POLITIQUE SECURITE DU SYSTEME D'INFORMATION

Approbation

	Name	Fonction	Date	Signature
Rédigé par	Yvon Kerhoas	Consultant Sécurité	09/10/2018	YVKE
Validé par	Cedric Lefèvre	RSI	10/10/2018	C_LE
	Frédéric Thoraval	RSSI	10/10/2018	FRTH
	Ludovic Defienne	RSI	10/10/2018	LUDE
	Geoffroy Noirfontaine	DPO / PO	10/10/2018	GENO
Approuvé par	Stéphane Bourva	Officier de Sécurité /DSI	17/10/2018	STBO

Table des modifications

Date	Version	Modifications	Auteur
05/02/2018	0.1	Création du document	Y.KERHOAS
28/02/2018	2.0	Validation du document	Y.KERHOAS
01/03/2018	2.0	Version livrable	Y.KERHOAS
17/04/2018	2.1	Définition périmètre 2018	F.THORAVAL
16/05/2018	2.2	Corrections diverses	Y. KERHOAS
09/10/2018	3.0	Evolution suite à audit à blanc	Y.KERHOAS

Sommaire

1 Grands principes

Ce document constitue la Politique de sécurité du système d'information du Groupe Infotel (PSSI).

Le Groupe Infotel s'engage à assurer une qualité de service optimale, en garantissant une réactivité importante lorsqu'un incident survient, ou que l'un de nos clients émet une demande.

Afin de préserver la disponibilité, l'intégrité, la confidentialité et la traçabilité (DICT) de l'information, le Groupe intègre dans ses activités une politique de sécurité de l'information, dans laquelle est présenté l'ensemble des mesures de sécurité ainsi que les règles de bonnes pratiques, applicables aux activités de l'entreprise.

Cet engagement et la volonté de respecter les règles de l'art en matière de sécurité de l'information démontrent l'intérêt du Groupe à s'engager dans cette politique.

Nos objectifs fondamentaux sont :

- Un engagement fort porté par la direction générale, une globalisation des bonnes pratiques à tous (périmètre certifié ou non) ;
- Des collaborateurs in et ex situ sensibilisés régulièrement garantissant le respect des règles établies ;
- La garantie de la continuité de service avec une surveillance de la conformité et un plan de reprise d'activité précis et éprouvé ;
- Le maintien d'une architecture résiliente avec une sécurité physique et logique assurée et une exploitation maîtrisée dans le respect DICT ;
- Le renforcement de l'image du Groupe et de la confiance de nos partenaires.

2 Introduction

2.1 S'engager : le maître mot

L'appréciation des risques en matière de sécurité de l'information se déroule à minima annuellement et est pilotée par le RSSI. Cette analyse peut également être déclenchée en cas de changements impactant, tant organisationnels que techniques.

Les résultats sont présentés en revue de direction et la décision quant au seuil d'acceptabilité des risques est décidée puis annoncée dans la lettre d'engagement rédigée par le dirigeant ou son représentant à l'attention des parties prenantes.

En découlent des actions qui sont identifiées et validées dans le Plan de Traitement des Risques (PTR) garant du suivi et du déroulement des initiatives en matière de réponse à l'appréciation des risques.

Une déclaration d'applicabilité nous permet de présenter les dispositions établies pour répondre aux 113 exigences de l'ISO27002 conformément à notre certification.

Une veille règlementaire et technologique précise déléguée à des experts par le RSSI ainsi que notre collaboration avec des organismes tels que la Commission Nationale de l'Informatique et des Libertés, le Syntec, l'Agence Nationale de la Sécurité Informatique nous permettent de mettre en œuvre des actions supplémentaires, de les piloter et de les contrôler dans le temps.

Ainsi, les mesures instaurées sont applicables à toutes les activités :

- Accès logiques et physiques ;
- Classification et transmission de la donnée ;
- Contrôle des accès aux données ;
- Identifiant unique, gestion des privilèges ;
- Implication du personnel ;
- Management des actifs ;
- Usage réseau ;
- Règlement intérieur.

2.2 Le contexte de l'entreprise

Le Groupe Infotel dispose d'un patrimoine d'informations sensibles constituant l'un de ses actifs les plus importants, sur lequel repose son image et sa capacité à maintenir et développer ses activités et ses publications.

Il recouvre :

- le patrimoine intellectuel, composé de toutes les informations concourant à son savoir et à son savoir-faire, notamment dans la conduite de projets métiers ;
- les informations relatives à ses clients, ses partenaires ou tout autre tiers avec lesquels elle est en relation, dont l'altération ou la divulgation pourrait porter atteinte à son image ;
- les informations relatives à son personnel dont la divulgation constituerait une violation de la vie privée.

Le Groupe Infotel, dans le cadre du domaine d'application du « SMSI ISO27001 », regroupe 12 sites assurant une activité de services auprès de ses clients.

Ces 12 sites couvrent une partie du territoire : Lille, Lyon, Rennes, Brest, Niort, Orléans, Nantes, Bordeaux, Le Mans, Mougins.

Infotel UK, dans le cadre du domaine d'application du « SMSI ISO27001 » regroupe 1 site assurant une activité de services auprès des clients du Groupe (Newcastle) et 1 site commercial (Londres).

L'ensemble des autres sites du Groupe Infotel est soumis aux mêmes règles que le périmètre concerné par la certification.

2.3 Périmètre de la PSSI

La politique de sécurité du système d'information (PSSI) du Groupe Infotel couvre l'ensemble des activités des sites avec toute la diversité que cela implique dans les usages, les lieux d'utilisation et les personnes concernées.

La PSSI concerne l'ensemble des activités et des métiers du Groupe Infotel.

En termes d'actifs, la PSSI inclût :

- **Les actifs matériels**
  - Les serveurs ;
  - Les équipements dédiés à la gestion de service (téléphonie, contrôle d'accès, etc.) ;
  - Les réseaux de communications internes à l'entreprise, filaires ou non, à vocation d'échanges de données informatiques, mais aussi de téléphonie, de visioconférence, de télésurveillance, etc. ;
  - Les systèmes d'information à usage personnel (ordinateur fixe ou portable, assistant personnel, logiciels divers, etc.) ;
  - Les systèmes de support de l'information et d'impression ;
  - Les prestations externes dans leur incidence sur la sécurité interne des systèmes d'information.
- **Les actifs immatériels**
  - Les données liées aux activités des agences ;
  - Les données administratives liées à la gestion de l'entreprise (ressources humaines, données comptables, etc.) ;
  - Les données associées aux échanges d'informations (affranchissement, téléphonie, informatique, réseau, etc.).
- **Les ressources humaines et morales**
  - Les administrateurs des systèmes et réseaux qui ont pour charge la maintenance des actifs informatiques ;
  - Les personnes impliquées dans le développement du système d'information ;
  - Les utilisateurs du système d'information ;
  - Les entreprises fournisseurs d'équipement ou prestataires de services.

2.4 Besoins de sécurité

La sécurité du système d'information repose sur quatre critères (DICT) :

- **Disponibilité**
  - Garantir que les éléments considérés (fichiers, courriels, applications, services numériques) sont accessibles au moment voulu par les personnes autorisées ;
- **Intégrité**
  - Garantir que les éléments considérés (fichiers, courriels…) sont exacts, complets et non modifiés ;
- **Confidentialité**
  - Garantir que seules les personnes autorisées ont accès aux éléments considérés (applications, fichiers…) ;
- **Traçabilité**
  - Garantir que les accès et tentatives d'accès aux « informations » sont tracés et que l'historique des évènements est conservé et exploitable en temps voulu.

Les besoins de sécurité s'appliquent aussi bien aux ressources du système d'information (postes informatiques, réseaux, applications, etc.) qu'aux données traitées par ces ressources. Il est nécessaire d'inventorier et de classifier ces données afin d'en identifier le degré de sensibilité et donc le besoin de protection nécessaire.

2.5 Menaces

Afin de mettre en place les moyens de sécurité adéquates, le Groupe Infotel utilise la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) pour, entre autre, identifier les sources de menaces et évaluer leur dangerosité au regard des vulnérabilités des actifs.

On distingue ainsi :

- Les attaques visant directement le système d'information
  - Vols de données ;
  - Modifications des données ;
  - Dénis de service…
- Les attaques visant les ressources informatiques
  - Vols de ressources ;
  - Détournements des ressources ;
  - Altérations des données ;
  - Emissions de malware…

- Les accidents
  - Sinistres naturels ;
  - Altérations accidentelles des données ou des ressources.

L'éventualité qu'une source de menace exploite la vulnérabilité d'un actif est évaluée en termes de risques. La criticité du risque tient compte des éventuels facteurs aggravants (négligence constatée, insuffisance d'informations, insuffisance de consignes…).

3 Principes et règles de Sécurité

3.1 Organisation de la Sécurité

Au sein du Groupe Infotel, la responsabilité générale de la sécurité du système d'information est assurée par le RSSI sous l'autorité de l'officier de Sécurité.

Il est assisté dans cette fonction par le responsable du système d'information (RSI), le Risk Manager et les process owner.

Les responsables de site (référents) sont responsables de la sécurité du système d'information de leur agence et répondent aux exigences exprimées par le RSSI.

Le RSSI, l'Officier de Sécurité, le RM, les RSI et les Process Owner constituent le COSI (Comité d'Orientation du Système d'Informations).

3.1.1 L'Officier de Sécurité

L'officier de Sécurité est le représentant légal de la direction générale sur tous les domaines de la sécurité. Il est le responsable de la mise en œuvre du projet ISO 27001 pour le Groupe Infotel.

3.1.2 Responsable de la Sécurité des Systèmes d'Information (RSSI)

Le RSSI assisté par le RSI assure sous l'autorité de l'Officier de Sécurité, les activités suivantes :

- Contribuer activement à l'élaboration d'une politique de sécurité cohérente admise par tous
- Mettre en œuvre la politique de sécurité ;
- Faire connaître et respecter la charte d'utilisation des moyens informatiques de l'entreprise ;
- Proposer des actions de sensibilisation et d'information de tous les utilisateurs aux aspects sécurité des systèmes d'information ;
- Etre l'intermédiaire direct en cas de problème entre la direction générale et les autorités.

3.1.3 Responsable des Systèmes d'Information (RSI)

Le RSI assure sous l'autorité du RSSI, les activités suivantes :

- Contribuer activement à l'élaboration d'une politique de sécurité cohérente admise par tous ;
- Mettre en œuvre la politique de sécurité ;
- Viser tous les projets de l'entreprise afin de veiller à la mise en œuvre des éléments technologiques nécessaires à l'application de la PSSI ;
- Gérer l'ensemble des composantes techniques du système d'information ;
- Préparer les reportings nécessaires à la maîtrise de la sécurité ;
- Mettre en œuvre les améliorations décidées en comité sécurité.

3.1.4 Les Pilotes de processus ou Process Owner (PO)

Ils ont en charge le suivi et la mise en œuvre des processus ISO 27001 qui leur sont confiés.

Ils s'appuient sur le RSSI et en réfèrent à l'Officier de sécurité.

3.1.5 Le pilote des risques (Risk Manager, RM)

Le pilote des risques de sécurité exerce les activités suivantes :

- Identifier les points de vulnérabilité du système d'information de l'entreprise;
- Hiérarchiser, formaliser les risques de sécurité ;
- Informer la direction générale du niveau de risque de sécurité du système d'information ;
- Mettre en œuvre les couvertures de risque appropriées décidées en comité de direction.

3.1.6 Le DPO

Infotel a nommé un DPO fin 2017. Le DPO a été déclaré en avril 2018 à la CNIL.

Il exerce les activités suivantes :

- Informer et conseiller le responsable du traitement ou le sous-traitant et les salariés de leurs obligations découlant de la législation en matière de données personnelles
- de veiller à la conformité de ces législations
- de coopérer et d'être l'interlocuteur privilégié de la CNIL

- d'être le point de contact des personnes concernées par un traitement de données personnelles pour toutes les questions relatives à ce traitement et pour l'exercice des droits que leur confère le règlement.

3.1.7 Les référents (Responsable de site)

Les référents sécurité :

- Veillent au quotidien à la mise en œuvre des procédures de sécurité pour la partie technique de l'exploitation : systèmes, réseaux, postes de travail et applications informatiques de leur périmètre ;
- Sont responsables de la mise en œuvre de la PSSI et du plan d'action sécurité dans leur périmètre ;
- Doivent s'assurer de la sensibilisation de leurs collaborateurs et de la mise à disposition des ressources nécessaires à la mise en œuvre de la démarche de sécurité de l'information sur leur périmètre.

3.1.8 Responsabilités des différents acteurs

Les acteurs intervenant en matière de sécurité des systèmes d'information doivent être informés de leurs responsabilités en matière de SSI.

Dans l'exercice de leur activité, ils sont liés à leur devoir de réserve voire à des obligations de secret professionnel.

3.1.9 Accès aux ressources informatiques

La mise à disposition et la restitution des moyens informatiques doivent être formalisées.

L'accès aux ressources doit être contrôlé (identification/authentification) et adapté aux droits de l'utilisateur (droits et privilèges, profil utilisateur).

3.1.10 Annexe Sécurité de la Charte informatique

Préalablement à son accès au système d'information, l'utilisateur doit prendre connaissance des droits et devoirs au travers de l'annexe sécurité de la charte informatique à l'intérieur du règlement intérieur de l'entreprise.

En cas de question il contacte le RSSI.

3.1.11 Cyber surveillance

La sécurité des systèmes d'information exige de pouvoir surveiller le trafic sur le réseau et tracer les actions effectuées. Les dispositifs mis en œuvre doivent être conformes à la règlementation en vigueur et respecter les principes de proportionnalité et de transparence.

4 Mise en œuvre de la PSSI

4.1 Sécurité des données

4.1.1 Disponibilité, confidentialité et intégrité des données

Le traitement et le stockage des données numériques, l'accès aux applications et services numériques et les échanges de données entre systèmes d'information doivent être réalisés selon des méthodes visant à prévenir la perte, la modification et la mauvaise utilisation des données ou la divulgation des données ayant un caractère sensible.

4.1.2 Protection des données

Les données doivent être classifiées selon leur niveau de sensibilité (il sera procédé régulièrement à un réexamen du niveau de sensibilité des données).

Avant toute cession ou mise au rebut d'un matériel ayant contenu des données sensibles, il est nécessaire de s'assurer que toutes les données sont effacées par un procédé efficace. Si cela s'avère impossible, les supports concernés devront être détruits.

4.1.3 Données à caractère personnel

Les traitements de données susceptibles de contenir des informations à caractère personnel (au sens de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés) doivent faire l'objet de déclaration ou de demande d'autorisation auprès de la CNIL, via le correspondant CIL de l'entreprise.

Les données à caractère personnel constituent des données sensibles qui doivent faire l'objet de protection.

A compter du 25 mai 2018, le RGPD (Règlement Général de Protection des données) est applicable à Infotel et renforce la loi CNIL.

Le Groupe Infotel a désigné un DPO (Data Protect Officer). Celui-ci assure le suivi et la gestion du traitement des données de ce type.

4.1.4 Chiffrement

Le chiffrement, en tant que moyen de protection, est utilisé pour le stockage et l'échange de données sensibles.

4.2 Sécurité du système d'information

4.2.1 Administration des serveurs

Les serveurs hébergent des données sensibles et fournissent des services numériques. Ils représentent des biens essentiels pour la réalisation des activités métiers.

La sécurité des données (disponibilité, intégrité et confidentialité) et des services numériques (disponibilité et intégrité) dépend du niveau de protection des serveurs qui les hébergent.

L'administration des serveurs est placée sous la responsabilité des RSI.

Les administrateurs SESAME ont un compte utilisateur classique et un compte administrateur nominatif pour les besoins nécessitant une élévation de pouvoir.

Les différents mots de passe administrateur sont stockés dans une base cryptée de GLPI.

4.2.2 Administration des postes de travail

L'administration des postes de travail est centralisée par les équipes SESAME. L'ensemble des comptes administrateurs sont sous le contrôle du RSSI.

4.2.3 Sécurisation des postes de travail et des moyens nomades

L'accès aux postes de travail et moyens nomades doit être protégé par mots de passe suffisamment robustes. Chaque mot de passe est personnel et confidentiel et à ce titre, il ne doit pas être divulgué à un tiers, quel qu'il soit, ni laissé sans protection.

Les utilisateurs veillent au bon déroulement des applications de sécurisation installés sur les moyens informatiques mis à leur disposition :

- Mise à jour effective de l'anti-virus ;
- Mise à jour du système d'exploitation et des applications présentes.

Les utilisateurs doivent signaler à l'administrateur les dysfonctionnements et les incidents.

Les utilisateurs prendront les mesures spécifiques adaptées en cas d'utilisation des moyens nomades en dehors de leur zone de sécurité (protection contre le vol, etc.).

4.2.4 Contrôle d'accès logique

Tout accès au système d'information est soumis à l'identification/authentification du demandeur et au contrôle de ses habilitations.

L'authentification doit se faire à travers l'annuaire LDAP de l'entreprise. Il importe de bien définir les autorisations et de n'attribuer que les privilèges nécessaires. Les accès doivent être tracés.

L'attribution et la modification des accès et privilèges d'un site doivent être validés par le Directeur Régional.

4.2.5 Contrôle d'accès physique

L'objectif est de protéger physiquement les actifs sensibles en veillant à ce que seules les personnes habilitées aient accès aux bâtiments, aux locaux techniques et locaux d'archives des différents sites du Groupe et que les accès soient tracés. Les actifs sensibles feront l'objet d'un inventaire régulièrement mis à jour.

Les bureaux susceptibles de contenir des données sensibles seront fermés par clé dans un premier temps puis accessibles par badge (bureau des managers, locaux sésame, locaux serveurs, secrétariats).

4.2.6 Sécurité des applications

La sécurité doit être prise en compte à toutes les étapes d'un projet. Pour cela un dossier de sécurité (initié lors de l'étape de GO/NOGO) doit accompagner chaque projet et préciser les objectifs, les méthodes et les mesures préconisés.

Les exigences de sécurité des projets sont basées sur le top 10 de l'OWASP et sont intégrées aux autres exigences des projets. Des guides de codage sécurisé sont fournis aux développeurs.

En particulier, les applications informatiques de gestion et les applications internet, doivent être sécurisées, en cohérence avec la sensibilité des informations traitées et échangées.

Chaque dossier doit être approuvé par le RSI.

Le Groupe Infotel n'autorise aucun développement externalisé des applications gérées dans son sein.

4.2.7 Réseau

L'administration du réseau de l'entreprise est placée exclusivement sous la responsabilité des équipes des RSI.

Les systèmes d'information doivent être protégés vis-à-vis de l'extérieur à l'aide de filtres d'accès appliqués sur les équipements en tête de son réseau.

Ces filtres s'appliquent tant sur les flux réseau entrants que sur les flux sortants.

La politique de définition des filtres d'accès décrivant les flux réseau entrants est systématiquement du type « tout ce qui n'est pas explicitement autorisé est interdit ».

Les serveurs doivent être spécifiquement protégés vis-à-vis des postes de travail et des autres serveurs.

Les serveurs potentiellement accessibles de l'extérieur feront l'objet d'une surveillance accrue.

L'accès externe aux serveurs par les moyens nomades s'effectue au travers de connexions dédiés et chiffrées (VPN).

L'accès au réseau sans-fil doit faire l'objet d'un contrôle spécifique et n'être possible qu'après authentification de l'utilisateur. Les accès doivent être tracés.

Une attention particulière doit être portée aux moyens nomades lors de l'introduction sur le réseau de l'entreprise pour éviter, notamment, de contaminer l'intérieur par des logiciels malveillants.

4.2.8 Maintien du niveau de sécurité

Le maintien du niveau de sécurité (en particulier, la vérification d'absence de risque lors de l'installation de nouveaux matériels ou logiciels ou de connexion de matériels mobiles) doit faire l'objet de dispositions techniques sous la responsabilité du RSSI.

Ces dispositions doivent intégrer le maintien au cours du temps de l'état de sécurité des différents matériels : application des correctifs, mises à jour des anti-virus, pare-feu, etc. Elles doivent préciser les conditions de surveillance du fonctionnement du système d'information de manière à s'assurer de son état de sécurité : analyse des traces, vérification des vulnérabilités, suivi des avis de sécurité.

4.2.9 Le Télétravail et VPN

Actuellement le télétravail, n'est pas mis en œuvre au sein du Groupe Infotel. Il est cependant possible pour des collaborateurs habilités de se connecter à distance au système d'information Infotel Conseil à l'aide d'une connexion VPN sécurisée.
La connexion VPN ne peut être effectuée que par une personne habilitée et depuis un poste de travail d'Infotel Conseil.

4.2.10 Les supports amovibles

Par défaut les supports amovibles de type Clé USB ou Disque Dur Externe ne sont pas autorisés pour les utilisateurs. Toutes fois une dérogation exceptionnelle peut être accordée avec des supports cryptés mis à disposition par Infotel.

4.3 Sécurité liée aux ressources humaines

L'objectif est :

- de garantir que les utilisateurs connaissent leurs responsabilités en terme de sécurité ;
- de réduire les risques d'accident, d'erreur et/ou de malveillance en intégrant les principes de sécurité dans la gestion des ressources humaines, du recrutement à la fin de collaboration ;
- de veiller à ce que les collaborateurs et sous-traitants quittent l'entreprise ou changent de poste selon une procédure définie et diffusée.

4.4 Mesure du niveau effectif de sécurité

4.4.1 Contrôle de l'efficacité du PSSI

Le contrôle de l'efficacité du PSSI s'opère sous la responsabilité du RSSI, du RSI, des process owner et du Risk Manager. Il est réalisé à partir d'un tableau de bord.

4.4.2 Audits

Le niveau de sécurité des systèmes d'information et la conformité de mise en œuvre des recommandations sur le terrain donnent lieu à des audits internes sous la responsabilité du RSSI et du RSI ou à des audits externes après accord du Groupe Infotel.

4.4.3 Journalisation, tableaux de bord

Le système d'information comprend des procédures de journalisation, centralisées et protégées, de l'utilisation des services numériques.

L'objectif est :

- de permettre de détecter des intrusions ;
- d'identifier les causes et les origines ;
- d'éviter des contaminations d'autres sites par rebond ;
- de restaurer le système.

4.4.4 Les fichiers de trace

Les fichiers de traces seront systématiquement analysés afin de repérer d'éventuels problèmes et de produire des statistiques et tableaux de bord.

Il importe de définir, et de faire connaître aux utilisateurs, les règles d'exploitation des fichiers de traces (contenu, durée de conservation, utilisation) dans le respect du « principe de proportionnalité » et des contraintes législatives et réglementaires concernant notamment le traitement des informations à caractère personnel.

4.4.5 Mise en garde

L'utilisation de certains matériels ou logiciels peut s'avérer préjudiciable à la sécurité du système d'information. Ces produits font l'objet de « mises en garde » de la part du RSSI indiquant soit des recommandations d'utilisation, soit une interdiction pure et simple.

4.4.6 Gestion d'incidents

Chaque acteur du système d'information, utilisateur ou administrateur, doit être sensibilisé à l'importance de signaler tout incident réel ou suspecté.

Une procédure de réaction connue de tous les utilisateurs est mise en œuvre en cas d'infection (ver, virus, cheval de Troie), faille de sécurité ou incident constaté ou soupçonné sur un poste de travail.

La signalisation des incidents aux responsables de la sécurité doit être systématique.

Les responsables de la sécurité du système d'information (RSSI, RSI, RM, référents) et leurs équipes apportent leur soutien aux collaborateurs touchés par un incident lié à la sécurité de l'information.

Toute infraction au règlement du SSI qui aurait des conséquences juridiques fera l'objet d'un dépôt de plainte par le RSSI auprès des autorités après avis de la direction générale;

La comptabilisation et la caractérisation des incidents feront l'objet d'indicateurs dans le tableau de bord SSI.

4.4.7 Contrôle de conformité

L'objectif est d'éviter toute violation de la propriété intellectuelle, des obligations contractuelles et des exigences de sécurité.

4.5 Processus de la PSSI

La mise en œuvre de la PSSI du Groupe Infotel se décline en cinq méta-processus :

- Gestion du SMSI ;
- Gestion des risques de sécurité ;
- Gestion des mesures de sécurité ;
- Gestion des incidents de sécurité ;
- Gestion de la conformité en sécurité.

Regroupant quatorze processus :

- Processus de déclaration, de diffusion et de revue des politiques de sécurité de l'information d'Infotel ;
- Processus d'organisation et d'administration de la sécurité de l'information ;
- Processus de gestion du niveau de sécurité des ressources humaines ;
- Processus de sécurisation du matériel informatique et de télécommunication ;
- Processus de sécurisation logique des accès ;
- Processus de sécurisation physique des accès et des actifs ;
- Processus de sécurisation de l'exploitation ;
- Processus de sécurisation des communications ;
- Processus de sécurisation de l'acquisition, du développement et de la maintenance des systèmes d'information ;
- Processus de sécurisation des relations avec les fournisseurs ;
- Processus de gestion des incidents liés à la sécurité de l'information ;
- Processus de gestion de la continuité ;
- Processus de contrôle ;
- Processus de maitrise des risques.

4.6 Procédure de la PSSI

A chacun des processus sont associées des procédures :

- Procédure de contrôle des accès physique ;
- Procédure de gestion de la PSSI ;
- Procédure du pilotage du SMSI ;
- Procédure de gestion du modèle procédural du SMSI ;
- Procédure de classification des données, informations, actifs matériels et locaux ;
- Procédure de gestion des actifs ;
- Procédure de gestion des audits ;
- Procédure de sécurisation RH ;
- Procédure de gestion des risques ;
- Procédure d'organisation des revues de direction ;
- Procédure de gestion de la communication, de la formation et de la sensibilisation ;
- Procédure de gestion des habilitations ;
- Procédure de contrôle des accès logiques ;
- Procédure de gestion des utilisateurs du S.I. ;
- Procédure de déclaration et traitement des incidents liés à la sécurité de l'information ;
- Procédure de gestion de la relation avec les fournisseurs ;
- Procédure de sécurisation des projets ;
- Procédure de sauvegarde des serveurs ;
- Procédure de mesures, analyse et amélioration continue ;
- Procédure d'exploitation SI (surveillance de la disponibilité du S.I.);
- Procédure d'exploitation SI (Surveillance des connexions au réseau);
- Procédure d'exploitation SI (Suivi des actifs) ;
- Procédure d'exploitation SI (Suivi des actifs 2) ;
- Procédure de gestion du Plan de continuité d'activité ;
- Procédure de cryptographie ;
- Procédure d'exploitation SI (Les pare-feu) ;
- Procédure de gestion des changements ;
- Procédure de gestion des vulnérabilités ;
- Procédure de Veille Technique et Réglementaire ;
- Transfert de l'information ;
- Impacts du RGPD.

5 Annexes

5.1 Sigles et abréviations

Sigle	Libellé
CIL	Correspondant Informatique et Libertés
CNIL	Commission nationale de l'informatique et des libertés
COSI	Comité d'Orientation du Système d'Information
DPO	Data Protection Officer
PCA	Plan de continuité d'activité
PSSI	Politique de Sécurité du Système d'Information
RM	Risk Manager
RSI	Responsable du Système d'Information
RSSI	Responsable de la sécurité des Systèmes d'Information
SMSI	Système de Management de la Sécurité de l'Information
SSI	Sécurité du Système d'Information

5.2 Glossaire

Terme	Définition
Journalisation	Fonction d'enregistrement des activités. L'enregistrement d'un historique permet de mettre en œuvre des fonctionnalités telles que les « derniers fichiers ouverts », les « dernières commandes tapées » ou les « dernières pages web consultées ».
Traces	Ce sont les journaux issus de la journalisation des évènements