LES GUIDES DE LA CNIL

GUIDE
LA SÉCURITÉ DES DONNÉES PERSONNELLES

Édition 2010

CNIL
Commission Nationale de l'Informatique et des Libertés

Sommaire

Ce guide est téléchargeable sur le site Internet de la CNIL : www.cnil.fr

Avant-propos

La place grandissante de l'informatique dans toutes les sphères de notre société entraîne la production, le traitement et la dissémination d'un nombre croissant de données personnelles.

Les menaces pesant sur les systèmes et réseaux d'information incluent la fraude informatique, le détournement de finalité, la captation frauduleuse, la perte de données, le vandalisme, ou encore les sinistres les plus fréquents, tels que l'incendie ou l'inondation.

La loi «informatique et libertés» impose que les organismes mettant en œuvre des traitements ou disposant de fichiers de données en garantissent la sécurité. Par sécurité des données, on entend l'ensemble des «précautions utiles, au regard de la nature des données et des risques présentés par le traitement», pour notamment, «empêcher que les données soient déformées, endommagées, ou que des tiers non autorisés y aient accès.» (Art.34 loi IL). Cette sécurité se conçoit pour l'ensemble des processus relatifs à ces données, qu'il s'agisse de leur création, leur utilisation, leur sauvegarde, leur archivage ou leur destruction et concerne leur confidentialité, leur intégrité, leur authenticité et leur disponibilité.

Ce guide s'adresse à tout responsable de traitement ainsi qu'à toute personne disposant d'un minimum de connaissances informatiques (administrateur système, développeur, responsable de la sécurité des systèmes d'information, utilisateur…) et souhaitant évaluer le niveau de sécurité dont doit bénéficier tout traitement de données à caractère personnel.

Il présente un ensemble de préconisations essentielles regroupées par fiches thématiques concernant la sécurité de données à caractère personnel.

Chaque fiche est structurée en trois sections :

- les précautions élémentaires ;
- ce qu'il ne faut pas faire ;
- pour aller plus loin.

La section «Pour aller plus loin» recommande des mesures additionnelles aux précautions élémentaires.

Parmi l'ensemble des préconisations, certaines sont issues de bonnes pratiques en matière de gestion de la sécurité des systèmes d'informations, tandis que d'autres résultent des règles relatives à la protection de données à caractère personnel du fait de la spécificité de ces informations.

Ce premier guide «sécurité» est évidemment perfectible. Aussi, le lecteur ne devra-t-il pas hésiter à nous contacter pour nous transmettre ses propositions en la matière.

Bien entendu, aux yeux des experts et des profanes, ce guide ne répondra pas complètement à leurs attentes, jugeant qu'il ne va pas assez ou trop loin. J'espère néanmoins qu'il satisfera au plus grand nombre, et je peux d'ores et déjà annoncer qu'un document plus élaboré est en cours de préparation.

Alex TÜRK

Président de la CNIL

La Commission Nationale de l'Informatique et des Libertés

La CNIL, autorité administrative indépendante, est chargée de veiller au respect des dispositions de la loi. A ce titre, elle assure des missions d'information, de conseil, d'expertise et de veille technologique.

La CNIL dispose de pouvoirs particuliers pour faire respecter la loi : elle contrôle la mise en œuvre des fichiers informatiques et peut également procéder à des vérifications sur place.

L'ensemble de ces informations est également disponible sur le site Internet de la CNIL :
http://www.cnil.fr/dossiers/securite

Introduction

Sécuriser un système informatique nécessite de prendre en compte tous les aspects de sa gestion. Cette sécurité passe par le respect de bonnes pratiques et le maintien de l'outil informatique à l'état de l'art quant aux attaques dont il peut faire l'objet. Toutefois, cette sécurité ne sera effective qu'à condition de faire preuve de rigueur notamment dans la délivrance (et le retrait) des habilitations ainsi que dans le traitement des inévitables incidents.

Afin de garantir que chaque utilisateur du système informatique n'accède qu'aux données qu'il a besoin de connaître, deux éléments sont nécessaires :

- la remise d'un identifiant unique à chaque utilisateur associé à un moyen de s'authentifier : **une méthode d'authentification** ;
- un contrôle a priori de l'accès aux données pour chaque catégorie d'utilisateurs : **une gestion des habilitations.**

La protection de données concernant des personnes impose en plus que celles-ci soient :

- *«collectées et traitées de manière loyale et licite» (Art. 6 al.1 loi I&L)*
- *«collectées pour des finalités déterminées, explicites et légitimes et ne soient pas traitées ultérieurement de manière incompatible avec ces finalités» (Art. 6 al.2 loi I&L).*

Ces obligations ne peuvent s'apprécier qu'à travers l'usage qui est fait du système informatique. Par conséquent, il est nécessaire de procéder à une **journalisation**, c'est-à-dire l'enregistrement des actions de chaque utilisateur sur le système pendant une durée définie.

En outre, la loi Informatique et Libertés dispose que les données soient «*exactes, complètes et si nécessaires mises à jour.*» (Art. 6 al.4 loi I&L). Ces obligations nécessitent que les systèmes d'information prévoient des mécanismes garantissant l'intégrité des données.

La loi dispose également que ces données soient «*conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées*» (Art. 6 al.5 loi I&L). Les systèmes doivent donc prévoir la suppression, l'archivage, ou encore l'anonymisation de ces données, lorsque leur durée de conservation est atteinte.

Enfin, **gérer les risques** constitue un moyen efficace de protéger les «*libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, à l'égard du traitement des données à caractère personnel*» (article premier de la Directive 95/46/CE).

Pour rappel, la CNIL peut procéder à des vérifications sur place. En outre, la formation restreinte peut prononcer diverses sanctions graduées : avertissement, mise en demeure, sanctions pécuniaires, injonction de cesser le traitement. Le montant des sanctions pécuniaires peut atteindre 150 000 euros lors du premier manquement constaté puis 300 000 euros, ou 5% du chiffre d'affaire hors taxes du dernier exercice, dans la limite de 300 000 euros , s'il s'agit d'une entreprise.

Le montant de ces sanctions est «proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement».

La CNIL peut également dénoncer pénalement les infractions à la loi dont elle a connaissance au Procureur de la République.

Termes & définitions

Authentification : «l'authentification a pour but de vérifier l'identité dont une entité se réclame. Généralement l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté. En résumé, s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité.» (ANSSI Agence Nationale de la Sécurité des Sustèmes d'Information).

Destinataire des données : «toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données» (Art. 3 loi I&L).

Donnée à caractère personnel : «toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne» (Art. 2 loi I&L).

Données sensibles : les «données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci» (Art. 8 loi I&L).

Responsable de traitement : «la personne, l'autorité publique, le service ou l'organisme qui détermine les finalités et les moyens dudit traitement, sauf désignation expresse par des dispositions législatives ou réglementaires relatives à ce traitement» (Art. 3 loi I&L).

Tiers : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données (directive 95/46/CE).

Traitement : sauf mention explicite, un traitement s'entend dans ce document comme un traitement de données à caractère personnel.

Traitement de données à caractère personnel : «toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction» (Art. 2 loi I&L).

Fiche n° 1 - Quels risques ?

La gestion des risques permet au responsable de traitement d'identifier quelles sont les précautions utiles à prendre «*au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès*» (article 34 de la Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

La Directive européenne Informatique et Libertés de 1995 précise encore que la protection des données personnelles nécessite de prendre des «*mesures techniques* **et** *d'organisation* **appropriées**» (Article 17).

Une telle approche permet en effet une prise de décision objective et la détermination de mesures parfaitement adaptées à son contexte.

Un risque est un scénario qui combine une situation crainte (atteinte de la sécurité des traitements et ses conséquences) avec toutes les possibilités qu'elle survienne (menaces sur les supports des traitements). On estime son niveau en termes de gravité (ampleur et nombre des impacts) et de vraisemblance (possibilité/probabilité qu'il se réalise).

Les précautions élémentaires

L'étude des risques doit être formalisée dans un document complet. Cette étude devra être mise à jour de manière régulière selon les évolutions du contexte et doit :

- **recenser** les fichiers et données à caractère personnel *(ex : fichiers client, contrats…)* et les traitements associés, automatisés ou non, en identifiant les supports sur lesquels *reposent ces* traitements :
  - les matériels *(ex : serveur de gestion des ressources humaines, CD-ROM…) ;*
  - les logiciels *(ex : système d'exploitation, logiciel métier…) ;*
  - les canaux de communication *(ex : fibre optique, Wifi, Internet…)* ;
  - les supports papier *(ex : document imprimé, photocopie…).*
- **déterminer** comment la vie privée des personnes pourrait être affectée par le biais de ces supports.
- Pour chaque traitement, **identifier et classer selon leur gravité les impacts sur la vie privée** des personnes en cas d'atteinte à :
  - la confidentialité *(ex : usurpations d'identités consécutives à la divulgation des fiches de paie de l'ensemble des salariés d'une entreprise)* ;

- la disponibilité *(ex : non détection d'une interaction médicamenteuse du fait de l'impossibilité d'accéder au dossier électronique du patient) ;*
- l'intégrité *(ex : modification des journaux d'accès dans le but de faire accuser une personne à tort).*

• **Étudier les menaces** qui pèsent sur chaque support **et les hiérarchiser** selon leur probabilité d'occurrence (vraisemblance).

Exemples de menaces : *vol d'un PC portable, contagion par un code malveillant, saturation des canaux de communication, photocopie de documents papier…)*. Une liste complète de menaces est fournie en annexe 1.

• **Étudier les risques**

Combiner chaque impact avec les menaces qui le concerne.

Hiérarchiser les risques ainsi obtenus selon leur gravité et leur vraisemblance.

• **Mettre en œuvre des mesures de sécurité**

Déterminer les mesures de sécurité pour réduire, transférer ou éviter les risques. Les fiches pratiques de ce guide donnent des exemples concrets de mesures destinées à couvrir les obligations issues de la loi informatique et libertés : confidentialité, intégrité, qualité des données, conservation, recueil du consentement….

Ce qu'il ne faut pas faire

• **Mener seul une étude de risques**. Impliquer les acteurs les plus appropriés à chaque étape (métiers, maîtrise d'œuvre, responsable du traitement…) afin de les sensibiliser aux risques, de les responsabiliser dans leurs choix et de les faire adhérer aux mesures de sécurité qu'ils auront choisies.

• **Réaliser une étude trop détaillée.** Il est aisé de se perdre dans un niveau de détail inapproprié. Celui-ci doit rester cohérent avec la taille du sujet étudié, l'objectif de l'étude et le niveau des risques.

• **Choisir des mesures inappropriées.** Il faut déterminer les mesures nécessaires et suffisantes pour traiter les risques, et que celles-ci soient adaptées aux contraintes de l'étude (budgétaires, techniques…).

Pour aller plus loin

- L'étude des risques permet de déterminer des mesures de sécurité à mettre en place. Il convient donc de **prévoir un budget** pour leur mise en œuvre.
- **L'emploi d'une véritable méthode** permet de disposer d'outils pratiques et d'améliorer l'exhaustivité et la profondeur de l'étude des risques. La boîte à outils d'EBIOS[1] peut être utilisée à cet effet http://www.ssi.gouv.fr/site_article173.html).
- En fonction des moyens disponibles, il peut également être utile de prévoir :
  - la **formation** des personnes chargées de réaliser les études de risques ;
  - un **audit sécurité** du système d'information.

1 - EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité – est la méthode de gestion des risques publiée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) du Secrétariat général de la défense et de la sécurité nationale (SGDSN). EBIOS est une marque déposée du SGDSN.

Fiche n° 2 - Authentification des utilisateurs

le responsable d'un système informatique doit être en mesure d'assurer que chaque utilisateur du système n'accède qu'aux données dont il a besoin pour l'exercice de sa mission. Pour cela, chaque utilisateur doit être doté d'un **identifiant qui lui est propre** et doit **s'authentifier** avant toute utilisation des moyens informatiques.

Les mécanismes permettant de réaliser l'authentification des personnes sont catégorisés en trois familles selon qu'ils font intervenir:

- ce que l'on sait, par exemple un mot de passe,
- ce que l'on a, par exemple une carte à puce,
- une caractéristique qui nous est propre, par exemple une empreinte digitale ou encore une signature manuscrite. Pour rappel, la loi Informatique et Libertés subordonne l'utilisation de la biométrie à l'autorisation préalable de la CNIL[2] .

L'authentification d'un utilisateur est qualifiée de forte lorsqu'elle a recours à une combinaison d'au moins deux de ces méthodes.

Les précautions élémentaires

- A propos des identifiants (ou logins) des utilisateurs, ceux-ci doivent, dans la mesure du possible, être différents de ceux des comptes définis par défaut par les éditeurs de logiciels. Les comptes par défaut doivent être désactivés. Aucun compte ne devrait être partagé entre plusieurs utilisateurs.
- Dans le cas d'une authentification des utilisateurs basée sur des **mots de passe**, leur mise en œuvre doit respecter les règles suivantes :
  - avoir une taille de **8 caractères minimum** ;
  - utiliser des **caractères de types différents** (majuscules, minuscules, chiffres, caractères spéciaux). Des moyens mnémotechniques permettent de créer des mots de passe complexe, par exemple
    - en ne conservant que les premières lettres des mots d'une phrase ;
    - en mettant une majuscule si le mot est un nom (ex : **C**hef) ;
    - en gardant des signes de ponctuation (ex : **'**) ;
    - en exprimant les nombres à l'aide des chiffres de 0 à 9 (ex : Un **->1**) ;

  Exemple, la phrase «un **C**hef **d'E**ntreprise **a**verti **e**n **v**aut **deux**» correspond au mot de passe **1Cd'Eaev2** ;
  - **changer** de mot de passe **régulièrement** (tous les 3 mois par exemple).
- Lorsque le **renouvellement** d'un mot de passe est consécutif à un oubli, une fois que le mot de passe a été réinitialisé, l'utilisateur doit être dans l'obligation de le changer dès sa première connexion afin de le personnaliser.

2 - A ce sujet, consulter notamment la fiche 12 – la biométrie sur le lieu de travail du Guide CNIL pour les employeurs et les salariés.
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_employeurs_salaries.pdf

Ce qu'il ne faut pas faire

- Communiquer son mot de passe à autrui ;
- stocker ses mots de passe dans un fichier en clair ou dans un lieu facilement accessible par d'autres personnes ;
- utiliser des mots de passe ayant un lien avec soi (nom, date de naissance…) ;
- utiliser le même mot de passe pour des accès différents ;
- configurer les applications logicielles afin qu'elles permettent d'enregistrer les mots de passe.

Pour aller plus loin

- Concernant les mécanismes d'authentification, il est recommandé de se référer aux *règles et recommandations concernant les mécanismes d'authentification préconisées* dans l'annexe B3 du Référentiel Général de Sécurité[3].
- En cas d'utilisation de méthodes d'authentification reposant sur des dispositifs tels que des cartes à puce ou des schémas d'authentification mettant en œuvre des algorithmes cryptographiques, ceux-ci doivent suivre les règles concernant le *choix et le dimensionnement des mécanismes cryptographiques* préconisées dans l'annexe B1 du Référentiel Général de Sécurité[4].
- Dans l'éventualité d'une authentification par des **dispositifs biométriques** il est nécessaire d'effectuer une demande d'autorisation auprès de la CNIL. D'une manière générale, la CNIL recommande l'utilisation de biométrie sans traces (contour de la main, réseaux veineux…) ou l'enregistrement des empreintes digitales dans un support individuel. Concernant des dispositifs **basés sur l'empreinte digitale**, il convient de se référer à la *Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données* situé à l'adresse internet http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNIL-biometrie/Communication-biometrie.pdf pour prendre connaissance de la doctrine de la CNIL en la matière.

3 - **http://www.references.modernisation.gouv.fr/sites/default/files/RGS_Mecanismes_Authentification_v1_0.pdf**
4 - **http://www.references.modernisation.gouv.fr/sites/default/files/RGS_Mecanismes_cryptographiques_v1_20.pdf**

Fiche n° 3 - Gestion des habilitations & sensibilisation des utilisateurs

Chaque utilisateur du système ne doit pouvoir accéder qu'aux données dont il a besoin pour l'exercice de sa mission. Concrètement, cela se traduit par la mise en place d'un **mécanisme de définition des niveaux d'habilitation** d'un utilisateur dans le système, et d'un **moyen de contrôle des permissions d'accès** aux données.

Il convient de veiller également à ce que les utilisateurs soient conscients des menaces en termes de sécurité, ainsi que des enjeux concernant la protection des données personnelles.

Les précautions élémentaires

- **Définir des profils d'habilitation** dans les systèmes en séparant les tâches et les domaines de responsabilité, afin de limiter l'accès à des données à caractère personnel aux seuls utilisateurs dûment habilités.
- **Supprimer les permissions d'accès des utilisateurs dès qu'ils ne sont plus habilités à accéder à un local ou à une ressource**, ainsi qu'**à la fin de leur période d'emploi.**
- Documenter les procédures d'exploitation, les tenir à jour et les rendre disponibles à tous les utilisateurs concernés. Concrètement, toute action sur le système, qu'il s'agisse d'opérations d'administration ou de la simple utilisation d'une application, doit être expliquée dans des documents auxquels les utilisateurs peuvent se référer.
- Rédiger une **charte informatique** et l'annexer **au règlement intérieur**.

Modèle d'une charte informatique :

1. Le rappel des règles de protection des données et les sanctions encourues en cas de non respect de la loi.
2. Le champ d'application de la charte, qui inclut notamment :
   - les modalités d'intervention du service de l'informatique interne ;
   - les moyens d'authentification ;
   - les règles de sécurité auxquelles se conformer, ce qui peut inclure par exemple de :
     - signaler au service informatique interne toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement ;
     - ne jamais confier son identifiant/mot de passe à un tiers ;
     - ne pas modifier les paramétrages du poste de travail ;
     - ne pas installer, copier, modifier, détruire des logiciels sans autorisation ;
     - verrouiller son ordinateur dès que l'on quitte son poste de travail ;
     - ne pas accéder, tenter d'accéder, ou supprimer des informations qui ne relèvent pas des tâches incombant à l'utilisateur ;
     - définir les modalités de copie de données sur un support externe, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant des règles préalablement définies.
3. Les modalités d'utilisation des moyens informatiques et de télécommunications mis à disposition comme :
   - le poste de travail ;
   - les équipements nomades ;
   - l'espace de stockage individuel ;
   - le réseau local ;
   - internet ;
   - la messagerie électronique ;
   - le téléphone.
4. Les conditions d'administration du système d'information, et l'existence, le cas échéant, de:
   - systèmes automatiques de filtrage ;
   - systèmes automatiques de traçabilité ;
   - gestion du poste de travail.
5. Les responsabilités et sanctions encourues en cas de non respect de la charte.

Ce qu'il ne faut pas faire

- Définir des comptes administrateur partagés par plusieurs personnes.

Pour aller plus loin

- Etablir, documenter et réexaminer une **politique de contrôle d'accès** en rapport avec la finalité du traitement.

La politique de contrôle d'accès doit inclure :

  - les procédures d'enregistrement et de radiation des utilisateurs destinées à accorder et à retirer l'accès au traitement ;
  - les mesures incitant les utilisateurs à respecter les bonnes pratiques de sécurité lors de la sélection et l'utilisation de mots de passe ou d'autres moyens d'authentification ;
  - les mesures permettant de restreindre et de contrôler l'attribution et l'utilisation des accès au traitement.

- **Classifier les informations** de manière notamment à indiquer si celles-ci sont des données sensibles. Cette classification permet de rendre compte du niveau de sécurité à appliquer.
- Envoyer régulièrement à tous les utilisateurs les mises à jour des politiques et procédures pertinentes pour leurs fonctions.
- Organiser des séances de formation et de sensibilisation à la sécurité de l'information. Des rappels périodiques peuvent être faits par le biais de la messagerie électronique.
- Prévoir la signature d'un **engagement de confidentialité** (cf. modèle de clause ci-dessous), ou prévoir dans les contrats de travail une **clause de confidentialité spécifique** concernant les données à caractère personnel.

Exemple d'engagement de confidentialité relatif aux données à caractère personnel :

Je soussigné Monsieur/Madame _____, exerçant les fonctions de _____ au sein de la société _____ (ci-après dénommé «la Société»), étant à ce titre amené à accéder à des données à caractère personnel, déclare reconnaître la confidentialité desdites données.

Je m'engage par conséquent, conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient modifiées, endommagées ou communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :

- ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité matérielle de ces données ;
- m'assurer, dans la limite des mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- assurer, dans la limite de mes attributions, l'exercice des droits d'information, d'accès et de rectification de ces données ;
- en cas de cessation des mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

J'ai été informé que toute violation du présent engagement m'expose notamment à des actions et sanctions disciplinaires et pénales conformément aux dispositions légales en vigueur.

Fait à xxx le xxx en xxx exemplaires

Nom :	Nom :
Signature :	Signature :

Fiche n° 4 - Sécurité des postes de travail

La sécurité des postes de travail passe par une mise en œuvre de mesures pour prévenir

- les tentatives d'accès frauduleux ;

- l'exécution de virus ;

- la prise de contrôle à distance, notamment via internet.

Les risques d'intrusion dans les systèmes informatiques sont importants et peuvent conduire à l'implantation de virus ou de programmes «espions».

Les précautions élémentaires

- **Limiter le nombre de tentatives d'accès** à un compte. En fonction du contexte, ce nombre peut varier entre trois et dix. Lorsque la limite est atteinte, il est préférable de bloquer la possibilité d'authentification à ce compte temporairement ou jusqu'à l'intervention d'un administrateur du système ;
- installer un «**pare-feu**» (*firewall*) logiciel, et limiter les ports de communication strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail ;
- utiliser des **antivirus régulièrement mis à jour ;**
- prévoir une procédure de **verrouillage automatique de session** en cas de non-utilisation du poste pendant un temps donné. Pour les opérations de maintenance, il convient de mettre fin à une session après une à cinq minutes d'inactivité. Pour d'autres opérations moins critiques (accès à une application métier par exemple), un délai de quinze minutes doit permettre de garantir la sécurité sans compromettre l'ergonomie d'utilisation ;
- prévoir d'**afficher**, lors de la connexion à un compte, **les dates et heures de la dernière connexion.**

Ce qu'il ne faut pas faire

- Utiliser des systèmes d'exploitation obsolètes (une liste mise à jour régulièrement est disponible à l'adresse internet http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/).

Pour aller plus loin

- **Limiter** les applications nécessitant des droits de niveau administrateur pour leur exécution ;
- **limiter les services** du système d'exploitation s'exécutant sur le poste de travail à ceux qui sont strictement nécessaires ;
- installer les **mises à jour critiques des systèmes d'exploitation** sans délai en programmant une vérification automatique périodique hebdomadaire ;
- mettre à jour les applications lorsque des failles critiques ont été identifiées et corrigées ;
- concernant les virus, se référer au document du CERTA disponible à l'adresse internet http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-007/ pour des recommandations plus complètes.

Fiche n° 5 - Comment sécuriser l'informatique mobile ?

La multiplication des ordinateurs portables, des clés USB et des smartphones rend indispensable d'anticiper la possible perte d'informations consécutive au vol où à la perte d'un tel équipement.

Les précautions élémentaires

- Prévoir des moyens de chiffrement pour les espaces de stockage des matériels informatiques mobiles (ordinateur portable, périphérique de stockage amovible tels que clés USB, CD-ROM, DVD-RW, etc.). Parmi ces moyens, on peut citer :
  - le chiffrement du disque dur dans sa totalité au niveau matériel ;
  - le chiffrement du disque dur dans sa totalité à un niveau logique via le système d'exploitation ;
  - le chiffrement fichier par fichier ;
  - la création de conteneurs[5] chiffrés.

Parmi les outils disponibles, des logiciels libres tels que TrueCrypt[6] (www.truecrypt.org) permettent de créer des containeurs chiffrés dont la sécurité repose sur un mot de passe.

De nombreux constructeurs de PC portables vendent des solutions avec disque dur chiffré : il convient de privilégier ces équipements et de s'assurer que le chiffrement est bien mis en œuvre par les utilisateurs.

Ce qu'il ne faut pas faire

- Conserver des données personnelles dans les équipements mobiles lors de déplacement à l'étranger. On peut consulter à ce sujet les préconisations formulées dans le document Passeport de conseils aux voyageurs publié par l'ANSSI disponible à l'adresse http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs_janvier-2010.pdf.

Pour aller plus loin

- Lorsque des appareils mobiles servent à la collecte de données en itinérance (ex : PDA, Smartphones ou PC portables, etc.), il faut sécuriser les données qui y sont stockées et prévoir un verrouillage de l'appareil au bout de quelques minutes d'inactivité. Prévoir aussi de purger ces équipements des données collectées sitôt qu'elles ont été introduites dans le système d'information de l'organisme.
- De plus en plus d'ordinateurs portables sont équipés d'un dispositif de lecture d'empreinte digitale. La mise en œuvre de tels dispositifs est soumise à l'autorisation de la CNIL.

5 - Par conteneur, il faut comprendre un fichier susceptible de contenir plusieurs fichiers.
6 - Il convient d'utiliser la version 6.0a qui bénéficie d'une certification de premier niveau par l'ANSSI.

Fiche n° 6 - Les sauvegardes et la continuité d'activité

Des copies de sauvegarde des données à caractère personnel doivent être faites et testées régulièrement, conformément à la politique de sauvegarde adoptée. Il faut également procéder à une sauvegarde des logiciels servant au traitement afin de garantir la pérennité de celui-ci.

Une sécurisation renforcée est requise pour les sauvegardes de données sensibles.

Il convient de prévoir la continuité d'activité en anticipant les pannes matérielles. Des mesures de protection physique contre les dommages causés par les incendies ou les inondations doivent être envisagées.

Les précautions élémentaires

- **S'agissant de la sauvegarde des données :**
  - effectuer des sauvegardes fréquentes pour éviter la perte d'information. Selon le volume d'informations à sauvegarder, il peut être opportun de prévoir des sauvegardes incrémentales[7] avec une fréquence quotidienne et des sauvegardes complètes avec une fréquence moindre (hebdomadaires ou bimensuelles) ;
  - prévoir de stocker les supports de sauvegarde sur un site extérieur, dans des coffres ignifugés et étanches ;
  - combiner une ou plusieurs des solutions suivantes pour sécuriser les sauvegardes soit en :
    - chiffrant les sauvegardes elles-mêmes ;
    - chiffrant les données à la source ;
    - prévoyant un stockage dans un lieu sécurisé.
  - suivre des règles en adéquation avec la politique de sécurité pour le convoyage éventuel des sauvegardes.
- **S'agissant de la continuité d'activité :**
  - mettre en place des détecteurs de fumée ainsi que des extincteurs. Ces systèmes doivent être inspectés annuellement ;
  - concernant les inondations, les matériels informatiques ne doivent pas être mis à même le sol, mais surélevés ;
  - à propos des matériels :
    - l'utilisation d'un onduleur est recommandée pour le matériel servant aux traitements critiques ;
    - il convient également de prévoir une redondance matérielle des unités de stockage par une technologie RAID[8].

7 - Une sauvegarde incrémentale consiste à n'enregistrer que les modifications faites par rapport à une précédente sauvegarde.

8 - RAID désigne des techniques de répartition de données sur plusieurs supports de sauvegardes (par exemple des disques durs) afin de prévenir la perte de données consécutives à la panne d'un des supports.

Ce qu'il ne faut pas faire

- Conserver les sauvegardes au même endroit que les machines hébergeant les données. Un sinistre majeur intervenant à cet endroit aurait comme conséquence une perte définitive des données.

Pour aller plus loin

- Concernant la continuité du service, prévoir de dimensionner tous les services généraux, tels que l'électricité ou l'alimentation en eau relatifs aux systèmes pris en charge, et les inspecter régulièrement pour écarter tout risque de dysfonctionnement ou de panne.

Pour les traitements revêtant des exigences fortes de disponibilité, prévoir de connecter l'infrastructure de télécommunications par au moins deux voies différentes.

Fiche n° 7 - La maintenance

Lors de la maintenance et des interventions techniques, la sécurité des données doit être garantie.

On recommande également de supprimer les données des matériels destinés à être mis au rebut.

Les précautions élémentaires

- Garantir que des données ne seront pas compromises lors d'une intervention de maintenance en appliquant une ou plusieurs des mesures énumérées ci-dessous :
  - l'enregistrement des interventions de maintenance dans une **main courante ;**
  - l'encadrement par un responsable de l'organisme lors d'interventions par des tiers ;
  - la configuration des systèmes critiques (serveurs, équipements réseau …) de manière à empêcher leur télémaintenance.
- Inspecter tout matériel contenant des supports de stockage avant sa mise au rebut ou sa sortie du périmètre de l'organisme, pour s'assurer que toute donnée sensible en a bien été supprimée de façon sécurisée.

A titre d'exemple, l'ANSSI accorde des certifications de premier niveau à des logiciels pour réaliser cet objectif (http://www.ssi.gouv.fr/archive/fr/confiance/certif-cspn.html).

Concernant la mise au rebut de matériels, on peut mentionner:

- les broyeurs et déchiqueteurs pour le papier ou les supports numériques tels que les CD et DVD ;
- les «dégausseurs[9]» pour les unités de stockage à technologie magnétique.

Ces préconisations concernent également les matériels en location lorsqu'ils sont retournés à l'expiration du délai contractuel.

- En matière d'**assistance sur les postes clients :**
  - les outils d'administration à distance doivent être configurés de manière à **recueillir l'accord** de l'utilisateur avant toute intervention sur son poste, par exemple en cliquant sur une icône ou encore en répondant à un message s'affichant à l'écran ;
  - l'utilisateur doit également pouvoir **constater si la prise de main à distance est en cours** et quand elle se termine, par exemple grâce à l'affichage d'un message à l'écran.

9 - Un «dégausseur» est un équipement réalisant une destruction irrémédiable de données confidentielles par démagnétisation.

Ce qu'il ne faut pas faire

- Installer des applications pour la télémaintenance qui sont vulnérables (ex : certaines versions de xVNC, cf. http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-035/).

Pour aller plus loin

- Il faut restreindre, voire interdire l'accès physique et logique, aux ports de diagnostic et de configuration à distance.

A titre d'exemple, il faut restreindre l'usage du protocole SNMP qui permet la configuration des équipements réseau par connexion sur le port TCP 161.

- Des préconisations concernant les matériels mis au rebut sont disponibles dans le document de l'ANSSI intitulé Guide technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter, disponible à l'adresse http://www.ssi.gouv.fr/archive/fr/documentation/Guide_effaceur_V1.12du040517.pdf.

Modèle de clauses de confidentialité pouvant être utilisées en cas de maintenance par une tierce partie

Chaque opération de maintenance devra faire l'objet d'un descriptif précisant les dates, la nature des opérations et les noms des intervenants, transmis à X.

En cas de télémaintenance permettant l'accès à distance aux fichiers de X, Y prendra toutes dispositions afin de permettre à X d'identifier la provenance de chaque intervention extérieure. A cette fin, Y s'engage à obtenir l'accord préalable de X avant chaque opération de télémaintenance dont elle prendrait l'initiative.

Des registres seront établis sous les responsabilités respectives de X et Y, mentionnant les date et nature détaillée des interventions de télémaintenance ainsi que les noms de leurs auteurs.

Fiche n° 8 - Tracabilité et gestion des incidents

afin d'être en mesure d'identifier a posteriori un accès frauduleux à des données personnelles, une utilisation abusive de telles données, ou de déterminer l'origine d'un incident, il convient d'enregistrer les actions effectuées sur le système informatique. Pour ce faire, le responsable d'un système informatique doit mettre en place un dispositif adapté aux risques associés à son système. Celui-ci doit enregistrer les évènements pertinents, garantir que ces enregistrements ne peuvent être altérés, et dans tous les cas conserver ces éléments pendant une durée non excessive.

Les précautions élémentaires

- Prévoir un système de journalisation (c'est-à-dire un enregistrement dans des «fichiers de logs») des activités des utilisateurs, des anomalies et des événements liés à la sécurité. Ces journaux doivent conserver les évènements sur une période glissante ne pouvant excéder six mois (sauf obligation légale, ou demande de la CNIL, de conserver ces informations pour une durée plus longue).

Prévoir au minimum la journalisation des accès des utilisateurs incluant leur identifiant, la date et l'heure de leur connexion, ainsi que la date et l'heure de leur déconnexion. Le format de l'horodatage doit de préférence prendre comme référence le temps UTC[10].

Dans certains cas, il peut être nécessaire de conserver également le détail des actions effectuées par l'utilisateur, telles que les données consultées par exemple.

Se référer au document du CERTA disponible à l'adresse internet http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-005, pour un exemple de mise en œuvre.

- Informer les utilisateurs de la mise en place d'un tel système.
- Protéger les équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés.
- Etablir des procédures détaillant la surveillance de l'utilisation du traitement et procéder périodiquement à l'examen des informations journalisées.
- Le responsable de traitement doit être informé dans les meilleurs délais des failles éventuelles de sécurité.
- En cas d'accès frauduleux à des données personnelles, le responsable de traitement devrait le notifier aux personnes concernées.

10 - Coordinated Universal Time

Ce qu'il ne faut pas faire

- Utiliser les informations issues des dispositifs de journalisation à d'autres fins que celles de garantir le bon usage du système informatique.

Pour aller plus loin

- Les horloges des différents systèmes de traitement de l'information d'un organisme ou d'un domaine de sécurité doivent être synchronisées à l'aide d'une source de temps fiable et préalablement définie.

Lorsque le traitement fait appel à des ressources réseau, la synchronisation des sources de temps peut être réalisée par le recours au protocole NTP[11].

- Le responsable de traitement doit **se tenir informé des vulnérabilités techniques** des systèmes et entreprendre les actions appropriées pour traiter le risque associé.

11 - Le protocole NTP (Network Time Protocol) permet de caler l'horloge d'un ordinateur sur une source d'horodatage fiable via le réseau.

Fiche n°9 - Sécurité des locaux

Afin de protéger efficacement les locaux où sont hébergés les traitements de données personnelles, prévoir :

- des alarmes afin de déceler une intrusion au sein d'une zone sécurisée ;
- des mesures afin de ralentir la progression des personnes parvenues à s'introduire ;
- des moyens afin de mettre fin à l'intrusion.

Les précautions élémentaires

- Restreindre les accès aux salles ou bureaux susceptibles d'héberger du matériel contenant des données au moyen de **portes verrouillées**, ou de sas d'accès pour les équipements les plus critiques.
- Installer des **alarmes anti-intrusion** et les vérifier périodiquement.

Ce qu'il ne faut pas faire

- **Sous-dimensionner ou négliger l'entretien de la climatisation** des salles hébergeant les machines : une panne sur cette installation a souvent comme conséquence l'arrêt des machines ou encore l'ouverture des portes des salles et donc la neutralisation de facto d'éléments concourant à la sécurité physique des locaux.

Pour aller plus loin

- Il faut protéger les zones sécurisées par des contrôles pour s'assurer que seul le personnel dûment habilité est admis dans ces zones. Pour ce faire, il convient de suivre les recommandations suivantes :
  - concernant les zones dans lesquelles des informations sensibles sont traitées ou stockées, des **dispositifs d'authentification doivent être prévus. Il peut s'agir** de cartes d'accès accompagnées d'un numéro d'identification personnel. Un journal des accès intervenus lors des trois derniers mois au plus doit être tenu à jour de façon sécurisée ;
  - à l'intérieur des zones à accès réglementé, exiger **le port d'un moyen d'identification visible** (badge) pour toutes les personnes ;
  - les visiteurs (personnel en charge de l'assistance technique, etc.) doivent avoir un accès limité. La date et l'heure de leur arrivée et départ doivent être consignées ;
  - Réexaminer et mettre à jour régulièrement les permissions d'accès aux zones sécurisées et les supprimer si nécessaire.

Fiche n° 10 - Sécurité du réseau informatique interne

Pour tous les services réseau, il faut identifier les fonctions réseau et les niveaux de service nécessaires au bon fonctionnement du traitement et n'autoriser que ceux-ci.

Les précautions élémentaires

- **Limiter les flux réseau au strict nécessaire.** Par exemple, si l'accès à un serveur web passe obligatoirement et uniquement par l'utilisation du protocole SSL, il faut autoriser uniquement les flux réseau IP entrants sur cette machine sur le port de communication 443 et bloquer tous les autres ports de communication.

  Se référer aux documents suivants du CERTA :

  - http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-001/, pour les questions de filtrage et pare-feux ;
  - http://www.certa.ssi.gouv.fr/site/CERTA-2005-REC-001/, pour la mise en œuvre de SSL.

- Sécuriser les accès au système d'information au moyen d'appareils informatiques nomades tels que des ordinateurs portables par la mise en place de connexions **VPN** reposant sur des algorithmes cryptographiques réputés forts[12] et mettant si possible en œuvre un matériel (carte à puce, boitier générateur de mots de passe à usage unique (OTP One Time Password), etc.).

- Recourir au chiffrement de la communication par l'usage du protocole SSL avec une clé de 128 bits lors de la mise en œuvre de services web.

Ce qu'il ne faut pas faire

- Utiliser le protocole telnet pour la connexion à distance aux équipements actifs du réseau (pare-feu, routeurs, switches). Il convient d'utiliser plutôt SSH ou un accès physique direct à l'équipement.

- Installer des réseaux WiFi. Si de tels équipements doivent être mis en œuvre, il est nécessaire de sécuriser les connexions par l'usage du **protocole WPA**, en choisissant le mode de chiffrement AES/CCMP.

Pour plus de détails sur l'accès aux réseaux sans fil, se référer aux mesures préconisées sur le site du CERTA à l'adresse http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002/.

12 - Cf. Fiche n°17 – Le chiffrement

Pour aller plus loin

- Le cloisonnement réseau permet notamment d'éviter que la compromission d'un poste n'entraîne celle de l'ensemble du système. En pratique, il est recommandé de segmenter le réseau en sous-réseaux logiques selon les services censés y être déployés.

Un exemple d'une telle architecture est représenté ci-dessous.

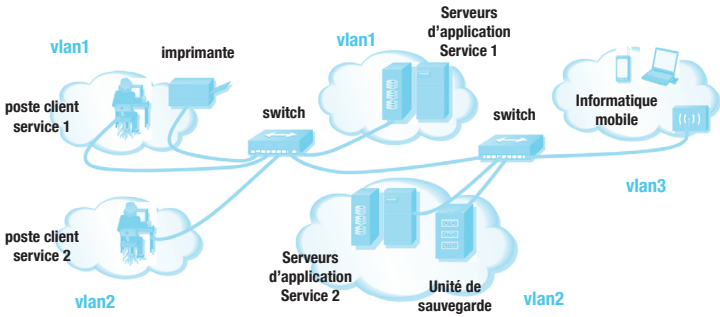


Figure 1: Exemple d'un réseau informatique cloisonné par VLAN

Pour mettre en œuvre un tel cloisonnement, plusieurs méthodes sont envisageables :

- la mise en place de réseaux physiques distincts : il est alors possible de cloisonner les différents réseaux en contrôlant les flux de données sur la base des adresses réseau ;
- le recours à des réseaux virtuels, dénommés VLAN : l'objectif de cette technologie est de regrouper certains matériels connectés à un équipement physique (switch) selon des critères logiques (par exemple l'appartenance à un département), dans le but de séparer les trafics réseau entre les différents groupes ainsi constitués.

Il est également possible de restreindre les connexions autorisées en différenciant par exemple un réseau interne pour lequel aucune connexion venant d'Internet n'est autorisée, et un réseau dit DMZ (DeMilitarized Zone ou zone démilitarisée en français) accessible depuis Internet.

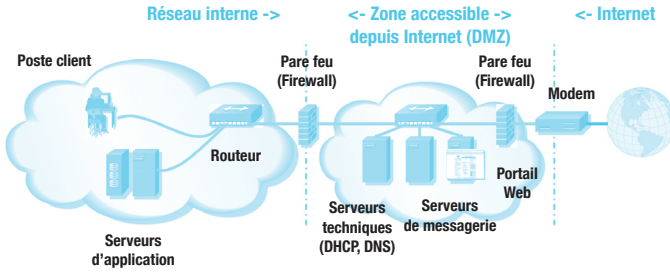


Figure 2: Exemple de mise en œuvre d'une DMZ

La mise en œuvre d'une DMZ nécessite l'installation de passerelles sécurisées (pare-feux) entre les réseaux à cloisonner afin de contrôler les flux d'information entrants et sortants.

- Des systèmes de détection d'intrusion (Intrusion Detection Systems ou IDS) peuvent être mis en place en vue d'analyser le trafic réseau en temps réel, afin d'y détecter toute activité suspecte évoquant un scénario d'attaque informatique. Le but de ces systèmes est de déjouer les attaques informatiques au plus tôt. Il convient de rappeler que les utilisateurs d'un réseau informatique doivent être avertis lorsqu'il est prévu une analyse des contenus transitant sur le réseau.
- Il peut être envisagé de mettre en place l'identification automatique de matériels comme moyen d'authentification des connexions à partir de lieux et matériels spécifiques. Cette technique utilise par exemple les identifiants uniques des cartes réseau (l'adresse MAC) afin de détecter la connexion d'un dispositif non répertorié et de router son trafic réseau de manière séparée.

Fiche n° 11 - sécurite des serveurs et des applications

Les serveurs sont les équipements les plus critiques et à ce titre, ils méritent des mesures de sécurité renforcées.

Les précautions élémentaires

- Changer les mots de passe par défaut par des mots de passe complexes devant respecter au minimum les règles suivantes :
  - avoir une taille de **10 caractères minimum** ;
  - utiliser des **caractères de types différents** (majuscules, minuscules, chiffres et caractères spéciaux) ;
  - **changer** de mot de passe notamment lors du **départ d'un des administrateurs.**
- Installer les mises à jour critiques des systèmes d'exploitation sans délai en programmant une vérification automatique hebdomadaire.
- En matière d'administration de bases de données:
  - ne pas utiliser les serveurs hébergeant les bases de données à d'autres fins (notamment pour naviguer sur des sites internet, accéder à la messagerie électronique …) ;
  - utiliser des comptes nominatifs pour l'accès aux bases de données, sauf si une contrainte technique l'empêche ;
  - mettre en œuvre des mesures et/ou installer des dispositifs pour se prémunir des attaques par injection de code SQL, scripts… ;
  - prévoir des mesures particulières pour les bases de données «sensibles» (chiffrement en base, chiffrement des sauvegardes).
- Assurer une continuité de disponibilité des données, ce qui nécessite notamment de prendre des précautions en cas d'installation ou de mises à jour de logiciels sur les systèmes en exploitation.
- Mettre à jour les applications lorsque des failles critiques ont été identifiées et corrigées.

Ce qu'il ne faut pas faire

- Utiliser des services non sécurisés (authentification en clair, flux en clair, etc…).
- Placer les bases de données dans une zone directement accessible depuis Internet.

Pour aller plus loin

- Les systèmes sensibles, c'est-à-dire tout système traitant de données sensibles ou jugées confidentielles pour l'entreprise, doivent disposer d'un **environnement informatique dédié** (isolé).
- S'agissant des logiciels s'exécutant sur des serveurs, il est conseillé d'utiliser des **outils de détection des vulnérabilités** (logiciels scanners de vulnérabilité tels que nmap (http://nmap.org/), nessus (http://www.nessus.org), nikto (http://www.cirt.net/nikto2) etc.) pour les traitements les plus critiques afin de détecter d'éventuelles failles de sécurité. Des systèmes de détection et prévention des attaques sur des systèmes/serveurs critiques dénommés Host Intrusion Prevention peuvent aussi être utilisés.
- Selon la nature de l'application, il peut être nécessaire d'assurer l'intégrité des traitements par le recours à des signatures du code exécutable garantissant qu'il n'a subi aucune altération. A cet égard, une vérification de signature tout au long de l'exécution (et pas seulement avant l'exécution) rend plus difficile la compromission d'un programme.

Fiche n° 12 - Sous-traitance

Les données à caractère personnel communiquées à ou gérées par des sous-traitants doivent bénéficier de garanties de sécurité.

Les précautions élémentaires

- Prévoir dans les contrats liant l'organisme et les sous-traitants une clause spécifique couvrant la confidentialité des données personnelles confiées à ces derniers. Un modèle de clause est fourni ci-après.
- Prendre des dispositions (audits de sécurité, visite des installations, etc…) afin de s'assurer de l'effectivité des garanties offertes par le sous-traitant en matière de protection des données. Cela inclut notamment :
  - le chiffrement des données selon leur sensibilité ou à défaut l'existence de procédures garantissant que la société de prestation n'a pas accès aux données qui lui sont confiées ;
  - le chiffrement de la liaison de données (connexion de type https par exemple) ;
  - des garanties en matière de protection du réseau, traçabilité (journaux, audits), gestion des habilitations, authentification, etc.
- Prévoir les conditions de restitution des données et de leur destruction en cas de rupture ou à la fin du contrat.

Ce qu'il ne faut pas faire

- Avoir recours à des services offrant des fonctionnalités d'informatique répartie[13] sans garantie quant à la localisation géographique effective des données.

Pour aller plus loin

- Concernant les données de santé, il est rappelé qu'un hébergeur se doit d'avoir un agrément délivré par le ministre de la Santé. Le référentiel de constitution d'un dossier est disponible sur le site http://esante.gouv.fr/.

13 - cloud computing.

Modèle de clauses de confidentialité pouvant être utilisées en cas de sous-traitance

Les supports informatiques et documents fournis par la société X à la société Y restent la propriété de la société X.

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226-13 du code pénal), il en va de même pour toutes les données dont Y prend connaissance à l'occasion de l'exécution du présent contrat.

Conformément à l'article 34 de la loi informatique et libertés modifiée, Y s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

Y s'engage donc à respecter les obligations suivantes et à les faire respecter par son personnel :

- ne prendre aucune copie des documents et supports d'informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la présente prestation prévue au contrat, l'accord préalable du maître du fichier est nécessaire ;
- ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat ;
- ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;
- prendre toutes mesures de sécurité, notamment matérielles, pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée du présent contrat ;
- et en fin de contrat, à procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies.

A ce titre, Y ne pourra sous-traiter l'exécution des prestations à une autre société, ni procéder à une cession de marché sans l'accord préalable de X.

X se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par Y.

En cas de non-respect des dispositions précitées, la responsabilité du titulaire peut également être engagée sur la base des dispositions des articles 226-5 et 226-17 du nouveau code pénal.

X pourra prononcer la résiliation immédiate du contrat, sans indemnité en faveur du titulaire, en cas de violation du secret professionnel ou de non-respect des dispositions précitées.

Fiche n°13 - L'archivage

On distingue habituellement trois catégories d'archives :

- Les bases actives ou archives courantes : il s'agit des données d'utilisation courante par les services en charge de la mise en œuvre du traitement ;
- Les archives intermédiaires : il s'agit des données qui ne sont plus utilisées mais qui présentent encore un intérêt administratif pour l'organisme. Les données sont conservées sur support distinct et sont consultées de manière ponctuelle et motivée ;
- Les archives définitives : il s'agit des données présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction. Elles sont alors régies par le livre II du Code du patrimoine et non par la loi «informatique et libertés».

Les archives doivent être sécurisées et chiffrées si les données archivées sont des données sensibles ou jugées confidentielles par l'entreprise.

Les précautions élémentaires

- Mettre en œuvre des modalités d'accès spécifiques aux données archivées du fait que l'utilisation d'une archive doit intervenir de manière ponctuelle et exceptionnelle.
- Suivre les préconisations données dans la fiche n°17 - Le chiffrement, s'agissant du chiffrement des archives.
- S'agissant de la destruction des archives, choisir un mode opératoire garantissant que l'intégralité d'une archive a été détruite.

A titre d'exemple, l'ANSSI accorde des certifications de premier niveau à des logiciels pour réaliser cet objectif (http://www.ssi.gouv.fr/site_rubrique54.html).

Selon la nature des supports, on peut mentionner :

- Les broyeurs et déchiqueteurs pour le papier ainsi que les supports numériques tels que les CD et DVD ;
- Les «dégausseurs» pour les unités de stockage à technologie magnétique.

Se référer au document *Guide technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter.* (http://www.ssi.gouv.fr/archive/fr/documentation/Guide_effaceur_V1.12du040517.pdf).

Ce qu'il ne faut pas faire

- Utiliser des supports ne présentant pas une garantie de longévité suffisante. A titre d'exemple, on peut mentionner les CD et DVD dont la longévité dépasse rarement 4/5 années.

Pour aller plus loin

- Plus d'informations sur les problématiques d'archivage sont disponibles sur le site des archives de France : http://www.archivesdefrance.culture.gouv.fr/gerer/archives-electroniques/.

Fiche n° 14 - L'échange d'informations avec d'autres organismes

la communication de données à caractère personnel doit être sécurisée, c'est-à-dire que la confidentialité, l'intégrité et l'authenticité des informations doivent être assurées.

La messagerie électronique et le fax, même s'ils apportent un gain de temps, ne constituent pas a priori un moyen de communication sûr pour transmettre des données personnelles. Une simple erreur de manipulation (e-mail erroné, erreur de numérotation du fax destinataire…) peut conduire à divulguer à des destinataires non habilités des informations personnelles et à porter ainsi atteinte au droit à la vie privée des personnes.

En outre la transmission via Internet de données nominatives comporte, compte tenu de l'absence générale de confidentialité du réseau Internet, des risques importants de divulgation de ces données et d'intrusion dans les systèmes informatiques internes.

Les précautions élémentaires

- Concernant la confidentialité de la communication :
  - Chiffrer les données avant leur enregistrement sur le support lorsque la transmission de données s'effectue par l'envoi d'un support physique (à technologie optique ou magnétique).
  - Lors d'un envoi via un réseau :
  - si cette transmission utilise la messagerie électronique, chiffrer les pièces à transmettre. A ce sujet, il convient de se référer aux préconisations de la fiche n°17 – Le chiffrement ;
  - s'il s'agit d'un transfert de fichiers, utiliser un protocole garantissant la confidentialité, tel que SFTP ;
  - si cette transmission utilise le protocole HTTP, utiliser le protocole SSL (HTTPS) pour assurer l'authentification des serveurs la confidentialité des communications.
- Dans tous les cas, la transmission du secret (clé de déchiffrement, mot de passe, etc.) garantissant la confidentialité du transfert doit s'effectuer dans une transmission distincte, si possible via un canal de nature différente de celui ayant servi à la transmission des données (par exemple, envoi du fichier chiffré par mail et communication du mot de passe par téléphone ou SMS).

- Si vous êtes amené à utiliser le **fax**, il est recommandé de mettre en place les mesures suivantes :
  - le fax doit être situé dans un local physiquement contrôlé et accessible uniquement au personnel habilité ;
  - l'impression des messages doit être subordonnée à l'introduction d'un code d'accès personnel ;
  - lors de l'émission des messages, le fax doit afficher l'identité du fax destinataire afin d'être assuré de l'identité du destinataire ;
  - doubler l'envoi par fax d'un envoi des documents originaux au destinataire ;
  - préenregistrer dans le carnet d'adresse des fax (si cette fonctionnalité existe) les destinataires potentiels.

Ce qu'il ne faut pas faire

- Transmettre des fichiers contenant des données personnelles en clair via des messageries web du type Gmail ou Hotmail.

Pour aller plus loin

• Concernant l'intégrité des données :

il est recommandé de calculer une empreinte sur les données en clair et de transmettre cette empreinte afin que l'intégrité des données soit vérifiée au moment de leur réception. Les calculs d'empreintes peuvent être réalisés à l'aide d'algorithmes de hachage tels que SHA-1 ou SHA-2. L'utilisation de SHA-2 est recommandée.

• Concernant l'authenticité des données :

l'émetteur peut signer les données avant leur envoi afin de garantir qu'il est à l'origine de la transmission. Une signature électronique requiert la mise en place d'une infrastructure de gestion de clés publiques[14] (en anglais Public Key Infrastructure, PKI) ;

l'utilisation d'algorithmes à clés publiques, lorsque les différents acteurs ont mis en place une **infrastructure de gestion de clés publiques**, apparaît particulièrement adaptée pour garantir la confidentialité et l'intégrité des communications, ainsi que l'authenticité de l'émetteur par l'utilisation de la signature l'électronique.

14 - Sur la notion de clé publique, voir la fiche n°17 – Le chiffrement

Une telle infrastructure consiste à délivrer une paire de clés privée/publique à l'ensemble des personnes susceptibles d'échanger des informations. Les clés publiques doivent être certifiées par une autorité de certification pour laquelle chacun des utilisateurs à le certificat[15] racine, ceci afin que l'authenticité des clés publiques soient garanties.

Les algorithmes mis en œuvre dans le cadre de cette infrastructure doivent suivre les préconisations de l'annexe B1 du Référentiel Général de Sécurité[16].

Ce référentiel précise notamment les longueurs de clé à considérer. À la date de rédaction de ce document, il est par exemple préconisé que :

- La taille minimale d'une clé RSA soit de 2048 bits, pour une utilisation ne devant pas dépasser l'année 2020 ;
- Pour une utilisation au-delà de 2020, la taille minimale de la clé RSA est de 4096 bits.

Ces valeurs sont données à titre indicatif, et sont dépendantes du contexte propre à chaque traitement.

- Dès lors que les données ont été reçues, que leur intégrité a été vérifiée par le destinataire et qu'elles ont été intégrées dans le système d'information, il est conseillé de détruire les supports ou fichiers ayant servi à leur transmission.

15 - Un certificat est constitué :
1.d'une valeur de clé publique
2.d'informations complémentaires permettant d'identifier le propriétaire de la clé (adresse email, nom…)
3. d'une signature par une clé publique d'une autorité de certification sur l'ensemble de ces informations.

16 - **http://www.references.modernisation.gouv.fr/rgs-securite**

Fiche n° 15 - Les développements informatiques

la protection des données à caractère personnel doit être partie intégrante du développement informatique afin d'empêcher toute erreur, perte, modification non autorisée, ou tout mauvais usage de celles-ci dans les applications.

Les précautions élémentaires

- Effectuer le développement informatique dans un environnement informatique distinct de celui de la production (par exemple, sur des ordinateurs différents, dans des salles machines différentes).
- **Prendre en compte les exigences de sécurité vis-à-vis des données à caractère personnel dès l'élaboration du service ou dès la conception de l'application.**

Ce qu'il ne faut pas faire

- **Utiliser des données à caractère personnel réelles pour les phases de développement et de test.** Si des données réelles sont néanmoins requises, il convient que celles-ci soient anonymisées (cf fiche n°16 – L'anonymisation)

Pour aller plus loin

- Le développement doit imposer des **formats de saisie et d'enregistrement des données qui minimisent les données collectées.** Par exemple, s'il s'agit de collecter l'année de naissance d'une personne, le champ du formulaire correspondant ne doit pas permettre la saisie du mois et du jour de naissance. Cela peut se traduire notamment par la mise en œuvre d'un menu déroulant limitant les choix pour un champ d'un formulaire.
- Les formats de données doivent être compatibles avec la mise en œuvre d'une durée de conservation.
- Le **contrôle d'accès** aux données par des catégories d'utilisateurs doit être intégré au moment du développement.
- Eviter le recours à des zones de texte libre. Si de telles zones sont requises, il faut faire apparaître soit en filigrane, soit comme texte pré-rempli s'effaçant sitôt que l'utilisateur décide d'écrire dans la zone, les mentions suivantes :

Les personnes disposent d'un droit d'accès aux informations contenues dans cette zone de texte. Les informations que vous y inscrivez doivent être PERTINENTES au regard du contexte. Elles ne doivent pas comporter d'appréciation subjective, ni faire apparaître, directement ou indirectement les origines raciales, les opinions politiques, philosophiques ou religieuses, les appartenances syndicales ou les mœurs de la personne concernée.

Fiche n° 16 - L'anonymisation

On distingue les concepts d'**anonymisation irréversible** et **d'anonymisation réversible**, cette dernière étant parfois dénommée **pseudonymisation**.

L'anonymisation irréversible consiste à supprimer tout caractère identifiant à un ensemble de données. Concrètement, cela signifie que toutes les informations **directement et indirectement identifiantes** sont supprimées et à rendre impossible toute ré-identification des personnes.

L'anonymisation réversible est une technique qui consiste à remplacer un identifiant (ou plus généralement des données à caractère personnel) par un *pseudonyme*. Cette technique permet la levée de l'anonymat ou l'étude de corrélations en cas de besoin.

Les précautions élémentaires

- Etre très vigilant dans la mesure où une ré-identification peut intervenir à partir d'informations partielles[17].
- Anonymiser une donnée personnelle en procédant comme suit :
  - **générer un secret suffisamment long et difficile à mémoriser**[18] ;
  - appliquer une fonction dite à sens unique sur les données : un algorithme convenant pour une telle opération est un algorithme de hachage à clé secrète, tel que l'algorithme HMAC[19] basé sur SHA-1.
- Si une donnée personnelle est anonymisée et non purement supprimée, il existe un risque de ré-identification[20].
  - En l'absence d'un besoin de levée de l'anonymat, prévoir de supprimer le secret afin de réduire ce risque.
  - Dans l'hypothèse où le secret doit être conservé pour une éventuelle levée de l'anonymisation ou une finalité de corrélation entre différentes données, prévoir de **mettre en place des mesures organisationnelles[21] pour garantir la confidentialité de ce secret**. Les accès à celui-ci doivent être tracés.

17 - A titre d'exemple, la ville et la date de naissance peuvent parfois suffire à identifier formellement une personne.
18 - Un exemple de chaine de caractères ayant valeur de secret est : f{rXan?cl$IPCk|Bb-aQWH6ud0;#oQt§.
19 - HMAC est spécifié dans le document RFC 2104, **http://www.ietf.org/rfc/rfc2104.txt**
20 - Il est possible d'associer la donnée originale à la donnée anonymisée dès lors que le secret est compromis et que la complexité de la donnée originale n'est pas suffisante. Les données personnelles possèdent souvent une complexité, autrement dit une entropie insuffisante. Par exemple, les patronymes français sont en nombre limité (inférieur à 1,5 millions), tous répertoriés.
21 - Un exemple de telle mesure consiste à partager la clé en trois paires de valeurs confiées à trois personnes différentes, nécessitant qu'au moins deux personnes se réunissent pour reconstituer la clé.

Ce qu'il ne faut pas faire

- Utiliser des mécanismes d'anonymisation non validés par des experts. Un bon algorithme d'anonymisation doit notamment :
  - être irréversible ;
  - avoir un très faible taux de collision : deux données différentes ne doivent pas mener à un même résultat ;
  - avoir une grande dispersion : deux données quasi-semblables doivent avoir des résultats très différents ;
  - pouvoir mettre en œuvre une clé secrète.

Pour aller plus loin

- Dans certains cas, il est conseillé d'appliquer une double anonymisation réversible : soit l'application d'une seconde anonymisation sur le résultat d'une première anonymisation. Ces deux anonymisations doivent utiliser des secrets différents, détenus par des organismes distincts.

L'algorithme FOIN (Fonction d'Occultation des Informations Nominatives) est un exemple d'algorithme à double anonymisation.

Fiche n° 17 - Le chiffrement

le **chiffrement,** parfois improprement appelé cryptage, est un procédé cryptographique permettant de garantir la confidentialité d'une information. Les mécanismes cryptographiques permettent également d'assurer l'**intégrité** d'une information, ainsi que l'**authenticité** d'un message en le signant.

On distingue deux familles cryptographiques permettant de chiffrer : la cryptographie symétrique et la cryptographie asymétrique :

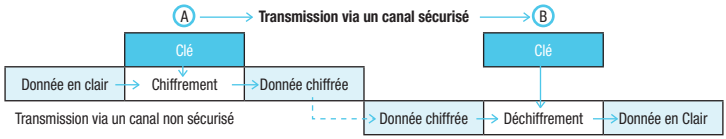
- la cryptographie symétrique comprend les mécanismes pour lesquels la même clé sert à chiffrer et à déchiffrer ;
- la cryptographie asymétrique comprend les mécanismes pour lesquels la clé servant à chiffrer, appelée clé publique, est différente de la clé servant à déchiffrer, appelée clé privée. On parle de paire de clés.

L'intérêt de la cryptographie asymétrique est multiple :

- Chaque personne n'a besoin que d'une paire de clés privée/publique. A contrario, la cryptographie symétrique nécessite d'avoir autant de clés différentes que de couples de personnes qui veulent communiquer confidentiellement ;
- Les clés publiques peuvent être rendues … publiques pour quiconque souhaitant vous envoyer un message confidentiel. Toutefois l'authenticité des clés publiques n'est ainsi pas garantie. Aussi la mise en œuvre de la cryptographie asymétrique dans le cadre d'échanges de messages s'inscrit le plus souvent dans la mise en place d'une Infrastructure de Gestion de Clés Publiques[22] ;

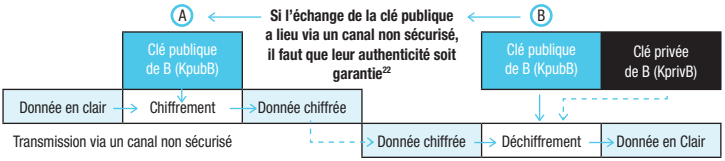
L'échange d'informations de manière confidentielle entre deux parties A et B s'effectue comme suit :

Chiffrement au moyen de la cryptographie symétrique :



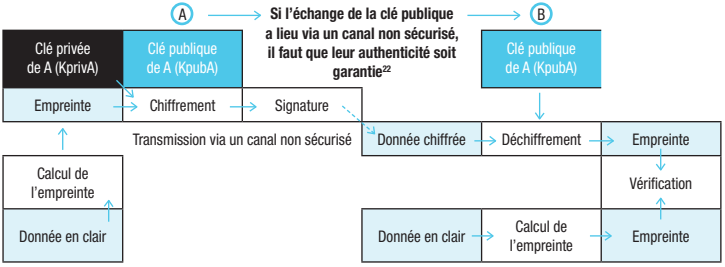
22 - Voir la fiche n°14 – L'échange d'informations avec d'autres organismes

Chiffrement au moyen de la cryptographie asymétrique :



Signature au moyen de la cryptographie asymétrique :

Du fait que la clé privée n'est détenue que par une personne, la cryptographie asymétrique permet de garantir l'imputabilité d'un message en le signant à l'aide sa clé privée. Ce que la cryptographie ne permet pas du fait du partage de la clé entre deux parties.



Les précautions élémentaires

- **Concernant le chiffrement symétrique :**
  - utiliser des algorithmes à l'état de l'art, tels que l'AES ou le triple DES ;
  - utiliser des clés cryptographiques de longueur au moins égale à 128 ou 256 bits et qui ne soient pas des clés faibles[23]. En outre, la génération des clés doit se faire au moyen de logiciels éprouvés, par exemple openSSL[24].

22 - Voir la fiche n°14 – L'échange d'informations avec d'autres organismes
23 - Un exemple de clé faible est la clé nulle :00000000000000000000000000000000
24 - **http://www.openssl.org/**

- **Concernant le chiffrement asymétrique :**
  - Utiliser des algorithmes éprouvés, tels que le RSA ou l'ECC ;
  - Concernant la longueur des clés, il convient de suivre les préconisations données en annexe B1 du Référentiel Général de Sécurité[25]. En outre, la génération des clés doit se faire au moyen de logiciels éprouvés, par exemple openSSL[24].

Ce qu'il ne faut pas faire

- Utiliser l'algorithme simple DES, algorithme considéré comme obsolète.
- Utiliser des logiciels ou des librairies cryptographiques n'ayant pas fait l'objet de vérifications par des tierces parties à l'expertise avérée.

Pour aller plus loin

- Le **chiffrement de documents** peut être réalisé au moyen de différents logiciels, dont notamment :
  - le **logiciel TrueCrypt**[26], permettant la mise en œuvre de conteneurs[27] chiffrés ;
  - le **logiciel Gnu Privacy Guard**, permettant la mise en œuvre de la cryptographie asymétrique et dont une version est disponible à l'adresse http://www.gnupg.org/index.fr.html. Il est suggéré de choisir des clés PGP DSA/ElGamal ayant au minimum une taille de 1536 bits, ou des clés RSA d'une taille minimale de 2048 bits ;
  - à défaut, il peut être envisagé d'utiliser un utilitaire de compression tel que ceux basés sur l'algorithme ZIP, dès lors qu'ils permettent le chiffrement à l'aide d'un mot de passe. C'est le cas notamment du **logiciel 7-Zip**.

24 - **http://www.openssl.org/**
25 - Cf **http://www.references.modernisation.gouv.fr/rgs-securite**
26 - Il convient d'utiliser la version 6.0a qui bénéficie d'une certification de premier niveau par l'ANSSI.
27 - Par conteneur, il faut comprendre un fichier susceptible de contenir plusieurs fichiers.

Acronymes

AES : Advanced Encryption Standard, un algorithme cryptographique symétrique considéré comme une référence.

DES : Data Encryption Standard, un algorithme cryptographique symétrique considéré comme dépassé.

DHCP : Dynamic Host Configuration Protocol, un protocole permettant la configuration dynamique des paramètres réseau d'une machine (y compris l'attribution de son adresse IP).

DNS : Domain Name Server, Serveur de nom de domaine, Ces serveurs font notamment la correspondance entre un nom de machine, par exemple www.cnil.fr, et une adresse IP, en l'occurrence 94.247.233.54.

DSA : Digital Signature Algorithm, un algorithme cryptographique de signature.

EBIOS : Une méthodologie d'évaluation des risques relatifs à la sécurité des Systèmes d'Information.

ECC : Elliptic Curve Cryptography, cryptographie basée sur les courbes elliptiques.

HMAC : une fonction de hachage permettant de garantir l'authenticité d'un message

HTTP : HyperText Transfer Protocol, le protocole du web.

HTTPS : HTTP sécurisé par SSL.

MAC : Medium Access Control, l'adresse MAC est un identifiant unique de chaque interface réseau.

RAID : Redundant Array of Independent Disks, désigne une technologie permettant de stocker des données sur plusieurs disques durs afin d'améliorer la tolérance aux pannes.

RSA : Un algorithme de cryptographie asymétrique, du nom de ses trois concepteurs Rivest, Shamir et Adelman.

SFTP : un protocole de communication fonctionnant au-dessus de SSH pour transférer et gérer des fichiers à distance.

SHA : Secure Hash Algorithm, une famille de fonctions de hachage standardisées (SHA-1, SHA256, etc.).

SI : Système d'Information.

SQL : Structure Query Language, le protocole servant à interroger ou manipuler des bases de données.

SSH : Secure SHell, un protocole sécurisé de connexion à distance en mode console.

SSL : Secure Socket Layer, un protocole qui permet notamment de sécuriser le trafic HTTPS.

VNC : Virtual Network Computer, un protocole permettant la prise de contrôle à distance d'un poste de travail.

VPN : Virtual Private Network, un canal de communication qui garantit la confidentialité des échanges.

Annexe 1 - Menaces informatiques

liste des menaces ciblant les systèmes informatiques et les fichiers à considérer en priorité :

- **pour les matériels :**
  - détournement de l'usage prévu (stockage de fichiers personnels sur l'ordinateur de bureau, stockage de documents sensibles sur une clé USB non prévue à cet effet…) ;
  - espionnage (observation d'un écran à l'insu de son utilisateur, géolocalisation d'un téléphone…) ;
  - dépassement des limites de fonctionnement (panne de courant, température excessive d'une salle serveur, unité de stockage pleine…) ;
  - détérioration (inondation ou incendie d'une salle serveur, dégradation du fait de l'usure naturelle, vandalisme…) ;
  - modification (ajout de périphérique, webcam, *keylogger*[28]…) ;
  - disparition (vol, perte, cession ou mise au rebut d'un ordinateur…).
- **pour les logiciels :**
  - détournement de l'usage prévu (élévation de privilèges, fouille de contenu, effacement de traces…) ;
  - analyse (balayage d'adresses réseaux, collecte de données de configuration…) ;
  - dépassement des limites de fonctionnement (injection de données en dehors des valeurs prévues, débordement de tampon…) ;
  - suppression totale ou partielle (bombe logique, effacement de code…) ;
  - modification (contagion par un code malveillant, manipulation inopportune lors d'une mise à jour…) ;
  - disparition (cession d'un logiciel développé en interne, non renouvellement de licence…).
- **pour les canaux de communication :**
  - écoute passive (écoute sur un câble réseau, interception…) ;
  - saturation (exploitation distante d'un réseau wifi, téléchargement non autorisé, assourdissement de signal…) ;
  - dégradation (sectionnement de câblage, torsion de fibre optique…) ;
  - modification (changement d'un câble par un autre inapproprié, modification de chemin de câble…),
  - disparition (vol de câbles en cuivre…) ;
  - attaque du milieu (*man in the middle*, rejeu/réémission d'un flux…).
- **pour les supports papier :**
  - détournement de l'usage prévu (falsification, effacement, utilisation du verso d'impressions papier en tant que brouillons…) ;
  - espionnage (lecture, photocopie ou photographie de documents…) ;
  - détérioration (vieillissement naturel, corrosion chimique, dégradation volontaire, embrasement lors d'un incendie…) ;
  - disparition (vol de documents, revente, perte, prêt, mise au rebut…).

28 - Dispositif d'enregistrement des frappes du clavier.

Une difficulté ? Une hésitation ?

Plus d'informations sur le site de la **CNIL** www.cnil.fr,

Une permanence de renseignements juridiques
par téléphone est assurée tous les jours de **10h à 12h et de 14h à 16h**
au **01 53 73 22 22**

Vous pouvez en outre adresser toute demande
par télécopie au **01 53 73 22 00**

Evaluez le niveau de sécurité des données personnelles dans votre organisme

Avez-vous pensé à ?

Fiche		Mesure	
1	Analyser les risques	**Recensez** les fichiers et données à caractère personnel et les traitements	❑
		Déterminez les menaces et leurs impacts sur la vie privée des personnes	❑
		Mettez en œuvre des **mesures de sécurité adaptées** aux menaces	❑
2	Authentifier les utilisateurs	Définissez un identifiant ***(login)*** unique à chaque utilisateur	❑
		Adoptez une **politique de mot de passe utilisateur rigoureuse**	❑
		Obligez l'utilisateur à **changer son mot de passe après réinitialisation**	❑
3	Gérer les habilitations & sensibiliser les utilisateurs	**Définissez des profils d'habilitation**	❑
		Supprimez les permissions d'accès obsolètes	❑
		Documentez les procédures d'exploitation	❑
		Rédigez une **charte informatique** et annexez-la au **règlement intérieur**	❑
4	Sécuriser les postes de travail	**Limitez le nombre de tentatives d'accès** à un compte	❑
		Installez un «**pare-feu**» *(firewall)* logiciel	❑
		Utilisez des **antivirus régulièrement mis à jour**	❑
		Prévoyez une procédure de **verrouillage automatique de session**	❑
5	Sécuriser l'informatique mobile	Prévoyez des **moyens de chiffrement** pour les **ordinateurs portables** et les unités de stockage amovibles (**clés USB**, CD, DVD…)	❑
6	Sauvegarder et prévoir la continuité d'activité	Effectuez des **sauvegardes régulières**	❑
		Stockez les supports de sauvegarde dans un endroit sûr	❑
		Prévoyez des moyens de sécurité pour le convoyage des sauvegardes	❑
		Prévoyez et testez régulièrement la **continuité d'activité**	❑
7	Encadrer la maintenance	**Enregistrez les interventions** de maintenance dans une **main courante**	❑
		Effacez les données de tout matériel avant sa **mise au rebut**	❑
		Recueillez l'accord de l'utilisateur avant toute intervention sur son poste	❑
8	Tracer les accès et gérer les incidents	Prévoyez un **système de journalisation**	❑
		Informez les utilisateurs de la mise en place du système de journalisation	❑
		Protégez les équipements de journalisation et les informations journalisées	❑
		Notifiez les personnes concernées des accès frauduleux à leurs données	❑
9	Protéger les locaux	**Restreignez les accès** aux locaux au moyen de **portes verrouillées**	❑
		Installez des **alarmes anti-intrusion** et vérifiez-les périodiquement	❑
10	Protéger le réseau informatique interne	**Limitez les flux réseau au strict nécessaire**	❑
		Sécurisez les accès distants des appareils informatiques nomades par **VPN**	❑
		Utilisez le protocole SSL avec une clé de 128 bits pour les **services web**	❑
		Mettez en œuvre le protocole WPA - AES/CCMP pour les réseaux WiFi	❑
11	Sécuriser les serveurs et les applications	Adoptez une **politique de mot de passe administrateur rigoureuse**	❑
		Installez sans délai les **mises à jour critiques**	❑
		Assurez une **disponibilité** des données	❑
12	Gérer la sous-traitance	Prévoyez une **clause spécifique** dans les contrats des sous-traitants	❑
		Assurez-vous de l'**effectivité des garanties** prévues (audits de sécurité, visites...)	❑
		Prévoyez les **conditions de restitution** et de destruction des données	❑
13	Archiver	Mettez en œuvre des modalités d'accès spécifiques aux données archivées	❑
		Détruisez les archives obsolètes de manière sécurisée	❑
14	Sécuriser les échanges avec d'autres organismes	**Chiffrez** les données avant leur envoi	❑
		Assurez-vous qu'il s'agit du **bon destinataire**	❑
		Transmettez le **secret** lors d'un envoi distinct et via un canal différent	❑