CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Politique de Sécurité des Systèmes d'Information (PSSI)

Document d'orientation de la sécurité des systèmes d'information du CNRS

Versions	Rédacteur	Autorité d'approbation	Date d'approbation
V1.0	Joseph ILLAND (FSD)	Arnold MIGUS (Directeur Général)	15 novembre 2006

Sommaire

Introduction : les enjeux de la PSSI

Le haut potentiel de recherches du CNRS confère un caractère stratégique à **la protection de son patrimoine scientifique et technique**.

Les atteintes peuvent tout aussi bien toucher ses données scientifiques ou technologiques que ses outils ou moyens scientifiques, techniques et humains.

La **sécurité des systèmes d'information (SSI)** s'impose comme une composante essentielle de la protection du CNRS dans ses intérêts propres et dans ceux liés à des enjeux nationaux (intérêts fondamentaux de la nation).

Bien que cela soit difficile à évaluer, l'insécurité a un coût qui se manifeste lors d'incidents ou de dysfonctionnements.

Face aux risques encourus, et dans le contexte fonctionnel et organisationnel propre à l'organisme, il convient d'identifier ce qui doit être protégé, de quantifier l'enjeu correspondant, de formuler des objectifs de sécurité et d'identifier, arbitrer et mettre en œuvre les parades adaptées au juste niveau de sécurité retenu.

Cela passe prioritairement par la définition et la mise en place au sein du CNRS d'une **« Politique de Sécurité des Systèmes d'Information » (PSSI).**

La PSSI relève d'une vision stratégique de l'organisme et traduit un engagement fort de la direction générale. Elle s'inscrit nécessairement sur le long terme.

Elle est conforme aux dispositions législatives et réglementaires et cohérente avec les politiques et directives de niveau supérieur (ministérielles et interministérielles) ; elle se doit également d'être cohérente avec les politiques de sécurité des organismes partenaires.

Elle se déclinera ensuite :

- au niveau de l'organisme par un approfondissement du contexte (enjeux, menaces, besoins) et une explicitation des dispositions de mise en œuvre, au travers d'un Schéma Directeur de la SSI et/ou d'un plan d'action SSI
- au niveau des unités, par la définition d'une PSSI d'unité tenant compte des particularités propres à chaque unité et, pour ce qui est des unités mixtes, intégrant les orientations des autres tutelles.

(CAPSEC (**C**omment **A**dapter une **P**olitique de **S**écurité pour les **E**ntités du **C**NRS) : méthodologie d'analyse de risques permettant à chaque unité de conduire une analyse de ses risques et de formuler des recommandations adaptées au contexte de l'unité).

Partie I : Contexte et objectifs

1) Le contexte du CNRS

Du fait de ses missions et de son organisation, le CNRS présente de nombreuses spécificités par rapport à d'autres entités (ministères, établissements publics, entreprises).

- **Le CNRS est le principal organisme national de recherche** avec 25 000 personnes directement rémunérées (dont 12 000 chercheurs) et un potentiel d'ensemble d'environ **60 000** personnes en englobant les personnels des unités mixtes.
- **La structure est très éclatée** : les unités propres de recherche du CNRS ainsi que les unités mixtes représentent plus de 1300 laboratoires implantés sur plusieurs centaines de sites.
- **L'organisation administrative s'appuie en région sur 19 délégations régionales.**
- **La structure est extrêmement ouverte**, située le plus souvent dans des campus où il est difficile de délimiter des zones à protéger
- Il s'agit d'une structure généralement **très imbriquée avec d'autres organismes**: le CNRS partage le plus souvent sa tutelle d'unités avec plusieurs organismes (universités, écoles d'ingénieurs, EPST, entreprises…) dont il faut intégrer la politique et les modes de fonctionnement ; par ailleurs le CNRS a rarement la maîtrise des infrastructures.
- **La diversité des activités de recherche** rend difficile des recommandations communes à des populations relevant de contextes professionnels très différents.
- **Les unités elles-mêmes sont très hétérogènes :** et il y a peu de similitude entre un grand laboratoire possédant des moyens financiers et humains importants, une culture et un savoir-faire en systèmes et réseaux et une petite unité de recherche qui a constitué son informatique par touches successives et sans personnel technique associé.
- **Le CNRS présente une forte dimension internationale**, avec plusieurs centaines d'accords de coopération internationale, 70 structures européennes et internationales, une dizaine de bureaux du CNRS implantés à l'étranger, plus de 40 000 missions annuelles à l'étranger, et l'accueil dans les unités d'environ **15 000 étudiants et chercheurs étrangers**, à titre permanent ou à titre de visites ou stages.
- **L'état d'esprit des chercheurs est par nature ouvert** et non naturellement enclin au respect de dispositions de sécurité contraignantes.
- **Le CNRS présente une sensibilité importante au regard de la protection du patrimoine scientifique et technique,** liée aux enjeux et liens de certaines recherches avec la défense ou aux risques de prolifération, ou plus souvent encore du fait de l'intérêt industriel et économique des retombées technologiques. La moitié des laboratoires est repérée comme « sensible » et 150 unités sont classées « Etablissements à Régime Restrictif (ERR)»**.**
- **La typologie des données à protéger est très variée** (données scientifiques, techniques ou de gestion de sensibilité très variable).

- **Les moyens financiers et humains** ne sont pas toujours adaptés à la mise en œuvre nécessaire des recommandations en matière de gestion de la sécurité et d'acquisition d'outils de protection.

En contrepartie le CNRS dispose d'atouts propres liés à la qualité et la compétence des personnels dans le domaine de l'informatique et des réseaux. S'y ajoutent un sens de l'initiative et un esprit d'équipe qui facilitent les relations et le fonctionnement en réseaux.

Le contexte législatif et réglementaire :

La mise en œuvre de systèmes d'information est soumise à des obligations relevant de nombreux textes d'ordre législatif et réglementaire qui confèrent un enjeu juridique important à cette activité.

On peut citer en particulier la loi sur la confiance en l'économie numérique (LCEN), la loi relative à l'informatique et aux libertés (loi CNIL), la loi relative à la fraude informatique (loi Godfrain), les instructions et recommandations interministérielles provenant du Secrétariat Général de la Défense Nationale (SGDN).

S'y ajoutent des dispositions relevant du code de la propriété industrielle, et des dispositions pénales (en particulier articles 226 et 227).

La sécurité des systèmes d'information fait par ailleurs l'objet d'une normalisation (norme ISO 27001).

Le corpus correspondant ainsi que le suivi de la jurisprudence font l'objet de documents de diffusion interne.

2) Le périmètre de la SSI au CNRS

La sécurité des systèmes d'information du CNRS doit nécessairement couvrir l'ensemble des systèmes d'information de l'organisme avec toute la diversité que cela implique dans les usages, les lieux d'utilisation, les méthodes d'accès, les personnes concernées. C'est ainsi que l'existence d'implantations à l'étranger et l'importance des missions extérieures lui confère également une dimension internationale.

Le périmètre de la SSI est donc très large.

Ce périmètre englobe les trois ensembles de systèmes d'information interconnectés par le réseau RENATER :

- le système d'informatique de gestion géré par la DSI et les délégations régionales
- les systèmes d'information des unités (bureautique, applications scientifiques, stockage, traitement et interprétation de données, applications INTERNET (dont sites Web institutionnels), messagerie…)
- quelques centres importants de ressources (calcul, données…).

Il inclut les unités mixtes dépendant du CNRS et d'autres tutelles. L'infrastructure étant en de nombreux endroits partagée avec d'autres organismes (universités, …), du personnel non CNRS est amené à travailler sur les systèmes d'information du CNRS.

Sont également à prendre en compte, dans le périmètre de la SSI, les équipements de l'entité ou ceux gérés par le service informatique d'une tutelle, sur lesquels s'exécutent les fonctions essentielles comme la communication (serveur de messagerie, machines internes cibles de connexion depuis l'extérieur), la gestion financière et comptable (serveur XLAB), la modélisation (serveur de calcul), la publication (serveur web, serveur d'impression), le stockage, le traitement et l'interprétation des données (serveur de fichiers, pilotage/contrôle de manipulations). Par ailleurs, du fait de l'évolution des technologies, certains systèmes (téléphonie, visioconférence, photocopieur, vidéosurveillance), traditionnellement en dehors du champ de l'informatique, font désormais partie du périmètre.

La SSI du CNRS 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.

Les usages liés à la mobilité (ordinateurs portables, connexions sans fil, assistants personnels, téléphones portables…) sont également à prendre en compte du fait que ces usages se pratiquent généralement en milieu non protégé**.**

L'utilisation d'un moyen informatique privé ou extérieur fait entrer l'équipement dans les ressources informatiques de l'unité et comme tel dans le périmètre de la SSI.

Toutefois ne sont pas compris dans ce périmètre les unités ayant des liens forts avec le CNRS (intégrant des équipes CNRS mises à disposition ou bénéficiant de financements…) mais échappant à sa tutelle.

3) Les besoins de sécurité

Il s'agit de protéger l'outil de travail (disponibilité), les données (confidentialité, disponibilité, intégrité), le personnel des unités et l'organisme.

Les critères de sécurité

La sécurité du Système d'Information repose sur trois critères :

- Confidentialité : « La confidentialité est la propriété qu'une information n'est ni disponible ni divulguée aux personnes, entités ou processus non autorisés » norme ISO 7498-2 (ISO90).
- Disponibilité : Propriété d'accessibilité au moment voulu des données et des fonctions par les utilisateurs autorisés.
- Intégrité : « L'intégrité est la prévention d'une modification non autorisée de l'information » norme ISO 7498-2 (ISO90).

Ces critères peuvent être quantifiés selon une échelle de besoins de sécurité (cf. ci-après une évaluation issue des travaux du groupe CAPSEC).

Confidentialité	Disponibilité	Intégrité
Perte de confidentialité sans conséquence	Délai supérieur à une semaine	Perte d'intégrité sans conséquence
Le sinistre ne risque pas de provoquer une gêne notable dans le fonctionnement ou les capacités de l'organisme. Ex : données publiques, visibles par tous.	Des services qui apportent un confort supplémentaire mais pas indispensable.	Le sinistre ne risque pas de provoquer une gêne notable dans le fonctionnement ou les capacités de l'organisme. Ex : aucune vérification.
Perte de confidentialité entraînant des gênes de fonctionnement	Délai > 8 heures et <= 1 semaine	Perte d'intégrité entraînant des gênes de fonctionnement
Susceptible de provoquer une diminution des capacités de l'organisme. Ex : données liées aux compétences ou savoir-faire internes, dans un contexte de groupe de confiance, dont vous protégez toutes les traces écrites.	Ressources pour lesquelles il existe une alternative. Ex : imprimantes.	Susceptible de provoquer une diminution des capacités de l'organisme. Ex : vérification des données, sans validation : des fautes d'orthographe sur une page web nuisent à l'image de marque du laboratoire
Perte de confidentialité entraînant des conséquences dommageables	Délai > 2heures et <= 8 heures	Perte d'intégrité entraînant des conséquences dommageables
Susceptible d'amoindrir les capacités de l'organisme, avec des conséquences telles que des pertes financières, sanctions administratives ou réorganisation Ex : données liées à un engagement de confidentialité dans un contrat.	Sans conséquence vitale humainement Ex : arrêt du réseau, de la messagerie, données vitales non disponibles...	Susceptible d'amoindrir les capacités de l'organisme, avec des conséquences telles que des pertes financières, sanctions administratives ou réorganisation Ex : données qui sont validées et contrôlées par des moyens techniques ou humains.
Perte de confidentialité entraînant des conséquences graves	Délai : entre temps réel et <= 2 heures	Perte d'intégrité entraînant des conséquences graves
Susceptible de provoquer une modification importante dans les structures et la capacité de l'organisme comme la révocation de dirigeants, la restructuration de l'organisme, des pertes financières. Ex : données secret défense.	Ressources qui mettent en péril la vie (humaine ou animale ou biologique). Ex : expériences biologiques ou physiques pilotées automatiquement, système de sécurité.	Susceptible de provoquer une modification importante dans les structures et la capacité de l'organisme comme la révocation de dirigeants, la restructuration de l'organisme, des pertes financières. Ex : données avec au moins deux niveaux de validation et de contrôle différents (techniques ou humains).

Les besoins de sécurité

Protection de l'outil de travail : les postes informatiques, les réseaux, les applications et les données, constituent « le Système d'Information » du CNRS. Cet ensemble est indispensable à la fois pour les activités nécessaires à la recherche, mais aussi pour la gestion des entités. La disponibilité et l'intégrité de cet outil doivent donc impérativement être placées à l'abri de menaces internes ou externes.

Protection des données : dans quelques cas il peut s'agir de « données classifiées de défense », mais le plus souvent il s'agit de « données sensibles » telles que :

- Les données scientifiques : liées à des contrats industriels, à un savoir-faire interne, expérimentales, liées à des coopérations nationales ou internationales, scientifiques, techniques, économiques, liées à la valorisation de la recherche, liées au centre de documentation, téléphoniques et de visioconférences
- Les données de gestion : authentification, gestion comptable et financière, gestion des ressources humaines, documents contractuels
- Les données nominatives : liées à la vie privée des personnes, liées à l'enseignement
- Les données stratégiques : informations d'ordre politique ou stratégique ou touchant des questions de défense, informations sécurité…

La protection des données sensibles suppose l'identification préalable de ces données, la détermination du type de protection nécessaire (confidentialité, disponibilité, intégrité) et l'évaluation de leur degré de sensibilité (quantification des besoins de sécurité).

La sensibilité des données est appréciée lors d'un inventaire au cours duquel des questions touchant à « la vie de la donnée » doivent être posées :

- Quel est son type ?
- Où réside t-elle ?
- Par qui est-elle partagée (« besoin d'en connaître ») ?
- Quelle(s) menace(s) est-elle susceptible de subir ?

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 et industrielle et ceux de la vie privée (fichiers nominatifs, cybersurveillance…). Dans ce cadre, la responsabilité administrative et pénale de la hiérarchie et des administrateurs systèmes et réseaux peut être recherchée.

4) Les menaces et les impacts

Les menaces

La mise à exécution de menaces volontaires ou involontaires, humaines ou matérielles peut porter atteinte au SI, aux personnels et à l'organisme. Il convient de distinguer ce qui relève **d'attaques délibérées (agressions)** et ce qui relève de **sinistres naturels** (incendie, explosion, inondations…).

Dans le cadre d'une étude de risques, il est possible de considérer les menaces comme la méthode EBIOS (*) le préconise, c'est-à-dire inventorier les menaces en considérant la probabilité que la menace devienne réalité ; la menace est prise en compte en fonction des critères suivants :

- Type d'élément menaçant : environnemental ou humain ou naturel
- Cause d'élément menaçant : délibérée ou accidentelle
- Potentiel d'attaque : opportunités ou ressources limitées, accidentel et aléatoire, haut degré d'expertise d'opportunité et de ressources

(*) EBIOS : *« Expression des Besoins et Identification des Objectifs de Sécurité »* : démarche d'analyse de sécurité élaborée par la Direction Centrale de la Sécurité des Systèmes d'Information du SGDN.

Un référentiel des menaces est disponible dans EBIOS. Il a été repris et adapté pour le CNRS dans le cadre des travaux du groupe CAPSEC.

Les Impacts

Les impacts des attaques sur les critères de sécurité peuvent se traduire ainsi :

Critères	Attaques	Impacts
confidentialité	**Divulgation, accès** par des tiers non autorisés et **détournement** à des fins délictueuses, de données confidentielles (touchant des travaux confidentiels, des données scientifiques ou technologiques, des données personnelles telles que médicales ou financières…), que ces données soient stockées ou échangées (messagerie)	Pertes du patrimoine scientifique ; pertes d'avance technologique et technique ; pertes financières ; contentieux juridique
disponibilité	**Vol de matériel**, **émission de malware** (virus, ver, déni de service…) **Sinistres**	Interruption de service ; paralysie ou désorganisation conduisant à l'incapacité opérationnelle de fonctionnement, de décision, de gestion, de sécurisation ; saturation de ressources, de systèmes d'alerte ; perte de données précieuses (scientifiques ou de gestion) par absence ou insuffisance de sauvegarde ; atteinte à la sécurité du personnel, des usagers ; perte d'image de marque
intégrité	**Modification accidentelle ou délibérée** (défiguration de sites Web…)**, piégeage** de systèmes d'information, **émission de malware** (bombes logiques, chevaux de Troie, sniffeurs…), **vol** ou **détournement** de moyens informatiques à des fins délictueuses (compromission de serveurs…)	Résultats de fonction incomplets ou incorrects ; expérimentations non crédibles ; prises de décisions inadaptées ; appropriation frauduleuse de biens ; prise de contrôle d'un système physique ; perte du patrimoine scientifique ; perte d'image de marque ; atteinte à des libertés individuelles (cybersurveillance indue…)

À partir des menaces retenues, il convient d'évaluer les risques pour chacune d'entre elles (probabilité d'occurrence et mesure des conséquences).

Les parades viseront donc à peser sur ces deux facteurs : réduire la probabilité d'occurrence, atténuer l'impact en cas de réalisation effective de la menace.

Inversement des éléments tels que la négligence, l'insuffisance de formation ou d'information, les insuffisances de management de la sécurité, l'absence de consignes claires… sont des facteurs aggravants du risque, en amplifiant la probabilité d'occurrence de la menace ou la conséquence de l'incident survenu. En conséquence il est nécessaire de procéder à une analyse de risques.

Partie II : Principes d'organisation et de mise en œuvre

1) Organisation de la SSI au CNRS

Pilotage

Au sein du CNRS, la responsabilité générale de la sécurité des systèmes d'information relève du directeur général du CNRS en tant qu'Autorité Qualifiée pour la Sécurité des Systèmes d'Information (**AQSSI**) du CNRS. Il est assisté dans cette fonction par le Fonctionnaire de Sécurité de Défense (**FSD**), également Fonctionnaire de Sécurité des Systèmes d'Information (**FSSI**) du CNRS.

Le pilotage stratégique est assuré de manière concertée par un comité de pilotage de la SSI présidé par une personnalité reconnue dans ce domaine et nommée par le directeur général du CNRS. Sont en particulier membres de ce comité, le FSD, le chargé de mission SSI, les directeurs de la DSI et de l'UREC, le secrétaire général du CNRS ou son représentant, un représentant de la DAJ, un représentant du département scientifique compétent, un représentant du HFD du ministère... Ce comité définit les grandes orientations de la SSI, validées par le directeur général du CNRS.

Par délégation du directeur général, le pilotage courant est de la responsabilité du FSD en concertation avec l'UREC au sein de laquelle est identifié un « chargé de mission SSI », fonctionnellement rattaché au FSD au titre de cette mission.

La mise en œuvre opérationnelle est assurée par l'UREC, qui gère la chaîne fonctionnelle et assure la conduite des différents projets et études techniques dans ce domaine. Pour cette dernière mission l'UREC s'appuie sur un réseau d'experts oeuvrant au niveau national ainsi que sur le réseau des coordinateurs régionaux.

La politique de sécurité des systèmes d'information du CNRS s'inscrit dans le cadre de la politique et des directives émanant de la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI), en charge de la sécurité des systèmes d'information au niveau national. Cette politique et ces directives sont relayées, pour ce qui est de la recherche, par le Haut Fonctionnaire de Défense du ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche et par le Fonctionnaire de Sécurité des Systèmes d'Information (FSSI) placé auprès de lui.

Pour la définition et la mise en œuvre de la politique de sécurité des systèmes d'information, une concertation étroite est donc menée avec la DCSSI et le service du HFD, ainsi qu'avec les autres partenaires que sont les universités, les autres organismes de recherche et le réseau RENATER.

Mise en œuvre

Chaîne organique et fonctionnelle au CNRS en matière de SSI

Chaîne organique

L'application des dispositions de protection des systèmes d'information relève de la responsabilité de la **chaîne organique** (direction générale du CNRS, départements scientifiques, délégations régionales, directions d'unités de recherche ou de services) avec l'accompagnement des entités spécialisées (DSI, pour ce qui est des systèmes d'information de gestion du CNRS, UREC pour ce qui est des réseaux et de leurs applications).

Les responsables hiérarchiques d'unités (directeurs d'unités de recherche, délégués régionaux pour ce qui est de leur délégation) sont responsables de la sécurité des systèmes d'information de leur unité.

Pour assurer cette fonction, ils disposent de l'appui de la chaîne fonctionnelle SSI du CNRS (et le cas échéant de celle d'autres tutelles) et des moyens internes spécialisés (qu'ils ont la charge de définir : désignation au sein de leur unité d'un chargé de la SSI – cf ci-après-)

Outre leur responsabilité hiérarchique interne sur les services de leur délégation, les délégués régionaux ont la responsabilité de la coordination des directeurs d'unité en matière de SSI, en particulier en ce qui concerne l'application des réglementations, directives et consignes relevant de la SSI, la bonne adéquation des moyens en liaison avec les autres partenaires institutionnels, l'application des plans de prévention et d'intervention, la gestion des incidents, les relations avec les autres tutelles.

Ils ont, au titre de ce rôle, autorité sur la coordination régionale de la SSI (CRSSI) qui relève de la chaîne fonctionnelle spécialisée de la SSI.

Chaîne fonctionnelle spécialisée de la SSI

Pour conduire la politique de sécurité des systèmes d'information et faciliter sa mise en œuvre, le CNRS, sous l'autorité du directeur général en tant qu'AQSSI, s'appuie sur une chaîne fonctionnelle interne spécialisée en SSI qui s'inscrit elle-même dans la chaîne fonctionnelle nationale animée par la Direction Centrale de la Sécurité des Systèmes d'Information (SGDN/DCSSI).

La chaîne fonctionnelle SSI du CNRS est composée comme suit :

Au niveau national

- des structures de pilotage définies ci-dessus (FSD, UREC et comité de pilotage stratégique de la SSI)
- de Responsables de la Sécurité des Systèmes d'Information (RSSI) de structures nationales, lorsque des moyens ou des thématiques nécessitent une approche coordonnée au niveau national au profit de plusieurs entités, sous la responsabilité de ces structures nationales. C'est en particulier le cas pour la DSI compte tenu de son implication nationale en tant que chargée des

applications de gestion et des systèmes d'information des délégations et en tant que gestionnaire des procédures de déclaration à la CNIL.

- d'experts SSI susceptibles d'être sollicités au niveau national sur des travaux permanents ou ponctuels en appui du travail technique et d'animation nationale de l'UREC.

Au niveau régional

- d'une coordination régionale de la SSI (**CRSSI**) oeuvrant selon les directives techniques (de métier) du FSD et de l'UREC et sous la responsabilité du délégué régional pour ce qui est de la mise en œuvre des actions de coordination régionale relevant des compétences des délégués ; cette CRSSI a en particulier pour missions :
  - le suivi de l'état de sécurité des unités du périmètre de la délégation régionale (documents de PSSI, identification du Chargé de la SSI dans l'unité, bilans de sécurité, appréciation des besoins…),
  - le suivi de la mise en œuvre des dispositions de SSI définies au niveau national, remontées des dysfonctionnements vers l'UREC voire le FSD,
  - les contacts avec les Responsables de la Sécurité des Systèmes d'Information d'autres tutelles,
  - la conduite d'actions de formation et d'information et d'actions de conseil et soutien à destination des Chargés de la SSI dans les unités (animation du réseau),
  - la conduite d'actions d'information et de sensibilisation des unités,
  - le conseil et soutien aux chargés de SSI des unités, en cas d'incident,
  - le relais d'information entre les chargés de SSI des unités, l'UREC et le FSD, au titre de la chaîne fonctionnelle SSI,
  - la participation aux exercices d'alerte et à la gestion de crise,
  - la participation en tant que de besoin et selon le degré d'expertise individuelle à des travaux menés au niveau national (groupes de travail, réunions de coordinations, actions de formation),
  - le suivi d'un tableau de bord régional SSI et la rédaction du bilan annuel régional.

Cette coordination régionale peut être assurée de manière collégiale, par une équipe de quelques personnes missionnées à cet effet, experts en SSI, associant dans la mesure du possible un expert SSI de la délégation et un ou plusieurs experts SSI d'unité de recherche locales.

Les conditions d'exercice (à temps partiel) de ces missions doivent être formalisées (missions affichées au titre de leur poste, conditions de déplacements liées à ces missions SSI….).

L'organisation de cette coordination régionale est arrêtée localement en concertation entre le FSD, l'UREC et le délégué régional.

Au niveau local

- des Chargés de la Sécurité des Systèmes d'Information (CSSI), spécialistes des systèmes d'information, et dont la mission est d'assister les directeurs d'unité dans l'exercice de leur responsabilité en matière de SSI.

Pour chaque unité doit être identifié un CSSI désigné par le directeur de l'unité. Dans le cas de structures légères ou relevant d'autres tutelles ou dans le cas d'unités partageant les mêmes infrastructures, le CSSI peut ne pas appartenir à l'unité, la fonction étant alors mutualisée.

L'identification d'un CSSI dans les unités classées ERR (Etablissements à Régime Restrictif) est prioritaire.

A défaut d'identification d'un CSSI spécifique, en interne ou en externe, le rôle est directement assuré par le directeur de l'unité.

Dans le cas d'unités mixtes, les dispositions contractuelles entre tutelles peuvent prévoir le mode d'exercice des responsabilités de SSI et en particulier la prise en charge par l'une des tutelles de tout ou partie de la responsabilité en matière de SSI. Le CSSI de l'unité relève alors de la chaîne fonctionnelle de cette tutelle, tout en gardant un lien de coordination avec les autres tutelles.

Sous l'autorité du directeur d'unité, le CSSI a en particulier pour missions de :

- promouvoir la mise en place d'une PSSI d'unité,
- veiller à la mise en place des mesures de sécurité nécessaires,
- veiller à l'application des instructions et recommandations,
- veiller à la bonne exploitation des avis des CERT RENATER et CERTA,
- sensibiliser les utilisateurs,
- prendre les bonnes mesures en cas d'incident (ou s'assurer qu'elles sont prises),
- veiller à la prise en compte de la sécurité dans la rédaction des contrats de sous-traitance et les cahiers des charges des applications,
- veiller au respect des formalités requises par la loi Informatique et Libertés pour les traitements de données à caractère personnel,
- assurer la veille en matière de SSI et les niveaux relationnels nécessaires en liaison avec la coordination générale et plus généralement la chaîne fonctionnelle SSI.

Selon l'importance et la structuration de l'unité, le CSSI peut être secondé dans ces fonctions par d'autres personnes de l'unité. La ventilation des tâches doit alors être précisée.

Il est important que les fonctions de CSSI soient officialisées et reconnues tant en interne qu'à l'extérieur de l'unité.

2) Coordination avec les autres tutelles

Principe général

L'application de la politique de sécurité des systèmes d'information doit tenir compte de la situation des unités et de l'éventuel partage de tutelle avec d'autres organismes.

Le directeur de l'unité a la charge d'arrêter la politique de SSI dans son unité. Celle-ci doit être conforme au document de politique générale de la SSI du CNRS, mais les règles d'application peuvent différer en fonction des consignes propres à la tutelle responsable de la SSI.

Le système d'information de l'unité fait partie du SI du CNRS. La PSSI interne adoptée satisfera notamment les points suivants :

- la préservation des accès au système d'information du CNRS (administration, gestion...)
- l'articulation interne au CNRS des responsabilités organiques et fonctionnelles en matière de SSI et en particulier la responsabilité du directeur d'unité.

Dans le cas des unités propres du CNRS, les dispositions organisationnelles telles que décrites supra s'appliquent et relèvent de la seule responsabilité du CNRS.
Lorsque ces unités sont soutenues par d'autres organismes sur le plan informatique, la politique SSI de l'unité demeure de la responsabilité du CNRS tout en tenant compte des contraintes locales de l'organisme hébergeur.

Dans le cas d'unités mixtes, les dispositions contractuelles qui régissent la tutelle de l'unité (contrat quadriennal) incluent celles relatives à la sécurité des systèmes d'information en définissant en particulier les responsabilités respectives. Ce document définit la PSSI de référence pour l'unité mixte. En tant que responsable de la SSI de son laboratoire, le directeur de l'unité :

- s'assure que les documents de PSSI de son unité (charte, gestion des traces…) sont en accord avec ceux de toutes ses tutelles (CNRS, EPST, universités...)
- désigne le CSSI de son unité, celui-ci étant le « correspondant sécurité » pour les autres tutelles. Ce CSSI fait partie des chaînes fonctionnelles de chaque tutelle et assure les liens d'information correspondants. Le CSSI de l'unité doit en particulier disposer de la part de ces tutelles de toutes les informations nécessaires à l'exercice de son activité.

En cas d'incident

Les incidents informatiques doivent remonter par la voie fonctionnelle de la tutelle responsable, en assurant l'information des autres partenaires, avec si nécessaire une concertation sur les suites à donner telles que les dépôts de plainte.

En situation de crise grave survenant dans l'unité, il y a lieu d'informer la cellule de crise régionale et si nécessaire la cellule nationale. Inversement, l'unité mixte sera informée par la chaîne hiérarchique CNRS et par la chaîne fonctionnelle SSI du CNRS en cas d'événements graves justifiant le déclenchement d'alertes nationales. La mise en œuvre des plans de posture (VIGIPIRATE) ou d'intervention (PIRANET) est déclinée au sein de l'unité

par le directeur d'unité, les responsables informatiques et le RSSI d'unité. Cette mise en œuvre est pilotée et suivie par la tutelle SSI de l'unité.

En cas de litige

Les éventuelles divergences sont à traiter au niveau du CSSI de l'unité, de la coordination régionale, voire du délégué régional ; les éventuels arbitrages sont à soumettre à la voie fonctionnelle SSI (UREC et FSD et FSSI du ministère si nécessaire).

Principales tutelles : les universités et EPST

Une grande partie des unités mixtes partage leur tutelle avec des établissements de l'enseignement supérieur.

Une coordination nationale existe entre le service du FSD du CNRS, l'UREC, le service du HFD du ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche, les pilotes des chaînes RSSI des universités (actuellement le CRU) et des chaînes FSD des universités, les RSSI des autres EPST, les CERTs (CERT-RENATER et CERTA).

Au niveau régional la coordination générale relève de la responsabilité du délégué régional ou de la CRSSI, par délégation. Les coordinateurs régionaux doivent pour leur part être en liaison avec les RSSI des universités et des EPST locaux et les FSD locaux.

En l'absence de dispositions contractuelles formelles, les présents principes de coordination doivent guider les relations entre le CNRS et les autres tutelles.

3) Déclinaison d’une PSSI au sein d’une entité du CNRS

Les unités doivent décliner à leur niveau la politique de sécurité des systèmes d’information de leur unité (PSSI d’unité)

Cette PSSI peut toutefois être commune à plusieurs unités relevant d’un cadre commun partageant les mêmes structures.

Inversement, dans le cas de structures importantes, l’élaboration de la PSSI de l’unité peut se faire selon des approches propres à des équipes internes lorsqu’elles disposent de systèmes d’information suffisamment distincts.

Une PSSI permet en effet à une entité (un laboratoire, une équipe de recherche ou un institut du CNRS, une direction, une délégation régionale…) d'avoir une approche méthodique et systématique pour garantir une sécurité homogène de son SI (Système d'Information).

À partir de documents, modèle générique et éléments de référence, l’entité définit sa propre PSSI adaptée à ses besoins.

Cette PSSI doit intégrer les politiques nationales de SSI des tutelles et en particulier celle de la tutelle principale en matière de SSI (si une telle tutelle est définie).

Une PSSI est également un document de dialogue entre les différents acteurs du SI (instances décisionnelles, responsables d’équipes de recherche ou de services, membres de l’entité, CSSI, Administrateurs Systèmes et Réseaux du service informatique s’ils sont distincts du CSSI, intervenants extérieurs, prestataires de services). Il est important que les personnels de l’entité participent au pilotage de la sécurité et donc ne la subissent pas.

À l'issue de ce dialogue, un consensus doit se dégager autour de la PSSI afin de définir une gestion cohérente des risques en fonction des moyens que l’entité peut ou doit investir dans la sécurisation de son SI.

Une fois validée en conseil de laboratoire, la PSSI permet d’une part de sensibiliser les membres du laboratoire à la sécurité du SI et de faire en sorte qu'ils s'approprient les éléments de sécurité, d’autre part de déterminer les solutions concrètes qui vont être mises en place au niveau de l’entité.

La PSSI d’une unité relève de l’initiative du directeur et du CSSI de l’unité.

Afin de faciliter la déclinaison d’une PSSI au sein de ses entités, le CNRS propose une méthodologie d’analyse de risques s’appuyant sur la méthode EBIOS de la DCSSI et développée dans le cadre des travaux du groupe CAPSEC.

4) Principes de mise en œuvre de la PSSI

La politique de sécurité des systèmes d'information du CNRS affiche un ensemble de principes d'ordre organisationnel et technique à caractère prioritaire. L'ensemble constitue un corps de doctrine pour la mise en œuvre de la SSI au sein des unités du CNRS.

Ces principes ont vocation à être explicités, voire complétés, dans le cadre d'instructions ou dispositions techniques dont la responsabilité d'élaboration, de diffusion et d'information relève de la chaîne fonctionnelle SSI.

La mise en œuvre des dispositions au niveau local (dans les entités) intègre le cas échéant les orientations d'autres tutelles, dans le cadre de la PSSI d'entité arrêtée par la direction de l'entité.

1) Organisation - Responsabilités

1.1 Responsabilité des différents acteurs

Les acteurs intervenant en matière de sécurité des systèmes d'information, au titre d'autorité hiérarchique ou au titre de la chaîne fonctionnelle 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. Ils peuvent si nécessaire faire l'objet d'une habilitation au secret de défense.

1.2 Accès aux ressources informatiques

La mise à disposition d'un utilisateur d'outils informatiques (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, CNRS ou non.

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

Le cas échéant l'accès à des systèmes d'information ou des applications spécifiques ou encore l'exercice de fonctions de gestion de ressources informatiques peut être conditionné à une habilitation de défense.

1.3 Charte informatique

Préalablement à son accès aux outils informatiques, l'utilisateur doit prendre connaissance des droits et devoirs que lui confère la mise à disposition par son entité de ces outils.

Cette information se fait au travers d'une charte ou de dispositions équivalentes intégrées dans le règlement intérieur. Le texte correspondant doit être conforme aux prescriptions nationales (du CNRS ou de la tutelle responsable de la SSI).

1.4 Cybersurveillance

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 réglementation en vigueur et respecter 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).

La mise en place de tels dispositifs donne lieu à des principes et règles arrêtés préalablement et diffusés au sein du CNRS (politique de gestion des traces par exemple).

1.5 Formation, sensibilisation

La formation, la sensibilisation et l'information des différents acteurs de l'expert SSI à l'utilisateur en passant par le responsable de l'entité sont cruciales pour la sécurité. Sous la responsabilité de la chaîne fonctionnelle SSI du CNRS, des actions en ce sens sont régulièrement menées au niveau local, régional et national.

Elles font l'objet d'une planification arrêtée au niveau du comité de pilotage de la SSI et donnent lieu à un suivi dans le cadre du tableau de bord de la SSI.

1.6 Infrastructure de Gestion de Clés

Le CNRS a défini et déploie au sein des unités une Infrastructure de Gestion de Clés (IGC). Cette IGC a pour objectif de permettre, par certificats électroniques, l'authentification de personnes ou de services voire le chiffrement des données, pour les échanges et les accès à des applications sécurisées.

Le déploiement de l'IGC est à destination des personnels relevant d'unités du CNRS (qu'ils soient ou non personnels CNRS). Il peut exceptionnellement s'étendre à l'extérieur du CNRS dans le cadre de projets avec des partenaires.

L'octroi de certificats électroniques à des personnels étrangers hors Union Européenne de statut non permanent peut être soumis à autorisation.

1.7 Veille technique et juridique

Une veille technique et juridique est assurée par l'UREC en liaison avec le FSD, la DAJ pour la partie juridique et la DSI pour les applications de gestion.

1.8 Gestion de la documentation SI

La gestion de la documentation SSI est assurée par l'UREC. La documentation comprend l'ensemble des dispositions législatives et réglementaires concernant la SSI, ainsi que l'ensemble des documents d'orientation nationale (PSSI, Schéma directeur SSI) et les instructions et recommandations techniques propres au CNRS.

2) Protection des données

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 des données avec des processus de restauration validés doit être mise en place.

2.2 Protection des données sensibles

Le stockage et la transmission de données « classifiées de défense » sont interdits sauf utilisation de moyens spécifiques agréés au niveau national.

Les données non classifiées mais présentant un caractère sensible doivent identifiées et le cas échéant repérées selon un niveau de sensibilité (en s'appuyant sur la méthodologie CAPSEC par exemple).

Pour l'évaluation de la sensibilité des données, on tiendra compte du fait que l'accumulation de données a priori anodines peut conduire à une information sensible.

Il sera procédé régulièrement à un réexamen de la sensibilité des données.

Les données sensibles devront impérativement faire l'objet d'une protection au niveau du contrôle d'accès, du traitement, du stockage ou de 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. Une donnée sensible ne doit pas faire l'objet d'un partage non contrôlé.
- Toute information sensible circulant sur un réseau externe doit être chiffrée.
- Tout support contenant des données sensibles transporté à l'extérieur (disquette, clé USB, cdrom, bande magnétique, etc., cela inclut aussi les ordinateurs portables) doit faire l'objet de mesure de protection contre le vol ou les informations contenues doivent être chiffrées.
- Les informations sensibles ne doivent pas 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 on devra impérativement mettre en œuvre des moyens de chiffrement, selon les dispositions définies au niveau national (cf ci-après).

2.3 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 des formalités requises de déclaration ou de demande d'autorisation auprès de la CNIL, sous la responsabilité du service gestionnaire de cette procédure au CNRS.

Les CSSI des entités, sous l'autorité de leur directeur d'entité, contribuent à l'information et la sensibilisation des responsables de traitement. Ils incitent à la correction d'éventuelles anomalies et en cas de difficulté font part des éventuels incidents à leur hiérarchie et à la chaîne fonctionnelle SSI.

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

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 particulièrement sensibles.

Les produits utilisés doivent faire l'objet d'un agrément au niveau national.

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

Le respect de ces dispositions et la mise en œuvre effective du chiffrement sont réalisés au vu de recommandations internes et avec l'appui et le conseil de la part de la voie fonctionnelle SSI du CNRS.

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.

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

3) Sécurisation du Système d'information

3.1 Administration des serveurs

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

L'administration des postes serveurs par les utilisateurs eux-mêmes doit demeurer l'exception et être justifiée en termes de besoins et de compétences.

3.2 Administration des postes de travail

L'administration des postes de travail individuels est normalement placée sous la responsabilité des administrateurs systèmes et réseaux de l'entité. L'administration des postes peut être assurée par les utilisateurs eux-mêmes sous réserve de s'inscrire dans la politique de sécurité de l'unité.

3.3 Sécurisation des postes de travail et des moyens nomades

Les utilisateurs veillent à la sécurisation de leur poste de travail, des moyens nomades mis à leur disposition ou de leur portable personnel. Une vérification du niveau de sécurité doit normalement être mise en place avant l'accès au réseau.

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

L'exploitation des moyens informatiques hors de leur zone de sécurité (micro-ordinateurs, portables, 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 l'entité de tout équipement informatique doivent avoir été autorisées.

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

3.4 Contrôle d'accès

L'accès au système d'information exige une identification et une authentification préalable. L'utilisation de comptes partagés ou anonymes doit être évitée. Des mécanismes permettant de limiter les services, les données, les privilèges auxquels à accès l'utilisateur en fonction de son rôle dans l'organisation doivent être mis en œuvre dans la mesure du possible.

Les accès doivent être journalisés.

L'attribution et la modification des accès et privilèges d'un service doivent être validées par le propriétaire du service. Pour les services sensibles, un inventaire régulièrement mis à jour en sera dressé. Il importe de bien différencier les différents rôles et de n'attribuer que les privilèges nécessaires.

3.5 Sécurité des applications

La sécurité doit être prise en compte à toutes les étapes d'un projet, interne ou externe, lié au système d'information de l'entité. Pour cela, un dossier de sécurité doit accompagner chaque projet et préciser les enjeux, les méthodes, les mesures préconisées, les jalonnements et les tableaux de bord éventuels

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

Les grands projets d'application de gestion doivent comporter une étude de sécurité approuvée par le RSSI de la DSI, le FSD, voire le directeur général (en tant qu'AQSSI) selon l'importance de l'application. L'analyse de sécurité correspondante peut s'inspirer utilement de la méthode EBIOS.

Les analyses de sécurité doivent intégrer les situations d'hébergement sur sites extérieurs.

3.6 Maintenance et téléaction internes

Lorsqu'elles utilisent un logiciel leur permettant d'intervenir à distance sur l'ordinateur d'un utilisateur, les personnes chargées de l'administration ou du support doivent l'en avertir et respecter les principes de la loi Informatique et Libertés.

La garantie d'une relation de confiance mutuelle repose sur le fait que l'utilisateur puisse conserver la maîtrise de son environnement.

3.7 Infogérance et télémaintenance externes

L'infogérance correspond au fait que des sociétés extérieures, chargées de gérer une partie de l'informatique du laboratoire, ont accès au SI depuis l'extérieur ou l'intérieur.

Il est alors important de mesurer les risques afin de définir précisément les droits d'accès appropriés pour ces sociétés. Les prestataires de service doivent respecter les conditions de sécurité (répondre aux mêmes normes) exposées ci-dessus pour la maintenance, auxquelles un contrôle renforcé sur les ressources mises à disposition doit être ajouté. Un contrat doit clairement préciser les responsabilités et l'imputabilité en cas d'incident.

L'externalisation de la gestion d'exploitation d'un composant critique pour le SI de l'entité est à proscrire, sauf dispositions de garantie spécifiques et validées au niveau national (UREC ou RSSI de la DSI).

Une entité utilisant la télémaintenance devra renforcer la surveillance de ces accès qui nécessitent souvent des privilèges élevés. Les contrats avec les sociétés de services devront contenir, le cas échéant, des engagements de responsabilité.

3.8 Clauses dans les marchés

Les marchés publics 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 la chaîne fonctionnelle SSI.

L'accès au système d'information de l'unité 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.

3.9 Réseau

Le SI doit être protégé vis-à-vis de l'extérieur à l'aide de filtres d'accès appliqués sur les équipements en tête de son réseau.

Une attention particulière doit être portée aux équipements nomades et PDA pour éviter, notamment, de servir de passerelle vis-à-vis de l'extérieur, de contaminer l'intérieur par des logiciels malveillants. D'une manière générale, leur connexion au SI ne doit pas modifier ou remettre en cause la sécurité du système d'information et doit être approuvée par le CSSI.

L'utilisation de réseaux de télécommunication externes au laboratoire met en relation des utilisateurs qui n'ont, a priori, pas les mêmes exigences de sécurité. Il est donc nécessaire de définir des modalités d'utilisation sécurisée pour les accès depuis l'extérieur comme les liaisons via ADSL. Il convient de définir les différents canaux de communication utilisés et formaliser pour chacun d'entre eux les règles d'utilisation par des contrats, des engagements de la part des utilisateurs, des tiers ou des équipes délocalisées (exemple : serveur de messagerie, sauvegardes opérées par un service externe au laboratoire).

Dans toute la mesure du possible le réseau interne doit être cloisonné afin d'isoler les différents services et usages et limiter l'impact d'incidents. En particulier il est vivement souhaitable d'isoler dans une zone semi-ouverte les services visibles de l'extérieur. De même l'accès au réseau sans fil doit être contrôlé et le réseau doit faire l'objet d'un chiffrement adapté.

Toute connexion d'un matériel au réseau doit être approuvé par le CSSI. Toute liaison vers l'extérieur autre qu'à travers le réseau de l'entité (modem, ADSL, GPRS, 3G par exemple) est interdite sauf besoins particuliers et après accord du CSSI.

3.10 Maintien du niveau de sécurité

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

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 SI de manière à s'assurer de son état de sécurité : analyse des journaux, vérification des vulnérabilités, suivi des avis de sécurité.

4) Mesure du niveau effectif de sécurité

4.1 Contrôle de gestion

La sécurité des systèmes d'information du CNRS fait l'objet de documents de cadrage, d'organisation et de planification.

Le contrôle de gestion de la SSI s'opère sous la responsabilité du FSD. Il donne lieu à un tableau de bord de la SSI.

4.2 Audits

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 externes, à des missions d'inspection (au sens de visite et échanges approfondis) réalisées par le fonctionnaire de sécurité de défense et à des auto-diagnostics selon la méthodologie définie par le CNRS et mise en œuvre depuis plusieurs années.

4.3 Journalisation, tableaux de bord

Le SI doit comprendre des dispositifs ou procédures de journalisation centralisée et protégée de l'utilisation des services. L'objectif est de permettre de détecter des intrusions ou des utilisations frauduleuses, de tenter d'identifier les causes et les origines, d'éviter des contaminations d'autres sites par rebond et de remettre en place le système.

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

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

4.5 Posture de sécurité

En matière de sécurité des systèmes d'information, le niveau normal des recommandations faites dans le cadre de la politique interne de SSI correspond aux dispositions jaunes et oranges du plan **Vigipirate.**

Ces recommandations sont rappelées régulièrement par le FSD via les délégations régionales du CNRS.

Les dispositions internes de sécurisation doivent permettre une réactivité suffisante en cas de passage au niveau rouge de mesures propres à la SSI.

Le plan d'intervention gouvernemental PIRANET fait l'objet annuellement d'exercices destinés à tester la réactivité de la chaîne d'intervention et la faisabilité des mesures préconisées.

4.6 Mises en garde

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

4.7 Gestion d'incidents

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

Une procédure de gestion des incidents est diffusée et mise en ligne permettant aux administrateurs systèmes et réseaux, responsables SSI et directeurs d'unité de réagir à bon escient et de transmettre l'information.

Le signalement des incidents à la chaîne fonctionnelle est systématique.

L'information des autorités hiérarchiques et de la délégation régionale est impérative lorsque l'incident peut mettre en cause l'entité dans son fonctionnement, sa sécurité, sa discipline interne, son image de marque…

L'opportunité d'une information directe du FSD doit être appréciée au regard de la gravité de l'incident et/ou du caractère sensible de l'entité concernée. Cette information doit être systématique si l'incident est susceptible d'implications juridiques (dépôt de plainte par exemple).

Dans le cas d'unités mixtes, il convient d'informer et le cas échéant de se concerter avec les autres tutelles.

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

Les vols d'ordinateurs ou de supports de données doivent être considérés comme des incidents de SSI et traités selon le même principe

4.8 Gestion de crise

Le plan de gestion de crise du CNRS intègre les risques liés à l'informatique ainsi que les risques susceptibles d'une incidence sur la sécurité des systèmes d'information. Pour ces incidents, le FSD est membre de la cellule de gestion de crise du CNRS.

Le FSD prévoit le dispositif organisationnel propre aux crises de nature informatique.

Il doit être informé dès le déclenchement de toute crise ayant une incidence sur la sécurité des systèmes d'information. Il veille à la bonne information des autres structures concernées dont la cellule nationale de gestion de crise du CNRS.

4.9 Plan de continuité

L'entité doit définir un plan de continuité et les procédures correspondantes. Ce plan doit permettre, dans un premier temps, de maintenir en mode dégradé les activités critiques, puis de récupérer et de restaurer toutes les fonctionnalités du système d'information.
