être prévue dès l'achat de tout élément du système d'information. Les travaux de maintenance doivent s'effectuer en présence de l'utilisateur du poste de travail et sous la surveillance d'un personnel technique ; ces travaux sont consignés dans un registre spécifique tenu par le correspondant local de sécurité.

Le recours à la télémaintenance est soumis à autorisation particulière du responsable local, qui en définit les modalités par écrit.

La mise en place d'un système de surveillance informatique contrôlant en permanence le réseau est préconisée.

Toute panne et toute opération de dépannage (déclenchement, intervention, remise en route) doivent être consignées sur un registre spécifique et propre à l'installation, tenu par le correspondant local de sécurité. Les travaux de dépannage doivent s'effectuer en présence de l'utilisateur du poste de travail et sous la surveillance d'un personnel technique.

Lors d'une intervention de dépannage, l'utilisateur doit prendre toutes mesures utiles telles que l'effacement des mémoires, la mise en sécurité des fichiers, l'effacement des informations confidentielles, etc. Si le retour en usine s'impose et que des informations confidentielles ou classifiées ne peuvent pas être effacées d'un support fixe, le personnel technique chargé de surveiller le dépannage doit détruire le support.

Article 4.
Mesures de contrôle du personnel.

I. ***L'IDENTIFICATION.***

Tout le personnel de l'établissement doit être répertorié dans un annuaire. Le responsable local octroie et contrôle les droits d'accès aux informations du système, c'est-à-dire dresse la liste nominative des personnes ayant le droit d'accéder à telle zone protégée, à telle catégorie de données et délivre les postes de travail en conséquence. Par ailleurs, il établit, tient à jour et diffuse la liste des membres du personnel de l'établissement autorisées à accéder au système en dehors des heures normales de service.

Outre les utilisateurs de l'établissement, il y a lieu de prendre en considération diverses personnes extérieures à l'établissement telles que les prestataires de services informatiques, les vacataires, les stagiaires, le personnel de maintenance et de dépannage, le personnel de nettoyage et enfin les visiteurs.

Ces personnes doivent être dûment informées des contraintes inhérentes à la sécurité informatique et des sanctions encourues. Compte tenu des risques liés à leur présence, le responsable local ne leur délivre que des autorisations d'accès temporaires, éventuellement renouvelables. En principe, l'accès de ces personnes aux zones protégées est interdit, sauf autorisation expresse du responsable local ; en ce cas, l'accès aux zones protégées requiert l'accompagnement d'un membre du personnel de l'établissement habilité par le responsable local et le port d'un badge distinctif.

II. *L'AUTHENTIFICATION.*

1. *Modalités.*

L'authentification permet de garantir que la personne ayant déclaré une identité est bien celle qu'elle prétend être. Elle peut être obtenue à partir de plusieurs moyens, résumés en trois méthodes de base, allant de la plus vulnérable à la plus solide :

- la méthode relative à ce que connaît la personne (mot de passe, code confidentiel…) ; - la méthode relative à ce que détient la personne (carte à piste magnétique, carte à puce…) ; - la méthode relative à ce qu'est la personne (caractéristiques biométriques…).

La protection par mot de passe est d'une efficacité limitée mais doit néanmoins être systématiquement utilisée dans l'attente de la mise en œuvre de solutions plus fiables (carte de professionnel de santé « *CPS* »…). Le mot de passe doit être secret, difficile à reconstituer par un tiers (6 caractères alphanumériques au minimum), limité dans le temps, non réutilisable et modifiable par l'utilisateur. Il ne doit pas être inscrit dans les scripts de connexions automatiques et ne doit pas être transféré sans nécessité sur les lignes de transmission. Il doit être changé régulièrement selon une périodicité si possible imposée par le système. Une périodicité mensuelle est acceptable.

2. *Précautions d'usage.*

Dans le cas d'un poste de travail connecté à un réseau et d'une demande d'accès à des ressources distantes, les deux interlocuteurs doivent être authentifiés, même si l'un des deux est un serveur. Le terme « interlocuteur » est ici entendu largement : il peut s'agir d'un individu, d'un logiciel, d'un matériel, d'un serveur… Cette authentification doit être mutuelle et garantie de bout en bout à travers le réseau. Dans le cas d'un poste autonome, seule l'authentification de l'utilisateur local est nécessaire.

Les systèmes d'exploitation comportent généralement des procédures d'accès privilégiés utilisées notamment pour le démarrage du système. La protection des accès à ces procédures doit faire l'objet d'une vigilance particulière, notamment en personnalisant fortement le mot de passe.

Il est souhaitable que tous les postes de travail connectés à un même système utilisent les mêmes procédures d'authentification.

La seule authentification en début de session ne suffit pas à garantir l'absence d'intrusions. En effet, l'utilisateur peut être amené à quitter son poste de travail en oubliant de clore la session et laissant ainsi l'accès à une tierce personne. En ce cas, il y a lieu de prévoir une déconnexion automatique après temporisation, une détection de l'enlèvement du support d'authentification et éventuellement une réauthentification périodique du support voire de l'utilisateur afin de parvenir à une authentification continue.

III. *L'HABILITATION.*

L'habilitation est le procédé permettant d'accorder à une personne le droit d'effectuer une action précise (création, consultation, modification, suppression…). Accordée par le responsable local, elle ne peut en aucun cas être définitive.

Deux niveaux d'habilitation se superposent : l'accès aux éléments matériels et logiciels du système d'information et l'accès aux données.

1. ***L'accès aux éléments matériels et logiciels.***

Une habilitation est nécessaire pour l'accès aux éléments du système d'information traitant d'informations confidentielles ainsi qu'aux éléments stratégiques du système (serveurs, routeurs, répartiteurs, autocommutateurs) de même que pour l'accès aux comptes « systèmes » des serveurs et routeurs. Les commandes « systèmes » ne doivent pas être accessibles aux utilisateurs. Les modems doivent être fermés en dehors des connexions.

Il est recommandé de ne proposer à l'utilisateur que l'environnement correspondant aux ressources (matériels, modules logiciels) pour lesquelles il a reçu une habilitation. Les personnes extérieures à l'établissement intervenant sur le système d'information doivent être habilitées.

Au niveau des autocommutateurs ou des serveurs de communication, il doit être fait appel si possible à des procédures logiques de déconnexion automatique au bout de quelques tentatives d'accès infructueuses.

Il est conseillé d'utiliser les facilités offerts en termes de sécurité par les réseaux, par exemple les groupes fermés d'abonnées du réseau *TRANSPAC*.

En cas d'interconnexions de réseaux, il est conseillé d'utiliser de préférence des passerelles de niveau 3 selon le modèle « open system interconnexion » (*OSI*).

2. ***L'accès aux données.***

Les utilisateurs sont répartis en catégories leur autorisant diverses opérations sur des données préalablement classées par nature (confidentiel médical, confidentiel personnel…). Tout accès non autorisé doit être impossible. Il est interdit d'utiliser les connexions et droits d'accès attribués à un autre utilisateur, même s'il appartient à la même catégorie de droit d'habilitation.

Les utilisateurs ne peuvent demander que les habilitations qui leur sont nécessaires. Ils ne doivent pas tenter de naviguer sur des fichiers qui ne les concernent pas ou de s'octroyer des droits d'accès privilégiés. En cas d'accès involontaire à des domaines étrangers à leurs fonctions, ils doivent terminer la session inutile et en alerter le correspondant local de sécurité.

L'accès du personnel technique de l'établissement ou de prestataires de services informatiques aux bases réelles doit être exceptionnel et rigoureusement contrôlé par le responsable local.

L'utilisation d'un système de messagerie à l'intérieur d'un établissement doit correspondre à son objet, faciliter la diffusion de l'information et améliorer la communication. Elle ne doit pas être déviée vers des besoins personnels ni vers l'échange de données confidentielles. A ce titre, une politique de contrôle est définie par le responsable local et mise en œuvre par le correspondant local de sécurité assisté du personnel technique.

Les systèmes qui mettent en liaison plusieurs établissements et qui entrent dans le cadre dit de « groupware » ne peuvent être mis en œuvre qu'après désignation par le responsable local d'un personnel technique chargé de son bon fonctionnement.

Article 5.

Mesures de protection des données.

I. ***LE CHIFFREMENT (où sécurité cryptographique).***

Compte tenu de la grande vulnérabilité aux intrusions qu'offrent en particulier les circuits téléphoniques, les lignes spécialisées, *NUMERIS* ou *TRANSPAC* et nouvellement les réseaux mondiaux de type INTERNET, il convient de sécuriser le système par le moyen du chiffrement.

Les informations confidentielles ne peuvent être transmises « en clair » que sur des circuits approuvés au niveau considéré. On appelle « circuit approuvé » un circuit dont les extrémités ainsi que les éventuels points de coupure sont maîtrisés, et dont le parcours est entièrement en zone contrôlée.

Le niveau d'approbation accordé au circuit dépend essentiellement du niveau de sécurité le plus faible sur tout son parcours. En règle générale, les circuits internes à un établissement peuvent être approuvés pour transmettre des informations confidentielles.

En l'absence de tels circuits, la protection des informations confidentielles doit être assurée par un moyen de chiffrement, sauf dérogation explicite et précise de l'autorité habilitée à cet effet.

L'acquisition de ces équipements de chiffrement doit faire l'objet pour les organismes de l'administration, d'une demande d'avis adressée au service central de la sécurité des systèmes d'information. Cette procédure pour le service de santé est mise en œuvre par le *BSIC*.

Les autres informations n'exigent pas la mise en œuvre de mesures de sécurité cryptographiques, sauf éventuellement en ce qui concerne les procédures d'authentification et de contrôle d'intégrité.

Les moyens de chiffrement, qu'ils soient autonomes ou intégrés aux équipements, doivent faire l'objet d'une gestion spécifique. Les clés de chiffrement sont à protéger tout particulièrement.

II. ***LES SAUVEGARDES.***

1. ***Supports de sauvegarde.***

Les supports contenant des informations confidentielles doivent être signalés par un moyen propre défini par le responsable local. Par exemple, les disquettes et bandes magnétiques sont repérées par une pastille de couleur dont la signification ne doit pas être divulguée, les éditions portent une mention « DIFFUSION RESTREINTE », « CONFIDENTIEL MEDICAL », « CONFIDENTIEL PERSONNEL »…

Il est recommandé de ne pas conserver de fichiers contenant des données confidentielles sur disques fixes, mais d'utiliser des supports amovibles.

Il est également recommandé de ne pas mélanger sur un même support des informations de niveaux de protection différents ; dans le cas contraire, le support portera un repère correspondant à la protection maximale des informations contenues.

Tous les fichiers sur supports magnétiques transmis à l'extérieur de l'établissement doivent être enregistrés sur des supports neufs.

Etant fragiles et sensibles à la poussière, aux éraflures, aux sources magnétiques, les supports doivent être rangés dans des boîtes appropriées, elles-mêmes stockées dans un endroit sûr, conforme à leur niveau de protection :

- les supports d'information non en cours d'utilisation (disquettes de logiciels de base, sauvegardes) doivent être conservés dans une armoire fermée à clé.

- les supports des données confidentielles doivent être stockés dans une zone spécifique et protégée, séparée du poste de travail.

Les documents en cours d'élaboration doivent être protégés de la même manière que ceux en exploitation.

Toutes les éditions d'informations confidentielles (exemplaires excédentaires, états erronés,…) doivent être détruits selon la procédure définie par le responsable local.

Sur les supports fixes et amovibles, les fichiers périmés contenant des données confidentielles doivent être effacés. Cette destruction ne doit pas être uniquement logique (suppression dans la liste des fichiers) mais doit être accompagnée d'un effacement physique pour prévenir toute lecture des secteurs non réalloués.

Les supports magnétiques amovibles contenant des données confidentielles et/ou classifiées doivent être effacés dès qu'ils ne sont plus utilisés ou lorsqu'ils vont être jetés. Le procédé d'effacement doit aller en cas de nécessité jusqu'à interdire la reconstitution de l'information initiale par analyse des résidus.

2. ***Procédures de sauvegarde.***

Les procédures de sauvegarde (réalisation, conservation, centralisation) sont définies par le responsable local en fonction des particularismes propres à chaque établissement et dans le respect des principes énoncés ci-après.

Généralités. Toutes les sauvegardes doivent être planifiées, leur réalisation mentionnée dans les registres tenus par le correspondant local de sécurité et leur conservation effectuée dans un local distinct de ceux contenant un poste de travail.

Durant leur manipulation, les supports de données confidentielles sont sous la surveillance de la personne habilitée et leurs mouvements doivent faire l'objet d'un enregistrement afin d'identifier à tout moment les détenteurs.

Chaque utilisateur doit tenir à jour et contrôler périodiquement l'inventaire des supports dont il a la charge.

La périodicité des sauvegardes est directement liée au rythme de modification du fichier. L'objectif à viser est que, en cas d'indisponibilité définitive du fichier en cours, le fichier sauvegardé ait une utilité significative pour la reprise des travaux.

Logiciels. Dès leur acquisition ou leur conception, le responsable local veille à la sauvegarde des logiciels (programmes d'application et systèmes d'exploitation).

Par la suite, une nouvelle sauvegarde est faite à l'issue de toute modification du logiciel, et au moins une fois par an.

Les règles d'accès aux fichiers sauvegardés se conforment à celles précédemment énumérées à l'article 4 point III *supra* de la présente instruction.

Pour garantir leur qualité, les sauvegardes doivent être testées régulièrement. En cas de panne, des tests d'intégrité des fichiers doivent être effectués. En cas d'incident réel ou présumé sur un fichier, celui-ci est reconstitué à partir des sauvegardes.

En cas de catastrophe (inondation, incendie…), les conditions de remise en route du système d'information dépendent de l'état constaté des installations, comprennent la reconstitution du système à partir des logiciels et fichiers sauvegardés, vérifiés et validés et dépendent surtout des procédures de fonctionnement en mode dégradé et de reprises définies dans le schéma directeur de sécurité informatique évoqué à l'article 7 *infra.*

III. ***LES ATTAQUES LOGIQUES.***

Les attaques logiques ont pour effet l'introduction d'informations parasites mettant en péril les données, voire l'ensemble du système d'information (virus…).

1. ***Généralités.***

Quelle que soit leur nature (système d'exploitation, logiciel d'application spécifique…) et sauf s'ils sont créés par l'utilisateur lui-même, les logiciels ne doivent être approvisionnés qu'auprès de fournisseurs agréés après approbation par le responsable local. Ils doivent être testés avant leur mise en service.

Un poste de travail ne doit jamais être utilisé à des fins autres que prévues. Les logiciels publicitaires ou de jeux sont interdits.

2. ***Fonctionnement anormal.***

En cas de fonctionnement anormal, l'utilisateur en rend compte immédiatement au correspondant local de sécurité et prend les mesures suivantes :

- déconnexion du poste de travail et de ses périphériques immédiats de toutes liaisons sur le réseau et éventuellement de toutes liaisons vers l'extérieur sans coupure de l'alimentation électrique ; - contrôle par un personnel technique des sauvegardes réalisées sur ce poste de travail.

Le travail ne peut reprendre sur ce poste qu'après accord du responsable local.

IV. ***CONTROLE D'INTÉGRITÉ.***

La gestion de la configuration d'un système ou d'un réseau informatique consiste à identifier, contrôler, enregistrer et vérifier toutes les modifications apportées au cours des phases de la conception, du développement, de la maintenance et de l'amélioration. Il est à noter que cette gestion doit englober tous les éléments du système y compris ceux de l'exploitation et de l'application ainsi que les matériels, micro logiciels et logiciels qui ont un rapport avec la sécurité.

Le contrôle d'intégrité doit entre autres englober les contrôles suivants :

- contrôles applicables aux modifications relatives à la spécification, à la conception, à la documentation de mise en œuvre, aux dispositifs d'essais,… ;

- contrôles applicables à la comparaison d'un système nouvellement créé, y compris les programmes utilitaires et les logiciels, avec la version précédente, afin de vérifier que seuls les changements prévus ont été effectués ;

- contrôles destinés à assurer que la version actuelle du système correspond toujours à la documentation et au programme associé ;

- contrôles applicables à la protection contre toute modification ou destruction non autorisée, de l'original ou de copies de tous les éléments servant à créer le système, y compris les programmes utilitaires et les logiciels.

TITRE III.
PROCÉDES D'ÉVALUATION DE LA SÉCURITÉ INFORMATIQUE.

Article 6.
La traçabilité.

A tout moment, le responsable local doit être en mesure de connaître si les objectifs de disponibilité, de confidentialité et d'intégrité ont bien été atteints et quelles ont été les actions susceptibles de nuire au système d'information qui ont été menées. A cet effet, les informations recueillies signalent l'identité de l'auteur et les moyens utilisés pour réaliser ces actions.

Les journaux doivent être adaptés aux besoins et, par l'intermédiaire de filtres et de seuils d'alerte, mettre en évidence les informations significatives.

Pour les applications informatiques, le niveau de détail doit permettre de différencier les actions de création, de consultation et de modification.

Tous les événements « réseau » et en particulier les connexions externes doivent être journalisées. Les actions réussies (sessions établies, transferts réussis) tout comme les échecs (refus de connexion, échec d'authentification) et les tentatives d'accès sont enregistrées.

Article 7.

Le schéma directeur de sécurité informatique.

Le dossier de sécurité informatique, constitué par le correspondant local de sécurité, est élaboré à partir du schéma directeur de sécurité informatique. L'élaboration du schéma directeur de sécurité informatique consiste à analyser en premier lieu les moyens de sécurité actuels de l'établissement, en second lieu les risques auxquels il peut être confronté et enfin les moyens à mettre en œuvre pour limiter, voire annihiler ces risques.

L'analyse concrète des moyens de sécurité existants est conditionnée par l'environnement spécifique à chaque établissement ; il n'est pas possible de la retracer dans un texte à portée générale tel qu'une instruction. En revanche, la présente instruction se propose d'établir une méthode d'analyse des risques potentiels utilisable quel que soit l'établissement concerné.

I. *ANALYSE DES RISQUES POTENTIELS.*

L'analyse des risques se traduit par la détermination de scenarii types représentant un lien de causalité entre un fait générateur et un résultat préjudiciable potentiel. Un même scénario type doit, pour chaque établissement, être décliné en fonction de ses moyens propres (entités, sites, locaux, domaines techniques…).

1. *Définition du risque.*

Le risque représente un danger ou un inconvénient plus ou moins probable pour le système d'information. Il est le résultat de la combinaison d'une part des vulnérabilités du système et d'autre part des menaces auxquelles ce système peut être confronté. Il peut avoir des répercussions directes ou indirectes (pertes financières, image de marque, perte de fiabilité, poursuites pénales…).

Les vulnérabilités sont des faiblesses, des failles intrinsèques au système d'information et pouvant porter sur chacun de ses éléments (le personnel, le matériel, l'organisation, les traitements et les télécommunications).

Les menaces sont des phénomènes extrinsèques, intentionnels ou accidentels, ayant pour cible le matériel ou les données.

2. *Détermination d'un scénario type.*

Le point de départ du raisonnement est la description du résultat préjudiciable, car il est le phénomène le plus aisé à constater. Ce préjudice peut revêtir la forme d'une détérioration concrète ou d'un dysfonctionnement.

Le second temps du raisonnement est la description du fait générateur du préjudice, c'est-à-dire de l'événement qui en a déclenché la réalisation immédiate. Enfin, il est souhaitable dans un troisième temps d'affiner encore l'analyse en remontant jusqu'à l'origine du fait générateur lui-même.

Exemple :

Le résultat préjudiciable « Altération des données d'un fichier » est constaté.

La seconde étape de l'analyse conduit aux hypothèses causales suivantes :

- « Erreur de saisie. »

- « Erreur de transmission. »

- « Dégradation du support des données. »

- « Erreur de programmation. »

Si la cause du dommage est, par exemple, la dégradation du support des données, la troisième étape conduit aux origines suivantes :

- « Vieillissement ou pollution. »

- « Dégradation physique pendant un transport. »

- « Dégradation physique pendant l'exploitation. »

- « Réécriture partielle sur un support. »

Si l'origine est, par exemple, la dégradation physique pendant un transport, on aboutit ainsi au scénario type suivant :

- « Altération des données d'un fichier » =>

- « Dégradation du support des données » =>

- « Dégradation physique pendant un transport ».

II. *UTILISATION DES SCENARII TYPES.*

La méthode d'utilisation des scenarii-types s'inspire des techniques utilisées dans des secteurs aussi divers que la défense nationale ou les assurances (*MELISA*, *MARION*, *AROME-Q*…).

Tous les scenarii types susceptibles d'intéresser l'établissement doivent être rassemblés, pondérés, puis classés en fonction de leur degré de nuisance. Ce classement permet de déterminer quels sont les risques majeurs pour l'établissement et, parmi eux ou à travers leur accumulation, le risque maximal admissible.

Le risque majeur est celui qui est susceptible de mettre l'établissement dans l'incapacité d'accomplir sa mission.

Le risque maximal admissible, c'est le niveau de perte, le seuil en-deçà duquel l'établissement peut encore continuer à accomplir cette mission.

III. *DÉTERMINATION DES MESURES DE SÉCURITÉ À PRENDRE.*

Les mesures de sécurité à mettre en œuvre sont celles permettant de maintenir les risques constamment en dessous du seuil maximale admissible. Ces mesures sont sélectionnées en fonction de l'audit des moyens dont dispose l'établissement et de ses contraintes propres.

En tout état de cause, en cas de survenue d'un sinistre majeur, le fonctionnement du système d'information en mode dégradé et les solutions de reprise (changement de matériel, doublement des équipements) doivent toujours être intégrés, ainsi que le plan d'évacuation et de destruction d'urgence (documents à conserver, à détruire…).

L'analyse globale des risques et des mesures de rétroaction est retracé dans le schéma directeur de sécurité informatique aboutissant ainsi à la définition de la politique de sécurité de l'établissement.

Pour le ministre de la défense et par délégation :

Le médecin général, sous-directeur études, planification, gestion,

Jérôme GUELAIN.

ANNEXE I.

CHARTE DE L'UTILISATEUR.

Je soussigné(e) *(grade, nom, prénom)* :

Service d'affectation :

Fonction :

reconnais avoir pris connaissance et obtenu copie :

- des dispositions légales et réglementaires relatives au secret professionnel médical ;

- des dispositions légales et réglementaires relatives aux données informatiques nominatives ;

- des articles 226-13, 323-1 à 323-7 et 413-9 à 413-12 du code pénal (cf. ANNEXE I bis),

et m'engage à respecter les consignes de sécurité suivantes :

1. Prendre toute précaution pour ne pas introduire de code parasite *(virus…)* dans les machines et mettre en œuvre tout moyen pour protéger mon poste de travail contre de telles intrusions.

2. En cas d'absence, quitter l'application qui se trouve sur ma station de travail ou éteindre mon micro-ordinateur si je travaille sur un poste isolé. En aucun cas ne laisser cet outil avec un programme nominatif lancé.

3. Ne pas laisser circuler des personnes étrangères au service dans les bureaux.

4. Choisir, gérer, garder secret et changer fréquemment mon mot de passe.

5. Prendre toute précaution pour contrôler mon travail avant validation, pratiquer les sauvegardes nécessaires et quitter l'application selon les procédures en vigueur.

6. Ne demander que les attributions ou les habilitations nécessaires.

7. Ne pas entreprendre d'actions telles que : tentative d'octroi de droits d'accès privilégiés, tentatives d'intrusion dans les applications qui ne me sont pas ouvertes.

8. Respecter la plus stricte confidentialité sur toute information à laquelle j'accède durant mes travaux et ne pas enregistrer de données confidentielles sur le disque local du poste de travail ou sur celui du serveur.

Date et signature de l'intéressé, Visa du chef de service,

ANNEXE I BIS.

ARTICLES 226-13, 323-1 A 323-7 ET 413-9 A 413-12 DU CODE PÉNAL.

Art. 226-13. « La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 100 000 francs d'amende. »

Art. 323-1. « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 100 000 francs d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 200 000 francs d'amende. »

Art. 323-2. « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 300 000 francs d'amende. »

Art. 323-3. « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de trois ans d'emprisonnement et de 300 000 francs d'amende. »

Art. 323-4. « La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

Art. 323-5. « Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1. L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26.

2. L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise.

3. La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution.

4. La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés.

5. L'exclusion, pour une durée de cinq ans au plus, des marchés publics.

6. L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent des retraits de fonds par le tireur auprès du tiré ou ceux qui sont certifiés.

7. L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article131-35. »

Art. 323-6. « Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.

Les peines encourues par les personnes morales sont :

1. L'amende, suivant les modalités prévues par l'article 131-38.

2. Les peines mentionnées à l'article 131-39.

L'interdiction mentionnée au 2o de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de laquelle l'infraction a été commise. »

Art. 323-7. « La tentative des délits prévus par les articles 323-1 à 323-3 est punie des mêmes peines. »

Art. 413-9. « Présentent un caractère de secret de la défense nationale au sens de la présente section les renseignements, procédés, objets, documents, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de protection destinées à restreindre leur diffusion.

Peuvent faire l'objet de telles mesures les renseignements, procédés, objets, documents, données informatisées ou fichiers dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale.

Les niveaux de classification des renseignements, procédés, objets, documents, données informatisées ou fichiers présentant un caractère de secret de la défense nationale et les autorités chargées de définir les modalités selon lesquelles est organisée leur protection sont déterminées par décret en conseil d'Etat. »

Art. 413-10. « Est puni de sept ans d'emprisonnement et de 700 000 francs d'amende le fait, par toute personne dépositaire, soit par son état ou sa profession, soit en raison d'une fonction ou d'une mission temporaire ou permanente, d'un renseignement, procédé, objet, document, donnée informatisée ou fichier qui a un caractère de secret de la défense nationale, soit de le détruire, détourner, soustraire ou de le reproduire, soit de le porter à la connaissance du public ou d'une personne non qualifiée.

Est puni des mêmes peines le fait, par la personne dépositaire, d'avoir laissé détruire, détourner, soustraire, reproduire ou divulguer le renseignement, procédé, objet, document, donnée informatisée ou fichier visé à l'alinéa précédent.

Lorsque la personne dépositaire a agi par imprudence ou négligence, l'infraction est punie de trois ans d'emprisonnement et de 300 000 francs d'amende. »

Art. 413-11. « Est puni de cinq ans d'emprisonnement et de 500 000 francs d'amende le fait, par toute personne non visée à l'article 413-10 de :

1. S'assurer la possession d'un renseignement, procédé, objet, document, donnée informatisée ou fichier qui présente le caractère d'un secret de la défense nationale.

2. Détruire, soustraire ou reproduire, de quelque manière que ce soit, un tel renseignement, procédé, objet, document, donnée informatisée ou fichier.

3. Porter à la connaissance du public ou d'une personne non qualifiée un tel renseignement, procédé, objet, document, donnée informatisée ou fichier. »

Art. 413-12. « La tentative des délits prévus au premier alinéa de l'article 413-10 et à l'article 413-11 est punie des mêmes peines. »

ANNEXE II.

MODÈLE DE NOTE D'INFORMATION POUR LES HOPITAUX DES ARMÉES.

Afin de faciliter votre accueil dans les différents services de l'hôpital, une carte personnelle porteuse ou non d'un « code barres » vous est remise. Cette carte ne contient que les données imprimées en clair. Elle permet, grâce à votre numéro de patient, une reconnaissance sûre par le système informatique de l'hôpital (système *AMADEUS*).

Les fichiers informatiques de l'hôpital sont plus complets et comprennent :

- des informations administratives, en particulier celles concernant les organismes assurant votre couverture sociale. Vous pouvez connaître la teneur exacte de ces informations, en vous adressant au service des hospitalisations et soins externes (*SHSE*). Il est d'ailleurs de votre intérêt qu'elles soient exactes afin de vous éviter d'avoir à supporter un paiement personnel éventuel. Il vous appartient donc, en cas de dépassement de la date mentionnée au verso et dans la partie supérieure droite de la carte, de faire mettre à jour votre dossier par le *SHSE* de l'hôpital. Cette date est identique à celle de la fin des droits portée sur votre carte d'assuré social ;

- des informations médicales, qui vous sont accessibles dans les mêmes conditions que celles portées sur le dossier médical traditionnel.

Conformément aux dispositions de la loi informatique et libertés (A) tout renseignement concernant votre dossier pourra être obtenu sur requête auprès de la :

Direction centrale du service de santé des armées

Bureau des systèmes d'information et de communication

14, rue Saint-Dominique

00459 Armées

Téléphone : 01-41-93-25-21 — Fax : 01-41-93-29-35.

(A) Articles 26, 27, 34 et 40 de la loi 78-17 du 06 janvier 1978 , relative à l'informatique, aux fichiers et aux libertés.

ANNEXE III.

MODÈLE DE FICHE D'INFORMATIONÀ APPOSER DANS LES SALLES D'ATTENTE DES CABINETS MÉDICAUX NON HOSPITALIERS ADAPTÉ DU TEXTE PROPOSÉ PAR LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS.

Ce cabinet médical dispose d'un ordinateur destiné à gérer plus facilement le fichier de ses patients (et à réaliser, le cas échéant, des travaux statistiques) ceci dans le strict respect du secret médical, sont également enregistrées des données relatives à votre aptitude qui pourront être communiquées au commandement.

Sauf opposition de votre part, certains renseignements vous concernant, recueillis au cours de votre consultation ou de votre hospitalisation pourront faire l'objet d'un enregistrement informatique réservé exclusivement à l'usage médical.

Conformément à la déontologie médicale et aux dispositions de la loi informatique et libertés, votre médecin traitant se tient à votre disposition pour vous communiquer ces renseignements ainsi que toutes informations nécessaires sur votre état de santé.

Tout médecin désigné par vous peut également prendre connaissance de l'ensemble de votre dossier médical.

Conformément aux dispositions de la loi informatique et libertés (A) tout renseignement concernant votre dossier pourra être obtenu sur requête auprès de la :

Direction centrale du service de santé des armées

Bureau des systèmes d'information et de communication

14, rue Saint-Dominique

00459 Armées

Téléphone : 01-41-93-25-21 — Fax : 01-41-93-29-35.

(A) Articles 26, 27, 34 et 40 de la loi 78-17 du 06 janvier 1978 , relative à l'informatique, aux fichiers et aux libertés.

ANNEXE IV.

RECOMMANDATIONS MINIMALESDE LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS SUR LES MESURES DE SÉCURITÉ LOGIQUE À ADOPTER POUR APPLICATIONS DE DONNÉES MÉDICALES FONCTIONNANT EN RÉSEAU.

1. RECOMMANDATIONS GÉNÉRALES.

1.1. **Modalités d'authentification des utilisateurs.**

La gestion des mots de passe.

Le code utilisateur individuel doit être distinct du nom de l'utilisateur.

Le mot de passe individuel doit être d'une longueur minimale imposée d'au moins six caractères alphanumériques.

En cas de mot de passe choisi par les utilisateurs, instauration au niveau du système d'une table des mots de passe interdits (par exemple : nom ou date de naissance des utilisateurs ; mots de passe courants type : *SESAME*, nom de l'organisme).

Interdiction de réutiliser un des trois derniers mots de passe.

Le personnel technique ne doit pas avoir la possibilité de lire les mots de passe. En cas de perte, il ne peut travailler que par remplacement.

1.2. **Modalités de connexion et de déconnexion.**

Impossibilité pour les utilisateurs de se connecter sous le même code utilisateur et le même mot de passe (interdiction des « login » génériques).

Indication systématique aux utilisateurs lors de la connexion, sous forme d'un affichage à l'écran des dates et heures de la dernière connexion sous les mêmes code utilisateur et mot de passe.

Journalisation des connexions.

En cas de frappes incorrectes successives du mot de passe (associé à un code utilisateur correct), invalidation du code utilisateur ou tout au moins déconnexion, blocage prolongé de l'accès et message demandant à l'utilisateur d'appeler le responsable du système.

Procédure de déconnexion automatique en cas de non-utilisation du système pendant un temps donné (time out).

Utilisation dans la mesure du possible de cartes à mémoire ou dispositifs analogues.

1.3. **La confidentialité des données.**

Utilisation dans la mesure du possible du codage des données nominatives.

Cryptage de tout ou partie des données dans le cadre de la réglementation française et européenne en vigueur.

En cas de connexion d'un des serveurs du réseau, sur un réseau international ouvert, type INTERNET, instauration de mesures de sécurités appropriées (par exemple, séparation physique des deux réseaux, ou de mise en place de « fire-walls » : barrières de protection logicielles).

1.4. **L'intégrité des données.**

Mise en place de protocoles de transmission adaptés permettant de vérifier la conformité des données reçues à celles émises.

En cas de numérisation et de compression de l'image, utilisation de procédés qui permettent de garantir l'intégrité de l'image.

2. RECOMMANDATIONS COMPLÉMENTAIRES EN FONCTION DE L'ARCHITECTURE DUTRAITEMENT.

Dans la mesure du possible, séparation des réseaux de gestion administrative et de suivi médical.

2.1. **En cas d'architecture client-serveur.**

Prendre les dispositions nécessaires pour gérer le rapatriement des données ou le transfert de fichiers sur micro-ordinateur en fonction des habilitations de chacun : limitation du transfert de fichiers complets, limitation du volume des informations rapatriées, journalisation des requêtes au niveau du serveur.

Restriction d'accès aux données en fonction des habilitations.

Limiter et contrôler la copie des informations sur les périphériques externes, recours à des disquettes formatées.

2.2. **Liaisons et serveurs télématiques.**

2.2.1. ***Les liaisons télématiques.***

Utilisation de dispositifs qui ne permettent la connexion que de sites distants reconnus (par exemple, groupement fermé d'abonnés sur le réseau X25 ; identification du numéro appelant en cas de recours au *RNIS*).

En cas de transfert de données par messagerie, utilisation de messageries sécurisées, permettant, notamment, le cryptage de certaines données.

2.2.2. ***Les serveurs télématiques.***

Implantation du serveur dans un local professionnel réservé à l'usage médical, sous la responsabilité d'un médecin garant de la sécurité physique et logique des données médicales.

Numéro de téléphone d'appel ou code d'accès au serveur ne figurant pas dans un annuaire public.

En cas de transmission de données médicales par le réseau téléphonique commuté (*RTC*), utilisation de codes secrets permettant de restreindre l'utilisation de certaines lignes aux utilisateurs habilités.

ANNEXE V.
CADRE GÉNÉRAL DU RAPPORT ANNUEL DE SÉCURITÉ INFORMATIQUE.

I. LE VOLET DE SÉCURITÉ GÉNÉRALE.

Le rapport doit aborder les principaux points concernant :

- l'organisation mise en place ;

- les actions menées,

et leurs résultats sur les plans :

- de la disponibilité de principaux systèmes d'information mise en œuvre dans l'établissement ;

- de la confidentialité des données traitées ;

- de l'intégrité des informations manipulées.

Des tableaux de synthèse pourront éventuellement être définis par le *BSIC*.

1. **Actions d'organisation.**

Composition et objets des réunions des intervenants de l'établissement en matière de sécurité informatique.

Composition et objet des réunions d'information et de sensibilisation.

Documentations diverses de sécurité informatique.

2. **Suivi des procédures.**

Suivi des inventaires des matériels et des logiciels.

Mise en place des documents de suivi de configuration.

Contrôle des sauvegardes.

Examens des journaux, mouchards et registres.

3. **Résultats.**

Pannes majeures : nombre, motifs, actions entreprises.

Vols d'équipements : nombre, motifs, actions entreprises.

Destruction d'équipements : nombre, motifs, actions entreprises.

Contrôles logiques (antivirus) : nombre d'anomalies.

Vérifications des données : des journaux :

- nombre d'anomalies apparentes ;

- nombre de vérifications approfondies ;

- nombre de « malversations » relevées :

- conduites suivies ;- sanctions.

4. **Conclusion** sur l'état de la sécurité informatique dans l'établissement incluant des propositions en vue de son amélioration.

II. LE VOLET DE SÉCURITÉ DES RESEAUX.

1. **Structure du réseau local.**

Type, nombre et fonctionnalité des serveurs.

Nombre de stations de travail connectées.

2. **Implantation du ou des serveurs dans l'établissement.**

Situation des locaux.

Protection d'accès aux locaux contenant des serveurs.

Vulnérabilités résiduelles.

Actions entreprises au cours de l'exercice de référence.

Actions futures planifiées.

3. **Protection des serveurs et des stations de travail.**

Gestion des mots de passe d'identification et protocole d'identification.

Périodicité de changement des codes d'accès (mots de passe).

Type d'antivirus implanté sur les stations et serveurs (nom et no de version).

Périodicité des mises à jour de la base de signature des virus.

Problèmes rencontrés (à détailler éventuellement), actions entreprises.

Améliorations éventuelles proposées.

4. **Suivi de l'activité.**

Pannes majeures : nombre motifs et actions entreprises.

Exploitation des journaux d'activité (périodicité et actions entreprises en cas de problème détecté).

5. **Sauvegardes des données et logiciels.**

Description succincte des procédures utilisées (périodicité, type de support, etc.).

Problèmes rencontrés.

Améliorations éventuelles proposées.

ANNEXE VI.

CRITÈRES À RETENIR POUR LE CHOIX D'UNE SALLE INFORMATIQUE.

1. OBJECTIFS.

L'infrastructure de la cellule d'exploitation informatique d'un établissement, doit présenter un seuil minimal de sécurité pour répondre à l'objectif fondamental qui est d'assurer la pérennité de l'outil informatique.

La démarche consiste dans ce domaine, à s'assurer que l'étude des risques faite lors de la construction de la salle informatique, ou *a posteriori*, ce qui est le cas le plus fréquemment rencontré (locaux existants), a débouché sur la mise en place de protections permettant d'éviter les sinistres, de réduire leurs conséquences et de garantir la continuité de l'activité. Dans ce dernier cas de figure, les éléments de cette fiche sont destinés à faciliter le choix de mesures correctives à appliquer qui seront à adapter en fonction des contraintes liées à l'infrastructure existante.

2. ÉLÉMENTS DETERMINANTS À PRENDRE EN COMPTE.

Le local informatique doit permettre de réaliser facilement la limitation des accès et le contrôle des issues périmétriques.

Sa situation au sein de l'établissement doit être déterminée, de telle manière que l'environnement dans lequel fonctionne le matériel et où opère le personnel soit exempt des pollutions majeures suivantes :

- particules en suspension dans l'air (cas rencontré par une proximité des ateliers par exemple,…) ;

- lieu exempt de vibrations, de magnétisme : la proximité d'une machinerie d'ascenseur qui peut générer des pollutions de ces deux types, ou d'un générateur de forte puissance (radiologie) ;

- lieu ne présentant pas dans son environnement immédiat de risques d'incendie (proximité d'un endroit de stockage de produits inflammables) ;

- température et hygrométrie des locaux inadaptées.

S'assurer que des études techniques ont résolu les éléments de sécurité relatifs :

- à la protection contre l'incendie (compartimentage des volumes, isolation appropriée, résistance au feu des matériaux), à l'évacuation des personnes, à la sécurité de la charpente et des toitures, à l'évacuation des fumées, à l'existence de prises d'eau,… ;

- à la protection contre l'eau : imperméabilité des locaux, drainage adéquat des eaux de pluies,… ;

- à la protection contre la foudre et les risques électriques : paratonnerre, prises de terre, disjoncteurs,… ;

- à la résistivité inférieure à 5 Ohms de la prise de terre, ce qui est la référence de beaucoup de machines informatiques.

S'assurer que le bâtiment permet l'installation aisée de dispositifs de sécurité destinés :

- à la détection de l'incendie ;

- à la détection et l'évacuation des eaux ;

- à l'aménagement de faux planchers et de faux plafonds ;

- au conditionnement de l'air (nécessité d'une installation de climatisation ou simple extraction d'air destinée à réguler température et hygrométrie de la salle ;

- à la possibilité de disposer d'une alimentation électrique stable ;

- aux possibilités de raccordement simple aux réseaux de télécommunications (répartiteurs) ;

- à la protection des accès, tout en tenant compte du volume et du poids des équipements à installer.

L'équipement des locaux, en terme de matériels et d'installation, doit respecter les contraintes suivantes :

- respecter la normalisation des chemins de câble : c'est un gage de minimisation des risques liés aux interventions à distance sur ces équipements ;

- respecter la distance préconisée entre le passage des conducteurs véhiculant des « courants faibles »et des « courants forts » ;

- choisir des équipements répondant à la norme *CEM* (compatibilité électromagnétique) ;

- mise en œuvre de dispositifs de secours de l'alimentation électrique.

ANNEXE VII.

MESURES À APPLIQUER EN MATIÈRE DE PROTECTION DES ÉLÉMENTS DU RESEAU, EN PARTICULIER DES COMPOSANTS ACTIFS.

ÉLÉMENTS À PRENDRE EN COMPTE.

Les éléments du réseau, en particulier les éléments actifs, qui sont répartis sur l'emprise de l'établissement sont des composants déterminants du système informatique. Leur fonctionnement peut être perturbé par des causes physiques, liées le plus souvent à l'alimentation en énergie électrique, mais également par des menaces dues à des actions humaines accidentelles ou malveillantes.

Les causes, rencontrées plus fréquemment en pratique, sont les suivantes :

- panne d'alimentation d'un composant actif du réseau entraînant un dysfonctionnement variable déterminé par sa fonction et sa place dans le réseau de l'établissement ;

- panne électrique d'un équipement indépendant du réseau mais dont l'alimentation est commune avec un composant actif ;

- destruction d'un port par branchement intempestif d'un matériel non compatible ;

- modification accidentelle ou malveillante de la configuration logicielle d'un composant actif, qui englobe des fonctions de sécurité ;

- accès à un répartiteur ou tout autre « nœud » du réseau et écoute par connexion illicite (utilisation d'une prise libre de l'équipement, par exemple).

MESURES À APPLIQUER.

Fermer à clé tout local « Télécom », toute armoire de répartiteur ou de sous-répartiteur d'étage. Lors d'intervention sur ces composants, un personnel compétent de l'établissement doit accompagner le technicien. Il lui permet l'accès physique aux ressources et veille à la mise en sûreté au décours de l'intervention. Durant l'opération il doit être vigilant sur les actions menées. Un registre des interventions doit être établi et tenu.

Veiller sur le plan de l'alimentation électrique des composants actifs du réseau, à la dispersibilité d'une alimentation spécifique secourue par onduleur indépendant.

Contrôler impérativement que d'autres appareils ne soient pas branchés en parallèle sur la même ligne.

Prévoir un dispositif limitant les surtensions.

Disposer d'un plan du câblage toujours actualisé.

Veiller scrupuleusement à l'inactivation des prises, et de toute entrée potentielle inutilisée.

Veiller à l'activation des fonctions de filtrage des composants actifs.

Contrôler régulièrement que la fonction d'administration des équipements actifs est verrouillée.

Assurer un audit régulier du bon fonctionnement de l'ensemble.

Le correspondant local a pour mission de surveiller le fonctionnement du réseau ; en cas de dysfonctionnement, il alerte le responsable local. Si le dysfonctionnement dépasse ses compétences techniques, le correspondant local s'adresse au *CeTIMA* ou à la société externe mandatée par la *DCSSA* pour assurer le support et le conseil en matière de réseau et de composants.

ANNEXE VIII.

MESURES A APPLIQUER EN MATIÈRE DE SAUVEGARDE DES DONNÉES.

1. ÉLÉMENTS À PRENDRE EN COMPTE.

La destruction accidentelle ou malveillante, d'un serveur de données ou d'un poste de travail, conduit dans le premier cas à l'indisponibilité des applicatifs et des données supportées par ce serveur, et dans le second à une perte de données, voire également d'applications qui sont le fruit d'un travail personnel. La perte de ces informations peut être définitive si les sauvegardes ne sont pas fiables.

Bien traitées sur les grands systèmes, objet de tâches courantes bien planifiées, les sauvegardes sur les postes de travail sont souvent insuffisantes voire même inexistantes :

- ne sont pas réalisées périodiquement mais seulement faites quand le personnel technique y pense ;

- sont incomplètes et ne prennent en compte qu'une partie des unités de stockage et donc des données ;

- ne sont pas validées et ne peuvent être relues lorsqu'une restauration est nécessaire.

Vécues le plus souvent comme une contrainte imposée par l'emploi de l'informatique, leur utilité n'est comprise souvent que lorsqu'il est trop tard !

2. MESURES À APPLIQUER.

Il appartient aux responsables de la sécurité et aux techniciens de sensibiliser les utilisateurs à l'intérêt et à la nécessité de réaliser des sauvegardes des données de façon systématique.

Des vérifications régulières s'assureront que ces mesures sont toujours appliquées dans le temps, aussi bien que sur les serveurs communs que sur les postes de travail individuels.

2.1.

Sauf disposition contraire donnée pour une application informatique, les sauvegardes seront réalisées alternativement sur un ensemble de supports différents. Trois jeux de supports permettent cette pratique qui a pour objectif d'autoriser la reprise des données, en cas d'incident, dans l'état où elles se trouvaient lors de la précédente sauvegarde (J — 1) et si un des supports de ce jeu était défaillant, il serait possible de repartir dans l'état de l'avant-dernière sauvegarde (J — 2) et en cas de besoin de la sauvegarde de l'avant-veille (J — 3).

2.2.

L'exécution de la procédure de sauvegarde doit être surveillée, l'absence de message « système » au cours et au terme de la procédure doit toujours laisser supposer à l'exploitant que la sauvegarde ne s'est pas déroulée correctement. Il lui appartient de renouveler la tentative sur le même jeu ou un jeu vierge si un support est suspect de défaillance. Jamais le jeu de la précédente sauvegarde (J — 2 et J — 3) ne doit être utilisé. La tenue d'un registre par serveur, comportant l'identification des supports employés et, le cas échéant, des incidents rencontrés, est obligatoire.

2.3.

Régulièrement, la fiabilité des informations sauvegardées doit être vérifiée. L'utilisation de commandes « systèmes » si elle permet d'apprécier l'existence des fichiers (ils sont « reconnus par le système ») ne permet pas de juger de la pertinence des données contenues dans ces fichiers. Dans le cadre des serveurs de l'établissement, une procédure, définie par le responsable technique de l'applicatif (*CeTIMA*), qui teste les possibilités de restauration, est à mettre en œuvre, sous son couvert, dans la mesure où elle n'est pas intégrée dans l'applicatif.

ANNEXE IX.

ÉVALUATION DES RISQUES D'ORIGINE HUMAINE.

Même s'il est souvent difficile dans la réalité de faire la différence entre un acte involontaire et l'intention délibérée de nuire, on peut toutefois distinguer :

I. LES ÉVÉNEMENTS ACCIDENTELS.

Anomalies dans la conception ou la modification d'un logiciel créant d'importantes perturbations avant que l'erreur ne soit localisée et corrigée.

Erreurs dans l'exploitation d'un système par introduction, par exemple, d'une commande erronée pouvant conduire à une perte de données.

Erreurs de paramétrage d'une application entraînant des perturbations dans la bonne marche d'un service.

Erreurs de saisie entraînant des répercussions immédiates et à distance (*ex. :* erreur d'attribution de données d'une personne à une autre).

II. LES DÉPARTS ET DÉMISSIONS DU PERSONNEL.

Les mouvements du personnel ayant développé des applicatifs insuffisamment documentés et ne respectant pas les normes du service peuvent conduire à des pertes d'exploitation en raison de l'impossibilité de corriger rapidement les programmes. Les données peuvent être également affectées.

III. LES ACTES DÉLICTUEUX.

3.1. **Vol. Sabotage matériel.**

Les vols d'écrans, d'imprimantes, de micro-ordinateurs d'autant qu'il s'agit de matériels portables, de disquettes et autres supports de données, de documentation sont les risques les plus fréquemment rencontrés.

3.2. **Détournement d'informations.**

Consultation illégale de données, voire copie de celles-ci avec une suite d'actions délictueuses pouvant résulter de leur utilisation.

3.3. **Détournement de logiciels.**

Ce type de malversation est en très forte augmentation avec l'essor de la micro-informatique. Il peut s'agir de copies illicites des logiciels mis en place dans le cadre du travail pour un usage privé, voire une revente…

3.4. **Fraude.**

Accès à des services et usage frauduleux de ceux-ci à partir des stations de travail.

3.5. **Sabotage immatériel.**

Mise en place de bombes logiques ou virus (programme de falsification ou de destruction qui, inséré dans un programme normal, va altérer son fonctionnement lors de l'apparition d'une condition particulière de déclenchement).

L'introduction d'un programme contaminé par un virus sur une station de travail peut, à l'image de son homologue biologique, se propager de proche en proche par le réseau et aboutir au blocage complet d'un

système. Le recours aux sauvegardes peut s'avérer vain puisque dans le cas habituel elles ont été préalablement contaminées.

IV. CONDUITE À TENIR.

Il est illusoire de vouloir dresser une liste exhaustive de toutes les menaces d'origine humaine qui planent sur un système d'information, « l'état de l'art » en la matière étant en perpétuelle évolution. Ces menaces s'exercent sur des vulnérabilités ou défauts de protection primaire ou résiduelle (après application de mesures de sécurité) des systèmes.

En conséquence, le correspondant local de sécurité du site devra s'efforcer, de déterminer le plus objectivement possible les menaces qui lui semblent pouvoir s'appliquer au système dont il a la charge, en précisant leur nature, les vulnérabilités du système sur lesquelles elles s'appuient, les moyens d'attaque, techniques ou non, nécessaires à leur réalisation effective et, compte tenu du profit que peut escompter l'attaquant, les moyens qu'il acceptera de consacrer à cette attaque.

Afin de faciliter cette tâche, les tableaux ci-après dressent une synthèse des principales menaces rencontrées, et de leurs conséquences potentielles au regard des vulnérabilités induites par les composants du système :

4.1. **Vulnérabilités liées au câblage et moyens physiques.**

Menaces.	**Atteinte disponibilité.**	**Atteinte intégrité.**	**Atteinte confidentialité.**
Rupture accidentelle ou malveillance d'un média.	Réseau.		
Dysfonctionnement par erreur de câblage (connexion illicite d'un équipement sur un élément du réseau auquel il ne devrait pas avoir accès, …).	Réseau.	Configuration.	
Ecoute par exploitation des rayonnements (capture d'écrans d'impressions ou d'informations numériques).			Données.
Ecoute par branchement d'une connexion illicite (« bretelle »).			Données.
Ecoute par analyse du trafic sur le réseau (*ex. :* branchement illicite sur une prise du réseau).			Données.

4.2. **Vulnérabilités liées aux équipements de télécommunication.**

Menaces.	**Atteinte disponibilité.**	**Atteinte intégrité.**	**Atteinte confidentialité.**
Destruction d'un port par connexion d'un équipement non compatible.	Réseau.		
Modification accidentelle ou malveillante de configuration.	Réseau.	Données.	
Altération du réseau par coupure inter-étages ou inter-bâtiments.	Réseau.		
Dysfonctionnement par conflit adresses réseau suite à raccordement illicite.	Réseau.		
Utilisation malveillante des outils de traces internes.		Données.	Données.
Relecture malveillante des disques portant des informations sensibles.			Données.
Interconnexion non sécurisée de réseaux hétérogènes pouvant conduire à une perte de confidentialité d'informations sensibles.	Réseau, données.	Données.	Données.

4.3. **Vulnérabilités liées aux serveurs et postes de travail.**

Menaces.	**Atteinte disponibilité.**	**Atteinte intégrité.**	**Atteinte confidentialité.**
	Service.		
Modification accidentelle ou malveillante des configurations.			
Intrusion logique sur le réseau.	Service, données.	Service, données, sécurité.	Données.
Intrusion via les accès extérieurs sur serveur de communications.	Réseau.	Données.	Données.
Blocage volontaire ou accidentel des accès extérieurs.	Réseau.		
Intrusion sur un compte utilisateur d'un serveur.	Données.	Données.	Données.
Intrusion sur un compte administrateur d'un serveur.	Service, données.	Service, données, sécurité.	Données.
Configuration malveillante d'un mot de passe de démarrage (« boot ») des stations.	Service, données.		
Infection informatique.	Service, données.	Service, données.	
Dysfonctionnement des sauvegardes.	Données.	Données.	
Accès illicite aux disques locaux d'une station d'administration.		Données.	Données.
Détournement des résultats d'une impression.			Données.
Agression des serveurs via leur console.	Service, données.	Service, données.	Données.

ANNEXE X.

PROCÉDURES DE TRANSFERTÀ METTRE EN ŒUVRE LORS DE LA MISE À JOUR DE PROGRAMMES OU DE DONNÉES DEPUIS LE SITE CENTRAL (CETIMA).

1. CONTEXTE D'UTILISATION.

La mise à jour des programmes et des données communes est rendue nécessaire dans les cas suivants :

1.1.

A la demande du site qui a relevé un dysfonctionnement et dont les premières investigations et/ou contact avec un personnel du *CeTIMA*, font apparaître un besoin d'intervention des techniciens sur le système de l'établissement.

1.2.

A la demande du *CeTIMA* afin de mettre à jour des programmes installés sur un serveur du site (prise en compte des fonctionnalités nouvelles ou corrections d'anomalies) ou des tables communes de données (*CIM* 10, *CDAM*,…).

Cette opération est réalisée grâce à une liaison téléinformatique directe entre l'établissement et le *CeTIMA* par l'intermédiaire d'un réseau national militaire ou public.

2. MODALITÉS DE MISE EN ŒUVRE.

2.1. **Préalables.**

Quelle que soit sa finalité, l'opération est subordonnée à un accord préalable des deux parties confirmé par échanges de télécopies ou par messagerie.

Cet accord ne peut être échangé qu'après validation explicite du maître d'ouvrage de l'application et de l'organisme chargé de sa qualification, qui informe auparavant les établissements des caractéristiques de la nouvelle version.

2.1.1.

Ces échanges précisent les motifs de l'intervention, les dates et heures de celle-ci ainsi que sa durée prévisible. Le *CeTIMA* devra préciser les opérations préalables nécessaires à l'échange (fichiers à sauvegarder, purge des fichiers temporaires, exécution de programmes particuliers,…).

2.1.2.

L'établissement procède à ces opérations et particulièrement à la réalisation des sauvegardes nécessaires.

2.1.3.

Dans les deux cas ci-dessus le responsable local doit habiliter le technicien chargé de l'opération en lui attribuant les droits correspondant au profil de cette catégorie de personnel ainsi qu'un mot de passe temporaire, conditions indispensables pour lui permettre d'accéder au système cible. En fonction de l'urgence ce dernier échange doit utiliser la modalité la plus adaptée.

2.2. **Avant l'intervention.**

Valider la liaison physique en :

- mettant le modem en service (commutateur en position « ON ») et brancher la fiche téléphonique dans la prise, dans le cas de liaison effectuée via le réseau *RTC* (réseau téléphonique commuté) ; - ou en vérifiant que le modem *TRANSPAC* est opérationnel.

2.3. **Au décours de l'intervention.**

2.3.1.

L'opération est terminée lorsque le technicien rend le contrôle du système à l'établissement.

2.3.2.

Couper la liaison physique en mettant le modem en position « *OFF* » et en débranchant la fiche de la prise téléphonique dans le cas de l'utilisation du réseau *RTC*.

2.3.3.

Supprimer ensuite l'habilitation du technicien du *CeTIMA*.

2.4. **Validation et contrôle des opérations.**

2.4.1.

Il appartient au site, avant de redistribuer les données et programmes transmis de contrôler l'intégrité des données ou la validité des nouveaux programmes (erreurs de transmission). Il est souhaitable pour cela qu'il dispose d'une configuration de test, machine de référence de l'établissement.

2.4.2.

Dans le cas contraire avertir le *CeTIMA* et préparer une nouvelle exécution de la procédure.

2.4.3.

Rendre compte à l'organisme de qualification des opérations réalisées et des résultats.

2.4.4.

Vérifier qu'une fiche d'intervention a bien été adressée par le *CeTIMA* décrivant les opérations réalisées, en référence aux décisions du maître d'ouvrage.

2.4.5.

Contrôler régulièrement les « journaux » d'exploitation des serveurs afin de vérifier leur concordance avec les interventions connues. Ceci est particulièrement important dans le cas de liaisons par *TRANSPAC*, où le modem reste constamment en fonction.

ANNEXE XI.

FICHES SPECIFIQUES AUX HOPITAUX DES ARMEES.

A) FICHE D'UTILISATEUR SYSTEME D'INFORMATION HOSPITALIERE.

Création.	Modification.	Suppression.
☐	☐	☐

Partie à remplir par l'intéressé(e) :

NOM : ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Prénom : ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ Date de naissance :

Service :

Unité fonctionnelle : Secteur :

Date d'affectation :

Grade (rayer les mentions inutiles) :

Officier général.
Officier supérieur.
Officier subalterne.
Sous-officier supérieur.
Sous-officier subalterne.
Militaire du rang.
Autre (précisez) :

Type de fonction et emploi occupé (rayer les mentions inutiles) :

Médical :
- responsable comité éthique ;
- consultant expert ;
- chef de service ;
- médecin ;
- médecine des collectivités.

Paramédical :
- surveillant ;
- infirmier ;
- infirmier de consultation ;
- élève ;
- diététicien ;
- kinésithérapeute ;
- manipulateur radio ;
- paramédical autre.

Administratif :
- secrétaire médical ;
- secrétaire administratif ;
- personnel CAG ;
- personnel SHSE ;
- personnel des archives ;
- autre personnel administratif.

Partie à remplir par le chef de service :

Signature autorisée : oui ☐ non ☐

Rendez-vous : oui ☐ non ☐

Réalisation actes : oui ☐ non ☐

Niveau d'administration (rayer les mentions inutiles) :

Utilisateur simple.	Environnement médical.	Administrateur service.

Date début des droits : Date fin des droits :

Matériels du service sur lesquels la personne est autorisée :

N° SSA.	N° SSA.	N° SSA.	N° SSA.	N° SSA.	N° SSA.
N° SSA.	N° SSA.	N° SSA.	N° SSA.	N° SSA.	N° SSA.

Signature de l'intéressé, *Signature chef de service,* *Signature responsable local,*

B) CONSEILS D'UTILISATION.

Le personnel de l'établissement chargé de saisir les données relatives aux droits d'accès ne prend aucune décision en ce domaine. Les données sont saisies au vu des renseignements fournis par les chefs de services, de la grille d'habilitation validée par le comité d'éthique et des expérimentations cliniques (fixation des droits d'accès en fonction des catégories de personnel) et des droits d'accès octroyés individuellement par le responsable local.

Ce même modèle de fiche est à utiliser pour toute modification ou suppression de droits.

La valeur de l'item « type de fonction et emploi occupé » correspond à une colonne de la grille d'habilitation. Elle détermine quels sont, par catégorie de données, les droits d'accès en consultation et mise à jour.

L'item « signature autorisée » (O/N) signifie que la personne est habilitée à signer des comptes rendus et courriers. Lorsqu'un document est signé, il est stocké sans possibilité de modification. Dans certains cas, un « erratum » peut lui être rattaché.

Les items « rendez-vous » et « réalisation d'actes » sont de type binaire et servent à filtrer le contenu de la liste déroulante dans l'application. Par exemple, une personne déclarée avec la valeur « non » pour l'item « rendez-vous » ne possédera pas d'agenda.

L'item « niveau d'administration » se décompose en trois niveaux hiérarchiques « utilisateur simple », « environnement médical » et « administrateur service ». Chaque niveau possède des droits supérieurs au niveau précédent. Par exemple, une personne déclarée avec le niveau « environnement médical » peut procéder à la déclaration et à la modification des thesaurus (CIM 10, CDAM) du service.

La « date de fin des droits » garantit que la personne ne pourra plus utiliser le système après cette date.

Enfin, le chef de service doit préciser sur quel(s) poste(s) du service la personne est autorisée à travailler.

Certaines personnes peuvent être autorisées à saisir des données d'activité pour un service dans lequel elles ne sont pas affectées. Cette autorisation est octroyée par le responsable local et nécessite l'accord des chefs des deux services concernés. Elle se matérialise par la fiche présentée au point C suivant.

A tout moment un chef de service peut obtenir du responsable local la liste des autorisations accordées au personnel de son service et au personnel autorisé à travailler pour son service.

C) FICHE D'AUTORISATION DE SAISIE POUR UN SERVICE.

Cette fiche doit être utilisée pour autoriser des personnels à saisir des données pour des services autres que leur service d'affectation.

Dans ce cas, les droits d'accès accordés sont identiques aux droits des personnels ayant la même fonction dans le service pour lequel les données peuvent être saisies.

Création.	Modification.	Suppression.
☐	☐	☐

Grade :

(Nom) (Prénom)

Service d'affectation :

Type de fonction et emploi occupé (rayer les mentions inutiles) :

Médical :
- responsable comité éthique ;
- consultant expert ;
- chef de service ;
- médecin ;
- médecine des collectivités.

Paramédical :
- surveillant ;
- infirmier ;
- infirmier de consultation ;
- élève ;
- diététicien ;
- kinésithérapeute ;
- manipulateur radio ;
- paramédical autre.

Administratif :
- secrétaire médical ;
- secrétaire administratif ;
- personnel CAG ;
- personnel SHSE ;
- personnel des archives ;
- autre personnel administratif.

est autorisé à saisir des données pour le service de

Autorisation permanente : oui ☐ non ☐

Autorisation temporaire jusqu'au ☐☐/☐☐/☐☐☐☐

Signature de l'intéressé, *Signature chef de service d'affectation,*

Signature responsable hospitalière, division information, *Signature chef de service bénéficiaire,*