Systèmes d'informations

Politique de sécurité

AVERTISSEMENT					
* Si ce document est à un indice supérieur à ceux précédemment diffusés, il les annule et les remplace. * Toute modification, édition, utilisation ou diffusion non autorisée est interdite.					
ETAT DES VERSIONS SUCCESSIVES					
INDICE	**DATE**	**OBSERVATIONS**	**REDAC.**	**VERIF.**	**APPROB.**
1.1	15/06/2006	Version initiale	**DSTI**		
1.2	28/03/2012	Evolution	**FMI/ESC/ JNR/OPA**		
2.1	Mai 2012	Suppression Annexe 2	**OPA**		

DOCUMENT ETABLI SOUS LA RESPONSABILITE DU/DES SIGNATAIRES				
Signataire	**Nom**	**Société/ Direction**	**Date**	**Visa**
Rédacteurs :	F. MIRRA/ JN RIBEYROL / E. SCHUPPE	SPIE SA	28/03/2012	
Approbateurs :	B. LOCHET / O. PARENT	SPIE SA	28/03/2012	

Sommaire

1. OBJET

Ce document définit les mesures, les rôles et les responsabilités liés à la sécurité des systèmes d'informations de SPIE et établit les principes de bases et approches adoptés par SPIE.

Ces principes s'appliquent à tout système informatique utilisé pour produire, traiter, collecter, consulter, échanger ou stocker de l'information.

Toute personne habilitée à utiliser les ressources informatiques de SPIE, ou à les développer et les intégrer, doit se conformer aux principes et règles édictés dans ce document.

2. DOCUMENTS ASSOCIES

2.1. DOCUMENTS DE REFERENCE

	Version	Date	Titre
ISO/CEI 27001:2005			Technologies de l'information Techniques de sécurité — Systèmes de gestion de la sécurité de l'information
ISO CEI 27002			Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la gestion de la sécurité de l'information

Si la version n'est pas indiquée, il s'agit de la dernière version applicable.

2.2. DOCUMENTS ANNEXES

	Version	Date	Titre
Annexe 1		15/06/2006	Précautions particulières pour les appareils informatiques portables
Annexe 2		15/06/2006	La protection juridique du logiciel par le droit de la propriété intellectuelle
Annexe 3		15/06/2006	Demande d'accès distant au réseau SPIE
Annexe 4		15 Mai 2012	Politique de sauvegarde des données

Si la version n'est pas indiquée, il s'agit de la dernière version applicable.

3. INTRODUCTION

SPIE dispose d'une infrastructure informatique rendant possible l'accès et le partage de l'information électronique pour tous les collaborateurs et personnes habilités. Cette ouverture implique d'assurer la sécurité des systèmes informatiques utilisés ainsi que des informations stockées.

Ce document «politique de sécurité des systèmes d'information » a été élaboré pour aider à la compréhension des responsabilités, des risques encourus et à l'identification des mesures à prendre.

SPIE est une société dans laquelle la notion de capacité d'adaptation à l'environnement est importante. Il peut donc se trouver des situations dans lesquelles l'application stricte de la politique mentionnée dans ce document est délicate voire impossible. La société a adopté le principe de gestion des risques dans la mise en œuvre des recommandations ce qui implique l'identification et la qualification des risques pour implémenter les mesures pratiques à coûts raisonnables pour de tels cas qui doivent cependant demeurer exceptionnels. L'identification et la qualification sont du ressort de la fonction systèmes d'informations, le management de la fonction devant valider les solutions retenues.

La vérification de la mise en œuvre des principes de sécurité des systèmes d'informations fait partie intégrante des missions de la Direction de l'Audit Interne.

La Direction des Systèmes d'Information, sous l'autorité et le contrôle de la Direction Générale, est la responsable de la définition des solutions technologiques et des processus en matière de sécurité des systèmes d'informations ainsi que de la mise à jour de ce document.

La mise en œuvre des mesures appropriées, sous la direction du management des unités, est de la responsabilité des collaborateurs de la fonction systèmes d'informations et ce sur leur périmètre d'action.

4. PRINCIPES GENERAUX

4.1. ENJEUX

La politique de sécurité des systèmes d'informations de SPIE est guidée par trois grands principes généraux :

- Confidentialité
- Intégrité
- Disponibilité

Ces principes sont déclinés ci-après afin de permettre la meilleure compréhension possible de leur définition et des enjeux qu'ils portent.

Confidentialité : toutes les données et programmes doivent être protégés contre toute publication non autorisée (interne ou externe).
Une divulgation non autorisée peut entraîner des pertes très importantes à la fois financières mais aussi de marché ou de spécificité de savoir-faire.

Intégrité : l'intégrité des données fait référence à l'authenticité d'origine, la précision et la complétude.
Beaucoup d'utilisateurs pensent que l'intégrité des données est assurée dès l'instant ou celles-ci sont stockées dans un système informatique ce qui n'est pas le cas du fait d'erreurs, d'omissions, de dysfonctionnements ou d'actes de malveillance. Toute erreur d'intégrité peut entraîner des pertes financières et/ou de réputations très importantes.
Toute donnée doit donc être protégée contre une création, modification ou suppression non autorisée ou impropre. Les données doivent être gérées par les seuls utilisateurs habilités à la faire.

Disponibilité : le terme de disponibilité fait référence au besoin de continuité de service.
L'utilisateur a besoin d'accéder au système d'informations pour pouvoir accomplir sa tâche dans l'entreprise. L'environnement, les mécanismes et les procédures doivent donc être mis en place afin que le système soit accessible et opérant en fonction des besoins de l'utilisateur et ce en dehors des périodes d'indisponibilité planifiées.

Le non-respect de ce principe peut avoir des effets sur la productivité et l'efficience des collaborateurs de SPIE ainsi que sur le respect d'engagements calendaires de la société vis-à-vis de tiers.

4.2. PROJETS DE SYSTEMES D'INFORMATIONS

Tout projet de systèmes d'information mené dans l'entreprise doit intégrer un volet sécurité informatique dans le respect des règles édictées par le présent document.

4.3. DEROGATIONS

Toute dérogation de la présente politique sécurité doit faire l'objet d'une acceptation formelle de la Direction des Systèmes d'Informations.

5. SECURITE LIEE AUX RESSOURCES HUMAINES

La direction de l'entreprise SPIE demande à ses salariés, contractant et utilisateurs tiers d'appliquer les règles de sécurité conformément à la politique de sécurité des systèmes d'informations.

L'entreprise permet à l'ensemble de ses salariés, contractants et utilisateurs tiers de bénéficier d'un niveau adéquat de qualification, formation et sensibilisation aux procédures de sécurité et à l'utilisation correcte des moyens de traitement de l'information, en vue de réduire le plus possible le risque lié à la sécurité.

Pour cela il faut veiller à ce que les salariés, contractants et tiers :

- Soient correctement informés sur leur fonction et responsabilités en matière de sécurité de l'information avant d'avoir accès aux systèmes d'information,
- Prennent connaissance des lignes directrices concernant les attentes en matière de sécurité dans le cadre de leurs fonctions,
- Soient incités à appliquer les politiques de sécurité.

6. SECURITE PHYSIQUE ET ENVIRONNEMENTALE

6.1. GENERALITES

6.1.1. Les équipements

Les équipements constituant les systèmes d'informations de SPIE doivent avoir été agréés par l'entreprise.

Sont considérés les équipements entrant dans les catégories suivantes :

- Serveurs,
- Stockages,
- Systèmes de communications,
- Les postes de travail (PC),
- Tout terminal permettant l'accès aux réseaux et données de l'entreprise (Incluant les terminaux téléphoniques),
- Copieurs et imprimantes multifonctions,
- Systèmes de sécurité

Par conséquent, tout accès à une donnée d'entreprise effectué depuis un terminal non fourni par l'entreprise doit être préalablement validé par SPIE et permettre l'application de la présente politique sécurité.

6.1.2. Assurances

Selon leur sensibilité et leur valeur économique les équipements doivent faire l'objet d'une souscription de contrat d'assurance couvrant les conséquences potentielles d'un sinistre informatique (Conséquences matérielles et immatérielles, directes et indirectes).

6.2. LES SYSTEMES PARTAGES

Tous les systèmes déterminants pour l'activité de l'entreprise (serveurs, stockage, équipements réseaux, ...) doivent être situés dans des zones sécurisées, protégées par des périmètres de sécurité définis, présentant des barrières de sécurité et des contrôles à l'entrée appropriés. En outre ces systèmes doivent être protégés de manière à réduire les risques de menace et de dangers environnementaux, des coupures de courant et autres perturbations sur les services généraux (eau, climatisation, …).

D'une manière générale, il est nécessaire de prendre en compte la sécurité physique de tous les points d'accès aux systèmes d'informations.

Le niveau de protection doit être proportionnel à l'importance du système.

Ces locaux dédiés à l'hébergement des systèmes doivent satisfaire aux caractéristiques suivantes :

- Un système de contrôle d'accès permettant de limiter l'accès des locaux aux seules personnes autorisées incluant la fonction traçabilité et historisation des accès,
- Une alimentation électrique sécurisée (onduleur, système de génération, ...) permettant d'assurer une stabilité et une continuité de service en cas d'interruption,
- Une climatisation garantissant un environnement optimal de fonctionnement permettant de tracer les paramètres de température et d'humidité,
- Un système de détection d'incendie et éventuellement d'extinction automatique,
- Une protection contre les dégâts des eaux excluant toute circulation de fluide intra salle.

Les locaux destinées à l'hébergement des médias de sauvegardes et d'archivages doivent être isolés des salles informatiques (voire dans un autre bâtiment et respecter les conditions énoncées ci-dessus).

Il faut interdire tout stockage de matières dangereuses ou combustibles dans les salles et prévoir et placer le matériel de lutte contre l'incendie à un endroit approprié.

Les équipements de connectivité réseaux (routeurs, lignes, switchs, hub, antenne, …) doivent être hébergés dans des locaux informatiques. Si ce n'est pas le cas, ceux-ci doivent être hébergés au sein d'un local à accès restreint auquel le personnel informatique compétent est autorisé à accéder.

Les câbles de télécommunication doivent être protégés contre toute interception ou dommage. Il faut donc veiller à :

- Protéger le câblage réseau contre les interceptions non autorisées ou les dommages en utilisant par exemple un conduit de câbles et en évitant d'être visible dans les zones passagères (couloir par exemple),

- Utiliser un marquage clairement identifiable sur les câbles et les matériels pour réduire le plus possible les erreurs de manipulation,

- Utiliser une liste documentée des raccordements pour réduire les possibilités d'erreur,

L'environnement dans lequel un système informatique est opéré peut avoir un effet majeur sur sa stabilité et donc sur ses données. En conséquence, les systèmes critiques ne pouvant être hébergés dans une salle prévue à cet effet, devront donc être pourvus d'un système assurant la continuité d'alimentation électrique.

6.3. SYSTEMES RELATIFS A DES DONNEES CLASSIFIEES

L'ensemble des mesures de sécurité destinées à garantir l'intégrité des bâtiments et des locaux spécifiquement dédiés aux informations ou supports classifiés, ainsi que la fiabilité des systèmes dans lesquels ils sont conservés, afin d'éviter toute perte, dégradation ou compromission, doivent respecter impérativement les exigences légales, règlementaires et/ou spécifiquement édictées pour l'affaire ou le client concerné.

6.4. LES MOYENS INDIVIDUELS

L'utilisateur est tenu de prendre les mesures raisonnables afin de protéger les biens informatiques de SPIE contre les dégâts, la perte, le vol ou une mauvaise utilisation.

Chaque utilisateur des systèmes d'information de SPIE doit avoir conscience que les moyens fournis le sont à des fins professionnelles.

En particulier, pour les postes portables et les appareils mobiles, l'attention doit être attirée sur les risques encourus (Ces risques ainsi que des recommandations sont exposés dans un document ci-joint en annexe1).

Tous les vols, dégâts doivent faire l'objet d'une déclaration immédiate à la fonction systèmes d'informations.

6.5. GESTION DU PARC MATERIEL

La fonction systèmes d'information assure la gestion globale du parc d'équipements informatiques de SPIE.

Le matériel doit être correctement maintenu pour garantir sa disponibilité permanente et son intégrité. Il faut donc veiller à ce que :

- le matériel soit entretenu conformément aux spécifications et intervalles recommandés par le fournisseur,
- seul le personnel habilité effectue des opérations de maintenance et dépannage,
- conserver un dossier de toutes les tâches de maintenance corrective et préventive.

Toute sortie de matériel, d'information ou de logiciels hors des locaux de SPIE doit se faire avec autorisation préalable.

En cas de mise au rebut du matériel il faut s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée. De même afin d'éviter toute fuite d'information vers des personnes non habilitées il convient de bien établir les procédures de mise au rebut des supports contenant des informations sensibles.

La démobilisation des matériels doit être réalisée dans des conditions environnementales respectant les règles en vigueur.

6.6. HEBERGEMENTS DE SYSTEMES PAR DES TIERS

Il faut veiller à ce que l'hébergement de systèmes de SPIE par un tiers respecte les directives de la politique de sécurité des systèmes d'informations en s'attachant tout particulièrement au volet confidentialité.

6.7. TRANSITS DES SUPPORTS PHYSIQUES

Lors du transport hors des locaux de SPIE de supports physiques contenant des données (CD, cartouches de sauvegardes, …) il faut veiller à protéger ces derniers contre les accès non autorisés ou l'altération.

L'emballage choisi doit donc être suffisant pour protéger son contenu de tout dommage physique. Le transporteur ou le coursier utilisé doivent être connus et habilités. Des procédures de contrôle et de mode de livraison doivent être définies.

7. SECURITE LOGIQUE

7.1. GENERALITES

Les données et les logiciels sont une richesse patrimoniale fondamentale de l'entreprise.

En fonction de la nature de la donnée, l'entreprise met en œuvre des systèmes de stockage et de protection appropriés.

Toute donnée de l'entreprise ne peut être stockée que sur une ressource ou support dont l'agrément a été formalisé par la fonction Systèmes d'Information.

Dans la mesure du possible, les systèmes permettront d'enregistrer le processus de génération et d'évolution des données (création, modification, ...).

7.2. GESTION DES DONNEES

7.2.1. Postes de travail

Le stockage des données sur les postes de travail est déconseillé, tout système partagé devant être privilégié. Cependant en cas de nécessité impliquant de recourir à ce type de stockage individuel, les utilisateurs ont la responsabilité de réaliser la sauvegarde régulière de leurs données. A ce titre, ils doivent être dotés d'un système approprié.

7.2.2. Externalisation

L'externalisation de données est possible dans le strict respect des lois et règlementations et de la politique de sécurité des systèmes d'informations de SPIE.

Une attention particulière doit être portée sur les données sensibles (Nécessaires à la poursuite des activités de l'entreprise) et celles qui peuvent être soumises à une règlementation particulière (Ex. données personnelles).

Les conditions opérationnelles et contractuelles adaptées doivent être adoptées avec les fournisseurs afin de mettre en place des services : conformes à la sensibilité de ces données, adaptés avec les niveaux de services requis et en mesure de garantir la réversibilité en cas de cessation du contrat de service.

7.2.3. Informations classifiées

Une information classifiée est une information sensible dont l'accès est restreint par une loi ou un règlement à un groupe spécifique de personnes.

Une habilitation est requise pour posséder des documents classifiés ou accéder à des données classifiées. Il y a généralement plusieurs niveaux de sensibilité, classés par un système hiérarchique du secret utilisé potentiellement par l'ensemble des gouvernements. L'action d'assigner un niveau de sensibilité à une donnée est appelée classification des données.

Le stockage et l'accès à ces informations doivent strictement respecter les mesures propres prescrites pour assurer la sécurité des informations classifiées. La fonction Systèmes d'Informations apporte son concours aux personnels habilités pour le conseil, la mise en œuvre et l'application de ces mesures.

7.3. LES SAUVEGARDES

Les sauvegardes de données sont réalisées sur les ressources partagées selon la fréquence définie dans la politique de sauvegarde du Groupe (Cf. Annexe).

Toutes les stratégies de sauvegarde sont établies par la fonction systèmes d'informations en prenant en compte les besoins des utilisateurs ainsi que les contraintes légales/réglementaires.

Des tests périodiques de restauration devront être effectués de façon systématique pour les systèmes critiques et par échantillonnage pour les autres systèmes.

Toute restauration des données doit être effectuée par la fonction systèmes d'informations.

7.4. LES CRYPTAGE DES DONNEES ET DES ECHANGES

Pour l'échange d'informations électroniques et de logiciels entre SPIE et une partie externe il est impératif de conclure des accords écrits.

Ces accords d'échange doivent intégrer les conditions de sécurité suivantes :

- Définition des responsabilités de gestion pour contrôler et informer de la transmission, de la répartition et de la réception,
- Etablissement des procédures d'information sur la transmission, la répartition et la réception,
- Définition des procédures de traçabilité,
- Etablissement de la propriété et des responsabilités pour la protection des données et les conformités des licences logicielles,
- Définition des normes techniques.

Dans les cas critiques où l'on doit veiller à l'intégrité et ou la confidentialité des données pour le stockage et la transmission un système de cryptographie doit être mis en œuvre.

7.5. PROTECTIONS

7.5.1. Généralités

Toutes les mesures préventives en adéquation avec l'exposition potentielle de SPIE doivent être adoptées afin de limiter les risques qui affèrent à des attaques de toutes natures, actions de malveillances ou d'intrusion dans les systèmes de l'entreprise.

Les mesures de protection mises en œuvre font l'objet formellement d'une revue annuelle.

7.5.2. Virus

Un système anti-virus intégrant automatiquement les dernières mises à jour de signature doit être installé sur chaque poste de travail et serveurs de SPIE.

Ce système doit analyser systématiquement et automatiquement tous les logiciels et données hébergés sur les systèmes de SPIE ou en provenance de support externe.

Les utilisateurs de SPIE doivent informer immédiatement la fonction systèmes d'informations de la suspicion ou de la présence de virus sur leur poste

Un système de supervision doit permettre d'identifier à tout instant l'état de mise à jour des signatures et les éventuelles attaques virales des systèmes connectés

En cas d'attaque virale la fonction systèmes d'informations est habilitée à fermer les accès aux ressources et ou les accès externes afin de confiner ou de limiter les impacts au sein du réseau SPIE.

7.5.3. Messages indésirables (Spam)

Un système anti-spam intégrant automatiquement les dernières mises à jour de signature doit être installé sur le système de messagerie utilisé par SPIE.

7.5.4. Mises à jour de sécurité

Les mises à jour de sécurité (« patchs ») sécurités fournis par les éditeurs doivent être déployées sur les systèmes dans la mesure de leur conformité à l'environnement de l'entreprise et de leur exploitabilité.

7.6. LES LOGICIELS

Les logiciels utilisés sur les systèmes de SPIE doivent avoir été agrées par l'entreprise.

Tous les logiciels accessibles sur le réseau SPIE et ou ses équipements doivent faire l'objet d'une acquisition de licence et ou de droit d'usage et être utilisés uniquement dans les conditions d'usage prévues contractuellement.
En particulier, il est nécessaire de vérifier le droit de faire une copie de sauvegarde, de l'usage pour des environnements hors production, ainsi que les clauses de déploiement.

La fonction systèmes d'informations assure la gestion globale des licences de logiciels utilisés par SPIE.

L'installation et la désinstallation des logiciels doivent être réalisées par la fonction.

L'entreprise met à disposition de la fonction systèmes d'informations un outil de gestion de parc des licences logicielles permettant de s'assurer de façon continue de la bonne adéquation entre les logiciels installés et utilisés par rapport à ceux acquis.

En cas de cession de licence à des tiers (Dans le cadre de fourniture associée à une affaire client par exemple) il est indispensable d'en vérifier la possibilité contractuelle.

7.7. DEVELOPPEMENT ET MAINTENANCE DES LOGICIELS

En cas de développement de produits logiciels et ou d'intégration de produits tiers à destination ou mis à disposition des clients de SPIE, il est nécessaire d'obtenir les conseils et l'accord des services juridiques en fonction du contexte en s'attachant aux aspects propriété intellectuelle et droits d'auteurs.

Pour les usages internes le recours à des logiciels produits par des éditeurs spécialisés doit être privilégié par rapport aux développements spécifiques internes. Cependant quand il est nécessaire de recourir à des développements internes il est important de s'assurer du bon respect de la sécurité en matière de développement et d'assistance technique.

Les acteurs impliqués dans le développement de logiciels doivent veiller principalement aux éléments suivants :

- Pérennité des outils de développement employés,
- Respect des règlements en vigueur relatifs aux accords de licences, distribution et propriété des codes sources utilisés,
- Accès aux codes sources,
- Gestion du cycle de vie des logiciels et conservation des évolutions réalisées,
- Documentation technique.

Selon les bonnes pratiques la mise à l'essai d'un nouveau logiciel doit être réalisée dans un environnement isolé des environnements de production et de développement. Ce cloisonnement permet de contrôler le nouveau logiciel et d'ajouter une protection supplémentaire pour les informations d'exploitation utilisées dans le cadre d'essai. Il s'agit notamment des correctifs logiciels, des « services packs » et d'autres mises à jour.

Lorsque des modifications sont apportées aux systèmes d'exploitation, il faut réexaminer et soumettre à essai les applications de gestion afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.

Des procédures formelles de contrôle des modifications doivent être établies afin de réduire le plus possible l'altération des systèmes d'information. En complément une politique de gestion des mises en production doit être définie et un système de gestion de configuration doit être mis en place.

Les collaborateurs chargés de l'assistance doivent être limités en accès aux seules parties du système sur lesquelles ils doivent intervenir.

7.8. CONTROLE D'ACCES

7.8.1. Principes

L'accès est individualisé et nominatif.

La fonction Systèmes d'Informations est responsable de la bonne application des règles au sein de l'entité dont il a la responsabilité.

Tous les systèmes mis en œuvre par SPIE doivent donner lieu à une authentification utilisateur.

En complément, les systèmes critiques doivent permettre une déconnexion automatique des utilisateurs en cas d'inactivité dépassant soixante (60) minutes au maximum ou la nécessité de ressaisir une authentification.

7.8.2. Habilitations

La délivrance des accès aux systèmes d'informations pour un collaborateur de SPIE est fonction des services et systèmes nécessaires pour effectuer les tâches attendues.

Toutes modifications dans le statut d'un collaborateur de SPIE entraînant une modification ou la fin de l'accès aux systèmes d'informations doivent être communiquées le plus rapidement possible à la fonction Systèmes d'Informations.

Celles-ci incluent le changement du statut d'un collaborateur intérimaire, le départ, l'absence pour longue durée, le licenciement ou les absences prolongées pour maladie. En telle situation l'administrateur système doit désactiver, archiver puis supprimer le compte de l'utilisateur.

En outre, les systèmes, quand cela est possible, doivent permettre le recoupement des informations avec le système d'information des ressources humaines.

En cas de départ d'un collaborateur utilisant des systèmes physiques d'authentification ceux-ci doivent être restitués impérativement à la société.

7.8.3. Droits privilégiés

Toutes les opérations nécessitant des droits privilégiés doivent être confiées à des administrateurs du système d'informations.

Si ces missions sont confiées à des tiers, en cas d'externalisation et ou de sous-traitance, la relation contractuelle doit intégrer toutes les obligations afférentes à la politique de sécurité des systèmes d'informations.

Le contrôle des accès privilégiés est effectué en auditant les systèmes assurant la traçabilité.

7.8.1. Tiers externes

Lorsqu'il est nécessaire de délivrer des accès au système d'informations de SPIE à des tiers, les contrôles appropriés doivent être imposés pour garantir la sécurité de l'environnement informationnel de l'entreprise.

Toute nouvelle connectivité d'un tiers doit être soumise à un examen de la sécurité destiné à garantir que le tiers en question exécute ses tâches opérationnelles de manière sûre et efficace.

Seul le niveau d'accès nécessaire à la réalisation de ces tâches doit lui être confié. Une fois établie, la nécessité du maintien de la connectivité du tiers doit être régulièrement examinée afin d'éliminer les connections redondantes ou obsolètes.

Les tiers bénéficiant d'un accès aux systèmes d'informations de SPIE doivent être informés qu'ils ont en tant qu'utilisateur des obligations semblables à celles des collaborateurs de SPIE.

Aucun matériel de tiers ne doit être connecté au réseau de SPIE sans avoir été au préalable validé par la fonction systèmes d'informations.

7.8.2. Comptes utilisateurs génériques

Les comptes utilisateurs génériques ou commun à plusieurs individus sont proscrits néanmoins lorsqu'il doit en être créé pour répondre à des contraintes techniques ou d'exploitation, la raison de sa création doit être documentée, le compte doit être revu périodiquement tous les semestres, et ses accès définis. Notamment la liste des personnes habilitées à utiliser ces comptes doit être précisée.

7.8.3. Administrateurs Systèmes

Les administrateurs systèmes sont soumis aux règles supplémentaires suivantes :

- Le compte administrateur ne doit être utilisé qu'en cas de nécessité technique,
- La création d'un compte doit suivre le processus défini par l'entreprise et dans tous les cas comporter la validation formalisée du responsable de la donnée qui sera accédée par le compte,
- Un administrateur ne peut modifier les droits d'accès à un compte impliquant l'accès à des données d'entreprise qu'avec l'accord formalisé du responsable de la donnée,
- Un administrateur ne peut modifier les droits d'accès à un compte impliquant l'accès à des données susceptible d'être personnelles qu'avec l'accord formalisé du Directeur des ressources humaines.

- Le maintien d'un compte nominatif d'un utilisateur absent de l'entreprise dont le compte permet l'accès à des données d'entreprise, est subordonné à l'accord formalisé du responsable de la donnée pour un délai de 30 jours révisables.

- Le maintien d'un compte nominatif d'un utilisateur absent de l'entreprise dont le compte permet l'accès à des données susceptible d'être personnelles, est subordonné à l'accord formalisé du Directeur des ressources humaines pour un délai de 30 jours révisables.

7.8.4. Gestion des données d'accès

Dans le strict respect des réglementations en vigueur relatives à la protection des données individuelles, tous les systèmes critiques assurent la traçabilité des accès (qui, quand et quoi).

La conservation des données liées aux comptes nominatifs doit respecter les durées déterminées par les lois ou règlementations.

7.9. GESTION DU MOT DE PASSE UTILISATEUR

Chaque utilisateur s'identifie par un compte nominatif et s'authentifie par un mot de passe.

Ce mot de passe est personnel et confidentiel. Il doit être géré avec attention et ne doit en aucun cas être affiché, divulgué ou communiqué à autrui. En outre celui-ci ne doit pas être programmé pour une utilisation automatique sur le poste.

Le mot de passe doit respecter les caractéristiques suivantes :

- Le nombre de caractères minimum est de huit (8) avec des combinaisons de caractères alphanumériques et spéciaux si le système le permet,
- La détermination du mot de passe ne doit pas reposer sur un système trivial à savoir identifiant ou relation évidente (prénom, nom du conjoint, ...),
- Le mot de passe a une durée de vie maximale de quatre-vingt-dix (90) jours,
- L'utilisateur ne pourra définir le même mot de passe deux fois de suite et ce jusqu'à la septième occurrence,
- Pour limiter les fraudes, tout compte informatique sera bloqué après 3 tentatives infructueuses,
- Lors de la première utilisation d'un système, l'utilisateur doit impérativement modifier le mot de passe qui lui a été attribué.

En cas de suspicion et ou de divulgation de mot de passe, ceux-ci doivent être changés immédiatement.

Un accès de recouvrement administrateur doit exister au sein du système d'information et l'utilisation de cet accès de recouvrement doit bénéficier d'une autorisation systématique du Directeur des ressources humaines.

7.10. SECURITE DU RESEAU

7.10.1. Principes

Tout point d'accès au réseau privé de SPIE est géré par la fonction Systèmes d'informations.

La protection du réseau privé de SPIE impose la mise en œuvre d'un point d'entrée et sortie unique vis à vis de l'extérieur.

Celui-ci doit être équipé d'un système reposant sur des outils matériels et logiciels (Firewall,…) définis et gérés par la Direction des Systèmes d'Information permettant les contrôles d'accès et le filtrage de ces derniers.

Ce filtrage s'applique en particulier aux adresses Internet (url), à la propagation de messages malveillants (spam), aux messages et données électroniques éventuellement porteurs de virus.

Dans le strict respect des réglementations en vigueur relatives à la protection des données individuelles, les activités des utilisateurs doivent être enregistrées dans un rapport d'audit afin de faciliter les investigations ultérieures et la surveillance du contrôle d'accès. Les équipements de journalisation et les informations enregistrées seront protégés contre les actes malveillants et les accès non autorisés. De même les activités des administrateurs système et réseaux seront enregistrées.

Les utilisateurs sont tenus de se conformer aux règles simples édictées dans le document « code d'utilisation de la messagerie et d'Internet » figurant en annexe 2 du présent document. Ce document est donné à titre d'exemple et doit être adapté en particulier en fonction des législations pays.

Les demandes d'accès permanents aux réseaux de données de l'entreprise depuis l'extérieur doivent faire l'objet d'une demande spécifique.

Un bon paramétrage des horloges internes des systèmes est important car il influe sur la précision des rapports d'audit. Un système de synchronisation des horloges sur l'ensemble du réseau de SPIE doit donc être opérationnel.

Tout poste portable fourni par l'entreprise accédant à un réseau public doit être protégé par un système de firewall et de l'anti-virus homologués par la Direction des Systèmes d'Informations.

L'ensemble des communications accédant aux systèmes d'informations de SPIE par utilisation des dispositifs d'accès externe font l'objet d'un chiffrement de type IPSEC ou SSL.

Toute interconnexion d'un lien réseau accédant directement à Internet et au réseau privé de l'entreprise est formellement prohibée.

7.10.2. Accès sans fils

Quand cela est nécessaire, l'entreprise fournira des systèmes sécurisés '"sans fil" (Wireless).

Ces systèmes, validés par la Direction des Systèmes d'Information, sont configurés par la fonction systèmes d'informations afin d'assurer la cohérence avec l'architecture globale du réseau privé de SPIE et avec la politique de sécurité des Systèmes d'informations.

D'une façon générale, toutes les spécifications suivent les meilleures pratiques des constructeurs en matière de sécurité informatique des points d'accès sans fil.

L'activation de la journalisation de l'activité du point d'accès est recommandée.

7.10.3. Noms de domaines

Les adresses Internet publiques ainsi que les relations avec les organismes de gestion des noms de domaines internet sont assurés par la Direction des Systèmes d'Informations.

8. FIN DU DOCUMENT

9. ANNEXES

ANNEXE 1

Précautions particulières pour les appareils informatiques portables

(Ordinateurs portables, Tablettes, PDA, Smartphone, …)

Les appareils portables sont fréquemment perdus ou volés dans des endroits tels que les aéroports, les taxis, les hôtels, les centres de conférence, mais aussi dans les bureaux durant la nuit ou le week-end. Pour éviter tout vol dans les bureaux, cas le plus fréquent de disparition chez SPIE, il est recommandé d'emporter son matériel avec soi durant la nuit ou le week-end. En cas d'impossibilité il faut éviter de laisser l'appareil sur le bureau, même relié à un câble de sécurité, mais plutôt le ranger dans un tiroir ou une armoire fermée à clef.

D'une façon générale les règles suivantes doivent être respectées :

Protéger l'accès général au poste par un mot de passe,
Eviter la proximité de tout liquide (boissons par exemple),
S'assurer que des copies de sauvegarde des données importantes sont effectuées,
Protéger les documents avec des données sensibles par des mots de passe complémentaires,
Ne pas installer de logiciels non agréés par SPIE.

En cas de voyage ou de déplacement il faut respecter autant que faire se peut les quelques consignes simples suivantes :

Ne pas laisser l'appareil hors de votre vue, même pour une courte période,
Conserver le numéro de série du matériel sur un document séparé de ce dernier en cas de perte ou de vol,
Eviter de voyager avec un emballage ou une mallette identifiant trop facilement l'objet transporté (mallette standard fabricant),
Ne pas placer l'appareil de façon visible dans un véhicule automobile (plage arrière, siège, ..),
Prendre l'appareil dans vos bagages à main pour les voyages en avion,
Placer en cas de contrôle au travers d'un détecteur d'objets sous rayons votre appareil en dernière position des bagages sur le tapis roulant afin de limiter les risques de vol du coté réception,
Ne pas exposer à la vue d'autrui des informations stockées sur l'appareil par exemple dans les trains ou les avions.

En cas de voyage dans un pays étranger il est impératif de se renseigner au préalable sur la réglementation locale concernant l'introduction sur le territoire d'appareils de cette nature ainsi que des logiciels utilisés (facture d'achats, certification fournisseurs, ..).

ANNEXE 2

La protection juridique du logiciel par le droit de la propriété intellectuelle
(Loi Française)

La loi n° 85-660 du 3 juillet 1985 relative aux droits d'auteur et aux droits des artistes interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle, a consacré la protection juridique des logiciels dans un article L. 112-2 du Code de la propriété intellectuelle.

Une directive communautaire du 14 mai 1991 Dir. cons. CE n° 91/250, 14 mai 1991, JOCE 17 mai, n° L 122, p. 42 a également posé comme principe que :
"les États membres protègent les programmes d'ordinateur par le droit d'auteur en tant qu'oeuvres littéraires au sens de la convention de Berne pour la protection des oeuvres littéraires et artistiques Cette directive a été transposée en droit français par la loi n° 94-361 du 10 mai 1994."

Objet de la protection : un logiciel original

Le logiciel peut se définir comme « l'ensemble des programmes, procédés et règles, et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble d'informations Arrêté du 22 décembre 1981 relatif « à l'enrichissement du vocabulaire de l'informatique », JONC 17 janvier 1982, p. 624 ». Cette définition est générique et concerne tout aussi bien le logiciel spécifique que le progiciel, le logiciel de base que le logiciel d'application, le logiciel propriétaire que le logiciel libre. D'après les statuts de l'Association francophone des utilisateurs de Linux et des logiciels libres (Association francophone des utilisateurs de Linux et des logiciels libres AFUL), « sont considérés comme libres les logiciels disponibles sous forme de code source » c'est-à-dire des logiciels dont l'architecture interne est partagée et diffusée librement, toute personne pouvant participer à l'élaboration du produit en proposant ses propres améliorations. Ce qui différencie un logiciel libre d'un logiciel propriétaire réside dans la diffusion ou non du code source du logiciel. En effet, un logiciel propriétaire est livré seulement sous sa forme de code exécutable (uniquement compréhensible par l'ordinateur) alors que le logiciel libre est fourni avec son code source, compréhensible par un homme. Il convient enfin de ne pas confondre le logiciel libre et le « freeware », dont les droits d'exploitation sont libres, l'auteur ayant décidé de les abandonner au domaine public, ou le « shareware ».

Une oeuvre originale

Pour bénéficier de la protection du droit d'auteur, le logiciel doit satisfaire comme toute oeuvre de l'esprit à l'exigence d'originalité. Selon les dispositions des articles L. 111-1 et L. 112-1 du Code de la propriété intellectuelle, sont protégés les droits des auteurs sur toutes les oeuvres de l'esprit quels qu'en soient le genre, la forme d'expression, le mérite ou la destination, dès lors qu'elles revêtent un caractère original, c'est-à-dire qu'il doit témoigner d'un effort créatif, porter l'empreinte de la personnalité de son auteur.

Logiciel libre et droit d'auteur

Le logiciel libre peut également être appréhendé par le droit d'auteur. En effet, le créateur initial d'un logiciel libre n'abandonne pas ses droits d'auteur sur son oeuvre, il concède seulement à chacun le droit d'utiliser celle-ci par le recours à une licence d'utilisation, à la condition que toute amélioration ultérieure soit rendue publique et que le logiciel ainsi modifié puisse circuler librement.

Le contrat de licence

Distinguer logiciel propriétaire et logiciel libre

On peut distinguer la licence d'utilisation des logiciels propriétaires, dans laquelle le code source n'est en principe jamais communiqué à l'utilisateur, et les licences de logiciels libres, dans lesquelles la communication des sources à l'utilisateur est un élément primordial.

Licence d'utilisation des logiciels propriétaires

Licence d'utilisation ou d'exploitation

Le contrat de licence contient les conditions et l'étendue des droits concédés à l'utilisateur pour un progiciel ou un logiciel spécifique.

On distingue la licence d'exploitation, conférant tout ou partie des droits d'exploitation définis ci-dessus à un utilisateur, et la licence d'utilisation, qui ne concerne comme son nom l'indique que le droit d'utiliser le logiciel.

La licence d'utilisation des progiciels, appelée « shrink wrap license », est un document pré imprimé se trouvant généralement dans l'emballage contenant le support du logiciel et éventuellement sa documentation. Dans ce cas, les conditions du contrat ne sont pas négociables pour l'utilisateur. A contrario, le contrat de licence d'utilisation d'un logiciel spécifique est généralement négocié par les parties.

Dans une licence d'utilisation de progiciel, en principe, seul le droit d'utilisation est concédé, l'auteur se réservant tous les autres droits parmi lesquels les droits de reproduction, de correction et d'adaptation.

Une licence personnelle, en principe

Le droit d'utilisation du logiciel doit être délimité quant à son étendue, sa destination, sa durée et sa territorialité. À défaut de précision, l'interprétation par le juge sera toujours faite en faveur de l'auteur, raison pour laquelle l'utilisateur doit s'assurer que la licence contient notamment les indications suivantes :

* le ou les sites d'exploitation concernés ;
* le type de matériel compatible ;
* le type et la version du système d'exploitation requis ;
* la configuration ;
* la ou les personnes utilisatrices ;
* le nombre de copies de sauvegarde ;
* la durée déterminée La licence à durée déterminée doit prévoir les modalités pratiques à respecter par l'utilisateur en fin de période d'utilisation (remise du logiciel et de sa documentation à l'éditeur, destruction des copies notamment), pour un trimestre ou un an, ou indéterminée. Il est néanmoins recommandé d'indiquer plutôt que « la licence est accordée pour la durée de protection légale du logiciel » (soit 70 ans si l'auteur est une personne morale, ou la vie de l'auteur + 70 ans, si l'auteur est une personne physique).

Restrictions d'utilisation

Toute utilisation du logiciel non prévue ou non conforme aux conditions de la licence est considérée comme illicite (cela fait d'ailleurs généralement l'objet d'une clause « contrefaçon » dans la licence d'utilisation).

L'utilisateur qui ne respecterait pas les stipulations du contrat de licence ou qui effectuerait une reproduction non autorisée du logiciel pourrait voir sa responsabilité civile et pénale engagée pour contrefaçon.

Les licences libres

Il existe trois grandes catégories de licences régissant actuellement les logiciels libres.

Les licences libres strictes

Objet de la licence GPL

La plus célèbre est la licence publique générale (ou GPC) GNU"s Not UnixGNU (GNU's Not Unix) créée en 1984 par Richard Stallman ; cette licence régit aujourd'hui la grande majorité des logiciels libres.

La GPL (General Public Licence) est destinée à garantir la liberté de partager, de modifier et de distribuer les logiciels librement accessibles. L'objet de la General Public LicenseGPL est la mise à disposition du logiciel aux utilisateurs et non le transfert ou l'abandon d'un droit de propriété sur celui-ci. C'est au titulaire des droits sur l'oeuvre originale qu'il appartient de décider de sa distribution sous licence GPL.

Droits de l'auteur et du licencié

La GPL oblige le donneur de licence à communiquer le code source du logiciel. Le licencié, quant à lui, s'engage à respecter le droit moral de l'auteur, c'est-à-dire le droit de paternité et le droit de divulgation des différentes versions du logiciel.

La GPL impose au licencié de demander l'autorisation de l'auteur pour utiliser son logiciel dans un logiciel soumis à une autre licence. Le développement du logiciel passe ensuite par la possibilité offerte à tous les licenciés de communiquer les modifications qu'ils ont apportées à des tiers qui peuvent participer au projet. Les licenciés peuvent donc redistribuer le logiciel mais il est interdit de le faire par le biais d'une sous-licence.

Les licences du domaine public

Une licence qui facilite le développement de logiciels propriétaires

Ce modèle de licence a été conçu à l'origine par l'université de Berkeley (Californie). Elle autorise la publication du code source de même que la copie gratuite tout en exigeant la mention des auteurs du logiciel libre, qu'il s'agisse d'une version d'origine ou modifiée. Cependant, la publication du code source ultérieur n'est pas obligatoire et ce type de licence n'oblige donc pas les utilisateurs à reverser les modifications apportées à la communauté.

Ce type de licence n'interdit donc pas le développement d'un logiciel propriétaire à partir d'une base de composants libres. Toutefois, le droit moral de l'auteur initial demeure et celui-ci peut, en cas d'adaptation ou de modification préjudiciable à son honneur ou sa réputation, faire valoir le droit au respect de l'oeuvre.

Les licences semi libres

À mi-chemin entre la licence stricte et la licence de domaine public

La licence stricte comporte un inconvénient majeur car, en intégrant un logiciel libre à un produit commercial, elle exige que le code source du produit issu de cette fusion soit également livré. À l'inverse, la licence de domaine public peut rendre possible l'appropriation de tout ou partie d'un logiciel libre. C'est la raison pour laquelle les licences semi libres ont été imaginées, afin de trouver un point d'équilibre entre ces

deux options. C'est la société Netscape qui est à l'origine de ces licences, avec la « Netscape Public License » qui couvre le code source du logiciel de navigation sur Internet. Ces licences imposent la publication de toute modification du code source mais n'empêchent pas d'intégrer les modules propriétaires livrés, eux, sans leur code source.

Défense des droits d'auteur

Le droit commun

Les sanctions à la violation des droits d'auteur

La violation des droits d'auteur est punie à titre principal de trois ans d'emprisonnement et de 300 000 € d'amende, et de cinq ans d'emprisonnement et 500 000 € d'amende lorsque ces délits ont été commis en bande organisée Articles L. 335-2, al. 2, et L. 335-4, al. 1, du Code de la propriété intellectuelle modifiés par la loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité (JO n° 59 du 10 mars 2004, p. 4567).

Conformément au droit commun Article 132-10 du Code pénal le maximum des peines d'emprisonnement et d'amende ainsi encourues est doublé en cas de récidive Article L. 335-9 du Code de la propriété intellectuelle, cette aggravation de la répression est également encourue « si le délinquant est ou a été lié par convention avec la partie lésée ».

Par ailleurs, l'article L. 335-8 du Code de la propriété intellectuelle permet de retenir la responsabilité pénale des personnes morales, pour lesquelles le taux maximal de l'amende applicable sera égal au quintuple de celui encouru par les personnes physiques.

Les peines complémentaires

À ceci peuvent également s'ajouter des peines complémentaires telles que :

* la fermeture totale ou partielle, définitive ou temporaire de l'établissement ayant servi à commettre l'infraction, pour une durée de cinq ans ou plus Article L. 335-5 du Code de la propriété intellectuelle qu'il convient de rapprocher, pour les personnes morales, avec le risque d'une interdiction, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement l'activité à l'occasion de laquelle l'infraction a été commise Article L. 335-8, 2°, du Code de la propriété intellectuelle.
* l'affichage et la publication intégrale ou par extraits de la condamnation peuvent également être ordonnés Article L. 335-6, alinéa 2, du Code de la propriété intellectuelle.
* la confiscation de tout ou partie des recettes procurées par l'infraction, des produits résultant de celle-ci et du matériel spécialement installé en vue de sa commission Article L. 335-6, alinéa 1, du Code de la propriété intellectuelle ceux-ci pouvant être remis à la victime ou à ses ayants droit afin de les indemniser de leur préjudice Article L. 335-7 du Code de la propriété intellectuelle dont la réparation intégrale pourra faire l'objet de condamnations indemnitaires complémentaires.

En matière de logiciels

Droit d'auteur et contrefaçon

Selon l'article L. 335-3, alinéa 2, du Code de la propriété intellectuelle, la violation de l'un des droits de l'auteur d'un logiciel définis à l'article L. 122-6 du même code est également un délit de contrefaçon.

Spécificités du droit pour le logiciel

Les éléments de ce délit présentent cependant certaines spécificités.

En effet, le droit moral de l'auteur du logiciel est très affaibli à l'égard du cessionnaire de ses droits, qui peut modifier l'œuvre logicielle tant que l'honneur ou la réputation de l'auteur n'en sont pas affectés.

Par ailleurs, l'auteur du logiciel ne conserve que le droit d'autoriser la location de son logiciel, dès que celui-ci a été mis sur le marché européen par l'auteur ou avec son consentement.

Pour le reste, la contrefaçon d'un logiciel pourra être retenue en cas de reproduction (permanente - stockage - ou provisoire) de celui-ci, ou encore de modification, traduction, adaptation, arrangement et reproduction pouvant en résulter.

ANNEXE 3

Engagement à faire signer lors de l'affectation d'un ordinateur portable

Je, soussigné(e) ……., déclare avoir pris connaissance des recommandations et exigences afférentes à la sécurité des Systèmes d'Informations et de la charte d'usage des Systèmes d'Informations.

Date : …….

Signature :……..

Nom et Validation du Responsable Informatique

L'original de ce document dûment renseigné, daté et signé sera conservé par votre Responsable Informatique et une copie transmise au Service du Personnel.

ANNEXE 4

Politique de Sauvegarde des données