Politique relative à la sécurité et à la confidentialité de l'information

Sécurité des données

(BLD DATA SEC)

TABLE DES MATIERES

1. Introduction

Le présent document fait partie intégrante de la méthodologie relative à la sécurité et à la confidentialité de l'information dans la sécurité sociale. Il est destiné aux responsables, aux sous-traitants de l'information, au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de la sécurité sociale (IPSS).

L'évolution rapide des technologies de stockage et de transmission numériques de données entraîne une augmentation considérable des risques pour la sécurité et la confidentialité, mais ce sont principalement la miniaturisation poussée et la mobilité accrue qui en découle qui requièrent des mesures adaptées.

En raison de cette évolution, il semble indiqué de mettre en place une politique de spécifique selon le type de support de stockage, la mobilité normalement escomptée et la possibilité d'envoi électronique de données. L'intégration éventuelle d'un dispositif de stockage numérique dans un appareil intelligent aura une influence sur les mesures de sécurité applicables et donc sur les droits d'utilisation. Outre une politique générale, il peut être nécessaire, dans certains cas, d'imposer des règles spécifiques pour un type d'appareil déterminé.

Pour plus de précisions concernant le type de données (données d'entreprise, données à caractère personnel, données sociales, données médicales), veuillez-vous référer à la politique relative à la classification des données. L'enregistrement, le traitement, la transmission de données ne sont pas autorisés, si ce n'est en appliquant les règles de cette politique ou avec l'autorisation explicite du service compétent.

La protection des données est abordée du point de vue de la mémoire et des techniques de transmission utilisées et se limite aux directives générales. Quoi qu'il en soit, les mesures nécessaires doivent être prises pour satisfaire aux dispositions légales en vigueur, notamment en matière de stockage, d'accès aux données et de discrétion. Le domaine couvert est celui des technologies et du matériel.

Le présent document traite des mesures en vigueur pour l'ensemble des données utilisées par l'institution dans le cadre de sa mission ou dans son infrastructure. Sont en d'autres termes concernées toutes les données enregistrées dans ou en dehors de l'institution, par elle ou en son nom, sur des supports de stockage analogiques ou numériques (en sa possession ou non), déplacées physiquement ou échangées électroniquement entre supports de stockage, quels qu'ils soient.

2. Sécurité des données

Toute organisation souscrit à la politique suivante relative à la sécurité et à la confidentialité de l'information pour l'ensemble des informations et systèmes d'information placés sous sa responsabilité :

- Toute organisation doit sécuriser l'accès aux données[1] nécessaires à l'application et à l'exécution de la sécurité sociale au moyen d'un système d'identification, d'authentification et d'autorisation.

1 Dans cette norme, le terme "donnée" ne désigne pas uniquement les données sociales à caractère personnel, mais tous les éléments logiques d'un système d'information qui en assurent le traitement. Exemples : programmes, applications, fichiers, utilitaires système et autres éléments du système d'exploitation.

Annexe A : Gestion du document

Gestion des versions

Date	Auteur	Version	Description du changement	Date d'approbation	Date d'entrée en vigueur
2007		V2007	Première version	10/10/2007	10/10/2007
2017		V2017	Intégration EU GDPR	07/03/2017	07/03/2017

Erreurs et oublis

Si des erreurs ou des problèmes sont constatés à la lecture du présent document, vous êtes prié en tant que lecteur de transmettre au conseiller en sécurité de la plateforme eHealth une brève description de l'erreur ou du problème ainsi que de sa place dans le document conjointement à vos données de contact.

Définitions

Dans un souci de cohérence de la terminologie et des concepts utilisés dans tous les documents de politique, toutes les définitions relatives à la sécurité et à la confidentialité de l'information sont centralisées dans un document intitulé "Définitions relatives à la sécurité et à la confidentialité de l'information".

Annexe B : Références

Ci-dessous figurent des documents qui ont servi d'inspiration au présent document.

- ISO, "ISO/IEC 27001:2013 Information Security Management System Requirements", septembre 2013, 23 pages
- ISO, "ISO/IEC 27002:2013 Code of Practice for Information Security Management", septembre 2013, 80 pages
- ISACA, "COBIT 5 for Information Security", mai 2012, 220 pages
- NIST, SP800-60 volume II revision 1, "Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories", août 2008, 279 pages

Ci-dessous figurent des références aux sites web qui ont servi d'inspiration au présent document.

- http://www.iso.org/iso/iso27001
- https://www.iso.org/standard/54534.html
- https://www.iso.org/standard/54533.html
- https://www.iso.org/fr/standard/68427.html
- http://www.isaca.org/cobit
- http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf

Annexe C : Directives relatives à la sécurité de l'information

A. Données sur support analogique

Il s'agit des données qui ne sont pas enregistrées sous forme numérique, généralement sur papier.

1 Création

Le support doit satisfaire aux normes de qualité que l'on peut raisonnablement attendre pour l'application. La création des données se fait autant que possible sur la base d'une source validée. La création des données doit être conforme à la réglementation en vigueur. Des mesures doivent être prises pour permettre le cas échéant de prouver l'authenticité du document. Pour la sécurité de l'information, la création des données sur support analogique doit être évitée au maximum.

2 Stockage

Les données non publiques doivent au moins être protégées par un périmètre physique avec contrôle d'accès. Les données médicales à caractère personnel doivent au moins être protégées par un double périmètre physique avec contrôle d'accès. Une liste nominative de toutes les personnes ayant accès au plus petit périmètre doit être dressée, avec mention de leurs autorisations spécifiques[2]. Partout où des documents originaux sont conservés, des mesures adéquates doivent être prises pour éviter des pertes liées aux effets de l'environnement.

3 Traitement

Les données à caractère personnel ne peuvent être traitées que par des personnes autorisées. Le traitement de données médicales s'effectue - sauf exceptions - dans un périmètre physique avec contrôle d'accès. Pour tous les traitements de données médicales, une liste nominative des personnes ayant un accès doit être dressée, avec mention de leurs autorisations spécifiques. Cette liste est placée sous la surveillance du médecin responsable du traitement des données médicales[3]. Le suivi du traitement doit être assuré de façon contrôlée.

4 Transport physique

Pour le transport de données dans le périmètre d'un bâtiment, aucune mesure de protection spécifique ne doit être prise, pour autant que le transport se fasse toujours sous la surveillance d'une personne autorisée. Le transport de données non publiques doit au moins être protégé par un périmètre physique et géré par un transporteur de confiance. Le transport de données médicales à caractère personnel doit au moins être protégé par un périmètre physique et géré par un service de transport interne. Si aucun transport interne ne peut être organisé, la protection doit être assurée à l'aide d'un container scellé, le tout géré par un transporteur de confiance. Pour les cas exceptionnels, il est possible de déroger à la règle moyennant autorisation du médecin responsable qui peut imposer des mesures de sécurité complémentaires. Pour chaque transport de données médicales à caractère personnel hors du périmètre physique, des données de transport (qui, quoi, quand) doivent être enregistrées.

5 Destruction

La destruction de documents contenant des données sociales à caractère personnel doit se faire de façon contrôlée La destruction peut se faire au moyen d'une déchiqueteuse ou en rassemblant les données dans des conteneurs spéciaux dont le contenu est détruit par une firme spécialisée. La destruction de données originales n'est possible qu'après en avoir averti le propriétaire et compte tenu des dispositions légales y afférentes. L'acte de destruction doit faire l'objet d'une autorisation.

[2] Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la sécurité sociale, art.26, § 2.

[3] Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la sécurité sociale, art.26, § 1, § 2.

B. Données numériques sur l'infrastructure fixe

Sont en l'occurrence concernée les données numériques enregistrées sur des postes de travail fixes, des serveurs et leurs systèmes de stockage. Par extension également, les données communiquées uniquement via un réseau interne fixe câblé (LAN) appartenant à l'institution. Dès qu'un poste de travail fixe est physiquement déplacé, les directives relatives au matériel mobile s'appliquent. Si des données enregistrées sont transportées autrement que via le réseau fixe, les directives relatives à la communication électronique s'appliquent. L'hypothèse retenue dans le cadre de cette distinction est que les appareils fixes et le réseau fixe sont efficacement protégés par la conjugaison de leur périmètre physique, de leur contrôle d'accès logique et des mesures de contrôle prises (prise de logs, monitoring). Dans le contexte de la transmission et du stockage électroniques, les implantations de l'institution peuvent être considérées comme relevant du même réseau fixe si les échanges de données internes présentent un taux élevé de protection et si l'accès physique à chaque bâtiment est suffisamment contrôlé. Le matériel non autorisé ne peut être raccordé au réseau fixe de l'institution. Ce réseau fixe doit être protégé de façon telle que la connexion de matériel non autorisé puisse être détectée ou empêchée.

1 Création

Le matériel doit satisfaire aux normes de qualité que l'on peut raisonnablement attendre pour l'application. La création des données se fait autant que possible sur la base d'une source validée. La création des données doit être conforme à la réglementation en vigueur. Des mesures doivent être prises pour permettre le cas échéant de prouver l'authenticité des données.

2 Stockage

Les données non publiques à caractère personnel ne peuvent pas être stockées sur le poste de travail fixe, si ce n'est pour la durée d'une session d'application. Les systèmes de stockage de données non publiques à caractère personnel doivent au moins être protégés par un double périmètre physique avec contrôle d'accès. Une liste nominative de toutes les personnes ayant accès au plus petit périmètre doit être dressée, avec mention de leurs autorisations.

3 Traitement

L'accès logique aux données non publiques doit être organisé via un système d'identification, d'authentification et d'autorisation. Le traitement de ces données ne peut se faire que via des postes de travail reliés au réseau fixe de l'institution. Le traitement à partir ou par l'intermédiaire d'un autre réseau relève des directives relatives à l'échange de données et/ou aux supports de stockage mobiles. Pour tous les traitements de données médicales, une liste nominative des personnes ayant un accès doit être dressée, avec mention de leurs autorisations spécifiques. Le traitement des données médicales est placé sous la surveillance du médecin responsable[4].

4 Transport

Le transport physique de ces données n'est autorisé que sous le contrôle du service informatique compétent et exclusivement dans le cadre de ses compétences légitimes. Des directives opérationnelles spécifiques s'appliquent dans ce cas. Le transport électronique de ces données n'est autorisé que sur le réseau fixe de l'institution. Si ces données sont envoyées hors du réseau fixe de l'institution ou autrement que via ce réseau fixe, les directives spécifiques pour l'échange de données s'appliquent.

5 Commentaire

Chacun des différents bâtiments centraux et régionaux forme un périmètre physique distinct. Si le réseau entre ces bâtiments présente un niveau élevé de protection, le réseau total dans et entre ces bâtiments peut être considéré comme faisant partie du même réseau fixe, pour autant que le périmètre physique soit sous contrôle de l'institution. Un appareil mobile (un laptop par exemple) spécialement configuré par le service ICT compétent pour être directement connecté au réseau fixe, peut être connecté au réseau et déconnecté par l'utilisateur lui-même. Les règles relatives au matériel mobile s'appliquent pour la protection des données. Le stockage de données non publiques requiert le périmètre physique du bâtiment et un deuxième périmètre physique au sein de celui-ci, par exemple une salle informatique ou un local fermé. Le stockage permanent de telles données sur un poste de travail fixe dans un local non fermé n'est de ce fait pas autorisé.

[4] Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la sécurité sociale, art.26, § 1, § 2.

C. Données sur support de stockage mobile

Sont en l'occurrence concernés les supports de stockages numériques et les appareils qui intègrent ou peuvent utiliser ces supports et ne sont pas en permanence connectés au réseau fixe (exemples : ordinateur portable, PDA, CD, DVD, disque dur externe, memory stick, mémoires flash, support de backup, stockage en cloud).

1 Généralités

Chaque échange de données de ou vers un support de stockage mobile relève des règles relatives à l'échange de données. L'utilisation de supports de stockage mobiles pour le traitement de données dans le cadre de la mission n'est autorisée que moyennant autorisation explicite et un objectif bien défini. Il n'est pas permis de relier directement un support de stockage mobile au réseau fixe de l'institution, si ce n'est moyennant autorisation du service compétent. La connexion d'un support de stockage mobile sur le matériel ou sur le réseau de l'institution, de quelque façon que ce soit, donne le droit à l'institution de prendre toutes les mesures de sécurité jugées nécessaires, en ce compris des contrôles antivirus, la prise de copies et un contrôle du respect du règlement d'ordre intérieur. L'utilisation d'un support de stockage ou de matériel non conforme aux règles de sécurité n'est pas autorisée.

2 Stockage

Le stockage de données confidentielles sur un appareil mobile nécessite le cryptage des données[5], à l'exception du stockage limité de données à caractère personnel dont le traitement constitue une exception explicite aux termes de la loi sur le respect de la vie privée[6]. Le stockage de données confidentielles sur un support de stockage ou un appareil mobiles n'est autorisé qu'après approbation par le service compétent de l'institution. Une sauvegarde régulière de toutes les données enregistrées sur un support de stockage mobile doit être effectuée sur le réseau fixe.

3 Traitement

Ce paragraphe ne s'applique que lorsque le matériel mobile est suffisamment intelligent, rendant possible le traitement des données. On parle de traitement en ligne si un accès au réseau fixe est requis pour le traitement des données et qu'il faut pour ce faire installer une connexion. Dans tous les autres cas, il s'agit d'un traitement hors ligne. Pour le transfert de données de/vers l'appareil portable, les directives relatives à l'échange de données s'appliquent également. Lors du traitement de données confidentielles, l'utilisateur prend les précautions nécessaires pour en empêcher l'accès à des tierces personnes.

- Traitement en ligne : un appareil mobile ne peut être directement connecté au réseau fixe que s'il a été spécifiquement configuré à cet effet ; dans tous les autres cas de traitement en ligne, la connexion doit toujours passer par l'extranet de l'institution. Pour les institutions primaires, cela signifie par l'extranet de la sécurité sociale. L'accès aux données en ligne sera lié, selon leur classification, à un niveau et une forme d'authentification adaptés. L'accès aux données confidentielles sur le réseau fixe doit être organisé via un système nominatif d'identification et d'autorisation qui permette d'identifier sans équivoque le matériel et l'utilisateur. Le traitement ne peut se faire sur des appareils qui ne supportent pas cette fonctionnalité. Aucune autre connexion ne peut être installée en parallèle, au risque de compromettre la sécurité du traitement en ligne.
- Traitement en ligne : lors du traitement de données hors ligne, l'utilisateur est responsable de la synchronisation des données modifiées à intervalles réguliers vers un support de stockage en ligne. En cas de traitement hors ligne, l'utilisateur est responsable de la mise à jour à intervalles réguliers du logiciel de protection.

4 Commentaire

Les appareils mobiles sont soumis à des normes de sécurité plus poussées que les appareils du réseau fixe. Les directives relatives aux appareils mobiles restent applicables, même si les appareils mobiles sont configurés pour être connectés au réseau fixe ou y sont effectivement connectés. De même, le matériel qui n'appartient pas à l'institution peut dans certains cas être utilisé pour le traitement de données non confidentielles, c'est le cas lors de la consultation d'un site web ou de ses e-mails sur le PC au domicile de l'utilisateur.

[5] En effet, la BCSS exige des mesures adaptées, conformément à la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la sécurité sociale, art. 22 et art. 26, § 3.

[6] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, art. 3, § 2.

D. Échange des données

1 Règles

Sont en l'occurrence concernée les échanges électroniques de données entre support de stockage et appareils fixes et/ou mobiles, pour autant qu'au moins un de ces supports de stockage ou appareils appartienne à l'institution ou soit sous-traité pour sa mission. L'échange de données entre appareils connectés au réseau fixe de l'institution a été traité dans le chapitre "Données numériques sur l'infrastructure fixe". Lors de l'échange de données confidentielles, la source et le destinataire du transfert de données doivent être une partie de confiance. Une authentification mutuelle est nécessaire lors de l'échange de données à caractère personnel. L'échange de données entre un support de stockage mobile et le réseau fixe doit toujours être contrôlable par le service compétent de l'institution. La transmission de données confidentielles doit toujours se faire sous forme cryptée. En principe, le cryptage du canal de transmission suffit. Si des doutes subsistent quant au niveau de protection du canal de transmission, les données elles-mêmes doivent être cryptées. Pour chaque échange électronique de données, les autorisations et la réglementation en vigueur doivent être strictement respectées. Si des espaces de stockage intermédiaires échappent au contrôle de l'institution, il importe de veiller à ce que d'éventuels restes du trafic de transmission soient cryptés. Les données médicales doivent être cryptées avant l'envoi, à moins que la transmission s'effectue dans le cadre d'une connexion end-to-end cryptée et contrôlée par l'institution.

2 Commentaire

Dès que des données quittent le réseau fixe (deviennent mobiles), les directives relatives à l'échange de données s'appliquent. Relèvent également de cette directive l'envoi et la réception externes d'informations via e-mail et internet. Lorsque des informations confidentielles sont envoyées à l'institution, même par une voie non sécurisée, elles doivent être enregistrées selon la classification des données concernées. L'envoi de données confidentielles via ces canaux sans mesures de protection complémentaires est tout à fait interdit. La synchronisation locale de données d'agenda par exemple est possible pour autant qu'aucune donnée confidentielle ne soit échangée.

Annexe D : Concepts de sécurité de l'information

1. Rétention de l'information

Une politique de rétention de l'information est un protocole convenu ou imposé qui détermine le délai pendant lequel l'information doit être conservée et accessible, suivant la réglementation et la législation éventuelles en vigueur ou la nécessité business ou personnelle.
Le délai de rétention de l'information est fonction de la nature du document et des dispositions légales.

Type de données - Exemples

Données utilisateurs et applications

- Rapports de réunion
- Contrats et licences
- Documents d'assurance
- Données à caractère personnel
- Données d'entreprise
- E-mail

Données système

- Microsoft Windows
- Linux Red hat
- Oracle virtual machine (OVM)

Les décisions suivantes doivent être prises :

- Les données sont-elles cruciales pour l'entreprise ; autrement dit, l'entreprise peut-elle continuer d'exister sans ces données ?
- S'agit-il de données à caractère personnel ? Leur conservation satisfait-elle à la réglementation relative à la vie privée ?
- Y a-t-il des raisons légales de conserver les données ?
- Quand les données ont-elles été utilisées pour la dernière fois ? Ne sont-elles pas pertinentes ?
- Des données doubles sont-elles conservées ?
- Tous les e-mails doivent-ils être conservés pour une utilisation directe ?

Il faut aussi savoir si les données sont cruciales pour l'entreprise ; autrement dit, l'entreprise peut-elle continuer d'exister sans ces données ?

- S'agit-il de données à caractère personnel ?
- Y a-t-il des raisons légales de conserver les données ?
- Quand les données ont-elles été utilisées pour la dernière fois ? Ne sont-elles pas pertinentes ?
- Des données doubles sont-elles conservées ?

En l'absence d'une réglementation, la conservation de l'information doit être limitée au délai nécessaire à la réalisation des objectifs pour lesquels l'information a été recueillie.

Remarque : du point de vue de la sécurité de l'information, l'accès à l'information doit être limité au propriétaire de l'information. Il est donc important de bien classifier les données suivant leur importance et leurs caractéristiques, ainsi que d'y associer un délai de rétention. Cette classification doit être réalisée par chaque section ou département responsable des documents.

2. Sauvegarde de l'information

Une sauvegarde consiste à copier des donnés de manière à pouvoir restaurer dans leur état initial des données corrompues ou perdues.

La même classification concernant la détermination de la rétention est donc valable ici aussi. Le délai de rétention d'une sauvegarde peut toutefois différer du délai de rétention des données présentes sur les différents appareils. L'accès à la sauvegarde dépend des procédures de sauvegarde de l'organisation. Celles-ci indiquent comment est réalisée une sauvegarde et où se trouvent les responsabilités.

Remarque : les paramètres complémentaires suivants peuvent donc être mentionnés dans le tableau de classification des documents :

- Une sauvegarde est-elle nécessaire ? Données système ?
- Tous les e-mails doivent-ils être conservés et donc sauvegardés ?
- Délai de rétention d'une sauvegarde ?
- Traitement des fichiers ROT (Redundant, Obsolete, Trivial) ?
- Les données doivent-elles être cryptées ? Comment le key management va-t-il alors être effectué ?
- Qui a accès à la sauvegarde ?
- S'agit-il de données cruciales ? RPO (Recovery point objective) / RTO (Recovery Time objective)

Pour éviter que des délais de rétention irréalistes soient spécifiés dans l'analyse des données, il faut préciser au responsable qu'il a un impact sur la facturation (interne). Chaque institution doit donc établir une politique de sauvegarde décrivant tous ces détails.

3. Archivage de l'information

L'archivage consiste à supprimer les données originales et à les transférer dans un environnement sécurisé où leur intégrité est assurée.

À l'expiration du délai de rétention des données, il peut être décidé d'archiver les données. Selon le programme d'archivage, plusieurs opérations peuvent alors être exécutées. Lors de l'archivage, les données sont copiées à un

autre endroit, éventuellement converties en un format "ouvert", horodatées et transférées - de préférence - vers un support non volatile, par exemple une worm tape ou un worm disk.[7] Avec ce type de support, les données archivées ne peuvent plus être modifiées pour des raisons légales. L'utilisation d'un format "ouvert" permet de lire les données archivées dans des versions plus récentes d'applications ou éventuellement de les importer dans des programmes concurrents.

Remarque : le tableau de classification des documents indique si des données peuvent être archivées et, si oui, pour combien de temps. À l'expiration du délai de rétention de l'archivage, le support physique doit être détruit par des sociétés spécialisées.

4. Destruction de l'information

Le protocole indique également comment des données peuvent être concrètement supprimées, conformément à la réglementation et à la législation en vigueur ou parce que les données sont superflues.

À l'expiration du délai de rétention de l'archivage, le support physique doit être détruit par des sociétés spécialisées (Destroy). Les données peuvent être supprimées de plusieurs manières :

- **A.** Clear : la suppression logicielle de données, par des commandes standard ou une réinitialisation des paramètres d'usine, cette dernière étant souvent recommandée pour les appareils mobiles et les routeurs/commutateurs.
- **B.** Purge : des techniques de laboratoire sont appliquées pour une suppression physique ou logique (techniques de cryptographie) du support (broyeur, démagnétisation), cette dernière nécessitant un logiciel spécifique. Pour les disques SSD, il existe généralement une procédure de sécurité pour effacer le disque. Celle-ci est généralement propre au fabricant, auprès duquel on peut trouver l'information exacte (chercher SSD secure erase utility). Pour les SSD également, il existe des logiciels commerciaux permettant d'effacer les données de façon sûre, par exemple "Parted Magic".
- **C.** Destroy : la destruction physique du support doit toujours être appliquée lorsque le support, par exemple un disque dur, est défectueux.
- **D.** Réinstallation : en cas de réutilisation d'appareils, il peut suffire d'installer une nouvelle image (type Ghost, Bare Metal), vu que celle-ci écrase totalement les données existantes.

Une attention particulière doit être accordée aux appareils utilisés sous le principe BYOD (Bring Your Own Device), via lequel des systèmes privés peuvent être connectés au réseau de l'institution. Le maillon le plus faible dans la sécurisation est dans ce cas l'utilisateur. En cas de vol de systèmes non sécurisés, les données sont exposées à de grands risques. Il existe des logiciels qui, une fois activés, peuvent rendent inexploitables les données des systèmes une fois qu'ils sont connectés à internet. Les mêmes principes valent pour le télétravail et les déplacements en dehors de l'institution. Une bonne protection physique doit être promue auprès de l'utilisateur.

5. Audit de l'information

Régulièrement, un audit doit être réalisé pour vérifier si la politique de sauvegarde et la classification de l'information sont à jour et bien appliquées. L'audit de l'information est l'œuvre d'une personne qui n'appartient pas au service chargé de la gestion des données. Cet audit de l'information débouche sur un rapport qui est débattu avec le responsable de l'institution en vue de déterminer les actions à entreprendre. Ensuite, un nouvel audit est réalisé pour vérifier si les adaptations demandées ont bien été apportées.
Pour réaliser cet audit de l'information, chaque institution doit rédiger un document d'audit (liste de contrôle) en adéquation avec ses politiques et classifications.

6. Incidents de sécurité de l'information

Les données sont sécurisées avec les identifiants. Il convient toutefois de prévoir une procédure qui sanctionne les infractions à la sécurité de l'information - délibérées ou non - étant donné que la fuite d'informations peut être très préjudiciable à l'entreprise et/ou à l'image.

[7] WORM : Write Once Read Many times

À titre d'exemple, nous pouvons citer le transport de supports par des sociétés qui assurent la maintenance sous garantie sur, par exemple, des disques, des serveurs... Il s'agit là d'une infraction à la sécurité de l'information. Ceci devrait être formellement spécifié sous forme contractuelle.
Chaque institution doit établir cette procédure, vu qu'une infraction ne touche pas chaque institution de la même manière. Il faut aussi prévoir l'interdiction du transport de supports par des sociétés externes.

7. Exceptions

Chaque règle a ses exceptions. Les données ne peuvent pas toujours être traitées de façon standard, en raison par exemple des contraintes techniques du matériel, d'un manque de stockage ou pour des raisons de confidentialité. Que ce soit à titre permanent ou temporaire, le modèle de classification est idéal pour indiquer les exceptions. Lorsque les exceptions ne sont pas enregistrées, elles risquent d'être "oubliées", pouvant conduire à terme à des situations fâcheuses. L'enregistrement de ces exceptions est la responsabilité de la personne qui rédige les documents de classification.

Annexe E : Lien avec la norme ISO 27002:2013

Nous renvoyons ici à la (aux) clause(s) principale(s) de la norme ISO 27002:2013 relative à l'objet du présent document.

Norme ISO 27002:2013	
Politique de sécurité	
Organisation de la sécurité de l'information	
Personnel sûr	
Gestion des moyens d'exploitation	**Oui**
Sécurisation des accès	
Cryptographie	**Oui**
Sécurité physique et de l'environnement	**Oui**
Sécurisation des processus	
Sécurité de la communication	
Achats, maintenance et développement de systèmes d'information	
Relations fournisseurs	
Gestion des incidents de sécurité	
Aspects de sécurité de l'information de la gestion de la continuité	
Respect	**Oui**

***** FIN DU DOCUMENT *****