RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

Délégation Interministérielle
pour la sécurité des Systèmes d'Information

N°600/DISSI/SCSSI

PROTECTION DES INFORMATIONS SENSIBLES

NE RELEVANT PAS DU SECRET DE DÉFENSE.

RECOMMANDATIONS
POUR LES POSTES DE TRAVAIL
INFORMATIQUES.

MARS 1993
Annule et remplace l'édition de janvier 1990
SERVICE CENTRAL DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

SOMMAIRE

INTRODUCTION

Les systèmes informatiques permettent d'obtenir rapidement et subrepticement de grandes quantités d'informations sensibles. Cette vulnérabilité est accrue par l'emploi d'ordinateurs individuels autonomes, en réseau ou faisant fonction de terminaux intelligents pour un ordinateur central ou un serveur.

Des utilisateurs autorisés peuvent perturber le fonctionnement du système ou tenter d'obtenir des informations qu'ils n'ont pas besoin de connaître. Le risque de compromission des informations s'accroît en proportion du nombre de personnes qui peuvent avoir accès à toutes les informations contenues dans le système. Le risque est d'autant plus élevé que la population en général et les agents de l'entreprise en particulier connaissent de plus en plus le domaine de l'informatique.

Le fait que les informations sont conservées par des moyens électroniques et qu'elles peuvent, en conséquence, faire l'objet de nouvelles formes d'agressions clandestines crée une tentation particulière pour ceux que l'on appelle les "pirates". Les risques de détournement d'informations, de manipulation de logiciel, d'introduction de virus sont élevés.

D'autre part, il existe des risques de mauvais fonctionnement du matériel ou du logiciel par suite d'une défaillance, d'une erreur de conception ou d'une intervention délibérée qui peuvent entraîner des altérations ou des destructions de données, l'impossibilité de poursuivre le traitement, ou l'arrêt du système.

Pour améliorer la sécurité face aux risques identifiés, les mesures à mettre en oeuvre doivent viser à assurer :

. la **disponibilité**, c'est-à-dire l'aptitude du système à remplir une fonction dans des conditions prédéfinies d'horaires, de délais ou de performances,

. l'**intégrité** qui garantit que l'information n'est modifiée que par une action volontaire et autorisée,

. la **confidentialité**, c'est-à-dire la tenue secrète des informations avec accès aux seules entités autorisées.

Les recommandations de ce document concernent les informations ne relevant pas du secret de défense, mais dont la destruction, la falsification, le détournement ou l'utilisation frauduleuse porterait atteinte aux intérêts nationaux, au patrimoine scientifique et technique, ou à la vie privée ou professionnelle des individus.

Ces informations sensibles peuvent, selon leur teneur, recevoir une mention de protection "Diffusion Restreinte", "Confidentiel Spécifique" ou "Secret Spécifique" au sein d'organismes civils et industriels.

Il appartient à chaque organisme, dans le cadre des prescriptions de la réglementation existante et de ses règles internes, de préciser la nature des informations devant recevoir une mention de protection Diffusion Restreinte, Confidentiel ou Secret Spécifique.

D'une manière générale, toutes les informations d'un organisme qui ne sont couvertes ni par le secret de défense, ni par une mention de protection de confidentialité spécifique, mais qui sont considérées comme non communicables au public, doivent recevoir la mention Diffusion Restreinte.

L'information traitée n'est pas seule à devoir être prise en compte ; un système peut être sensible par lui-même. Une application donnée peut être sensible sans que, pour autant, les informations traitées le soient.

Il est donc impératif que tout rédacteur, tout propriétaire d'information, tout responsable de système, en détermine clairement le niveau de sensibilité et en tire toutes les conséquences.

OBJET DU DOCUMENT

Le présent document recommande l'ensemble des mesures à mettre en oeuvre par les divers responsables d'un organisme pour assurer la protection des informations sensibles ne relevant pas du Secret de Défense et qui sont traitées, manipulées ou stockées par des moyens informatiques.

Ces recommandations concernent notamment :

. les logiciels qui sont coûteux ou dont le vol, la détérioration ou la divulgation peut mettre l'organisme en difficulté,

. les informations de **diffusion restreinte** ou de **confidentialité spécifique** qui, soumises à l'obligation de discrétion professionnelle ne doivent pas être divulguées. Pour les informations d'un niveau de sensibilité supérieure comme le **secret spécifique**, les organismes devront veiller à renforcer les mesures recommandées dans ce document.

Les organismes devront établir leurs directives internes à partir de ces recommandations.

Dans le texte, le vocable organisme désigne une entité ayant une structure hiérarchisée, dotée de moyens techniques, humains et financiers. Ce peut être une entreprise, une société, un département ministériel,...

En raison de l'usage de plus en plus intensif de micro-ordinateurs ou de stations de travail individuels, ces recommandations concernent plus particulièrement les postes de travail autonomes et ceux connectés à un réseau. Cependant, elles peuvent être adaptées à d'autres types de système ou d'autres types d'environnement.

A. **Les postes de travail autonomes** sont des ensembles constitués chacun d'une unité centrale et de tous les périphériques qui lui sont raccordés

mais qui n'est pas connectée électroniquement à une autre unité de traitement et qui ne peut transférer électroniquement des renseignements qu'à ses propres périphériques.

Les mesures de protection d'un système informatique autonome comprennent toutes les fonctions, caractéristiques et dispositifs de sécurité des matériels et des logiciels, les procédures d'exploitation, de comptabilisation et d'audit, les mesures de contrôle de l'accès à la zone informatique et aux ressources matérielles et logicielles ainsi que les mesures de contrôle du personnel nécessaires pour assurer un niveau acceptable de protection aux informations sensibles qui doivent être traitées dans ce système informatique.

B. **Les postes de travail connectés à un réseau** modérément étendu peuvent être connectés à des systèmes fortement décentralisés notamment à des systèmes situés en dehors de l'organisme.

Les mesures de protection d'un système informatique connecté comprennent les dispositifs de sécurité de ce système considéré comme autonome et les composantes et dispositifs supplémentaires associés au réseau en tant que tel (par exemple les télécommunications sur le réseau, les mécanismes et procédures d'authentification et d'identification de sécurité à travers le réseau,...), et nécessaires pour assurer un niveau acceptable de protection aux informations sensibles qui doivent être traitées dans le réseau informatique et par les systèmes informatiques qui en font partie.

NB : Les recommandations A et B sont regroupées dans ce document. Les recommandations en italique ne concernent que les postes de travail connectés à un réseau.

SECTION 1 ADMINISTRATION ET ORGANISATION DE LA SÉCURITÉ

Chaque organisme doit mettre en place une structure de sécurité qui garantit la bonne exécution des mesures de sécurité qu'il impose.

Cette structure de sécurité doit être disjointe de celle en charge des technologies de l'information (informatique et télécommunication). Son organisation et son administration doivent être parfaitement définies et connues de tout le personnel de l'organisme.

Bien que cette structure dépende étroitement de l'organisation de l'organisme, les fonctions citées ci-après doivent être dans tous les cas remplies.

1.1. Les partenaires de la sécurité et leur rôle

1.1.1. **L'utilisateur du poste de travail** appelé **utilisateur** dans le texte, est responsable vis-à-vis de l'autorité hiérarchique de l'utilisation globale du poste de travail qui lui a été confié. Il doit respecter les règles de sécurité édictées par l'autorité hiérarchique et se tenir en relation permanente avec le correspondant local de sécurité.

1.1.2. ***Le responsable d'exploitation, l'administrateur système, le gestionnaire de réseau*** *appelés* ***gestionnaires*** *dans le texte, sont des utilisateurs particuliers. Ils sont responsables du bon fonctionnement du réseau, des serveurs de fichiers, de communication, d'impression qui y sont connectés. Ils doivent avoir une bonne compétence en informatique et en télécommunication, et présenter un haut degré de confiance.*

1.1.3. **L'autorité hiérarchique** gérant les ressources humaines et financières, appelée **autorité** ou **autorité responsable** dans le texte est, au niveau d'un site, responsable de l'ensemble des postes de travail et de leur sécurité, de l'octroi et de la gestion des droits d'accès aux diverses ressources informatiques. Elle doit sensibiliser les utilisateurs aux risques encourus par l'usage de l'informatique et leur donner les moyens d'y faire face.

1.1.4. **Le correspondant local de sécurité** des systèmes d'information appelé **correspondant de sécurité** dans le texte, est le représentant de l'autorité centrale de sécurité de l'organisme, elle-même obligatoirement située au plus haut niveau de décision. Il est le conseiller en matière de sécurité des systèmes d'information auprès des utilisateurs et de l'autorité. Il est le garant de la sécurité. En particulier, il doit veiller à l'efficacité des mesures choisies et installées, et doit avoir une vue complète de toutes ces mesures. Il doit, en conséquence, avoir une compétence reconnue dans le domaine. En raison de la sensibilité de ses activités, il doit être digne de la plus grande confiance. En aucun cas il ne se substitue à l'autorité hiérarchique.

1.2. Les procédures

1.2.1. Tout nouvel utilisateur d'un poste de travail doit lire, approuver et signer un **engagement de responsabilité** avant d'avoir droit à accéder aux ressources informatiques de l'organisme. Ce document doit contenir les règles de base de l'organisme en matière de sécurité dans le domaine et doit préciser les sanctions auxquelles l'utilisateur s'expose en les enfreignant (cf. document joint à titre d'exemple).

1.2.2. Le correspondant de sécurité est choisi et nommé par l'autorité locale après accord de l'autorité centrale de sécurité.

1.2.3. *Les gestionnaires sont choisis et nommés par l'autorité locale en fonction de leur compétence et de leur intégrité.*

1.2.4. *Dans le cas d'un réseau local étendu, c'est-à-dire connecté à d'autres réseaux locaux du même type, un* ***comité de sécurité des réseaux*** *doit être créé. Son action doit être permanente. Elle consiste à évaluer les menaces, à donner des avis et des directives aux utilisateurs et à améliorer la sécurité du réseau face aux menaces, par exemple en décidant de mettre en place des moyens techniques de sécurité. Ce comité est composé des correspondants de sécurité locaux, des représentants des autorités hiérarchiques concernés et de spécialistes dans le domaine des réseaux.*

SECTION 2 SÉCURITÉ PHYSIQUE

Des mesures de sécurité physique doivent être prises pour empêcher l'accès non autorisé à des informations sensibles, l'emploi non autorisé de matériel et la privation de certains moyens, ainsi que pour protéger un matériel informatique très coûteux et fragile.

2.1. Emplacement

2.1.1. Les emplacements où sont installés les postes de travail, *ceux des serveurs de télécommunication* 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 sensibilité et du type de leur contenu. Par exemple, *les serveurs* ou les supports de sauvegarde doivent être conservés dans des zones bien protégées et équipées d'alarmes anti-intrusion et incendie.

2.2. Installation du matériel informatique

2.2.1. Outre les moyens de protection habituellement recommandés pour protéger les sites informatiques 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 informatiques traitant des informations sensibles non classifiées doivent respecter les consignes qui suivent.

2.2.2. Pendant l'absence du personnel, les locaux où se trouvent les postes de travail doivent être fermés à clé. Les locaux de plus grande vulnérabilité doivent être contrôlés par un système anti-intrusion et éventuellement équipés d'un système d'alarme.

2.2.3. Les alarmes doivent être régulièrement vérifiées et testées, un rythme hebdomadaire est souhaitable.

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

2.2.5. Les procédures de réaction à une alarme (arrêt et remise en service, intervention, réparation, information de l'autorité responsable,...) doivent être définies. Elles doivent être régulièrement testées. Un rythme mensuel est souhaitable.

2.2.6. Pour limiter les risques de compromission par rayonnement ou conduction parasites des informations sensibles, il convient d'utiliser des matériels respectant les normes de compatibilité électromagnétiques en vigueur et de les installer en suivant les prescriptions du constructeur. Les postes de travail, les unités de traitement, les terminaux connectés ou non doivent notamment être situés le plus loin possible du domaine public.

2.3. Contrôle de l'accès du personnel aux matériels

2.3.1. 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 peut être verrouillée.

2.3.2. Certains micro-ordinateurs sont maintenant équipés de cadenas incorporés qui permettent d'éviter une ouverture frauduleuse du boîtier de l'unité centrale, c'est un élément à prendre en considération lors du choix d'un matériel. Ces mesures prennent davantage d'importance si un disque non amovible est utilisé.

2.3.3. Un inventaire complet des matériels doit être fait au moins une fois par an. Indépendamment des inventaires, si un matériel a disparu, il convient d'en avertir immédiatement l'autorité responsable.

2.3.4. Les supports d'information sensibles, non en cours d'utilisation telles les disquettes de logiciel de base ou les sauvegardes, doivent être conservés dans une armoire fermée à clé.

2.3.5. En dehors des heures ouvrables ou en l'absence du personnel, 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 l'autorité responsable.

2.4. Contrôle de l'accès du personnel aux bâtiments

2.4.1. Les zones particulièrement sensibles doivent comporter un contrôle d'accès spécifique. Des procédures d'accès doivent être définies et des responsabilités attribuées pour leur mise en oeuvre et le contrôle de leur application. Des réactions rapides et efficaces doivent être possibles en cas de nécessité.

2.4.2. Les procédures d'accès aux bâtiments peuvent être différentes selon la catégorie de personnel. Par exemple, trois catégories peuvent être envisagées :

. les permanents, qui passent plus de la moitié de leur temps dans le bâtiment, un simple macaron indélébile et visible peut être apposé sur leur badge,

. les autres personnes de l'organisme doivent être suivies visuellement durant leur déplacement dans le bâtiment aux abords des zones sensibles,

. les visiteurs doivent être accompagnés par un permanent.

2.4.3. Il est conseillé d'utiliser, s'il existe, le contrôle d'accès prévu dans l'organisme en l'adaptant aux besoins locaux afin de bénéficier des moyens et des procédures déjà mises en place.

SECTION 3 SÉCURITÉ EN MATIÈRE DE PERSONNEL

Toute personne pouvant entrer dans un lieu contenant du matériel informatique peut être à même d'empêcher le bon fonctionnement de ce matériel ou de l'endommager, et avoir accès à des informations sensibles en cours d'impression ou d'affichage. Quiconque possède la compétence technique nécessaire ainsi qu'une connaissance suffisante d'un système informatique auquel il a accès peut mettre en danger la sécurité de ce système. Le personnel qui a légitimement accès à des installations informatiques peut donc se trouver particulièrement bien placé pour acquérir de façon illicite et subreptice des informations, ou pour en permettre l'extraction par des personnes non autorisées. En outre, certaines personnes exerçant des fonctions essentielles, programmeurs de système, analystes de système, consultants, etc..., peuvent avoir une connaissance particulièrement approfondie des dispositifs de sécurité, et donc la possibilité d'y porter atteinte.

3.1. Responsabilités et procédures

3.1.1. L'autorité responsable doit définir et contrôler les droits d'accès aux informations sensibles dont elle a la charge, c'est-à-dire dresser la liste de ses informations sensibles, dresser et tenir à jour la liste nominative des personnes ayant le droit d'y accéder, faire appliquer les mesures de protection qui garantissent leur sécurité, délivrer les postes de travail aux utilisateurs en conséquence.

3.1.2. Les habilitations et les droits d'accès doivent être accordés en tenant compte de la catégorie de personnel concernée. Les procédures de contrôle doivent être établies en conséquence. Trois catégories de personnel doivent être considérées :

. les prestataires de service comme les analystes de système, les programmeurs,... qui développent les applications sensibles, conçoivent, mettent en oeuvre et maintiennent les dispositifs de sécurité. Ils sont responsables de la réalisation des mesures de sécurité demandées.

. les utilisateurs qui connaissent les applications et doivent respecter les procédures de sécurité définies par l'autorité responsable et réalisées par les prestataires. Ils doivent s'assurer que les dispositifs de protection installés sont adéquats. Ils sont responsables de la sécurité de leur poste de travail. En particulier, ils doivent le protéger ainsi que les données qu'il contient.

. le personnel extérieur comme le personnel de maintenance, les stagiaires ou visiteurs temporaires, le personnel de nettoyage ou de dépannage auxquels certaines zones sensibles doivent être interdites ou éventuellement autorisées avec la présence continue d'une personne habilitée.

3.1.3. Tout personnel de chaque catégorie devant avoir accès aux ressources informatiques de l'entreprise doit au préalable signer un document d'engagement de responsabilité (cf. section 1.). Ce document peut contenir des éléments spécifiques à chacune des catégories de personnel.

3.1.4. L'autorité responsable doit être consciente des risques encourus par l'intervention des personnels extérieurs à l'entreprise et veiller à ne délivrer que des autorisations d'accès temporaires éventuellement renouvelables.

3.1.5. L'utilisation des postes de travail en dehors des heures ouvrables doit être contrôlée par l'autorité responsable. En particulier, elle doit établir, tenir à jour et diffuser à tout son personnel la liste nominative des personnes habilitées à travailler en dehors des heures ouvrables.

3.1.6. Le propriétaire d'un poste de travail doit s'assurer que toute personne à qui il prête son poste, dispose bien des mêmes habilitations que lui-même à accéder aux informations et qu'il respecte les consignes de sécurité.

3.2 Formation et sensibilisation

3.2.1. L'autorité hiérarchique doit tenir informé son personnel des risques dus à l'usage de l'informatique et mettre en place un plan de sensibilisation pour les différentes catégories de personnel.

3.2.2. Les procédures de sécurité établies doivent être connues de tout le personnel. L'autorité responsable doit s'en assurer régulièrement, en particulier lorsqu'elles ont évolué, ont été modifiées ou supprimées.

3.2.3. Les personnels amenés à mettre en place les dispositifs techniques de sécurité tant matériels que logiciels doivent être formés en conséquence. Compte tenu de l'évolution extrêmement rapide des techniques dans ce domaine une grande vigilance est nécessaire. Une attention particulière doit être accordée à la formation du correspondant de sécurité.

3.2.4. Des rappels réguliers des consignes élémentaires de sécurité doivent être faits. Par exemple, les bureaux doivent être nets de tout document en-

dehors des heures ouvrables, les portes fermées, les corbeilles à papier vides de documents sensibles.

SECTION 4 SÉCURITÉ DES DOCUMENTS

Dans un système informatique, le volume et la compacité des informations traitées, les facilités d'accès, la commodité et la rapidité avec lesquelles elles peuvent être copiées, parfois à distance, imposent l'application de strictes mesures de sécurité des documents afin de protéger les informations d'un accès non autorisé, d'une divulgation, modification ou destruction.

Il est important de se rappeler que le mot "document" désigne tous les types de support d'informations sensibles, documents en papier, supports magnétiques, microfilms et microfiches, rubans d'imprimante, etc...

4.1. Manipulation et protection des informations

4.1.1. Chaque utilisateur étant responsable de la sécurité de son poste de travail, il doit prendre les mesures qu'il convient pour protéger ses données. *Les données des serveurs sont de la responsabilité du gestionnaire désigné.*

4.1.2. Les informations sensibles doivent être identifiées par un moyen propre à chaque support et défini par le règlement intérieur de l'entreprise ou par l'autorité responsable. Par exemple, les disquettes seront repérées par une pastille de couleur collée, les listes sorties par les imprimantes porteront une en-tête indiquant DIFFUSION RESTREINTE, CONFIDENTIEL.....

4.1.3. Il est recommandé de ne pas mélanger sur un même support des informations de niveaux de sensibilité différents. Toutefois, dans le cas où un disque contiendrait des informations de plusieurs niveaux de sensibilité, il devra porter un repère correspondant à la sensibilité maximale des informations qu'il contient.

4.1.4. Lorsqu'ils fonctionnent sans surveillance, les postes de travail doivent être protégés. Par exemple, l'imprimante ou l'écran graphique sera pourvu de scellés visibles, attachés de manière à ce qu'une intervention physique soit rapidement apparente et attire immédiatement l'attention.

4.1.5. Dans la mesure où il doit demeurer sans utilisation pendant plus d'une heure, le poste de travail doit être mis hors tension ou dans l'impossibilité d'être mis en service s'il n'est pas installé dans un local fermé à clé et protégé.

4.1.6. Les documents propres aux éléments de sécurité (dossier de sécurité, mots de passe, originaux des logiciels du système, ...) doivent être isolés et stockés dans des zones protégées.

4.1.7. Les écrans des postes de travail doivent être disposés de telle sorte qu'ils ne puissent pas être vus par des personnes non autorisées, dès lors que des informations sensibles peuvent y apparaître. En particulier, ils ne doivent pas faire face aux fenêtres et aux portes. Les écrans doivent être effacés ou éteints quand une personne non autorisée est proche du poste de travail.

4.2. Manipulation et protection des supports

4.2.1. Hors des périodes où ils sont effectivement utilisés, les supports des données sensibles doivent être stockés dans une zone spécifique et protégée, séparée du poste de travail.

4.2.2. Les disquettes sont fragiles et sensibles à la poussière, aux éraflures, aux sources magnétiques. Elles doivent être rangées dans des boites appropriées, elles-mêmes stockées dans un endroit sûr conforme à leur niveau de sensibilité.

4.2.3. Les supports contenant des informations sensibles doivent être sous surveillance continue durant leur manipulation, par l'utilisateur du poste de travail *ou par le gestionnaire désigné* qui doit enregistrer tous les transferts afin de suivre les déplacements et identifier à tout moment les détenteurs.

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

4.2.5. Les supports amovibles ne doivent pas rester dans un poste de travail qui fonctionne sans surveillance dans un local non fermé et non protégé. Ils doivent être retirés et stockés dans une zone appropriée.

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

4.2.7. L'accès à la zone protégée de stockage des documents doit être contrôlée et réservée aux personnes mandatées.

4.3. Destruction des résidus

4.3.1. Tous les documents sensibles n'ayant plus d'utilité (papier carbone, exemplaires excédentaires, états erronés,...)

doivent être détruits selon la procédure définie par l'autorité responsable.

4.3.2. Les supports magnétiques amovibles contenant des données sensibles doivent être effacés dès qu'ils ne sont plus utilisés ou lorsqu'ils vont être jetés, et avant lorsqu'ils doivent être expédiés en dehors de l'entreprise. Le procédé d'effacement doit interdire la reconstitution de l'information initiale par analyse des résidus produits par l'hystérésis magnétique du matériau.

SECTION 5 SÉCURITÉ DES ORDINATEURS

Les dispositifs de sécurité du matériel et du logiciel peuvent contribuer, séparément et conjointement, à la sécurité d'un système informatique, en permettant :

. l'identification et l'authentification des périphériques, des supports et des utilisateurs, qui constituent les éléments de base sur lesquels doit reposer tout système de sécurité ;

. un contrôle d'accès garantissant que les utilisateurs ne peuvent employer que les matériels, les logiciels et les données auxquels ils sont autorisés à accéder, et que tout accès non autorisé est effectivement rendu impossible ;

. une détection et une surveillance grâce auxquelles toute tentative d'accès non autorisé ou incorrect est décelée et signalée ;

. des contrôles d'intégrité garantissant l'absence de modifications malveillantes sur les logiciels, les fichiers, les transmissions de données ;

. le chiffrement garantissant la confidentialité des informations sensibles. L'utilisation de dispositifs de chiffrement doit faire l'objet d'une demande d'avis adressée au Service Central pour la Sécurité des Systèmes d'Information.

5 1. Matériels informatiques

5.1.1. Choix du matériel : tout choix de matériel informatique doit intégrer la composante "sécurité". Le correspondant local de sécurité doit donner son avis sur le matériel et le fournisseur.

5.1.2. Installation du matériel : l'installation, le branchement et la première mise en route de l'équipement, s'effectuent en présence du correspondant local de sécurité. A défaut, un compte-rendu lui est adressé.

5.1.3. Gestion de la configuration : chaque utilisateur doit posséder et tenir à jour la configuration de ses matériels, type d'équipement, numéro de série, nombre et nature des connexions extérieures. La configuration est également communiquée au correspondant local de sécurité.

5.2. Contrôle d'accès

5.2.1. Chaque poste de travail doit être pourvu d'un contrôle d'accès logique. Les techniques à utiliser sont l'identification et l'authentification. L'identification se borne à reconnaître et enregistrer l'identité sous laquelle se présente l'utilisateur dans une population préalablement recensée. Cette identité est généralement connue mais peut être facilement usurpée. L'authentification permet de garantir que la personne ayant décliné une identité est bien celle qu'elle prétend être. S'il est concevable d'utiliser un

même identifiant pour un groupe de personnes, l'authentification, quant à elle, ne doit concerner qu'un et un seul individu.

5.2.2. L'authentification seule en début de session ne suffit pas pour garantir l'absence d'intrusions. L'utilisateur amené à quitter son poste de travail peut oublier de clore la session, laissant l'accès à une tierce personne. L'attaquant peut également se mettre à l'écoute sur la ligne d'un utilisateur autorisé, attendre que celui-ci s'authentifie puis lui couper la ligne pour se l'approprier. Il peut encore se mettre en coupure sur la ligne pour ajouter aux informations transmises par l'utilisateur des commandes parasites sans que celui-ci s'en aperçoive.

Pour couvrir le risque de l'utilisateur quittant son poste sans clore la session, on peut prévoir une déconnexion automatique après temporisation, détecter l'arrachage éventuel du support d'authentification et éventuellement réauthentifier périodiquement le support, voire l'utilisateur afin de procéder à une authentification continue.

Pour interdire les attaques sur la ligne autres que le brouillage, il est nécessaire de procéder à un contrôle d'intégrité ou à un chiffrement systématique des échanges.

5.2.3. Dans le cas d'un poste de travail connecté à un réseau, en cas de demande d'accès à des ressources distantes, il est nécessaire d'authentifier les deux interlocuteurs, même si l'un des deux est un serveur. En effet, il faut comprendre interlocuteur au sens large, ce peut être un individu, un logiciel, un matériel, un serveur... Il s'agit d'une authentification mutuelle. Cette authentification doit être garantie de bout en bout à travers le réseau.

5.2.4. Dans le cas d'un poste autonome, il est seulement nécessaire d'authentifier localement la personne, le logiciel ou le matériel ayant accès.

5.2.5. Les moyens d'authentification se font à partir de trois méthodes de base :

. ce que connaît l'entité (mot de passe, code confidentiel,...),

. ce que détient l'entité (carte à piste magnétique, carte à puce, authentifieur,...),

. ce qu'est l'entité (caractéristiques biométriques,...).

Ces moyens d'authentification vont du plus vulnérable au plus solide. Compte tenu de l'avance des technologies, le contrôle d'accès le plus répandu est celui réalisé à l'aide de mot de passe. Cependant des solutions permettant de remplacer l'usage du mot de passe par des techniques plus fiables doivent être recherchées.

5.2.6. La protection par mots de passe est d'une efficacité limitée puisqu'un intrus peut toujours par une attaque passive, par exemple par écoute sur la ligne, se les procurer. Elle n'en
doit pas moins être utilisée dans l'attente de solutions plus sûres car elle est préférable à l'absence de protection. Les mots de passe doivent comporter au moins six caractères alphanumériques et doivent être changés régulièrement,

une périodicité de trois mois est acceptable. Ils ne doivent pas être divulgués, ni réutilisés.

5.2.7. Les systèmes d'exploitation comportent généralement des procédures d'accès privilégiées utilisées notamment pour le démarrage du système. La protection des accès à ces procédures doit être particulièrement soignée, en particulier il convient de personnaliser le mot de passe qui y accède.

5.3. Logiciels

5.3.1. Les logiciels font partie de la configuration du système, ils doivent en conséquence être soumis aux mêmes règles que les matériels informatiques (cf. 5.1.).

5.3.2. Acquisition : quelle que soit leur nature (système d'exploitation, progiciel, logiciel d'application spécifique), les logiciels, sauf s'ils sont créés par l'utilisateur lui-même, ne doivent être approvisionnés qu'auprès de fournisseurs agréés par le correspondant local de sécurité ou acquis auprès d'autres utilisateurs de l'organisme sous son contrôle. Ils doivent être suffisamment testés avant d'être mis en service.

Parmi les systèmes d'exploitation et les progiciels, doivent être retenus en priorité ceux qui permettent :

. une protection renforcée des outils de contrôle d'accès (mots de passe, codes d'identification, etc...),

. une protection contre les instructions et logiciels parasites (virus informatiques, bombes logicielles, etc...),

. un contrôle d'intégrité.

Le correspondant doit suivre l'évolution des techniques dans ces domaines.

5.3.3. Conception : le développement des logiciels destinés à manipuler des informations sensibles doit s'appuyer sur des méthodologies rigoureuses dont le choix et le contrôle de bon emploi sont de la responsabilité de l'autorité.

En particulier, la sécurité des accès et l'octroi des droits d'accès pour les bases de données de type relationnel et à caractère sensible doivent être soigneusement étudiés et mis en place dès le début de la conception. Leur suivi doit être assuré.

5.3.4. Utilisation : l'intégrité et la non divulgation des logiciels manipulant des données sensibles sont de la responsabilité de l'utilisateur.

Ces logiciels doivent être particulièrement protégés, et d'accès aux seules personnes autorisées par l'autorité responsable.

Les règles principales de sécurité sont les suivantes :

. effacement de ces logiciels en mémoire vive avant de quitter le poste de travail,

. stockage des supports en armoire fermant à clé,

. en cas de fonctionnement anormal, compte-rendu immédiat au correspondant local de sécurité, et isolement du poste de travail.

5.3.5. Divers : un poste de travail destiné exclusivement ou partiellement à traiter des informations sensibles ne doit jamais être utilisé à des fins autres que celles prévues. Les progiciels publicitaires, les jeux, etc... sont notamment interdits.

5.4. Fichiers

5.4.1. Responsabilité : l'intégrité, la confidentialité et la sauvegarde des fichiers sont de la responsabilité de l'utilisateur autorisé du poste de travail, qui doit établir et tenir à jour les listes complètes de ses fichiers sensibles, pour les données de son poste. *Pour les serveurs, le gestionnaire désigné assure cette mission.*

A des fins de contrôle, les relevés des fichiers sensibles sur supports fixes doivent mentionner la date de dernière utilisation. Ces listes doivent être stockées dans des zones protégées, et les fichiers sensibles repérés par marquage sur les supports. L'utilisateur du poste de travail *ou le gestionnaire pour les serveurs,* doit rendre compte au correspondant local de sécurité de toute anomalie constatée susceptible d'affecter la sécurité.

5.4.2. Accès : les droits d'accès aux informations doivent être définis par l'autorité hiérarchique. Ils consistent à préciser les fichiers accessibles par l'utilisateur et les fonctions autorisées (lecture, écriture, destruction,...). Cela implique que les informations aient été préalablement classées en fonction de leur sensibilité et selon une grille de référence.

5.4.3. Utilisation et stockage : il est recommandé de ne pas conserver de fichiers sensibles permanents sur disques fixes, mais d'utiliser des supports amovibles.

Les supports amovibles contenant des fichiers sensibles doivent impérativement :

. être stockés dans des armoires fermant à clé, sinon dans des armoires fortes,

. être marqués de façon apparente et indélébile.

Il faut éviter les fichiers "dormants". Ces derniers doivent être détruits par les procédures habituelles. Les fichiers sensibles ou non sur supports magnétiques devant être transmis à l'extérieur de l'organisme doivent être enregistrés sur des supports neufs n'ayant pas encore été utilisés.

5.4.4. Sauvegarde : les fichiers sensibles doivent être régulièrement dupliqués sur supports magnétiques amovibles. Le support doit être testé périodiquement pour garantir la restitution correcte du document.

La périodicité de la duplication est à fixer par l'utilisateur, elle dépend essentiellement du rythme de modification des fichiers.

Les fichiers dupliqués sont stockés en zone protégée.

L'utilisateur tient à jour un cahier de sauvegarde de ses fichiers sensibles.

5.4.5. Destruction : les fichiers sensibles périmés doivent être effacés.

Cette destruction ne doit pas être uniquement logique par suppression dans la liste des fichiers, mais doit être accompagnée d'un effacement physique pour prévenir toute possibilité de lecture des secteurs réalloués.

Les supports de type "bande magnétique" doivent être détruits physiquement.

5.5 Maintenance

5.5.1. La maintenance est une opération programmée qui doit pouvoir être effectuée avec la sécurité voulue.

Les travaux de maintenance doivent s'effectuer en présence et sous la surveillance de l'utilisateur du poste de travail.

La télémaintenance est déconseillée. Elle est soumise à autorisation particulière du correspondant local de sécurité, qui en définit les modalités.

5.6 Dépannage

5.6.1. Toute panne et toute opération de dépannage (déclenchement, intervention, remise en route) sont consignées sur un registre propre à l'installation et mis à la disposition du correspondant local de sécurité.

En cas d'intervention pour dépannage d'un quelconque composant du poste de travail, l'utilisateur est responsable des mesures de sécurité à prendre : effacement des mémoires, mise en sécurité des fichiers, effacement des informations sensibles, etc... Au cas où des informations sensibles ne peuvent pas être effacées des supports fixes, l'utilisateur doit surveiller continuellement l'intervention ou à défaut détruire le support (pas de retour en usine).

5 7 Surveillance et vérification

5.7.1. L'autorité doit définir et mettre en place des procédures de surveillance et de vérification de ses systèmes d'information. Ces procédures doivent permettre de découvrir rapidement les accès ou tentatives d'accès non autorisés et permettre de prendre des mesures en conséquence.

5.7.2. L'autorité doit veiller à ce que les divers registres (maintenance, dépannage, fichiers sensibles,...) soient tenus à jour et disponibles pour d'éventuelles inspections .

5.7.3. Une méthode rationnelle d'évaluation de la sécurité des systèmes installés ou en projet doit être recherchée et appliquée. Cette méthode devra fournir aux divers responsables les éléments leur permettant d'améliorer cette sécurité.

SECTION 6 PROCÉDURES DE SAUVEGARDE ET D'URGENCE

Dans cette section sont indiquées les procédures à appliquer en matière de sauvegarde courante des fichiers, applications et systèmes d'exploitation. Sont traitées dans un deuxième temps les mesures curatives à prendre lorsque sont constatées des circonstances "catastrophiques" dont l'origine et la maîtrise échappent totalement à l'utilisateur.

Les procédures d'urgence sont destinées à minimiser les conséquences d'événements imprévisibles et/ou dont la maîtrise échappe à l'utilisateur. On distingue les pannes "habituelles" de tout ou partie du poste de travail, les attaques logiques et les catastrophes de tout genre.

6.1 Procédures de sauvegarde des fichiers de données

6.1.1. Certains fichiers ne nécessitent pas de procédure particulière de sauvegarde, ce sont les "fichiers 1 fois", créés pour ne pas être modifiés, et qui, soit ne présentent aucune difficulté de reconstruction, soit sont destinés à être sauvegardés par ailleurs (courrier sensible par exemple).
Les autres fichiers doivent faire l'objet de sauvegardes régulières.

6.1.2. La responsabilité des sauvegardes incombe à l'utilisateur qui doit tenir à jour un cahier d'exécution des sauvegardes/consultables sur sa demande par le correspondant de sécurité.

6.1.3. 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.

A titre d'exemple, la sauvegarde est à entreprendre lorsque les informations sensibles contenues dans le fichier en cours et la précédente sauvegarde diffèrent de plus de 20% ou lorsque le temps nécessaire à la reconstitution du fichier en cours à partir de cette sauvegarde dépasse 1 journée entière. Les valeurs indiquées (20% et 1 journée) sont modulables selon la politique de sécurité propre à l'organisme.

6.1.4. Les fichiers sauvegardés sont normalement conservés sous la responsabilité de l'utilisateur dans un meuble fermant avec une clé, dont il est le seul détenteur et qui est situé dans une zone différente de celle du poste de travail. A défaut, ils peuvent être stockés dans un meuble, fermant à clé, accessible à plusieurs utilisateurs. Selon la politique interne à l'organisme, le correspondant de sécurité peut imposer des directives particulières pour la conservation des sauvegardes, par exemple leur centralisation dans un local particulier, ce qui dégage normalement la responsabilité de l'utilisateur en ce qui concerne l'intégrité physique de ses sauvegardes.

6.1.5. L'accès à un fichier sauvegardé se fait sous la responsabilité de son créateur qui peut l'autoriser à un tiers. Pour ce dernier cas, et si les fichiers

sauvegardés sont centralisés, une procédure d'accès doit être établie par l'autorité.

6.1.6. L'utilisateur est responsable de la qualité de ses sauvegardes. A ce titre, il doit effectuer périodiquement un test de lisibilité des fichiers sauvegardés.

6 2. Procédures de sauvegarde des logiciels

6.2.1. Les logiciels (programmes d'application et systèmes d'exploitation) traitant, pouvant traiter et/ou contenant des données sensibles doivent tous être sauvegardés.

6.2.2. La responsabilité des sauvegardes incombe à l'utilisateur qui doit tenir à jour un cahier d'exécution des sauvegardes, consultable sur sa demande par le correspondant de sécurité.

6.2.3. Dès son acquisition ou sa création, un logiciel doit être sauvegardé.

Par la suite, une nouvelle sauvegarde est à faire à l'issue de toute modification du logiciel, et au moins une fois par an. Les sauvegardes annuelles doivent être conservées.

6.2.4. Les règles de conservation, d'accès et de contrôle de lisibilité des sauvegardes des logiciels sont identiques à celles relatives aux sauvegardes des fichiers de données.

6.3. Procédures d'urgence : cas des pannes courantes

6.3.1. Il s'agit des pannes techniques affectant le fonctionnement du poste de travail : panne de matériel, défaut du logiciel, défaillance de l'environnement technique (télécommunications, alimentation électrique). A l'issue du dépannage, les actions de reprise diffèrent selon que l'on traite des logiciels ou des fichiers de données.

6.3.2. Sauf circonstance particulière où la panne n'a de toute évidence pu altérer les logiciels (cas à déterminer par une compétence informatique), les logiciels sont recopiés à partir des versions sauvegardées.

6.3.3. Les fichiers de données sont reconstitués par l'utilisateur à partir des fichiers sauvegardés, sauf dans deux circonstances qui nécessitent l'assistance d'une compétence informatique : panne apparemment sans influence possible sur les fichiers ou urgence de la reprise des travaux décidée par l'autorité.

6.3.4. Dans tous les cas de pannes, des tests d'intégrité des fichiers sont à effectuer. Un quelconque incident détecté ou soupçonné entraîne la reconstitution à partir des sauvegardes.

6.4. Procédures d'urgence : cas des attaques logiques

6.4.1. Il s'agit d'attaques du type virus, bombe logique,... Les mesures à prendre ne sont pas propres aux systèmes traitant des informations sensibles, il s'agit des mesures minimales applicables à tous les systèmes.

6.4.2. Les mesures sont les suivantes :

. déconnecter le poste de travail et ses périphériques immédiats de toutes liaisons depuis et vers l'extérieur, sans couper l'alimentation électrique,

. alerter au plus tôt le correspondant de sécurité et une compétence informatique, ainsi qu'éventuellement le gestionnaire. Eux seuls sont aptes à décider des actions appropriées,

. faire impérativement contrôler les sauvegardes qui ont été réalisées sur ce poste de travail.

6.4.3. Le travail ne pourra reprendre sur le poste qu'après accord du correspondant de sécurité au vu des résultats acquis par les compétences en informatique et, éventuellement par le gestionnaire.

6.5. Procédures d'urgence : cas des "catastrophes"

6.5.1. Il s'agit des situations dont la maîtrise échappe aux possibilités ou aux moyens de l'utilisateur.

On distingue :

. les "catastrophes" sans préavis : inondation, incendie, explosion, attentat à la bombe, séisme,...

. les "catastrophes" avec préavis : ouragan, menace de subversion, d'émeute, de grève,...

6.5.2. Les préavis sont à utiliser pour effectuer la sauvegarde des fichiers et la mise en sécurité des fichiers et logiciels originaux.

6.5.3. Dans tous les cas, les conditions ultérieures de remise en route dépendent de l'état constaté des installations. Elles comprennent le contrôle des sauvegardes préalablement à la reconstitution du système à partir des logiciels et fichiers de données déclarés bons.

SECTION 7 SÉCURITÉ DES COMMUNICATIONS

La sécurité des informations sensibles traitées ou transmises par les systèmes de télécommunications doit être assurée. Les autorités doivent tenir compte de la grande vulnérabilité aux intrusions qu'offrent en particulier les circuits téléphoniques, les lignes spécialisées, ou TRANSPAC.

La sécurité des communications comporte essentiellement deux volets :

. la sécurité cryptographique,

. la sécurité des voies de transmission et des accès .

7.1. Sécurité cryptographique

7.1.1. Les informations très sensibles 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 site d'un organisme peuvent être approuvés pour transmettre des informations de diffusion restreinte.

7.1.2. En l'absence de tels circuits, la protection des informations très sensibles peut être assurée par un moyen de chiffrement dont la fourniture, l'exportation ou l'utilisation sont soumises :

a) à déclaration préalable lorsque ce moyen ne peut avoir d'autre objet que d'authentifier une communication ou d'assurer l'intégrité du message transmis ;

b) à autorisation du Premier ministre dans les autres cas.

7.1.3. Les informations peu sensibles n'exigent pas la mise en oeuvre de mesures de sécurité cryptographiques. Sauf éventuellement en ce qui concerne les procédures d'authentification et de contrôle d'intégrité.

7.1.4. Les moyens de chiffrement, qu'ils soient autonomes ou intégrés aux équipements, ainsi que les moyens d'authentification, doivent être pris en compte dans le cadre d'une gestion spécifique. Les clés de chiffrement sont à protéger tout particulièrement.

7.2. Sécurité des voies de transmission et des accès

7.2.1. Tout système informatique, y compris les réseaux, assurant le transfert d'informations sensibles ou non doit être protégé contre tout accès qui porterait atteinte aux objectifs de sécurité (disponibilité, intégrité, confidentialité).

7.2.2. Outre les mesures et procédures énumérées dans les autres sections, des précautions sont à prendre dans les domaines suivants :

. protection et surveillance des têtes d'arrivée de lignes,

. protection et surveillance des répartiteurs, des modems,

. surveillance des branchements pirates sur les lignes de transmission,

. suivi des tentatives de connexion,

. surveillance des opérations de maintenance. Un descriptif précis des interventions effectuées doit être demandé.

7.2.3. Au niveau des autocommutateurs ou des serveurs de communication, il doit être fait appel, autant que faire se peut, à des procédures logiques de

déconnexion automatique au bout de quelques tentatives infructueuses d'accès.

7.2.4. Dans la mesure du possible, il est conseillé d'utiliser les facilités offertes en terme de sécurité, par les réseaux, par exemple les groupes fermés d'abonnés du réseau TRANSPAC.

7.2.5. Dans le cas d'interconnexions de réseaux, il est conseillé d'utiliser de préférence des passerelles de niveau 3 selon le modèle OSI.

SECTION 8 GESTION DE LA CONFIGURATION

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, micrologiciels et logiciels qui ont un rapport avec la sécurité.

Le plan de gestion de la configuration doit entre autre, faire état des aspects suivants :

. contrôles applicables aux modifications relatives à la spécification, à la conception, à la documentation de mise en oeuvre, aux dispositifs d'essais,...

. contrôles applicables à la comparaison d'un système nouvellement créé, y compris les programmes utilitaires et les progiciels, 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 progiciels.

ANNEXE

ENGAGEMENT DE RESPONSABILITÉ

Je reconnais avoir pris connaissance des règles de sécurité suivantes, relatives à l'usage d'un poste de travail qui donnent accès aux ressources informatiques

du.....(organisme)

(énoncé des règles de sécurité)

et m'engage à respecter toutes les procédures qui m'ont été transmises.

Pleinement conscient de mes responsabilités, je reconnais être informé des conséquences du non respect de ces procédures.

.....	.....	.....
(Nom, Prénom)	(Date)	(Signature)