Politique de Sécurité des Systèmes d'Information (PSSI)

Document d'orientation de la sécurité des systèmes d'information de l'École normale supérieure

Version	Rédacteur	Autorité d'approbation	Date d'approbation
V1.00	Groupe de travail PSSI	Conseil d'administration	14/04/2010

1 Introduction

1.1 Le contexte de l'École normale supérieure

L'École normale supérieure est un établissement d'enseignement et de recherche fondé en 1794. Elle comporte quatorze départements d'enseignement et de recherche qui couvrent l'essentiel des disciplines littéraires et scientifiques. Ainsi, la section Lettres regroupe les départements de géographie, d'histoire, d'histoire et de théorie des arts, de littératures et langages, de philosophie, de sciences de l'Antiquité et de sciences sociales ainsi que le centre d'enseignement et de recherche sur l'environnement et la société (CERES), le collectif histoire et philosophie des sciences, l'espace des cultures et langues d'ailleurs. Quant à la section Sciences, elle est structurée en départements de biologie, chimie, informatique, mathématiques, physique, sciences cognitives et terre-atmosphère-océans. Chaque département regroupe des unités de recherche généralement dirigées en co-tutelle avec d'autres organismes (établissements publics scientifiques et techniques, universités et établissements d'enseignement supérieur et de recherche, etc.). En outre, de nombreux laboratoires sont impliqués dans des collaborations en France ou à l'étranger. Les activités d'enseignement font aussi largement appel à des partenaires de différents établissements avec lesquels il existe des liens forts.

L'École normale supérieure accueille environ 2500 élèves et étudiants dont certains sont recrutés par concours ayant des épreuves communes avec d'autres écoles. Ils peuvent bénéficier d'une chambre qui est à leur disposition durant les périodes scolaires au sein de l'École normale supérieure.

Enfin, l'établissement héberge en son sein plusieurs bibliothèques, en particulier celle de Lettres, extrêmement riches en ouvrages et qui accueillent de nombreux lecteurs externes.

Le fonctionnement de l'établissement est assuré par un ensemble de services prenant en charge l'administration, la logistique, la scolarité, la gestion du patrimoine, la restauration, l'hébergement, l'entretien des locaux, les ressources informatiques, la médecine préventive... Dans ce cadre, certains personnels bénéficient d'un logement.

L'École normale supérieure, regroupant au total 5000 personnes environ, occupe des locaux situés dans quatre espaces géographiques distincts. Un premier site comporte plusieurs bâtiments dans le cinquième arrondissement de Paris (29, 44, 45, 46 et 48 rue d'Ulm, 24 rue Lhomond). Les autres sites sont situés 48 boulevard Jourdan (75014 Paris), 1 rue Maurice Arnoux (92120 Montrouge) et à Foljuif (77140 Saint-Pierre-lès-Nemours). Enfin, l'École normale supérieure est tutelle principale ou secondaire d'unités de recherche hébergées dans d'autres établissements comme, par exemple, le Collège de France.

1.2 La sécurité des systèmes d'information

L'usage des systèmes d'information est soumis à de nombreux textes législatifs et réglementaires : la loi relative à l'informatique et aux libertés (loi « Informatique et Libertés »), la loi relative à la fraude informatique (loi Godfrain), la loi pour la confiance dans l'économie numérique (LCEN), 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 intellectuelle et des dispositions pénales. La délinquance informatique a connu une progression fulgurante au cours de ces dernières années. Tout cela conduit à la mise en place de mesures permettant de restreindre les risques encourus.

Le présent document a pour ambition d'établir une référence pour la mise en œuvre de la politique de la sécurité des systèmes d'information (PSSI) au sein de l'établissement en prenant en compte ses différentes spécificités ainsi qu'en considérant les relations privilégiées avec les partenaires déjà cités.

Cette PSSI fera l'objet de mises à jour en fonction de l'évolution interne ou externe des systèmes d'information et de l'usage qui en est fait.

Chacune des composantes de l'École normale supérieure devra la mettre en application en l'adaptant à son propre contexte pour constituer une PSSI opérationnelle.

Dans le cas d'entités gérées en co-tutelle ou ayant une convention d'hébergement, le contrat d'association définit les responsabilités en termes de sécurité des systèmes d'information. La PSSI de l'entité doit alors respecter toutes les règles de la PSSI de l'École normale supérieure.

Ce document s'appuie sur la norme ISO 27001 et suivantes, portant sur la sécurité des systèmes d'information. Le terme « entité » désignera une composante de l'École normale supérieure, qu'il s'agisse d'une structure administrative, d'enseignement ou de recherche.

1.3 Le besoin en sécurité

Les actifs décrits dans le paragraphe 3 constituent le « système d'information » de l'École normale supérieure. Il est indispensable à la fois pour les activités nécessaires à l'enseignement, à la recherche et à la gestion. Ce système d'information comporte de nombreuses vulnérabilités d'origines diverses : structures organisationnelles insuffisamment robustes, routines de gestion ou procédures défaillantes, pannes d'équipements, environnement physique mal contrôlé, multiplicité des intervenants, dépendance à des tiers défaillants, assemblage de composants dont la compatibilité n'est pas garantie, défaillance humaine, etc. Ces vulnérabilités, si elles sont « exploitées », peuvent avoir des conséquences dommageables pour l'École normale supérieure en termes de temps de travail, de perte d'information, de coût financier, d'image de marque, de réputation...

Le « système d'information » doit donc impérativement être placé à l'abri de menaces internes ou externes. Les données doivent être protégées afin de garantir qu'elles ne soient ni accessibles à des tiers, ni altérées. Les services et applications fournis doivent être disponibles, fiables et garantir des résultats corrects. De plus, 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 (droits d'auteurs, brevets...) et ceux de la vie privée (fichiers nominatifs, cybersurveillance…). Dans ce cadre peuvent être recherchées les responsabilités administratives ou pénales des différents acteurs : l'utilisateur, les administrateurs systèmes et réseaux et leurs hiérarchies.

La protection du système d'information suppose au préalable d'identifier les actifs en réalisant un inventaire qui intègre notamment les biens matériels (équipements, infrastructure...) et les biens immatériels (données, services...). A chacun de ceux-ci doivent être associés un « propriétaire » et une estimation de sa valeur. Outre l'aspect financier, cette valeur inclut l'intérêt stratégique de l'actif pour l'entité et ses tutelles ou pour l'École normale supérieure. Celui-ci se définit en termes de besoin en disponibilité, en intégrité, en confidentialité auquel s'ajoutent éventuellement les contraintes juridiques. Il convient ensuite de déterminer les menaces potentielles associées à chacun de ces biens et leur probabilité d'occurrence dans le contexte particulier de leur exploitation. On doit distinguer ce qui relève d'une volonté délibérée ou d'une situation accidentelle. Ces éléments sont la base de l'analyse de risque qui conduit au choix stratégique des mesures à appliquer. Celles-ci peuvent consister à réduire le risque, à le transférer à des tiers ou à l'accepter avec ses conséquences.

2 L'organisation de la sécurité des systèmes d'information

2.1 L'organisation générale

La politique de sécurité des systèmes d'information de l'École normale supérieure s'inscrit dans le cadre de la politique et des directives émanant de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), en charge de la sécurité des systèmes d'information au niveau national. Cette politique et ces directives sont relayées, pour ce qui concerne la recherche et l'enseignement, 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.

Au sein de l'École normale supérieure, la responsabilité générale de la sécurité des systèmes d'information relève de son directeur en tant qu'autorité qualifiée pour la sécurité des systèmes d'information (AQSSI) de l'établissement. Il est assisté dans cette fonction par les responsables de la sécurité des systèmes d'information (RSSI titulaire et suppléant). Les orientations stratégiques de la SSI sont définies par un comité de pilotage.

La politique de sécurité des systèmes d'information est relayée par le responsable de chacune des entités de l'École normale supérieure qui doit en assurer la mise en œuvre en l'adaptant au contexte local.

2.2 Le comité de pilotage

La définition des orientations techniques de la politique de sécurité des systèmes d'information de l'établissement est assurée par un comité de pilotage qui a en charge de la transcrire dans un document PSSI.

Il est présidé par le directeur de l'École normale supérieure. Il est constitué des membres suivants :

- le directeur de l'École normale supérieure ou son représentant
- le secrétaire général de l'École normale supérieure ou son représentant
- le directeur des études littéraires ou scientifiques ou son représentant
- les responsables de la sécurité des systèmes d'information titulaire et suppléant de l'École normale supérieure
- le directeur du centre de ressources informatiques
- le correspondant « informatique et libertés » de l'École normale supérieure
- un représentant des départements littéraires
- un représentant des départements scientifiques
- un représentant des élèves et étudiants nommé par les élus de cette catégorie au Conseil d'administration
- un représentant des personnels enseignants-chercheurs nommé par les élus de cette catégorie au Conseil d'administration et au Comité technique paritaire de l'établissement
- un représentant des personnels BIATOS/ITA nommé par les élus de cette catégorie au Conseil d'administration et au Comité technique paritaire de l'établissement

Le comité de pilotage peut, à sa discrétion, inviter des personnalités extérieures pour l'assister dans ses tâches. Par délégation du directeur de l'École normale supérieure, le pilotage courant relève de la responsabilité des RSSI en concertation avec le secrétaire général.

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

2.3 La mise en œuvre de la sécurité des systèmes d'information

La mise en œuvre de la PSSI consiste notamment en l'application des dispositions de protection des systèmes d'information. Elle relève de la responsabilité de la chaîne organique (direction de l'École normale supérieure, directions des départements et instituts, directions des unités de recherche, directions des services) avec l'accompagnement des pôles spécialisés (centre de ressources informatiques (CRI), services informatiques des départements ou des laboratoires, autres services informatiques). Les responsables hiérarchiques d'entités (directeurs des départements, directeurs des laboratoires de recherche, directeurs des études, responsables des services administratifs) sont responsables de la sécurité des systèmes d'information au sein de leur entité. Pour assurer cette fonction, ils disposent de l'appui de la chaîne fonctionnelle SSI de l'Éducation nationale (et le cas échéant de celle des autres tutelles) et des moyens internes spécialisés. Ils ont la charge de désigner au sein de leur entité un correspondant de la sécurité des systèmes d'information (CSSI).

2.4 Chaîne fonctionnelle spécialisée de la sécurité des systèmes d'information

Pour conduire la politique de sécurité des systèmes d'information et faciliter sa mise en œuvre, l'École normale supérieure, sous l'autorité du directeur 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 l'Agence nationale de la sécurité des systèmes d'information (SGDN/ANSSI).

La chaîne fonctionnelle SSI de l'École normale supérieure est composée comme suit :

- du secrétaire général, correspondant local du Haut fonctionnaire de défense (HFDS). Il est chargé de :
  - la protection du patrimoine scientifique et technique
  - la préparation des mesures de défense, de vigilance et de prévention de crise
  - la gestion des situations d'urgence (plan Vigipirate, pandémies,...)
  - l'exécution des plans de défense et de sécurité
- de deux responsables de la sécurité des systèmes d'information (RSSI), nommés par le directeur de l'École normale supérieure. Correspondants auprès des structures nationales de la SSI, ils contribuent activement à l'élaboration d'une politique de sécurité cohérente et à sa mise en œuvre. Ils en assurent au sein de l'établissement le suivi de l'état. Ils ont pour mission :
  - le suivi de la mise en œuvre des dispositions de SSI définies au niveau national
  - le relais des informations relatives à la sécurité en provenance des « Computer Emergency Response Team » (CERT) notamment le CERT-Renater, le CERTA, et de l'unité réseaux du CNRS (UREC)
  - la validation des projets d'établissements en ce qui concerne les aspects SSI
  - les remontées des dysfonctionnements vers les CERT et notamment le CERT-Renater
  - 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 coordination, actions de formation)

- les contacts avec les responsables de la sécurité des systèmes d'information des autres tutelles
- le rappel des règles à respecter concernant les chartes en vigueur : charte déontologique RENATER, charte d'utilisation des moyens informatiques et du réseau d'établissement
- la rédaction des documents de la SSI, notamment la PSSI d'établissement et la charte de bon usage des systèmes d'information au sein de l'établissement
- l'analyse des bilans de sécurité et l'appréciation des besoins
- la mise en place d'opérations de prévention
- l'identification des CSSI dans les entités
- la conduite d'actions de formation et de conseil à destination des CSSI dans les entités (animation du réseau)
- le relais d'informations entre les instances nationales et les CSSI des entités, au titre de la chaîne fonctionnelle SSI
- la conduite d'actions d'information et de sensibilisation des entités
- le conseil et soutien aux correspondants de SSI des entités, en cas d'incident

Pour mener ces missions, les deux RSSI travaillent conjointement et disposent des mêmes prérogatives. L'un est désigné comme titulaire, l'autre comme suppléant. En cas de désaccord, la voix du titulaire est prépondérante sur celle du suppléant. En cas de besoin, ils peuvent faire appel à une équipe de quelques personnes spécialisées dans le domaine, par exemple des experts SSI d'entités locales.

- des correspondants de la sécurité des systèmes d'information (CSSI), spécialistes des systèmes d'information, dont la mission est d'assister les directeurs d'entité dans l'exercice de leur responsabilité en matière de SSI. Chaque directeur d'entité doit désigner un CSSI. Dans le cas de structures de taille importante, il est souhaitable que soient désignés deux CSSI (un titulaire et un suppléant). Dans le cas de petites entités partageant les mêmes infrastructures, la fonction de CSSI peut être mutualisée. A défaut de désignation d'un CSSI spécifique, le rôle est directement assuré par le directeur de l'entité. La désignation d'un CSSI dans les entités classées (par exemple : établissements à régime restrictif (ERR) au CNRS) est prioritaire. Le CSSI agit sous l'autorité du directeur d'entité dans le périmètre qui lui est assigné. Il a en particulier pour missions :
  - de promouvoir la mise en place d'une PSSI d'entité conforme à la PSSI d'établissement
  - de veiller à la mise en place des mesures de sécurité nécessaires
  - de veiller à l'application des instructions et recommandations
  - de veiller à la bonne exploitation des avis des CERT-Renater et CERTA
  - de sensibiliser les utilisateurs
  - de mettre en place des opérations de prévention
  - de prendre les mesures appropriées en cas d'incident (ou s'assurer qu'elles soient prises)
  - d'appliquer les mesures demandées par la chaîne fonctionnelle SSI et notamment les RSSI de l'École normale supérieure
  - d'établir les rapports d'incidents demandés par la chaîne fonctionnelle SSI
  - de veiller à la prise en compte de la sécurité dans la rédaction des contrats de sous-traitance et les cahiers des charges des applications
  -

- de veiller au respect des formalités requises par la loi « Informatique et Libertés » pour les traitements informatiques de données à caractère personnel
- d'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.

La fonction de CSSI doit être officialisée et reconnue tant en interne qu'à l'extérieur de l'entité.

- du correspondant « informatique et libertés » (CIL) désigné par le directeur de l'École normale supérieure qui veille à la bonne application de la loi « Informatique et Libertés » dans l'établissement. Il doit établir et maintenir un registre des traitements mis en œuvre.

2.5 Clauses relatives aux acteurs de la SSI

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 par leur devoir de réserve, voire par des obligations de secret professionnel. Ils peuvent, si nécessaire, faire l'objet d'une habilitation au secret défense.
Ils doivent préserver la confidentialité sur les aspects personnels et nominatifs et ne doivent pas communiquer sur les incidents en-dehors du cadre de la PSSI.

2.6 Documents associés à la SSI

Les orientations stratégiques de la sécurité des systèmes d'information de l'École normale supérieure sont décrites dans ce document appelé « Politique de sécurité des systèmes d'information ». Il définit le contexte de l'établissement en termes de SSI, l'organisation de la SSI et les besoins en sécurité. Rédigé par le comité de pilotage de la SSI, il est soumis à l'approbation du Conseil d'administration de l'École normale supérieure. Il en est de même pour les procédures de mises à jour.

Il est complété par :

- un document précisant les objectifs de sécurité et les mesures devant être mises en place pour les atteindre, les procédures de gestion d'incidents et les plans de gestion de crise. Rédigé par le comité de pilotage, il devra mentionner les références aux paragraphes de l'annexe A de la norme ISO 27001. Il est soumis à l'approbation du directeur de l'École normale supérieure et fait l'objet d'une révision annuelle.
- une charte de bon usage des SI au sein de l'établissement. Rédigée par le comité de pilotage, elle est soumise à l'approbation du directeur de l'École normale supérieure et fait l'objet d'une révision annuelle.
- des documents précisant les aspects réglementaires et techniques.

Les entités doivent définir leur propre document de PSSI par référence à la PSSI d'établissement. Cette PSSI doit être approuvée par le directeur de l'entité, validée par les RSSI et diffusée aux personnels de l'entité et aux tiers concernés.

2.7 Suivi et bilan de la SSI

Des réunions permettant d'assurer une communauté d'actions entre les différents acteurs de la SSI au sein de l'École normale supérieure doivent être organisées régulièrement. Au cours de ces réunions, il est établi un bilan des incidents relevés ainsi que des procédures mises en œuvre. Si nécessaire, il est soumis au comité de pilotage des amendements à la politique de sécurité des

systèmes d'information.

Chaque année, les RSSI établissent un rapport décrivant l'état de la sécurité des systèmes d'information au sein de l'École normale supérieure.

3 Périmètre de la SSI au sein de l'École normale supérieure

Le besoin en sécurité des systèmes d'information (SSI) de l'École normale supérieure couvre l'ensemble des systèmes d'information localisés sur les sites de l'établissement. Cela implique une forte diversité à la fois dans les lieux d'utilisation, les personnes concernées et les usages rencontrés. Le niveau de sécurité à appliquer doit être considéré en fonction du type de fonctionnalités, du type de données concernées (vitales pour le fonctionnement de l'établissement, à caractère nominatif, de l'espace privé...) et des interactions existant entre les systèmes ou les réseaux.

En termes d'actifs, le périmètre de la SSI inclut notamment :

- les actifs matériels :
  - les serveurs hébergeant les systèmes d'information dédiés à l'administration centrale de l'établissement (comptabilité, ressources humaines, scolarité, restauration...) gérés par le centre de ressources informatiques (CRI)
  - les serveurs hébergeant les systèmes d'information dédiés à l'enseignement, à la recherche ou à l'administration des départements, instituts, laboratoires ou services (serveurs de calcul, équipements scientifiques dédiés au pilotage d'expériences, banques de données, stockage...)
  - les serveurs hébergeant les systèmes d'information dédiés à la communication (messageries, web, échanges de données...)
  - les équipements dédiés à la gestion de service (téléphonie, contrôle d'accès...)
  - les systèmes d'information des services et des entités à usage personnel (ordinateur fixe ou portable, assistant personnel, logiciels bureautiques, de traitements de données, de modélisation...)
  - les postes de travail mis à la disposition des élèves, étudiants et visiteurs (postes de consultation des bibliothèques)
  - les systèmes de support de l'information (disques, CD, DVD, clé USB) et d'impression (imprimantes, photocopieurs...)
  - les réseaux de communication internes à l'établissement, filaires ou non, à vocation d'échange de données informatiques mais aussi de téléphonie, de vidéoconférence, de télésurveillance
  - les prestations externes dans leur incidence sur la sécurité interne des systèmes d'information (télémaintenance d'équipements, personnels sous-traitants...)
  - l'usage d'un moyen informatique privé ou extérieur connecté au réseau de l'établissement

  Remarques :

  - ✓ L'usage des systèmes d'information au sein des chambres (hébergement des élèves) ou des appartements (hébergement des personnels) est hors du périmètre de cette PSSI, sauf en ce qui concerne les échanges d'information réalisés à travers les réseaux filaires ou non de l'École normale supérieure et de ses prestataires de services. Rappelons que le fournisseur d'accès internet actuel

(RAP/RENATER) restreint par contrat l'utilisation de son réseau à un usage à vocation d'enseignement et de recherche.

- ✓ Les équipements portables appartenant à l'établissement restent partie intégrante de la PSSI même lorsqu'ils sont utilisés en dehors des sites.

- les actifs immatériels :
  - les données liées à l'activité de recherche réalisée au sein de l'établissement y compris au titre de collaborations ou de contrats. Cela inclut les données destinées à la publication ou à la vulgarisation (livres, photographies, films...)
  - les données liées à l'activité d'enseignement (supports de cours, cours en ligne...)
  - les prestations scientifiques ou littéraires (service de bases de données, services web...) proposées à des communautés d'usagers internes ou externes à l'établissement
  - les données administratives liées à la gestion (ressources humaines, données comptables, données patrimoniales,...), à la recherche (contrats de recherche...) et à l'enseignement (concours d'entrée à l'École normale supérieure, gestion pédagogique des élèves...)
  - les données médicales liées aux personnes
  - les données associées à la gestion des services d'hébergement et de restauration
  - les données associées aux services gérant les échanges d'informations (affranchissement, téléphonie, informatique, réseau...)
  - les données associées à la gestion de la sécurité des personnes et des biens (contrôle d'accès, hygiène et sécurité...)
  - les données et prestations dédiées à la communication de l'École normale supérieure
  - et d'une manière plus générale toutes les données et prestations associées à l'établissement

  Remarque : les données propres à l'établissement se trouvant hors de l'établissement restent partie intégrante de la PSSI.

- les ressources humaines et morales :
  - les administrateurs des systèmes et réseaux (ASR) qui ont pour charge à titre principal ou non la maintenance des actifs informatiques
  - les personnes impliquées dans le développement des systèmes d'information
  - les utilisateurs des systèmes d'information, personnels statutaires, contractuels, élèves ou étudiants de l'École normale supérieure
  - les tiers définis comme étant toute personne morale ou physique (entreprises, associations...) qui n'est pas placée sous l'autorité du directeur de l'École normale supérieure.

    Cela inclut notamment :

    - les partenaires institutionnels (CNRS, EHESS, INRA, INRIA, INSERM, universités et établissements d'enseignement supérieur et de recherche...) et les personnels rattachés à ces institutions quel que soit leur statut (personnels statutaires ou contractuels, étudiants...)
    - les fondations et les personnes agissant en leur nom
    - les associations à but non lucratif et les personnes agissant en leur nom
    - les partenaires industriels avec lesquels il est établi des conventions de recherche et

les personnes mandatées par ceux-ci dans le cadre du contrat

- les entreprises fournisseurs d'équipements ou prestataires de services, y compris leurs sous-traitants et les personnels mandatés par ceux-ci dans ce cadre
- les personnes externes utilisant à titre gracieux ou payant les systèmes d'information de l'École normale supérieure

4 Objectifs de sécurité et mesures

La politique de sécurité des systèmes d'information de l'École normale supérieure définit un ensemble de principes organisationnels et techniques à caractère prioritaire. Ils 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. Ils constituent les fondamentaux de la mise en œuvre de la SSI dans les entités qui doivent prendre les dispositions nécessaires à leur application au sein de leur périmètre. Ces principes doivent être complétés et adaptés aux besoins spécifiques de ces entités. Pour les structures multi-tutelles, ils doivent de plus intégrer le cas échéant les orientations de ces autres tutelles, dans le cadre de la PSSI que ces dernières ont définie.

Les objectifs de sécurité et les mesures préconisées sont développés dans un document complémentaire.

5 Mise en œuvre de la PSSI

5.1 Applicabilité de la PSSI

Après validation des documents, la politique de sécurité des systèmes d'information est applicable. Le comité de pilotage s'assure de sa mise en œuvre.

5.2 Manquement à la politique de la sécurité des systèmes d'information

5.2.1 Mesures applicables par les administrateurs informatiques et réseaux (ASR)

Les responsables informatiques et réseaux peuvent en cas d'urgence user de mesures conservatoires :

- déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation
- suspendre l'activité d'un processus qui nuirait au bon fonctionnement des systèmes d'information
- isoler un système informatique du réseau si celui-ci présente un comportement qui mettrait en péril la sécurité des systèmes d'information
- isoler ou neutraliser provisoirement toute donnée ou fichier qui mettrait en péril la sécurité des systèmes d'information

Ils doivent en informer le CSSI de l'entité concernée et les RSSI. Ils ont un devoir de confidentialité et ne doivent communiquer sur l'incident que ce qu'ont à en connaître les autres personnes. Ils doivent veiller au mieux à ne pas modifier un environnement pour le recueil de preuves, si l'incident détecté nécessite ultérieurement un dépôt de plainte.

5.2.2 Mesures applicables par les CSSI

Le CSSI d'une entité veille au respect de la PSSI par les utilisateurs de l'entité. En cas de manquement observé, il doit rappeler les règles en vigueur aux utilisateurs concernés et peut appliquer provisoirement les mesures conservatoires suivantes :

- déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation
- restreindre ou interdire à un utilisateur les accès à ses comptes sur les systèmes d'information de l'entité
- imposer un changement de mot de passe à un utilisateur
- suspendre l'activité d'un processus sur un système
- isoler du réseau le ou les systèmes d'information concernés
- bloquer les connexions externes du ou des systèmes d'information concernés
- imposer l'installation de logiciels ou des mises à jour de sécurité sur le ou les systèmes d'information concernés

Le CSSI doit cependant informer le plus rapidement possible l'utilisateur de cette situation. Ces mesures doivent être limitées au temps nécessaire à un retour à des conditions normales. La mise en œuvre de ces mesures n'implique pas obligatoirement une responsabilité du « propriétaire » du compte ou du système informatique concerné. Elles ont pour objectif de préserver la sécurité des systèmes d'information et n'ont pas vocation à être des sanctions.

En cas de faits graves ou de récidives, le CSSI doit, de plus, informer immédiatement les RSSI de l'École normale supérieure. Il a un devoir de confidentialité et ne doit mentionner aux autres utilisateurs que le strict nécessaire.

Le CSSI doit veiller au mieux à ne pas modifier un environnement pour le recueil de preuves, si l'incident détecté nécessite le dépôt d'une plainte.

5.2.3 Mesures applicables par les RSSI

A la suite d'un manquement observé à la PSSI, les RSSI peuvent appliquer ou demander d'appliquer les mesures décrites au paragraphe précédent à tout utilisateur ou à tout système de l'École normale supérieure.

De plus, sur la base des analyses d'activités, de la détection de comportement atypique, d'avis du CERT ou d'autres autorités reconnues, les RSSI peuvent être amenés à alerter les utilisateurs concernés ou à requérir des informations auprès d'eux. Celles-ci peuvent être assorties du blocage des flux réseaux partiels ou totaux provenant d'un ou plusieurs systèmes d'information, ou d'un sous-réseau, ou de la suspension des accès aux systèmes d'information.

En cas d'incidents graves, comme ceux susceptibles d'entraîner le dépôt d'une plainte ou entachant l'image de l'École normale supérieure ou de l'une des tutelles d'une entité, mais aussi une récidive à un manquement à la PSSI ou une non réponse à une requête d'information, les RSSI peuvent convoquer un utilisateur. Cette convocation se traduit par un entretien entre l'utilisateur concerné et les RSSI. Il est rappelé les conditions de l'incident et, si nécessaire, les règles de la PSSI en vigueur et discuté des mesures devant être prises. A l'issue de celui-ci, les RSSI peuvent prendre une ou plusieurs des mesures suivantes :

- considérer l'incident comme clos et sans suite
- demander l'application de mesures spécifiques et maintenir, s'il y a lieu, l'application de la suspension du droit d'usage des systèmes d'information à l'École normale supérieure jusqu'à la réalisation de ces mesures

- rappeler les obligations en vigueur à l'utilisateur. Une information est alors faite à la chaîne hiérarchique et à la chaîne fonctionnelle
- remettre le traitement de l'incident à la chaîne hiérarchique. Une information est alors faite à la chaîne fonctionnelle

Dans le cas particulier d'utilisateurs externes ayant un compte ouvert sur un système d'information de l'École normale supérieure, les RSSI peuvent procéder ou demander à procéder à la clôture définitive de ce compte.

En cas d'incidents portant préjudice à l'École normale supérieure ou à l'une des entités du périmètre de la PSSI, les RSSI peuvent proposer le dépôt d'une plainte auprès du procureur de la République.

En cas d'incidents susceptibles d'entraîner des mesures disciplinaires, les règles en vigueur s'appliquent.

* * *

Groupe de travail ayant participé à l'élaboration de ce document :

- Olivier Abillon, Directeur des études scientifiques
- Jean-François Barbé, Directeur du CRI
- Jacques Beigbeder, Responsable de la sécurité des systèmes d'information
- Audrey Gillot, Secrétariat général
- Mathias Kende, Élève scientifique élu au conseil d'administration
- Simon Larger, Secrétariat général
- Rémy Portier, CSSI CNRS département de physique
- Bénédicte Sabatier-Labeyrie, CSSI CNRS département de sciences sociales
- Pierre Vincens, Responsable de la sécurité des systèmes d'information – suppléant

Glossaire

A propos des SI (Systèmes d'Information)

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information rattachée au Secrétaire général de la défense nationale créée par décret du 7/7/2009

AQSSI : Autorité Qualifiée pour la Sécurité des Systèmes d'Information (Directeur d'établissement)

ASR : Administrateur des Systèmes et Réseaux

CSSI : Correspondant de la Sécurité des Systèmes d'Information

DCSSI : Direction Centrale de la Sécurité des Systèmes d'Information rattachée au Premier ministre (remplacée par l'ANSSI)

PSSI : Politique Sécurité des Systèmes d'Information

RSSI : Responsable de la Sécurité des Systèmes d'Information

SMSI : Système de Management de la Sécurité de l'Information. Les termes SGSI (Système de Gestion de la Sécurité de l'Information) et SGSSI (Système de Gestion de la Sécurité des Systèmes de l'Information) sont des quasi-synonymes, ISMS (Information Security Management System) étant le terme anglais

OzSSI : Observatoire Zonal de la sécurité des systèmes d'information

Autres termes et sigles

BEFTI : Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information

CERT : Computer Emergency Response Team. Ces organismes ont pour mission la centralisation des demandes d'assistance suite aux incidents de sécurité (attaques) sur les réseaux et les systèmes d'information, le traitement des alertes et la réaction aux attaques informatiques, l'établissement et la maintenance d'une base de données des vulnérabilités, la diffusion d'informations sur les précautions à prendre pour minimiser les risques d'incident et leurs conséquences, et enfin la coordination avec les autres entités chargées de la sécurité. L'ENS dépend du CERT-Renater

CIL : Correspondant « Informatique et Libertés »

CNIL : Commission Nationale de l'Informatique et des Libertés

CRU : Comité Réseau des Universités

HFD : Haut Fonctionnaire de Défense

P2P ou peer-to-peer : principe de communication via un réseau regroupant un ensemble d'ordinateurs où chacun d'eux joue à la fois le rôle de client et serveur vis-à-vis d'une ressource (fichiers, flux audio ou vidéo, téléphonie, calcul,...)

RAP : Réseau Académique Parisien fournisseur pour l'ENS de la connexion à l'internet via RENATER

RENATER : Réseau NAtional de télécommunications pour la Technologie, l'Enseignement et la Recherche constitué en Groupement d'intérêt public. Pour l'utiliser, il impose une charte d'usage

Rezo : Partie du réseau informatique de l'ENS couvrant l'ensemble des thurnes et offrant donc aux élèves l'accès à l'internet. Cet accès est commun avec les autres entités et se fait via RAP/RENATER

UREC : Unité Réseaux du CNRS (UPS836). C'est une unité propre de service rattachée au Secrétaire général du CNRS