ACADÉMIE
DE CRÉTEIL

Liberté
Égalité
Fraternité

Politique de Sécurité des Systèmes d'Information de l'Académie de Créteil

Présenté au Comité Social Académique – 2024

Documents de référence
Réglementations
Instruction Interministérielle n°901 relative à la protection des SI sensibles
Instruction Interministérielle n°1300 publié en 2020
Réglementation Générale de Sécurité
Schéma Directeur de la Sécurité des Systèmes d'Information du MEN publié en 2005
Circulaire n°2004-035 du 18 février 2004
Plan Vigipirate de l'État
Code de l'Education
Politique de la Sécurité des Systèmes de l'Information de l'Etat
Recommandations
Commission Nationale de l'Informatique et des Libertés (CNIL)
Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

Annexes	
Annexe 1	Référentiel d'exigences de sécurité pour les SI des services Académiques
Annexe 2	Référentiel d'exigences de sécurité pour les SI des établissements d'enseignement du premier et du second degré
Annexe 3	Notice d'élaboration d'une charte des usages numériques en école et établissement scolaire
Annexe 4	Charte régissant les usages des systèmes d'information et du numérique par les personnels de l'académie de Créteil
Annexe 5	Charte des administrateurs informatiques de l'académie de Créteil
Annexe 6	Analyse de risques - Indicateurs
Annexe 7	Glossaire

Sommaire

I. Objet

La Politique de Sécurité des Système d'Information Académique (PSSI-A) décrit l'ensemble des principes fondateurs et structurants gouvernant la définition des moyens réglementaires, organisationnels ou techniques à mettre en œuvre pour la sécurité des Systèmes d'Information.

Elle est un instrument de cohérence pour l'ensemble de l'académie.

Ce document à orientation stratégique s'arrête, par vocation, aux principes généraux et exigences fonctionnelles, sans traiter de la manière de réaliser la fonction spécifiée, sans décrire les mécanismes qui dépendent de la technologie disponible.

C'est un élément stable, structurant et permanent de l'académie.

La PSSI-A s'appuie et intègre les exigences:

- de la Politique de la Sécurité des Systèmes de l'Information de l'Etat (PSSI-E)
- du référentiel général de sécurité (RGS)
- du référentiel général de protection des données (RGPD)
- des règles établies par le Ministère de l'Éducation Nationale (MEN) à laquelle l'académie se conforme pour le bon fonctionnement des environnements numériques de travail, des téléservices et du Réseau d'Accès et de Consolidation des Intranets de l'Education (RACINE)
- les obligations légales.

Elle est proposée par le Responsable de la Sécurité des Systèmes d'Information (RSSI), validée par le Directeur des Systèmes d'Information (DSI) et approuvée par l'Autorité Qualifiée pour la Sécurité des Systèmes d'Information (AQSSI).

II. Chaîne de responsabilités et champ d'application

II.1. Etat et académie

II.1.A. Autorité Qualifiée en Sécurité des Systèmes d'Information

Conformément au SDSSI du MEN publié en 2005, l'Autorité Qualifiée en Sécurité des Systèmes d'Information (AQSSI) est le recteur d'académie.

L'AQSSI, conseillée par le Responsable de la Sécurité des Systèmes d'Information (RSSI) arbitre la stratégie de Sécurité des Systèmes d'Information (SSI), identifie les moyens associés et prescrit les dispositifs adaptés au sens de la circulaire 2004-035 du 18 février 2004.

Son champ d'action en matière de SSI concerne les Systèmes d'Information (SI):

- des services académiques,
- des établissements scolaires du second degré (EPLE),
- des écoles.

II.1.B. Responsable de la Sécurité des Systèmes d'Information

Le RSSI, nommé et mandaté par l'AQSSI, définit et veille à la bonne réalisation de la présente PSSI-A.

Ses missions principales sont:

- Assurer le pilotage de la démarche de cybersécurité sur le périmètre organisationnel,
- Constituer et coordonner un réseau interne de Correspondants de Sécurité
- Copiloter le Comité de la Confiance Numérique (SSI, RGPD),
- Définir et décliner la PSSI-A (prévention, protection, détection, résilience, remédiation), en cohérence avec la PSSI-E et les directives interministérielles,
- Veiller à l'application de la PSSI-A,
- Contrôler le niveau de sécurité du SI par l'évaluation des risques résiduels,
- Assurer un rôle de conseil, d'information, de formation, de sensibilisation et d'alerte, auprès des directions, partenaires, administrateurs informatiques et utilisateurs,
- S'assurer de la mise en place des solutions et des processus opérationnels pour garantir la protection des données et le niveau de sécurité des SI,
- Assurer la coordination avec les différents organismes et partenaires dont les collectivités territoriales.

II.1.C. Comitologie de la Sécurité des Systèmes d'Information

Comité de la Confiance Numérique

Pour un besoin de contrôle et de suivi, un Comité de la Confiance Numérique (CCN) se réunit une à deux fois par an afin de:

- Veiller à la bonne application de la PSSI-A,
- Suivre les incidents de sécurité,
- Evaluer l'efficacité de l'académie sur les problématiques SSI,
- Présenter les campagnes de formation et de sensibilisation.

Le CCN est composé de membres permanents:

- L'Autorité Qualifiée pour la Sécurité des Systèmes d'Information (AQSSI),
- Le Conseiller à la Sécurité du Numérique (CSN),
- Le RSSI et son adjoint,
- Le Délégué Académique à la Protection des Données (DPD),
- Le Directeur des Systèmes d'Information (DSI).

et de membres invités:

- Le Secrétaire Général d'Académie,
- Le Secrétaire Général adjoint,
- Les Secrétaires Généraux de DSDEN,
- Le Délégué Académique au Numérique Educatif (DANE),
- Les Correspondants de Sécurité.

Commission d'Homologation

Tout système d'information doit faire l'objet d'une décision d'homologation de sa sécurité avant sa mise en exploitation dans les conditions d'emploi définies. L'homologation est l'acte selon lequel l'autorité atteste formellement auprès des utilisateurs que le système d'information est protégé conformément aux objectifs de sécurité fixés.

En fonction de leur criticité ou de leur périmètre, la décision d'homologation est prise par le RSSI ou la commission d'homologation. Cette décision s'appuie sur une analyse de risques adaptée aux enjeux du système considéré, et précise les conditions d'emploi.

La Commission d'Homologation de Sécurité des Systèmes d'Information (CHSSI) est composée du RSSI académique et de son adjoint, de l'ISR, des experts concernés par l'objet de l'homologation et le cas échéant de représentants des collectivités territoriales.

Les indicateurs, en **Annexe 6**, permettront d'apprécier la criticité (niveau de risque) à partir de critères de gravité et de vraisemblance.

Comité Opérationnel de la Gestion des Incidents de Sécurité

En cas d'incidents de sécurité[1] survenant sur les SI des services académiques, des EPLE, des écoles ou sur les ENT, un processus de chaîne d'alerte d'incidents de sécurité doit être enclenché.

En fonction de la criticité des incidents, le Comité Opérationnel de la Gestion des Incidents de Sécurité (COGIS) peut se réunir pour organiser une stratégie de résolution d'incidents et de communication.

Le COGIS est composé du RSSI académique et de son adjoint, des experts opérationnels et métiers concernés par l'objet de l'incident et le cas échéant de représentants des collectivités territoriales.
Le RSSI académique coordonnera les différentes actions.

II.1.D. Audits des Systèmes d'Information

Le RSSI s'assure par des audits ponctuels que les prescriptions de sécurité sont mises en œuvre:

- de manière inopinée,
- à la suite d'un incident de sécurité ou de détection de vulnérabilités,
- à la demande d'un responsable de site.

1 Un incident de sécurité est un événement qui porte atteinte à la disponibilité, la confidentialité ou l'intégrité d'un bien. Exemples : utilisation illégale d'un mot de passe, vol d'équipements informatiques, intrusion dans un fichier ou une application, etc.

Ces audits peuvent prendre la forme d'une analyse de l'architecture du SI, d'audits de codes, d'analyse de risques ou de tests d'intrusion.

Le RSSI et ses correspondants de sécurité sont chargés de la mise en œuvre de la sécurité sur l'infrastructure technique et sur les dispositifs spécifiques de sécurité dans l'ensemble des services académiques, écoles et établissements du second degré.

II.2. Ecoles, établissements du second degré et collectivités territoriales

L'État est prescripteur de la sécurité.

La loi n°2013-595 du 8 juillet 2013 s'est attachée en ses articles 19, 21 et 23 à clarifier la répartition des compétences entre l'État et les collectivités territoriales en matière d'équipement informatique des établissements scolaires du second degré, et notamment en matière d'acquisition et de maintenance de ces équipements.

- Ainsi, au titre de l'équipement et du fonctionnement des écoles qui relèvent de leur compétence depuis 1983 en vertu des articles L212-4 et L212-5 du code de l'éducation, la **Commune** a la charge de l'installation, du fonctionnement et de l'entretien des matériels mis à disposition des élèves dont font partie les équipements et la maintenance des matériels informatiques, y compris dédiés à la sécurité. Ces équipements doivent être conformes aux exigences en matière de cybersécurité et de protection des mineurs.
- Ainsi, au titre de l'équipement et du fonctionnement des collèges qui relèvent de leur compétence depuis 1983 en vertu des articles L212-2 du code de l'éducation, le **Département** a la charge de l'ensemble des dépenses informatiques, matérielles ou logicielles qui sont nécessaires au fonctionnement régulier de l'établissement et au bon déroulement de la scolarité des élèves, y compris de leur maintenance. Ces équipements doivent être conformes aux exigences en matière de cybersécurité et de protection des mineurs.
- Ainsi, au titre de l'équipement et du fonctionnement des lycées qui relèvent de leur compétence depuis 1983 en vertu des articles L212-6 du code de l'éducation, la **Région** a la charge de l'ensemble des dépenses informatiques, matérielles ou logicielles qui sont nécessaires au fonctionnement régulier de l'établissement et au bon déroulement de la scolarité des élèves, y compris de leur maintenance. Ces équipements doivent être conformes aux exigences en matière de cybersécurité et de protection des mineurs.

Dans ce cadre, les charges relevant de la collectivité territoriale ne concernent que les infrastructures propres des établissements.
Les applications nationales[2] ne rentrent pas dans ce cadre.

Les charges portent sur tous les aspects des infrastructures:

- équipements actifs réseaux,
- matériels et dispositifs de sécurité,
- serveurs de données,
- terminaux.

Pour les établissements du second degré, les équipements informatiques des zones administratives et pédagogiques ainsi que les Espaces Numériques de Travail (ENT) font ainsi partie des « matériels informatiques et logiciels (...) » mentionnés dans les articles L313-2 et L214-6 du Code de l'Education.

La collectivité est responsable en matière de surveillance et de sécurité durant les activités dont elle est l'organisatrice.
Ce point est particulièrement important dans le cas de locaux informatiques mis à disposition de tiers par la collectivité en dehors du temps scolaire.

La présente PSSI-A prend en compte les exigences et contraintes de tous les utilisateurs de l'établissement: pédagogie, gestion et échange entre les membres de la communauté éducative.

Un conventionnement entre la collectivité territoriale et l'académie précisant les responsabilités respectives est de nature à faciliter la gestion:

- pour les engagements de service (disponibilité),
- des données de connexion et d'authentification,
- des règles d'accès aux différents journaux.

La collectivité doit mettre à disposition de chaque chef d'établissement et du RSSI un outillage permettant de vérifier par des audits ponctuels que les règles édictées dans la PSSI-A sont effectivement mises en œuvre.

Les écoles du premier degré n'ayant pas de personnalité morale, les responsabilités en termes de SSI sont réparties entre plusieurs acteurs:

- La responsabilité juridique de l'État est portée par le DASEN, par délégation du recteur d'académie.
- Le directeur d'école organise la surveillance des élèves. Il contribue en cela avec les enseignants à l'application de la protection des mineurs dans les usages de l'internet au sens de l'a circulaire 2004-035 du 18 février 2004.
- Le directeur d'école a obligation de signaler tout incident ou défaillance au maire, au RSSI et à son autorité hiérarchique.

2 Application informatique mise à disposition de l'ensemble des établissements par le ministère. Par exemple, pour les actes de gestion financière ou de resssources humaines.

Dans les établissements du second degré, le chef d'établissement est la personne juridiquement responsable, placée sous l'autorité de l'AQSSI.
Il est chargé de:

- prendre « toutes les dispositions, en liaison avec les autorités administratives compétentes, pour assurer la sécurité des personnes et des biens, l'hygiène et la salubrité de l'établissement », conformément aux dispositions de l'article R421-10 du Code de l'Education,
- prendre des mesures générales de prévention et d'organisation du service public de l'éducation garantissant la sécurité, y compris en matière informatique,
- signaler tout incident de sécurité ou défaillance au RSSI.

III. Référentiels SSI

Les référentiels SSI sont un ensemble de directives qui s'imposent pour la sécurisation des Systèmes d'Information.
Ils fixent notamment les règles que doivent respecter les usagers ainsi que les acteurs des systèmes d'information contribuant à la sécurité des échanges numériques.

III.1. Services Académiques

Ce référentiel est applicable au périmètre des services académiques:

- le Rectorat,
- les DSDEN,
- les circonscriptions du premier degré,
- les centres d'information et d'orientation d'État (CIO).

Son application est assurée par la DSI académique. Les différents items du référentiel sont détaillés en **Annexe 1** Référentiel d'exigences de sécurité pour les systèmes d'information des services académiques.

III.2. Ecoles et établissements du second degré

Ce référentiel est applicable au périmètre des écoles:

- écoles maternelles,
- écoles élémentaires,
- écoles primaires,
- écoles d'application regroupements pédagogiques intercommunaux (RPI).

et des établissements du second degré:

- collèges,
- lycées d'enseignement général et technologique,
- lycées d'enseignement professionnel,
- groupements d'établissements (GRETA),

- écoles régionales du premier degré (ERPD),
- écoles régionales d'enseignement adapté (EREA),
- internats de la réussite.

Les différents items du référentiel sont détaillés en **Annexe 2** Référentiel d'exigences de sécurité pour les systèmes d'information des établissements d'enseignement du premier et du second degré.

III.3. Le réseau RACINE

Le réseau Racine est une infrastructure de télécommunication inter-services permettant l'interconnexion des différents Intranets des sites, leur ouverture à des clients distants (télétravail, nomadisme, etc.) et la sécurité des échanges.

Il se base sur:

- une politique de sécurité commune à l'ensemble des services,
- un accès à Internet déjà opérationnel au travers de RENATER,
- un respect massif des normes de l'Internet,
- un Extranet d'établissements scolaires fortement développé.

Le projet RACINE définit:

- une organisation en zones de confiance avec des niveaux d'habilitation,
- un plan d'adressage IP respectant les standards de l'Internet et commun à l'ensemble des services,
- un réseau sécurisé sur RENATER interconnectant l'ensemble des services (rectorats, administration centrale) et s'ouvrant sur des postes distants;
- une autorité de certification recouvrant les principes de la signature électronique.

III.3.A. Les Zones de Confiance

- Le réseau RACINE,
- Le réseau RACINE-AGRIATES pour les EPLEs,
- Le réseau RACINE-API pour les postes isolés,
- Le réseau ADRIATIC pour les collectivités,
- Le réseau RACINE-PACS pour les partenaires extérieurs,
- Le réseau interministériel ADER/RIE.

III.3.B. Le Plan d'Adressage

Des adresses IP distinctes sont fournies à chacune des académies intégrées au réseau RACINE.
En cas de besoin, l'ISR tient à disposition des collectivités ce plan d'adressage.

III.3.C. Le Réseau VPN

L'interconnexion des sites repose sur des liaisons VPN (Ipsec) ou du MPLS nécessitant l'utilisation de mécanismes cryptographiques.
Les suites cryptographiques doivent être pleinement compatibles avec les exigences du RGS.

III.3.D. La Politique de Certification

La Plateforme Nationale de Confiance Numérique (PNCN) délivre des certificats de type SHA2 garantissant la confiance globale du réseau.

IV. Chartes Informatiques

Les chartes informatiques décrivent les obligations des usagers du SI.
Elles permettent de définir les droits et limitations concernant l'utilisation des services numériques dans l'institution. Les chartes visent principalement à sensibiliser les usagers et à prévenir d'éventuels usages abusifs.

IV.1. Charte régissant les usages des systèmes d'information et du numérique par les personnels de l'académie de Créteil

La charte en **Annexe 3** définit les règles d'usages et de sécurité que l'institution et l'utilisateur s'engagent à respecter: elle précise les droits et devoirs de chacun.

IV.2. Charte des administrateurs informatiques

La charte en **Annexe 4** a pour objet de préciser les droits et obligations des administrateurs informatiques dans l'exercice de leur fonction.

Elle s'applique à tout administrateur informatique amené à intervenir sur le système d'information de l'académie de Créteil dans le périmètre des services académiques, des écoles ou des établissements du second degré, qu'il soit fonctionnaire, contractuel, stagiaire, vacataire ou prestataire.

IV.3. Notice d'élaboration d'une charte des usages du numérique

Le Bulletin Officiel n°9 du 24 février 2004 indique que chaque école et établissement scolaire doit mettre en place une charte de l'utilisation d'Internet annexée au règlement intérieur.
La notice d'élaboration en **Annexe 5**, accompagne les écoles et établissements scolaire, à la rédaction d'une charte des usages du numérique qui devra être annexée aux règlements intérieurs.

V. Glossaire

L'**Annexe 7** présente un glossaire de la PSSI-A.