

*Nota : ce document a été émis et est géré par DSI/ PDSI / DSIG*

## **POLITIQUE DE SECURITE DU SYSTEME D'INFORMATION**

Ce document définit les principes directeurs de la sécurité des systèmes d'information de l'INERIS :

- S'appuyer sur un système de pilotage de la sécurité des SI, complet et structuré
- Cartographier et appliquer des mesures de protection proportionnées aux risques encourus
- Agir sur les comportements
- Maîtriser les accès aux SI
- Respecter les meilleures pratiques et s'inscrire dans une logique d'amélioration continue

## SOMMAIRE

<b>1. INTRODUCTION : LES ENJEUX DE LA PSSI .....</b>	<b>3</b>
<b>2. PRINCIPES ET OBJECTIFS DE LA PSSI.....</b>	<b>3</b>
2.1. Périmètre d'application .....	4
2.2. Besoins de sécurité.....	5
2.3. Cartographie des risques .....	6
2.4. Menaces et mesures de sécurité .....	6
<b>3. PRINCIPES D'ORGANISATION ET DE MISE EN ŒUVRE.....</b>	<b>7</b>
3.1. Organisation & Responsabilités.....	7
3.1.1. Dispositions légales et réglementaires .....	7
3.1.2. Responsabilité des différents acteurs .....	8
3.1.3. Accès aux ressources informatiques, sensibilisation .....	9
3.1.4. Charte informatique .....	9
3.1.5. Cyber surveillance.....	9
3.2. Protection des données.....	10
3.2.1. Disponibilité, confidentialité et intégrité des données.....	10
3.2.2. Protection des données sensibles.....	10
3.2.3. Données à caractère personnel.....	11
3.2.4. Chiffrement.....	11
3.2.5. Réparation, cession, mise au rebut .....	12
3.3. Sécurisation du SI .....	12
3.3.1. Administration des serveurs et des postes de travail .....	12
3.3.2. Postes de travail et des moyens nomades.....	12
3.3.3. Contrôle d'accès .....	13
3.3.4. Sécurité des applications et projets SI .....	13
3.3.5. Infogérance et prestations externes .....	14
3.3.6. Réseau.....	14
3.3.7. Maintien du niveau de sécurité.....	15
3.4. Suivi et contrôle de la PSSI .....	15
3.4.1. Contrôle de gestion et audits .....	15
3.4.2. Journalisation, tableaux de bord .....	16
3.4.3. Gestion d'incidents .....	16
3.4.4. Sanction des violations des règles de sécurité.....	17

## 1. INTRODUCTION : LES ENJEUX DE LA PSSI<sup>1</sup>

Le haut niveau d'expertise des études et recherches menées à l'INERIS confère un **caractère critique à la protection de son patrimoine scientifique et technique**.

Les atteintes à la sécurité peuvent toucher les données scientifiques, techniques ou commerciales mais également les moyens scientifiques, techniques ou humains.

La **Sécurité des systèmes d'Information (SSI)** est une composante essentielle pour la protection des intérêts propres à l'INERIS, pour les intérêts de ses clients et ceux liés aux enjeux nationaux (intérêts fondamentaux de la nation).

La **PSSI**<sup>1</sup> concerne la maîtrise d'ouvrage et la maîtrise d'œuvre face aux risques encourus et pour les choix en termes de gestion des risques. Elle conduit à identifier ce qui doit être protégé, à formuler des objectifs de sécurité et à identifier, arbitrer et mettre en œuvre les mesures adaptées au niveau de sécurité retenu.

La PSSI reflète la **vision de la direction générale** de l'INERIS en matière de SSI. Elle matérialise la reconnaissance de l'importance accordée par la direction à la SSI et s'inscrit sur le long terme.

La présente PSSI est globale et comporte **peu de mesures techniques**.

Elle devra évoluer pour tenir compte des changements qui peuvent affecter le SI de l'INERIS et son environnement, tels que des nouvelles menaces, un changement du plan stratégique de l'Institut ou de la législation.

## 2. PRINCIPES ET OBJECTIFS DE LA PSSI

La PSSI établit un cadre visant à protéger les biens essentiels de l'INERIS des conséquences liées aux menaces d'origines accidentelles ou malveillantes pesant sur les ressources informatiques et de télécommunication de l'Institut.

Pour cela la PSSI traite à la fois des notions de sûreté et de sécurité en traitant des sources de menaces accidentelles, délibérées ou non (humaines internes, humaines externes, bugs, pannes, phénomènes naturels, sinistres internes, ...).

---

<sup>1</sup> Politique de Sécurité des Systèmes d'Information

Ainsi elle a pour objectifs :

- D'assurer la continuité de l'activité en sécurisant et fiabilisant le fonctionnement des SI de l'INERIS ;
- De protéger le SI contenant des informations dont la divulgation, le vol ou l'altération auraient directement ou indirectement des conséquences graves pour INERIS, ses partenaires, ses clients ou son personnel ;
- De soutenir les projets de développement et d'innovation de l'INERIS en faisant de la sécurité des SI un facteur d'opportunité et de croissance ;
- De contribuer à la performance globale de l'INERIS en recherchant les synergies internes et en réduisant les incidents de sécurité des SI.

Elle se traduit par un ensemble de dispositions organisationnelles et techniques, dans le respect des lois et règlements applicables, dont ce document intitulé « Politique de Sécurité du SI de l'INERIS » fixe les grands principes en rappelant les responsabilités induites pour l'ensemble des collaborateurs.

## **2.1. PERIMETRE D'APPLICATION**

Toutes les activités de l'INERIS obéissent aux principes énoncés par la PSSI qui doivent être respectés dans chaque entité de l'INERIS par l'ensemble de ses salariés et contractuellement par ses fournisseurs et partenaires.

Les contraintes imposées par nos partenaires et clients doivent également être évaluées, analysées et validées au cas par cas au regard de leur compatibilité à la PSSI de l'INERIS.

La PSSI s'applique à l'ensemble des ressources informatiques et de télécommunication, dont les « actifs informatiques services » (infrastructure réseaux, messagerie, accès internet, applicatifs métiers, ...), les « actifs informatiques logiciels » (logiciels d'applications, systèmes, outils de développement et utilitaires...), et enfin les « actifs informatiques physiques » (serveurs, postes de travail, routeurs...) y compris les locaux informatiques et les supports de stockage (disques, cartouches magnétiques, cloud...).

Les usages liés à la mobilité (ordinateurs portables, WiFi/4G, smartphones...) sont également concernés, notamment parce qu'ils se pratiquent souvent dans des environnements non protégés.

L'utilisation d'un moyen informatique privé ou extérieur pour un usage professionnel le fait entrer dans le périmètre de la PSSI.

La PSSI intègre également les prestations externes telles que l'hébergement de serveurs et la sous-traitance dans leur incidence sur la sécurité interne des systèmes d'information.

**2.2. BESOINS DE SECURITE**

La sécurité du Système d'Information repose sur les critères suivants :

- La disponibilité (D), définie comme le fait que les acteurs autorisés ont effectivement accès aux actifs dans les conditions prédéfinies. Cela inclut les circonstances exceptionnelles à couvrir si nécessaire par un plan de continuité des activités ;
- L'intégrité (I), définie comme la protection de l'exactitude et de l'intégralité des actifs ;
- La confidentialité (C), définie comme le fait que les actifs ne sont accessibles que par les acteurs autorisés à y accéder ;
- La traçabilité (preuve et contrôle) (T), définie comme la nécessité de pouvoir déterminer les actions opérées sur l'actif (qui a fait quoi et quand).

Les exigences de sécurité prennent en compte les contraintes légales et réglementaires et l'impact du non-respect de chaque exigence de sécurité.

Elles font l'objet d'une réactualisation régulière.

Le propriétaire de la donnée est responsable de sa sécurité. Il peut pour exercer sa responsabilité, s'appuyer sur la contribution de spécialistes en sécurité et en gestion de risques.

Les besoins de sécurité s'appliquent aussi bien aux ressources du système d'information (postes informatiques, réseaux, applications...) qu'aux données traitées par ces ressources. Ils visent :

- La protection de l'outil de travail : les postes informatiques, les réseaux, les applications et les données, constituent « le Système d'Information ». Les risques doivent être maîtrisés ;
- La protection des données : L'inventaire et la classification de ces données (scientifique, gestion, personnel ...) permet d'en identifier le degré de sensibilité et donc le besoin de protection nécessaire ;
- La protection juridique : la mise en œuvre des systèmes d'information s'inscrit dans un cadre législatif et réglementaire destiné en particulier à protéger les droits de propriété intellectuelle, industrielle et ceux de la vie privée (fichiers nominatifs, cyber-surveillance...).

### 2.3. CARTOGRAPHIE DES RISQUES

La maîtrise des risques SI de l'INERIS s'appuie sur l'identification, la classification des informations et des ressources utilisées pour leur traitement et l'évaluation permanente des risques encourus.

Les principes d'action induits sont :

- La systématisation de la démarche de classification sécurité des actifs IT afin de les sécuriser de façon appropriée selon les 4 critères standards : Disponibilité, Intégrité, Confidentialité, Traçabilité ;
- La définition des plans de prévention et de protection en croisant les besoins et exigences formulés par chaque responsable Métier avec l'évaluation permanente des risques ;
- L'évaluation des risques en croisant les scénarios de menaces pesant sur les biens supports avec les vulnérabilités existantes et les impacts induits. (Menaces X vulnérabilités X impacts).

Cette analyse de risque doit permettre, selon les cas, de :

- Réduire, transférer ou accepter les risques ;
- Mettre en perspective les impacts potentiels des situations de risque avec le coût des mesures de protection ;
- Surveiller les risques acceptés pour s'assurer qu'ils restent à un niveau acceptable.

### 2.4. MENACES ET MESURES DE SECURITE

Afin de mettre en place les moyens de sécurité adéquate, une analyse de risque a été réalisée, en distinguant :

- Les attaques visant directement le système d'information : vol de données (et éventuellement les ressources contenant ces données), modification des données, déni de service...
- Les attaques visant les ressources informatiques : vol de ressources, détournement des ressources, altération des données, émission de malware...
- Les accidents : sinistres naturels, altération accidentelle des données ou ressources...

Pour chaque menace, le risque a été mesuré en évaluant la probabilité que celle-ci devienne réalité et en détectant les éventuels facteurs aggravants (négligence constatée, insuffisance d'information, de consignes...).

### 3. PRINCIPES D'ORGANISATION ET DE MISE EN ŒUVRE

#### 3.1. ORGANISATION & RESPONSABILITES

Au sein de l'INERIS, la responsabilité générale de la sécurité des systèmes d'information relève du Directeur des Systèmes d'Information en tant qu'AQSSI<sup>2</sup>. Il est assisté dans cette fonction par le Responsable de l'unité Production, assurant la fonction de RSSI<sup>3</sup>, également Suppléant AQSSI.

Le pilotage courant est de la responsabilité du RSSI qui assure la mise en œuvre opérationnelle pour le contrôle des données entrantes et sortantes.

La gestion de la SSI s'appuie sur un système de management de la sécurité des SI validé au sein du COSI<sup>4</sup>, afin de définir les exigences de sécurité et les plans d'action qui en découlent.

Lorsqu'il traite de SSI, le COSI est composé d'interlocuteurs disposant d'une connaissance adéquate des enjeux métiers et des contraintes spécifiques.

Le RSSI<sup>5</sup> gère la documentation de référence précisant les dispositions de fond qui découlent de la PSSI (exigences, procédures et guides méthodologiques).

##### 3.1.1. Dispositions légales et réglementaires

La PSSI<sup>6</sup> de l'INERIS s'inscrit dans le cadre de la politique et des directives émanant de la DCSSI<sup>7</sup> de l'Etat, en charge de la sécurité des systèmes d'information au niveau national. Cette politique et ces directives sont relayées, par le FSSI<sup>8</sup> du SDSIE<sup>9</sup> du Ministère de tutelle de l'Ineris.

Elle est conforme aux règles définies par l'ANSSI<sup>10</sup> :

- Décret 2011-1425 du 2 Novembre 2011 et Arrêté du 3 Juillet 2012
- Circulaire interministérielle N°3415 du 7 Novembre 2012
- Instruction interministérielle N° 901/SGDSN/ANSSI

<sup>2</sup> AQSSI : Autorité Qualifiée pour la Sécurité des Systèmes d'Information

<sup>3</sup> RSSI : Responsable de la Sécurité des Systèmes d'Information

<sup>4</sup> COSI : Comité des Systèmes d'Information

<sup>5</sup> RSSI : Responsable de la Sécurité des Systèmes d'Information

<sup>6</sup> PSSI : Politique de Sécurité des Systèmes d'information

<sup>7</sup> DCSSI : Direction Centrale de la Sécurité des Systèmes d'Information

<sup>8</sup> FSSI : Fonctionnaire de Sécurité des Systèmes d'Information

<sup>9</sup> SDSIE : Service de Défense, Sécurité et Intelligence Economique

<sup>10</sup> ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

Par ailleurs, dans le cadre de ses activités de développement et d'exploitations de téléservices pour la tutelle, l'INERIS est soumis au RGS<sup>11</sup>.

Pour certaines activités, l'Instruction Interministérielle 1300 (IGI 1300) s'applique également à l'institut et nécessite un système de management de la SSI formalisé.

Enfin, s'appliquent à l'INERIS, et doivent être considérées dans la PSSI les réglementations générales :

- La loi Informatique et Liberté ;
- Le Règlement Général sur la Protection des Données (RGPD)
- Les lois sur la fraude informatique et la cybercriminalité ;
- Les lois sur la protection de la propriété intellectuelle et la protection des logiciels ;
- Les lois protégeant les personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;
- La réglementation sur Internet : l'INERIS est tenu de mettre en œuvre tout moyen en vue d'enrayer le téléchargement illégal sur Internet.

### 3.1.2. Responsabilité des différents acteurs

**Chaque responsable d'application ou de projet Métier détermine le besoin en sécurité** des activités dont il a la charge. Il intègre les règles relatives à la sécurité des SI dans les processus opérationnels dont il a la charge et s'assure que le personnel qui lui est rattaché est informé et sensibilisé.

Selon leur criticité, les projets de systèmes d'information font l'objet d'une analyse de risque conduite par le RSSI et la MOA<sup>12</sup>.

Elle s'effectue selon 4 axes d'analyse d'impacts :

- **axe « Mission »** : évaluation de l'impact vis à vis des missions de l'INERIS ;
- **axe « Légal »** : évaluation de l'impact vis-à-vis de la conformité légale et réglementaire ;
- **axe « Image »** : évaluation de l'impact d'image de l'INERIS ;
- **axe « financier »** : évaluation de l'impact financier.

Lorsqu'elle élabore un projet ou des demandes concernant le SI, la MOA devra exprimer les besoins de sécurité associés.

<sup>11</sup> RGS : Référentiel Général de Sécurité (Décret 2010-112 du 2 février 2010 et Arrêté du 6 mai 2010)

<sup>12</sup> Maîtrise d'ouvrage



Les projets dont au moins l'un des axes est jugé critique pour la MOA ou la DSI, sont considérés comme des « Projets Critiques » et doivent faire l'objet d'un suivi et d'une validation de la part du Responsable Sécurité du SI.

### 3.1.3. Accès aux ressources informatiques, sensibilisation

La mise à disposition d'outils informatiques à un utilisateur (stations de travail, postes nomades, applications...) doit être formalisée à l'arrivée, au changement de fonction et au départ de l'intéressé, qu'il soit personnel permanent ou non, salarié de l'INERIS ou non.

L'accès aux ressources doit être contrôlé (identification, authentification) et adapté au droit d'en connaître de l'utilisateur (droits et privilèges, profil utilisateur).

Chaque utilisateur est informé et sensibilisé à la PSSI. Il s'engage contractuellement à respecter les règles de sécurité et les bons usages édictés, à ne pas contourner les dispositifs de sécurité et à informer sa hiérarchie de tout incident ou anomalie constatés.

### 3.1.4. Charte informatique

Préalablement à tout accès aux outils informatiques, l'utilisateur doit prendre connaissance des droits et devoirs qui sont les siens compte tenu de la mise à sa disposition des outils et services associés.

C'est l'objet de la « charte informatique » adossée au règlement intérieur de l'INERIS. L'utilisateur doit veiller au respect de la charte, de la PSSI et des règles d'usages.

### 3.1.5. 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 sont conformes à la réglementation en vigueur et respectent les principes de proportionnalité (adaptation du niveau des moyens à l'enjeu effectif de la sécurité) et de transparence (information des partenaires sociaux et utilisateurs).

Leur mise en place donne lieu à des principes et règles diffusés au sein de l'INERIS (politique de gestion des traces par exemple).

**3.2. PROTECTION DES DONNEES****3.2.1. Disponibilité, confidentialité et intégrité des données**

Le traitement et le stockage de données informatisées, l'accès à des services ou à des applications internes ou externes et de manière générale 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.

En particulier une sauvegarde régulière avec des processus de restauration éprouvés est mise en place.

**3.2.2. Protection des données sensibles**

Les données présentant un caractère sensible doivent être identifiées et être régulièrement réexaminées.

Les données sensibles devront impérativement faire l'objet d'une protection pour le contrôle d'accès, le traitement, le stockage ou l'échange pour en assurer la confidentialité :

- L'accès à une donnée sensible ne doit être possible qu'après authentification et contrôle de l'autorisation.
- Toute information sensible circulant sur un réseau externe doit être chiffrée selon les modalités préconisées par la DSI.
- Tout support contenant des données sensibles transporté à l'extérieur (ordinateur portable, stockages amovibles, cd-rom, bande magnétique, etc...) doit faire l'objet de mesure de protection contre le vol et ne contenir que des informations chiffrées.
- Les informations sensibles ne doivent en aucune façon être stockées ou traitées sur des systèmes informatiques non maîtrisés (cybercafé par exemple).
- Le stockage chez un prestataire externe de données sensibles est interdit, sauf dispositions contractuelles de protection ou chiffrement des données.
- Pour le stockage et l'échange informatisé de données particulièrement sensibles pour la nation, des moyens de chiffrement devront impérativement être mis en œuvre selon les dispositions définies au niveau national (cf ci-après).

### 3.2.3. Données à caractère personnel

Le traitement des données personnelles est réalisé conformément au règlement général sur la protection des données (RGPD), Règlement (UE) 2016/679 du 27 avril 2016.

La protection des données à caractère personnel repose sur plusieurs piliers, en particulier : la transparence et la licéité ; les droits des personnes physiques concernées ; la sécurité des données ; la limitation des finalités, la minimisation des données ; la pertinence et la durée de conservation d'une donnée.

La sécurité des données constitue donc l'un des piliers essentiels de la protection des données à caractère personnel.

Les données doivent être gérées de manière à garantir un niveau de sécurité adapté au risque numérique. Les responsables des traitements de données personnelles doivent s'assurer de la mise en œuvre des « mesures techniques ou organisationnelles appropriées », qui peuvent notamment inclure le « chiffrement des données » et des « moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience ».

L'INERIS dispose d'un Délégué à la Protection des Données (DPD) tel que défini par le RGPD.

Le DPD et le RSSI doivent être immédiatement informés de tout incident de sécurité concernant des données personnelles.

### 3.2.4. Chiffrement

Le chiffrement constitue un moyen privilégié de protection des données. Il est d'emploi obligatoire pour le stockage et l'échange de données.

Dans certains cas (ex. diffusion restreinte), les produits utilisés doivent faire l'objet d'un agrément au niveau national (ANSSI).

Tout chiffrement implique la mise en œuvre de procédures permettant de restituer en toutes circonstances les données. Cela peut se faire par séquestre de clés, procédure de recouvrement, voire maintien d'une copie en clair en environnement sécurisé.

Le respect de ces dispositions et la mise en œuvre effective du chiffrement sont réalisés avec l'appui et le conseil de la part du RSSI et de la DSI.

### 3.2.5. Réparation, cession, mise au rebut

Avant tout envoi en réparation, cession ou mise au rebut d'un matériel, il convient de s'assurer que toutes les données ont bien été effacées par un procédé efficace et selon les recommandations techniques nationales (ANSSI).

Si cela s'avère impossible, à cause d'une panne par exemple, les supports concernés devront être démontés et détruits.

## **3.3. SECURISATION DU SI**

### 3.3.1. Administration des serveurs et des postes de travail

L'administration des serveurs est placée sous la responsabilité des administrateurs systèmes et réseaux de la DSI.

L'administration des postes de travail individuels est placée sous la responsabilité des équipes « Poste de travail » et du support de l'unité Production de la DSI.

Les équipes « postes de travail » et du support peuvent intervenir à distance pour des opérations de maintenance sur le poste de travail d'un utilisateur après l'en avoir averti et en respectant les principes de la loi Informatique et Libertés et le Règlement Général sur la Protection des Données (RGPD).

### 3.3.2. Postes de travail et des moyens nomades

Les utilisateurs veillent à la sécurisation de leur poste de travail et des moyens nomades mis à leur disposition. Une vérification du niveau de sécurité doit normalement être réalisée avant l'accès au réseau.

L'accès aux postes de travail (et aux moyens nomades) est protégé par mots de passe. Les mots de passe constituent des données personnelles et confidentielles, ils doivent être suffisamment robustes et renouvelés régulièrement, et ne doivent pas être divulgués ni laissés sans protection.

L'exploitation des moyens informatiques hors de leur zone de sécurité (micro-ordinateurs, portables, stockages externes, imprimantes déportées ...) et donc plus vulnérables aux vols nécessite des mesures spécifiques adaptées (protection contre le vol, chiffrement...) de la part de l'utilisateur.

La sortie et l'utilisation à l'extérieur de tout équipement informatique doivent avoir été autorisées par le Responsable de la Sécurité des Systèmes d'Information (RSSI).

La connexion par des moyens nomades de l'INERIS au système d'information d'un tiers doit respecter les règles de sécurité de l'INERIS.

### 3.3.3. Contrôle d'accès

L'accès au système d'information exige une identification et une authentification préalable. L'utilisation de comptes partagés ou anonymes n'est pas autorisée. Des mécanismes permettant de limiter les services, les données, les privilèges auxquels à accès l'utilisateur en fonction de son rôle dans l'organisation sont mis en œuvre.

Tous les accès sont journalisés.

L'attribution, la modification des droits d'accès et des privilèges d'un SI ou service doivent être validées par le responsable du système concerné. Il importe de différencier au mieux les différents rôles et de n'y associer que les privilèges nécessaires. Les habilitations et les droits d'accès doivent être audités régulièrement et mis à jour.

### 3.3.4. Sécurité des applications et projets SI

Tout projet informatique doit prendre en compte, dès son lancement, les exigences de sécurité définies par les responsables métiers en accord avec le RSSI des actifs impactés. Le processus de prise en compte et de validation de la sécurité doit être intégré dans la démarche de conduite de projet.

L'intégration des aspects sécurité inclut au minimum les étapes suivantes :

- Évaluation de la criticité sécurité et spécification des exigences de sécurité du projet par la maîtrise d'ouvrage assistée au moins du Responsable Sécurité du SI ;
- Définition de la solution informatique et des mécanismes de sécurité par le chef de projet assisté du Responsable Sécurité du SI. Cette solution doit répondre aux exigences de sécurité spécifiées par la MOA ;
- Validation formelle de la solution sécurisée dans le cadre de la gouvernance des projets SI ;
- Validation formelle de l'architecture sécurisée dans l'environnement réel de production par le Responsable Sécurité du SI et homologation éventuelle.

L'intégration des aspects sécurité au sein de la démarche de conduite de projet permet de s'assurer :

- de la planification systématique et de la coordination par le chef de projet des étapes propres à la sécurité ;
- de la prise en compte des coûts liés à la sécurité dans toutes les phases de vie d'un système d'information (projet, exploitation en phase de maintenance...).

### 3.3.5. Infogérance et prestations externes

L'infogérance par des sociétés extérieures chargées de gérer ou maintenir une application de l'INERIS, nécessite parfois des accès au SI.

Les droits d'accès appropriés aux besoins de la prestation sont attribués par le RSSI en fonction du besoin et de l'analyse des risques.

Les prestataires de service doivent respecter les mesures de sécurité de la présente politique, ainsi que des mesures spécifiques si nécessaire. Les contrats relatifs à des prestations informatiques (intégration de logiciels, infogérance, maintenance...) doivent comporter des clauses de confidentialité voire d'agrément et d'habilitation de personnes. Des dispositions contractuelles types sont proposées par le RSSI et le service juridique.

L'accès au système d'information de la part de personnels d'entreprises extérieures doit être conforme à la politique générale d'accès aux moyens informatiques. Les obligations correspondantes, notamment la signature de la charte utilisateur, doivent être mentionnées dans les dispositions contractuelles.

Les accès pour intervention depuis l'extérieur sont tracés et journalisés.

### 3.3.6. Réseau

L'administration du réseau de l'établissement est placée sous la responsabilité de l'unité Production de la DSI et du RSSI.

Les flux réseau entre les différents systèmes doivent être maîtrisés, contrôlés et filtrés selon le principe « tout ce qui n'est pas explicitement autorisé est interdit ».

Le réseau interne doit être cloisonné afin d'isoler les différents services et usages et limiter l'impact d'incidents.

Les serveurs accessibles de l'extérieur feront l'objet d'une surveillance accrue (outils d'analyse des traces, de métrologie...). L'accès externe aux serveurs par les moyens nomades de l'INERIS s'effectue au travers de connexions dédiées et chiffrées (VPN).

L'accès au réseau sans fil est contrôlé, fait l'objet d'un chiffrement adapté et nécessite une authentification de l'utilisateur. Les accès sont journalisés.

Une attention particulière doit être portée aux équipements nomades (Portable, SmartPhone, Tablette...) en raison des risques spécifiques qu'ils induisent (passerelle vis-à-vis de l'extérieur, contamination par des logiciels malveillants). D'une manière générale, seuls les dispositifs approuvés par le RSSI ont la capacité de se connecter au réseau interne. Leurs usages ne doivent pas modifier ou remettre en cause la sécurité du système d'information.

### 3.3.7. Maintien du niveau de sécurité

Le maintien du niveau de sécurité 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... Elles doivent préciser les conditions de surveillance du fonctionnement du SI de manière à s'assurer de son état de sécurité : analyse des journaux, vérification des vulnérabilités, suivi des avis de sécurité...

Des programmes de sensibilisation du personnel, une administration rigoureuse des mécanismes de sécurité en place et une gestion des incidents de sécurité sont organisés de façon à contribuer au maintien du niveau de sécurité.

## **3.4. SUIVI ET CONTROLE DE LA PSSI**

Le suivi de l'application de la politique de sécurité s'inscrit dans le dispositif de contrôle interne de l'INERIS.

Les plans de contrôles sont définis par le RSSI (revue de comptes, audits, ...) :

- Les opérationnels concernés et leurs hiérarchies réalisent les contrôles ;
- Le Responsable de la Sécurité des SI exerce un contrôle de second niveau en vérifiant que les plans de contrôles sont bien réalisés. Les résultats des contrôles sont partagés entre la DSI et le Responsable de la Sécurité des SI :
  - le RSSI définit les contrôles permanents portant sur la sécurité des SI,
  - la synthèse de ces contrôles est transmise au COSI et à la Direction Générale.

Les contrôles de troisième niveau relèvent du système de management de la qualité de l'INERIS.

### 3.4.1. Contrôle de gestion et audits

La sécurité des systèmes d'information de l'INERIS fait l'objet de documents de cadrage, d'organisation et de planification. Le contrôle de gestion de la SSI donne lieu à un tableau de bord présenté au COSI.

Le contrôle de gestion de la SSI s'opère sous la responsabilité du RSSI, après validation et sous le contrôle de l'AQSSI, en l'occurrence le DSI.

Le niveau de sécurité des systèmes d'information et la conformité de mise en œuvre des recommandations sur le terrain peuvent donner lieu à des audits internes sous la responsabilité du RSSI ou des audits externes sous la supervision du RSSI et après accord de l'AQSSI (le DSI) ou de la DG.

### 3.4.2. Journalisation, tableaux de bord

Le SI doit comprendre des dispositifs ou procédures de journalisation centralisés et protégés de l'utilisation des services. L'objectif est de permettre la détection des intrusions ou des utilisations frauduleuses, l'identification des causes et des origines, la prévention des contaminations par rebond.

La durée de conservation et de sauvegarde des fichiers de trace à des fins de preuve est précisée dans le document relatif à la gestion des traces.

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 des contraintes législatives et réglementaires concernant notamment le traitement des informations à caractère personnel.

### 3.4.3. 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, ceci inclut le vol de moyens informatiques ou de supports de données. Le signalement des incidents au RSSI et aux autorités hiérarchiques doit être systématique.

Lorsque l'incident peut mettre en cause la fonction de l'INERIS, le RSSI doit être informé directement, voire, parallèlement, l'AQSSI, selon la gravité de l'incident (données sensibles...).

Selon le niveau de sensibilité de l'incident, le RSSI, après avis de l'AQSSI, en informe les autorités compétentes (service du MTES, DGA...).

Toute infraction susceptible d'implications juridiques fera l'objet d'un dépôt de plainte par le RSSI auprès des autorités compétentes et après avis de l'AQSSI.

Les données statistiques relatives à la gestion des incidents sont intégrées dans le tableau de bord de la SSI.

Le RSSI et l'AQSSI doivent être informés dès le déclenchement de toute crise ayant une incidence sur la sécurité des systèmes d'information ou nécessitant une vigilance particulière sur ces derniers.



#### 3.4.4. Sanction des violations des règles de sécurité

Les interactions entre les composants des Systèmes d'Information de l'INERIS sont nombreuses et contribuent à la complexité de sa sécurité. Aussi, tout non-respect, même ponctuel, de la Politique de Sécurité est susceptible de conséquences dommageables pour tout ou partie de l'activité de l'INERIS. À ce titre, tout non-respect est susceptible d'être sanctionné.

Ainsi, toute tentative de contournement des mécanismes de sécurité mis en place par l'INERIS est une faute professionnelle.

La charte informatique adossée au règlement intérieur de l'Ineris, précise le caractère fautif du non-respect des règles de sécurité.