

# **POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION (PSSI FranceAgriMer)**

**Mise à jour en date du 15/05/2024**

## Diffusion :

- Ensemble du personnel de FranceAgriMer, quel que soit le lieu d'exercice de l'activité (siège, délégations nationales, services territoriaux de FranceAgriMer) ;
- Personnel externe intervenant auprès de FranceAgriMer et disposant d'un droit d'accès aux systèmes d'information (partenaires, prestataires de services, corps de contrôle ou missions d'audit externes, ...).

## Date de mise en application :

La présente Politique sécurité des systèmes d'information (PSSI) de l'Etablissement entre en vigueur le jour de sa diffusion.

La PSSI en date du 09/01/2023 est abrogée.

## Table des matières

1. Cadre réglementaire de la sécurité des systèmes d'information .....	4
2. Objectif de la sécurité des systèmes d'information.....	5
3. Champ d'application .....	5
4. Lignes directrices de la stratégie de sécurité .....	6
5. Organisation de la sécurité.....	7
6. Objectifs de sécurité.....	8
7. Mise en œuvre .....	10
<b>Fin du document</b> .....	<b>11</b>

# Introduction

---

**Le présent document formalise la Politique de sécurité des systèmes d'information (PSSI) arrêtée par la Directrice ou le Directeur général(e) de FranceAgriMer.**

La PSSI définit la stratégie et les orientations générales pour la sécurisation des systèmes d'information de l'Etablissement et fixe les principaux objectifs du pilotage de la sécurité des systèmes d'information au sein de l'Etablissement.

L'information est une ressource très importante de l'organisation qu'il est nécessaire de protéger de manière adaptée en fonction des enjeux et de son niveau de sensibilité.

Le système d'information peut être défini comme l'ensemble organisé des ressources (personnel, données, procédures, matériel, logiciel, etc.) qui permet à l'Etablissement de collecter, stocker, traiter et distribuer les informations nécessaires à ses activités sous forme de textes, images, sons, ou de données codées. Le système d'information coordonne ainsi les activités de l'organisation grâce à la structuration des échanges et lui permet d'atteindre ses objectifs.

L'informatisation croissante permet d'améliorer la productivité mais expose en même temps les organisations à de nouveaux risques ; l'accroissement des réseaux augmente également le risque. Un dysfonctionnement des systèmes d'information impactera directement l'organisation et la nécessité de sécuriser les systèmes d'information s'impose à l'Etablissement.

Des mesures de protection adaptées aux risques identifiés doivent donc être mises en œuvre afin de maintenir les informations et les activités dans les meilleures conditions de sécurité possible.

Une politique de sécurité n'est pas une finalité en soi. L'intention profonde d'un tel document est d'informer, mobiliser, conseiller, éclairer, orienter la mise en œuvre de dispositifs, procédures, moyens de sécurité garantissant le niveau de protection approprié au regard des activités stratégiques de l'organisation.

Tout acteur, qu'il soit agent de FranceAgriMer ou personnel externe travaillant au bénéfice de l'Etablissement, doit prendre conscience des enjeux de FranceAgriMer et prendre part à son niveau et par un comportement adapté, réfléchi et mesuré à une protection efficace et pérenne de ses systèmes d'information.

En application de la lettre du Premier ministre du 17 juillet 2014, la PSSI de FranceAgriMer s'appuie sur les orientations proposées par la PSSI Etat (PSSIE) qui couvrent à la fois les aspects techniques et organisationnels de la SSI.

La PSSI constitue la base du système de management de la sécurité des systèmes d'information (SMSI) de l'Etablissement.

## **1. Cadre réglementaire de la sécurité des systèmes d'information**

- L'arrêté du 27 avril 2007 portant désignation des autorités qualifiées de sécurité des systèmes d'information au sein de l'administration centrale, des services déconcentrés et des établissements sous tutelle du ministère de l'agriculture et de la pêche ;
- La circulaire du Premier ministre du 17 juillet 2014, portant sur la politique des systèmes d'information de l'Etat, et comportant en annexe le document de politique de sécurité des systèmes d'information de l'Etat fixant un ensemble de règles de protection applicables aux systèmes d'information de l'Etat ;
- Le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;
- Le règlement (UE) n°1306/2013 du Parlement européen et du Conseil du 17 décembre 2013 relatif au financement, à la gestion et au suivi de la politique agricole commune ;
- Le règlement délégué (UE) n°907/2014 de la Commission du 11 mars 2014, publié le 28/08/2014, complétant le R. (UE) n°1306/2013 du Parlement européen et du Conseil, relatif au financement, à la gestion et au suivi de la politique agricole commune.

Et d'une manière plus générale :

- La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;
- Le décret n° 2007-284 du 2 mars 2007 fixant les modalités d'élaboration, d'approbation de modification et de publication du référentiel général d'interopérabilité (RGI) ;
- L'arrêté du 20 avril 2016 portant approbation du référentiel général d'interopérabilité (V2) ;
- La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
- La loi n° 92-597 du 1 juillet 1992 relative au code de la propriété intellectuelle (partie législative) ;
- La loi n° 92-684 du 22 juillet 1992 portant réforme des dispositions du code pénal relatives à la répression des crimes et délits contre les personnes ;
- La loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications ;
- Le décret n°2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques ;
- Le décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne ;
- Le code des postes et des communications électroniques, et notamment l'article L34-1 livre II, chapitre II ;
- Le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), dit RGPD.
- La directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/172, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), dite NIS 2.

## **2. Objectif de la sécurité des systèmes d'information**

La **sécurité des systèmes d'information (SSI)** est l'ensemble des moyens techniques, organisationnels, juridiques et humains visant à empêcher l'utilisation non-autorisée, le mauvais usage, la modification ou le détournement du système d'information.

La sécurité est un enjeu majeur pour l'Etablissement ainsi que pour l'ensemble de son environnement afin de maintenir l'accès aux informations, la cohérence de l'ensemble du système d'information et la confiance des acteurs et usagers, internes et externes.

Les mesures de sécurité mises en œuvre ont pour finalité de garantir un niveau de protection approprié des activités et de permettre à l'Etablissement de répondre à ses objectifs dans les meilleures conditions au regard des menaces devenues aujourd'hui permanentes.

Assurer la sécurité du système d'information est une activité du management du système d'information (**SMSI**). Depuis 2017, le SMSI de FranceAgriMer est certifié ISO/IEC 27001 sur le périmètre « organisme payeur du Fonds européen agricole de garantie (FEAGA) ».

## **3. Champ d'application**

La PSSI s'applique à tous les systèmes d'information opérationnels qui participent au fonctionnement des processus essentiels de l'Etablissement et concerne l'ensemble des actifs (appelés également « biens support ») qui ont de l'importance en matière d'information et qui sont nécessaires à l'accomplissement des tâches :

- les informations gérées : bases de données, fichiers, manuels utilisateur, procédures de gestion, dossiers de travail, plan de continuité, ...
- les logiciels utilisés : logiciels applicatifs, systèmes, ...
- les moyens matériels mis à disposition : matériels informatiques, de communication, meubles, espaces de travail, ...
- les services rendus : informatiques, communications, commodités générales (chauffage, climatisation,...).

La PSSI s'applique à l'ensemble du personnel de l'Etablissement, quel que soit le lieu où l'activité est exercée (siège, services FranceAgriMer en DRAAF, délégations nationales, personnel en situation de travail à distance, ...), ainsi qu'aux personnes extérieures intervenant pour l'Etablissement (partenaires, prestataires de services, ...).

En matière de SSI, les agents des services territoriaux de FranceAgriMer qui exercent leurs activités au sein des DRAAF sont soumis à un régime particulier précisé dans les conventions établies entre la Directrice ou le Directeur général(e) de FranceAgriMer et chaque Préfet de région :

*« Les agents affectés aux missions de FranceAgriMer sont installés dans les DRAAF et sont soumis, de ce fait, aux dispositions définies par la PSSI du Ministère de l'agriculture, de l'agroalimentaire et de la forêt (MAAF) et par la note relative aux droits et devoirs des utilisateurs des systèmes d'information associée. Les exigences de sécurité issues de la politique de sécurité des systèmes d'information (PSSI) de FranceAgriMer sont prises en compte dans la PSSI du MAAF, notamment sur tous les aspects liés à l'environnement de travail.*

*Toutefois, le système d'information (SI) de FranceAgriMer est dans le champ d'application exclusif de la PSSI de FranceAgriMer. Les conditions d'accès au SI et l'utilisation des ressources SI de FranceAgriMer restent soumises aux exigences définies par la PSSI de FranceAgriMer, dont l'application est sous le contrôle du Responsable SSI (RSSI) de FranceAgriMer.*

La mission intitulée « sécurité des systèmes d'information » est assurée sur place par l'agent de sécurité des systèmes d'information (ASSI) de la DRAAF désigné par l'Autorité qualifiée des systèmes d'information (AQSSI) conformément à l'arrêté du 27 avril 2007.

L'ASSI est le correspondant SSI (CSSI) du Responsable SSI (RSSI) de FranceAgriMer et a un rôle prépondérant dans le processus d'identification et de remontée des incidents. Il sera l'interlocuteur privilégié lors des audits menés par les corps de contrôle externe sur les missions de FranceAgriMer et aura à répondre, en relation avec les responsables concernés (DRAAF, FSSI et MSSI) du MAAF, des dispositions prises sur place en matière de SSI.

La formation (ou la sensibilisation) à la SSI des agents affectés aux missions de FranceAgriMer en DRAAF sera réalisée dans le cadre du plan de formation organisé par le MAAF».

## **4. Lignes directrices de la stratégie de sécurité**

La politique de sécurité des systèmes d'information de l'Etat (PSSIE), élaborée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en relation avec les ministères, fixe des principes et un ensemble de règles de protection. La stratégie de sécurité de l'Etablissement s'appuie sur les lignes directrices fournies par la PSSIE et les principes stratégiques définis par l'ANSSI rappelés ci-après :

- P1. Lorsque la maîtrise de ses systèmes d'information l'exige, l'administration fait appel à des opérateurs et des prestataires de confiance.
- P2. Tout système d'information de l'Etat doit faire l'objet d'une analyse de risques permettant une prise en compte préventive de sa sécurité, adaptée aux enjeux du système considéré. Cette analyse s'inscrit dans une démarche d'amélioration continue de la sécurité du système, pendant toute sa durée de vie. Cette démarche doit également permettre de maintenir à jour une cartographie précise des systèmes d'information en service.
- P3. Les moyens humains et financiers consacrés à la sécurité des systèmes d'information de l'Etat doivent être planifiés, quantifiés et identifiés au sein des ressources globales des systèmes d'information.
- P4. Des moyens d'authentification forte des agents de l'Etat sur les systèmes d'information doivent être mis en place.
- P5. Les opérations de gestion et d'administration des systèmes d'information de l'Etat doivent être tracées et contrôlées.
- P6. La protection des systèmes d'information doit être assurée par l'application rigoureuse de règles précises. Ces règles découlent de la PSSIE.
- P7. Chaque agent de l'Etat, en tant qu'utilisateur d'un système d'information, doit être informé de ses droits et devoirs mais également formé et sensibilisé à la cyber-sécurité. Les mesures techniques mises en place par l'Etat dans ce domaine doivent être connues de tous.
- P8. Les administrateurs des systèmes d'information doivent appliquer, après formation, les règles élémentaires d'hygiène informatique.
- P9. Les produits et services acquis par les administrations et destinés à assurer la sécurité des systèmes d'information de l'Etat doivent faire l'objet d'une évaluation et d'une attestation préalable de leur niveau de sécurité, selon une procédure reconnue par l'ANSSI (« labellisation »).
- P10. Les informations de l'administration considérées comme sensibles, en raison de leurs besoins en confidentialité, intégrité ou disponibilité, sont hébergées sur le territoire national.

## **5. Organisation de la sécurité**

En application de l'article 4 de l'arrêté du 27 avril 2007 du Ministre de l'Alimentation, de l'Agriculture et de la Pêche, **la Directrice ou le Directeur général(e) de l'Etablissement est désignée «Autorité qualifiée de la sécurité des systèmes d'information (AQSSI)».**

L'AQSSI est responsable de la politique menée en la matière dans l'Etablissement. Elle définit et met en place l'organisation nécessaire pour garantir une bonne sécurité des systèmes d'information. L'AQSSI s'engage à œuvrer pour l'amélioration continue du SMSI.

L'AQSSI est assistée par le responsable de la sécurité des systèmes d'information (RSSI) de l'Etablissement pour le pilotage et la gestion de la politique de SSI au sein de FranceAgriMer. Le RSSI soumet les mesures d'application de la PSSI à validation de l'AQSSI et veille à leur application.

L'organisation de la sécurité assure la cohérence des actions au travers d'une chaîne de responsabilité, coordonnée par le RSSI, qui passe par les directeurs et responsables des entités constituant l'Etablissement, les correspondants SSI nommés en délégations nationales et les agents SSI des DRAAF (désignés par la Mission Défense et Sécurité et les responsables sécurité du MAA). Elle repose également sur les utilisateurs des systèmes d'information et, plus particulièrement, sur les responsables informatiques.

Le pilotage de la Sécurité des systèmes d'information s'appuie sur plusieurs instances de gouvernance :

- **Le Comité de pilotage du SMSI (COPIL SSI)**

Le COPIL SSI réunit l'ensemble des responsables de direction et des processus qui interviennent au pilotage du système de management de la sécurité de l'information, notamment sur le périmètre des aides FEAGA, objet de la certification ISO 27001:2022.

Le COPIL SSI se réunit en tant que de besoin et a minima deux fois par an, sous la présidence de l'AQSSI ou de son représentant, afin de faire le point sur le bon fonctionnement du SMSI :

- Examen des résultats des analyses de risques SSI, des risques résiduels et des plans de traitement des risques proposés, soumis à validation de l'AQSSI ;
- Suivi d'avancement et enrichissement du plan d'actions d'amélioration du SMSI, notamment pour le périmètre d'activités soumis à certification ISO 27001:2022 ;
- Examen des non conformités relevées et propositions d'actions correctives ;
- Etude des projets de politiques techniques de sécurité (PTS) proposés par le RSSI en déclinaison de la PSSI ;
- Examen des incidents déclarés et des suites données ;
- Examen des propositions d'homologation des télé-services de l'Etablissement au Référentiel général de sécurité (RGS) portées par le RSSI ;
- Examen des résultats des revues de direction effectuées par la mission d'audit interne.

Le COPIL SSI recherche en outre les opportunités d'amélioration continue, prend connaissance de l'ensemble des résultats d'audit, interne et externe, et statue sur les décisions prises à la suite de leurs recommandations.

- **Le Comité de projet du SMSI (COPRO SSI)**

Le COPRO SSI réunit l'ensemble des responsables de la mise en œuvre opérationnelle de la SSI au sein de l'Etablissement, notamment sur le périmètre des aides FEAGA, objet de la

certification ISO 27001:2022. Le RSSI, le chef du service des systèmes d'information, le chef du service Arborial, le chef du service des ressources humaines, le chef de la mission d'audit interne et le délégué à la protection des données sont membres de droit de ce comité. D'autres responsables d'entités ou de processus peuvent être invités à participer au COPRO SSI selon les sujets à l'ordre du jour.

Le COPRO SSI veille notamment à la mise en œuvre des décisions prises par le COPIL SSI et constitue une force d'analyse et de proposition.

Le COPRO SSI se réunit en tant que de besoin et a minima une fois avant chaque COPIL SSI, sous la présidence du Secrétaire général ou de son représentant.

- **Le Comité de pilotage du Plan de Continuité d'Activité (COPIL PCA)**

Le COPIL PCA réunit l'ensemble des responsables de direction et des responsables de processus qui participent au pilotage de la continuité d'activité de l'Etablissement.

Le COPIL PCA se réunit en tant que de besoin et a minima deux fois par an, sous la présidence de l'AQSSI ou de son représentant. Il a pour objectif de s'assurer que l'Etablissement dispose d'un plan de continuité d'activité adapté et opérationnel. Sont notamment inclus dans le périmètre du COPIL PCA :

- l'élaboration du PCA ;
- le bilan de la mise en œuvre du PCA à l'occasion des situations de crise ;
- le pilotage des tests du PCA ;
- le suivi d'avancement et enrichissement du plan d'actions PCA.

Le COPIL PCA recherche les opportunités d'amélioration continue en se basant notamment sur les résultats d'audit, les conclusions des tests PCA et les bilans effectués lors des situations de crise.

## **6. Objectifs de sécurité**

Les principaux objectifs de sécurité retenus pour FranceAgriMer sont présentés ci-dessous en fonction des thèmes traités par la PSSIE.

### **Thème : Politique, Organisation et Gouvernance de la sécurité des systèmes d'information**

Objectif	Libellé de l'objectif
<b>Objectif 01</b>	Définir et formaliser la PSSI de l'Etablissement en s'appuyant sur la PSSIE et mettre en place une organisation adéquate, garantissant la prise en compte préventive et réactive de la sécurité au sein de l'Etablissement.

### **Thème : Ressources humaines**

Objectif	Libellé de l'objectif
<b>Objectif 02</b>	Responsabiliser les agents et les intégrer comme acteurs dans la démarche SSI

### **Thème : Gestion des biens**

Objectif	Libellé de l'objectif
<b>Objectif 03</b>	Tenir à jour une cartographie détaillée et complète des SI
<b>Objectif 04</b>	Qualifier l'information de façon à adapter les mesures de protection

### **Thème : Intégration de la SSI dans le cycle de vie des systèmes d'information**

Objectif	Libellé de l'objectif
----------	-----------------------



<b>Objectif 05</b>	Réaliser une analyse de risques adaptée aux enjeux du système considéré pour préciser les conditions d'emploi et procéder à l'homologation de sa sécurité avant sa mise en exploitation
<b>Objectif 06</b>	Assurer le maintien en condition de sécurité des systèmes d'information en veillant à gérer dynamiquement les mesures de protection, tout au long de la vie du SI
<b>Objectif 07</b>	Utiliser les produits et services labellisés par l'ANSSI afin de renforcer la protection des SI
<b>Objectif 08</b>	Assurer la maîtrise des prestations et veiller aux exigences de sécurité lorsqu'il est fait appel à de la prestation par des tiers

### Thème : Sécurité physique

Objectif	Libellé de l'objectif
<b>Objectif 09</b>	Définir des périmètres de sécurité physique au niveau du site avec des zones spécifiques abritant les SI et veiller à définir des règles s'appliquant aux zones d'accueil du public et aux locaux techniques
<b>Objectif 10</b>	Assurer la sécurité physique des salles informatiques en organisant le découpage des locaux en zones de sécurité, en définissant les conditions d'hébergement et d'accès et en veillant au bon fonctionnement des moyens généraux
<b>Objectif 11</b>	Veiller à la sécurité du SI de sûreté utilisé pour les activités de contrôle d'accès, de vidéosurveillance, de gestion technique des bâtiments et de sécurité incendie

### Thème : Sécurité des réseaux

Objectif	Libellé de l'objectif
<b>Objectif 12</b>	Assurer la sécurité de l'usage des réseaux
<b>Objectif 13</b>	Assurer la sécurité des réseaux locaux et maîtriser les interconnexions de réseaux locaux
<b>Objectif 14</b>	Prendre des dispositions de sécurité appropriées pour la mise en place d'accès spécifiques qui devront être limités et faire l'objet d'une supervision adaptée
<b>Objectif 15</b>	Assurer la sécurité de l'usage des réseaux sans fil et maîtriser leur déploiement, leur configuration et leur usage
<b>Objectif 16</b>	Assurer la sécurité des mécanismes de communication et de routage et veiller à les configurer pour se protéger des attaques
<b>Objectif 17</b>	Disposer d'une cartographie détaillée des réseaux et des interconnexions et la tenir à jour

### Thème : Architecture des SI

Objectif	Libellé de l'objectif
<b>Objectif 18</b>	Appliquer les principes de défense en profondeur à l'architecture matérielle et logicielle des infrastructures

### Thème : Exploitation des SI

Objectif	Libellé de l'objectif
<b>Objectif 19</b>	Assurer la protection des informations sensibles en confidentialité et en intégrité, en définissant et en mettant en œuvre des mesures de protection renforcées
<b>Objectif 20</b>	Assurer la sécurité des ressources informatiques avec un durcissement des configurations et la surveillance des interventions opérées sur celles-ci
<b>Objectif 21</b>	Organiser la gestion des autorisations et le contrôle d'accès logique aux ressources pour authentifier les usagers et contrôler leurs accès, en fonction d'une politique explicite d'autorisations
<b>Objectif 22</b>	Assurer la sécurité de l'exploitation en fournissant aux administrateurs les outils nécessaires à l'exercice des tâches SSI et configurer ces outils de manière sécurisée
<b>Objectif 23</b>	Assurer la défense des systèmes d'information par une vigilance de tous, des actions permanentes des exploitants et une gestion dynamique de la sécurité de l'équipe en charge de la SSI.

<b>Objectif 24</b>	Assurer la sécurité des ressources informatiques en s'appuyant sur des procédures adaptées et sur la maîtrise des outils de supervision.
--------------------	--

#### **Thème : Sécurité du poste de travail**

Objectif	Libellé de l'objectif
<b>Objectif 25</b>	Assurer la sécurité des postes de travail en durcissant leurs configurations et en organisant la protection des postes utilisateurs (réaffectation du poste et récupération des informations, gestion des privilèges, protection des informations, nomadisme)
<b>Objectif 26</b>	Assurer la sécurité des copieurs multifonctions par un paramétrage adapté afin de diminuer leur surface d'attaque
<b>Objectif 27</b>	Assurer la sécurité de la téléphonie pour protéger les utilisateurs contre des attaques malveillantes
<b>Objectif 28</b>	Appliquer des paramétrages de sécurité aux postes de travail et réaliser un contrôle régulier de leur conformité

#### **Thème : Sécurité du développement des systèmes**

Objectif	Libellé de l'objectif
<b>Objectif 29</b>	Prendre en compte la sécurité comme une fonction essentielle dans le développement des SI dès la phase de conception des projets
<b>Objectif 30</b>	Intégrer la sécurité dans le développement des logiciels en appliquant une méthodologie de sécurisation du code produit et en s'appuyant sur des référentiels de sécurité
<b>Objectif 31</b>	Assurer la sécurité des applications à risques en mettant en place des fonctionnalités de filtrage applicatif

#### **Thème : Traitement des incidents**

Objectif	Libellé de l'objectif
<b>Objectif 32</b>	Organiser les chaînes opérationnelles SSI pour partager l'information (alertes, incidents) dans le respect des règles de prudence et mutualiser les opérations de remise en état, de façon à lutter efficacement contre les attaques

#### **Thème : Continuité d'activité**

Objectif	Libellé de l'objectif
<b>Objectif 33</b>	Organiser la gestion de la continuité d'activité en se dotant de plans de continuité et en veillant à les tester régulièrement

#### **Thème : Conformité, audit, inspection, contrôle**

Objectif	Libellé de l'objectif
<b>Objectif 34</b>	Effectuer des contrôles (audits, inspections) et des exercices réguliers de façon à mesurer les progrès accomplis et corriger les manquements

## **7. Mise en œuvre**

Les 34 objectifs de sécurité globaux retenus par la Direction générale afin de garantir la sécurité des systèmes d'information de l'Etablissement font l'objet d'actions concrètes qui s'appuient sur les mesures préconisées par la PSSIE. Lorsque cela est nécessaire, les règles énoncées par la PSSIE peuvent être adaptées pour l'Etablissement, conformément aux termes de l'article 8 de la PSSIE.

Ce dispositif doit permettre une meilleure maîtrise de la sécurité des SI par la mise en œuvre de mesures de protection proportionnées aux enjeux et en adéquation avec les risques encourus. Le choix des mesures de sécurité est effectué en s'assurant que les actions prévues et les coûts engendrés sont proportionnés aux risques et à la réduction des dits risques.

Ces actions sont traduites dans un plan d'action formalisé soumis à validation de la Direction générale.

Le RSSI est en charge de la coordination de la mise en œuvre des actions et rend compte régulièrement de leur suivi au Comité de pilotage de la Sécurité des Systèmes d'Informations.

**Fin du document**