ACADÉMIE
DE VERSAILLES
Liberté
Égalité
Fraternité

L'ACADÉMIE
vous accompagne

POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION DE L'ACADÉMIE DE VERSAILLES

Sommaire

Préambule

Cette politique académique de sécurité des systèmes d'information (PSSIA) est établie par l'académie de Versailles, en vue de garantir la sécurité des systèmes d'information mis à disposition et constitue le cadre de référence permettant aux différents acteurs (DSI académique, collectivités territoriales) d'opérer les choix d'architectures informatiques et de sécuriser leur mise en œuvre.

Deux référentiels d'exigences de sécurité sont présentés dans ce document :

- le référentiel d'exigences à destination des services académiques,
- le référentiel d'exigences à destination des écoles et établissements du premier et du second degré publics situés sur le territoire de l'académie de Versailles.

Ce document précise, d'une part, les devoirs des différents acteurs qui partagent juridiquement les compétences et réaffirme la chaîne de responsabilité en matière de sécurité des systèmes d'information et d'autre part, il énumère les mesures à mettre en œuvre pour assurer la protection des systèmes et des individus, et détermine les modalités d'évaluation des dispositifs mis en place à cet effet.

Il est révisé annuellement mais peut toutefois, en cas d'urgence, faire l'objet d'avenants ponctuels sur décision de l'autorité qualifiée en sécurité des systèmes d'information (AQSSI).

1. Fondements juridiques

La PSSIA s'appuie sur les réglementations suivantes :

- instruction interministérielle n°901 relative à la protection des systèmes d'information sensibles,
- instruction Interministérielle n°1300 de 2020,
- référentiel Général de Sécurité (RGS),
- schéma directeur de la SSI du MEN publié en 2005,
- circulaire N°2004-035 du 18 février 2004,
- plan Vigipirate de l'Etat,
- schéma Directeur des ENT (SDET),
- code de l'Éducation.

LA PSSIA s'appuie également sur les recommandations de la CNIL (Commission Nationale de l'Informatique et des Libertés) et de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

2. Chaîne de responsabilités

2.1 État et académie

L'Etat est prescripteur de la sécurité.

Conformément au schéma directeur de la sécurité des systèmes d'information (SSI) du ministère de l'Éducation Nationale publié en 2005, l'autorité qualifiée en sécurité des systèmes d'information (AQSSI) est la rectrice de l'académie.

La rectrice, conseillée par le Responsable de la Sécurité des Systèmes d'Information (RSSI), arbitre la stratégie 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 services académiques, les établissements scolaires (EPLE) et les écoles. Il s'étend à tout le système d'information.

Le RSSI est nommé et mandaté par l'autorité qualifiée pour définir et veiller à la bonne réalisation de la politique de sécurité. Ses missions principales sont :

- animer le pilotage de la SSI,
- constituer et coordonner un réseau interne de correspondants de sécurité,
- mettre en place les plans de sécurité adaptés, en cohérence avec la politique de sécurité des systèmes d'information de l'Etat et les directives interministérielles,
- contrôler régulièrement le niveau de sécurité du système d'information par l'évaluation des risques résiduels,
- informer et sensibiliser les utilisateurs du système d'information aux problématiques de la sécurité,
- améliorer la sécurité des systèmes d'information par une veille technologique active ainsi que par une participation aux groupes de réflexion ad hoc,
- assurer la coordination avec les différents organismes concernés, dont les collectivités territoriales de l'académie.

En cas d'incident de sécurité survenant sur les SI des services académiques, des écoles, des EPLE ou sur les ENT, la chaîne d'alerte académique doit être saisie sans délai par l'ouverture d'un ticket sur la plate-forme d'assistance académique, afin d'en informer le RSSI, qui se chargera de coordonner les différentes actions nécessaires.

Le RSSI s'assure par des audits ponctuels que les prescriptions de sécurité sont mises en œuvre, soit de manière inopinée, soit à la suite d'un incident de sécurité. Ils peuvent prendre la forme d'une analyse de l'architecture du système d'information, d'audits de code source d'application, d'analyse des risques ou des tests d'intrusion.

Le correspondant de sécurité est chargé de la mise en œuvre de la sécurité sur l'infrastructure technique (équipements de sécurité, versions logicielles, carnets d'exploitation des serveurs) et sur les dispositifs spécifiques de sécurité (filtres, sondes de détection, antivirus...).

Les correspondants de sécurité académiques sont affectés à la DSI :

- ingénieurs Sécurité Racine,
- responsables des EMIP (Équipes de Maintenance Informatique de Proximité).

2.2 Écoles, EPLE et collectivités territoriales

La loi n° 2013-595 du 8 juillet 2013 d'orientation et de programmation pour la refondation de l'école de la République s'est attachée, en ses articles 19, 21 et 23, à clarifier, sans la modifier, la répartition des compétences entre l'Etat 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, telle qu'elle résulte des premières lois de décentralisation, bien avant le développement et la généralisation des outils numériques dans la vie courante des écoles et établissements scolaires.

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, le fonctionnement et 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, qui constituent une dépense obligatoire. 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 sa compétence depuis 1983 en vertu de l'article L. 213-2 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 la maintenance de ces matériels et logiciels, laquelle est d'ailleurs fréquemment intégrée dans les marchés passés en vue de leur acquisition.

Ainsi, au titre de l'équipement et du fonctionnement des lycées, qui relèvent de sa compétence depuis 1983 en vertu de l'article L. 214-6 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 la maintenance de ces matériels et logiciels, laquelle est d'ailleurs fréquemment intégrée dans les marchés passés en vue de leur acquisition.

Dans ce cadre, les charges relevant de la collectivité territoriale ne concernent que les infrastructures propres des établissements. Les applications « nationales », c'est-à-dire les applications informatiques mises à disposition de l'ensemble des établissements par le ministère (par exemple pour les actes de gestion financière ou de ressources humaines) ne rentrent pas dans ce cadre.

Les charges relevant de la collectivité portent sur tous les aspects des infrastructures : équipements actifs réseaux, matériels de sécurité, serveurs de données, terminaux. Les matériels et dispositifs de sécurité en font partie, puisqu'ils sont indispensables au bon fonctionnement des infrastructures et équipements.

La collectivité est responsable en matière de surveillance et de sécurité durant les activités dont elle est l'organisatrice (c'est notamment le cas des temps de restauration scolaire et de garderie). Ce point est particulièrement important dans le cas de locaux informatiques mis à disposition de

tiers par la collectivité en dehors du temps scolaire (par exemple pour des associations, des dispositifs de soutien scolaire).

La collaboration entre l'académie et les collectivités territoriales est essentielle en matière de sécurité, dans la mesure où la politique de sécurité des systèmes d'information doit prendre en compte les exigences et contraintes de tous les utilisateurs dans les différents secteurs intéressant la vie de l'établissement : pédagogie, gestion, échanges entre les membres de la communauté éducative.

Le conventionnement entre la collectivité territoriale et les services du rectorat est de nature à faciliter la tâche de chacun, dès lors qu'elle précise les responsabilités respectives, mais également celles de l'ensemble des utilisateurs dans les établissements, au regard notamment des engagements de service (délais de rétablissement du service, disponibilité, etc.), des données de connexion et d'authentification et des règles d'accès aux informations (journaux d'événements et autres).

La collectivité doit mettre à disposition de chaque chef d'établissement (dans le second degré) et de l'AQSSI (via le RSSI académique) un outillage leur permettant de vérifier par des audits ponctuels que les règles édictées ci-dessous sont effectivement mises en œuvre (dossier d'architecture technique avec schémas des architectures, journaux électroniques d'activité, règles des pares-feux, etc.).

2.2.1 Aspects spécifiques au premier degré

Les écoles désignent les :

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

Les écoles du premier degré n'ayant pas la personnalité morale, les responsabilités en termes de sécurité des systèmes d'information sont réparties entre plusieurs acteurs.

Le service éducatif est organisé au sein de l'école par l'État représenté par la rectrice ou le recteur d'académie. La responsabilité juridique de l'État devant le juge est portée par le DASEN, par délégation de la rectrice ou le recteur, pour ce qui concerne les écoles du premier degré.

Le directeur d'école organise la surveillance des élèves (article 2 du décret n°89-122 du 24 février 1989). Il contribue en cela avec les enseignants à l'application des mesures de protection des mineurs dans les usages de l'internet au sens de la circulaire 2004-035 du 18 février 2004. Responsable de la sécurité des personnes et des biens dans son école, le directeur a obligation de signaler tout incident ou défaillance au maire et à l'autorité académique.

2.2.2 Aspects spécifiques au second degré

Les établissements du second degré désignent :

- les collèges,
- les lycées d'enseignement général et technologique,
- les lycées d'enseignement professionnel,
- les groupements d'établissements (GRETA),
- les ERPD (Écoles Régionales du Premier Degré),
- les EREA (Écoles régionales d'Enseignement Adapté),
- les internats de la réussite,
- les CIO.

Les équipements en zones administrative et pédagogique ainsi que les espaces numériques de travail (ENT) font partie des « matériels informatiques et logiciels prévus pour leur mise en service, nécessaires à l'enseignement et aux échanges entre les membres de la communauté éducative », que mentionne les articles L. 213-2 et L. 214-6 du code de l'éducation, et comptent ainsi parmi les dépenses à la charge des départements et des régions.

Dans l'établissement scolaire, le chef d'établissement est la personne juridiquement responsable, placée sous l'autorité de la rectrice de l'académie lorsque celle-ci agit en sa qualité d'AQSSI.

À cet égard, il convient de rappeler que, dans les collèges et les lycées, le chef d'établissement, en qualité de représentant de l'État, « prend toutes 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 du 3° de l'article R. 421-10 du code de l'éducation. Il est chargé, à ce titre, de prendre des mesures générales de prévention et d'organisation du service public de l'éducation garantissant la sécurité, y compris en matière informatique.

3. Périmètre d'application des référentiels SSI

3.1 Référentiel des services académiques

Ce référentiel est applicable dans l'ensemble des services académiques, qui comprend :

- le rectorat,
- les DSDEN,
- les circonscriptions du premier degré,
- les centre d'information et d'orientation (CIO) d'Etat.

Son application est assurée par la DSI (Direction des Systèmes d'Information) académique. Les items du référentiel sont détaillés dans l'annexe 1, intitulée « Référentiels d'exigences de sécurité pour les systèmes d'information des services académiques ».

3.2 Référentiel des écoles et des établissements du second degré

Ce référentiel est applicable dans les écoles du premier degré, dont la typologie est détaillée au paragraphe 2.2.1 et dans les établissements du second degré (EPLE), dont la typologie est détaillée au paragraphe 2.2.2.

Les items du référentiel sont détaillés dans l'annexe 2, intitulée « Référentiel d'exigences de sécurité pour les systèmes d'information des établissements d'enseignement du premier et du second degré ».

4. Cadre organique du réseau RACINE

Les réseaux RACINE (Réseau d'Accès et de Consolidation des Intranets de l'Éducation) sont des réseaux privés virtuels qui offrent et garantissent un environnement d'accès sécurisés aux systèmes d'information de l'Éducation nationale pour toute communauté d'utilisateurs « ayants droit » quel que soit le lieu où ces utilisateurs exercent leurs activités professionnelles.

Les réseaux RACINE sont indépendants de toute infrastructure de transport. Ces accès deviennent, par là même, indépendants du niveau de sécurité de chacune des infrastructures externes de réseaux traversées.

Ils se basent sur :

- une organisation en zone 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 privé virtuel sécurisé interconnectant l'ensemble des services,
- une autorité de certification.

Le plan d'adressage RACINE est tenu à disposition des collectivités territoriales en cas de besoin par l'ingénieur sécurité Racine (ISR) basé au sein de la DSI académique.

Les zones de confiance sont :

- le réseau RACINE pour la fourniture d'un support sécurisé pour les échanges d'informations entre le réseau de l'administration centrale et les services académiques,
- le réseau RACINE-AGRIATES (Accès Généralisé aux Réseaux Intranet Académiques et Territoriaux pour les établissements Scolaires) pour la fourniture d'un support sécurisé pour les échanges d'informations entre le réseau de l'administration des établissements et le rectorat,
- le réseau RACINE-ADRIATIC (Accès des Départements et des Régions aux Intranet Académiques et aux TICs) pour la fourniture d'un support sécurisé pour les échanges d'informations entre le réseau Internet du rectorat et les collectivités,
- le réseau RACINE-API (Accès Postes Isolés) pour la fourniture d'un support sécurisé permettant l'accès des postes isolés des utilisateurs « ayants droit » aux services des ressources nécessaires au bon exercice de leurs fonctions ou missions.

Ces réseaux reposent sur un VPN IPsec (site à site ou client à site) nécessitant l'utilisation de mécanismes cryptographiques. Les suites cryptographiques doivent être pleinement compatibles avec les exigences du RGS.

L'usage de certificats de type SHA2 délivrés par la Plate-forme Nationale de Confiance Numérique (PNCN), autorité de certification du ministère, qui garantit la confiance globale du réseau, est exigé.

L'interconnexion des intranets, notamment dans le cadre d'AGRIATES, peut-être basée sur des mécanismes de transport de type MPLS (MultiProtocol Label Switching).

5. Homologation de sécurité

Les systèmes d'information ou applications manipulant des données confidentielles ou sensibles doivent faire l'objet d'une homologation. Le RSSI décide si leur mise en œuvre doit être soumise à un simple avis ou à l'avis d'une commission d'homologation, en fonction de leur criticité ou de leur périmètre.

La commission d'homologation est composée de l'équipe du RSSI académique, des ingénieurs sécurité RACINE (ISR) et des experts concernés par l'objet de l'homologation et le cas échéant des représentants des collectivités territoriales.

Les avis peuvent concerner tout ou partie du SI, dont entre autres :

- des pare-feu ou des équipements de sécurité,
- des architectures techniques et applicatives,
- des infrastructures ou applications,
- des infrastructures de sûreté (vidéosurveillance, alarmes).

6. Chartes

Des chartes précisant les obligations des usagers sont publiées. Elles permettent de définir les droits et les obligations des membres de la communauté éducative concernant l'utilisation des services numériques de l'établissement. Les chartes visent principalement à prévenir ou limiter d'éventuels usages abusifs.

Les chartes proposées en annexe 3 peuvent être intégrées dans les règlements intérieurs.

Trois versions de chartes sont proposées, en fonction du public concerné :

- annexe 3 : notice d'élaboration d'une charte des usages numériques en école et établissement scolaire,
- annexe 4 : charte des personnels académiques,
- annexe 5 : charte des administrateurs de systèmes d'information.

7. Nommage et marquage des documents

Chaque document émis au sein de l'institution doit être marqué par un niveau de confidentialité indiquant le cercle de personnes ou de services vers lequel il peut être diffusé. L'annexe 6 présente les différents types de marquage à utiliser et impose des règles de nommage des documents.

8. Glossaire

AGRIATES : Accès Généralisé aux Réseaux Intranet Académiques et Territoriaux pour les établissements Scolaires

AQSSI : Autorité Qualifiée pour la Sécurité des Systèmes d'Information

CIO : Centre d'Information et d'Orientation

DSDEN : Direction Départementale de l'Éducation Nationale

ENT : Espace Numérique de Travail

EREA : École régionale d'Enseignement Adapté

ERPD : École Régionale du Premier Degré

GRETA : Groupement d'ÉTAblissements

ISR : Ingénieur Sécurité RACINE

MEN : Ministère de l'2ducation Nationale

MPLS : MultiProtocol Label Switching

PNCN : Plate-forme Nationale de Confiance Numérique

RACINE : Réseau d'Accès et de Consolidation des Intranets de l'Éducation

RGS : Réglementation Générale de Sécurité

RPI : Regroupements pédagogiques intercommunaux

RSSI : Responsible de la Sécurité des Systèmes d'Information

SDET : Schéma Directeur des ENT

SSI : Sécurité des Systèmes d'Information

VPN : Virtual Private Network (réseau privé virtuel)

9. Annexes

Annexe 1 : référentiels d'exigences de sécurité pour les systèmes d'information des services académiques.

Annexe 2 : référentiel d'exigences de sécurité pour les systèmes d'information 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 des personnels académiques.

Annexe 5 : charte des administrateurs de systèmes d'information.

Annexe 6 : Nommage et marquage des documents.