La politique générale de sécurité (PGS)
du vice-rectorat
de la Nouvelle-Calédonie,
direction générale des enseignements

Version 2.0 du 15/12/2015, validée par monsieur le vice-recteur de la Nouvelle-Calédonie, directeur général des enseignements.

Propriété du vice-rectorat de la Nouvelle-Calédonie – Reproduction interdite sans autorisation préalable

Documents de référence

PSSI de l'Etat
Référentiel Général de Sécurité
IGI 1300
Cadre commun de la sécurité des systèmes d'information et de télécommunications
Charte d'usage des systèmes d'information par les personnels du vice-rectorat de la Nouvelle-Calédonie
Charte « administrateurs » du vice-rectorat de la Nouvelle-Calédonie.
Règles d'hygiène de la SSI – ANSSI
Guide d'intégration de la SSI dans les projets (Guide GISSIP) – ANSSI
Guide de maturité – ANSSI Méthode d'analyse des risques EBIOS - ANSSI
Guide Gérer les risques sur les libertés et la vie privée – CNIL
Norme ISO 27001 – Système de la Management de la Sécurité de l'Information (SMSI)
Norme ISO 27002 – Bonnes pratiques relatives à la sécurité de l'information
Norme ISO 27005 – Gestion des risques sur les informations
Politique générale de sécurité (PGS) de l'académie de Caen
Politique générale de la sécurité des systèmes d'information académiques du pôle SSI

Propriété du vice-rectorat de la Nouvelle-Calédonie – Reproduction interdite sans autorisation préalable

SOMMAIRE

I. Avant-propos

L'information et les systèmes d'information associés représentent des ressources essentielles à la bonne réalisation des missions de l'Éducation nationale.

La politique générale de sécurité établit le cadre stratégique, organisationnel et méthodologique dans lequel est conduite l'identification des enjeux et la réduction des risques que court le vice-rectorat du fait de tout dysfonctionnement potentiel, qu'il soit accidentel ou intentionnel.

Cette politique, qui s'impose à l'ensemble du vice-rectorat de la Nouvelle-Calédonie, direction générale des enseignements s'appuie sur plusieurs principes directeurs.

De ces principes découlent les documents d'organisation fondés sur la séparation entre responsabilité stratégique et responsabilités opérationnelles, elles-mêmes réparties entre les domaines, les utilisateurs et les structures opérationnelles.

Afin de mener à bien ses missions, le ministère de l'éducation nationale et le vice-rectorat ont développé des systèmes d'informations tant dans les domaines pédagogiques qu'administratifs. Il y a désormais une forte adhérence de notre institution à ces systèmes d'information.

Le système d'information du vice-rectorat est caractérisé par la diversité des missions, la dispersion des sites, leur nombre et leur situation géographique. Cette dispersion est accentuée par des différences fondamentales entre sites tant en terme de ressources, d'accès que de missions.

Il est, de plus, confronté à des évolutions stratégiques telles que la gestion des identités ou les espaces numériques de travail, à des évolutions politiques comme la répartition des compétences avec les collectivités territoriales ou technologiques liées en particulier au développement du nomadisme ou de la voix sur IP.

Cette dispersion conjuguée aux différentes évolutions a accru les risques auxquels notre système d'information est confronté. Faire face à ces risques implique de mettre en place une politique de sécurité des systèmes d'informations.

Propriété du vice-rectorat de la Nouvelle-Calédonie – Reproduction interdite sans autorisation préalable

II. Périmètre d'application de la politique générale de sécurité

Le champ d'application de la politique générale de sécurité de l'information du vice-rectorat de la Nouvelle-Calédonie, direction générale des enseignements se décompose en plusieurs périmètres fonctionnels :

- la pédagogie,
- la gestion,
- les services du vice-rectorat de la Nouvelle-Calédonie,
- les EPENC (établissements publics d'enseignement de la Nouvelle-Calédonie),
- les échanges avec les collectivités.

Il prend également en compte :

- la politique système d'information inter ministérielle de l'État,
- la politique système d'information du ministère,
- le référentiel général de sécurité,
- les règles établies par le ministère de l'Éducation nationale à laquelle le vice-rectorat de la Nouvelle-Calédonie se conforme pour le bon fonctionnement des environnements numériques de travail, des télé-services, du réseau d'accès et de consolidation des intranets de l'Éducation nationale ou réseau RACINE,
- les obligations légales.

Enfin, il tient compte des systèmes d'information propres aux différents sites du vice-rectorat de la Nouvelle-Calédonie, direction des enseignements.

La protection de l'information et la sécurité des systèmes d'information du vice-rectorat intègre également l'interconnexion de ses systèmes d'information avec l'ensemble de ses partenaires qu'il s'agisse d'autres administrations de l'Etat ou des collectivités locales.

Elle prend en compte les relations qui la lient avec l'opérateur pour l'accès et l'utilisation du réseau local ainsi qu'avec le GIP Renater pour l'utilisation du réseau national de l'enseignement, de la technologie et de la recherche.

Enfin, elle incorpore le partage de compétences avec les collectivités locales afin que celles-ci puissent d'une part assumer leurs compétences sur les espaces numériques de travail, l'entretien et la maintenance des infrastructures et des équipements informatiques (Loi sur la refondation de l'école), et, d'autre part, gérer les droits pour les élèves ou leur famille relatifs à l'action sociale.

Propriété du vice-rectorat de la Nouvelle-Calédonie – Reproduction interdite sans autorisation préalable

III. Principes directeurs

L'appréciation des enjeux stratégiques de sécurité est réalisée en fonction de leurs impacts sur les valeurs essentielles :

- la garantie de disponibilité et de qualité du service public d'enseignement,
- la confiance des usagers dans leurs échanges avec l'administration,
- l'éducation à la citoyenneté,
- l'égalité des chances,
- l'engagement du vice-rectorat et de tous les acteurs concernés par notre mission d'enseignement à respecter les obligations légales,
- la protection des personnes et des biens,
- l'entretien de relations sociales de qualité,
- la participation des parents d'élèves à la vie scolaire,
- la protection des investissements de l'Etat,
- le respect des intérêts légitimes et justifiés des partenaires et fournisseurs,
- la préservation de l'environnement,
- la protection et la valorisation de l'image du ministère et du vice-rectorat de la Nouvelle-Calédonie,
- la protection du patrimoine historique et culturel du vice-rectorat de la Nouvelle-Calédonie,

Il est obligatoire de se doter de mesures de prévention et de protection adéquates et proportionnées à ces enjeux.

Leurs mise en œuvre, par des pratiques appropriées participent à la garantie de :

- la disponibilité des informations et des moyens de la traiter,
- l'intégrité des informations et des moyens de la traiter,
- la confidentialité des informations gérées,
- la preuve avec la traçabilité des moyens de traitement de l'information.

Propriété du vice-rectorat de la Nouvelle-Calédonie – Reproduction interdite sans autorisation préalable

IV. Les responsabilités

IV.1. La sécurité de l'information est une responsabilité essentielle du management.

- La responsabilité de la sécurité de l'information incombe au vice-recteur qui est l'autorité qualifiée pour la sécurité des systèmes d'information prévue dans l'instruction générale interministérielle 901 et l'instruction générale interministérielle 1300 approuvée par l'arrêté du 2 décembre 2011. Cette responsabilité ne peut être déléguée.

  Chaque responsable de structure opérationnelle est aussi responsable de la mise en application des exigences de sécurité définies dans la politique générale de sécurité du vice-rectorat de la Nouvelle-Calédonie et les référentiels associés.

IV.2. Chaque composante informationnelle et ressource du système d'information a « un propriétaire »

- On entend par composante informationnelle les données, informatiques ou non, les ressources et les applications informatiques qui traitent ou transportent de l'information.
- Le concept de propriétaire se comprend en termes de responsabilités, et non au sens de propriété juridique. Les chefs de service sont propriétaires de leurs données métier.
- Afin de contribuer à la préservation des valeurs essentielles du vice-rectorat, le besoin de sécurité afférent à chaque composant informationnel et informatique est clairement identifié en termes de disponibilité, d'intégrité, de confidentialité et de preuve.
- Il appartient à chaque acteur, créateur, propriétaire ou responsable de définir le besoin de sécurité inhérent à tout type d'information. Ces attributs de sensibilité déterminent une classification des composants.

IV.3. Chaque propriétaire connaît et maîtrise les risques des composants dont il a la charge

- Dans la conduite de tout projet, il est responsable de l'expression de besoin en matière de sécurité et de la vérification de la satisfaction de ceux-ci.
- Il est responsable de la définition du niveau de besoin de sécurité approprié et de l'identification des risques relatifs aux composants dont il a la charge.
- Il est responsable en conséquence de l'application des mesures de protection et de la conduite des plans de réduction des risques afférents.
- Il est en mesure de connaître, d'approuver ou de révoquer les droits accordés sur les composants dont il est propriétaire.
- Compte tenu du caractère fortement transverse de la sécurité de l'information, notamment dans la conception des plans de réduction de risque, une responsabilité opérationnelle transversale (le RSSI) est établie pour assister les propriétaires dans ces travaux.

IV.4. La sécurité dans la réalisation et l'exploitation des composants techniques est du ressort de la maîtrise d'œuvre informatique.

- La division des services informatiques (DSI) du vice-rectorat, en tant que maîtrise d'œuvre, est responsable de la détermination et de la mise en œuvre des dispositifs de sécurité concernant les ressources techniques nécessaires au support des composants informationnels. De ce fait, elle s'implique dans le processus de cartographie des risques conduit par les propriétaires des composants informationnels.

- Dans le cadre des cycles projet, elle est responsable de la réponse à l'expression de besoin sécurité exprimée par les propriétaires.
- Elle met en œuvre les plans de réduction de risques en collaboration avec les propriétaires des composants informationnels.

IV.5. La responsabilité individuelle : chaque intervenant, quel que soit sa fonction, est un acteur de la sécurité

La mise en œuvre de la politique de sécurité du vice-rectorat prend en compte le facteur humain. Il convient d'obtenir la participation active du personnel et en particulier de l'encadrement pour limiter les risques liés aux accidents ou à la malveillance.

La sécurité repose également sur le personnel et l'organisation. Elle nécessite un encadrement et un effort permanents.

- La mise en place de la sécurité de l'information est faite dans le respect des principes de confiance, d'autonomie et de responsabilité individuelle, inhérents aux missions du vice-rectorat.
- Chaque utilisateur ou intervenant sur le système d'information, qu'il soit personnel de l'Éducation nationale ou intervenant extérieur travaillant pour le compte du vice-rectorat, est responsable par son comportement prudent et respectueux des lois et des règles, de la protection des informations et des ressources associées.
- Ces principes s'accompagnent, tant pour la préservation des valeurs du vice-rectorat que pour la sécurisation des collaborateurs eux-mêmes, d'une attribution des droits aux intervenants adaptée au besoin des missions qui leurs sont confiées et à leur durée.

IV.6. Le devoir d'information sur les responsabilités individuelles

- Les responsabilités individuelles, leurs limites, les conditions d'usage des informations font l'objet d'une communication à chaque utilisateur et administrateur technique ou fonctionnel.
- Le vice-rectorat de la Nouvelle-Calédonie, direction générale des enseignements mobilise ses collaborateurs pour protéger son capital « information ». Il ne suffit pas de définir des mesures de protection techniquement sophistiquées, si les utilisateurs ne sont pas sensibilisés et formés sur les règles et l'importance de l'information qu'ils manipulent.
- Des campagnes de sensibilisation sont mises en œuvre de manière récurrente afin d'obtenir la participation complète et active de chacun des collaborateurs du vice-rectorat.

Propriété du vice-rectorat de la Nouvelle-Calédonie – Reproduction interdite sans autorisation préalable

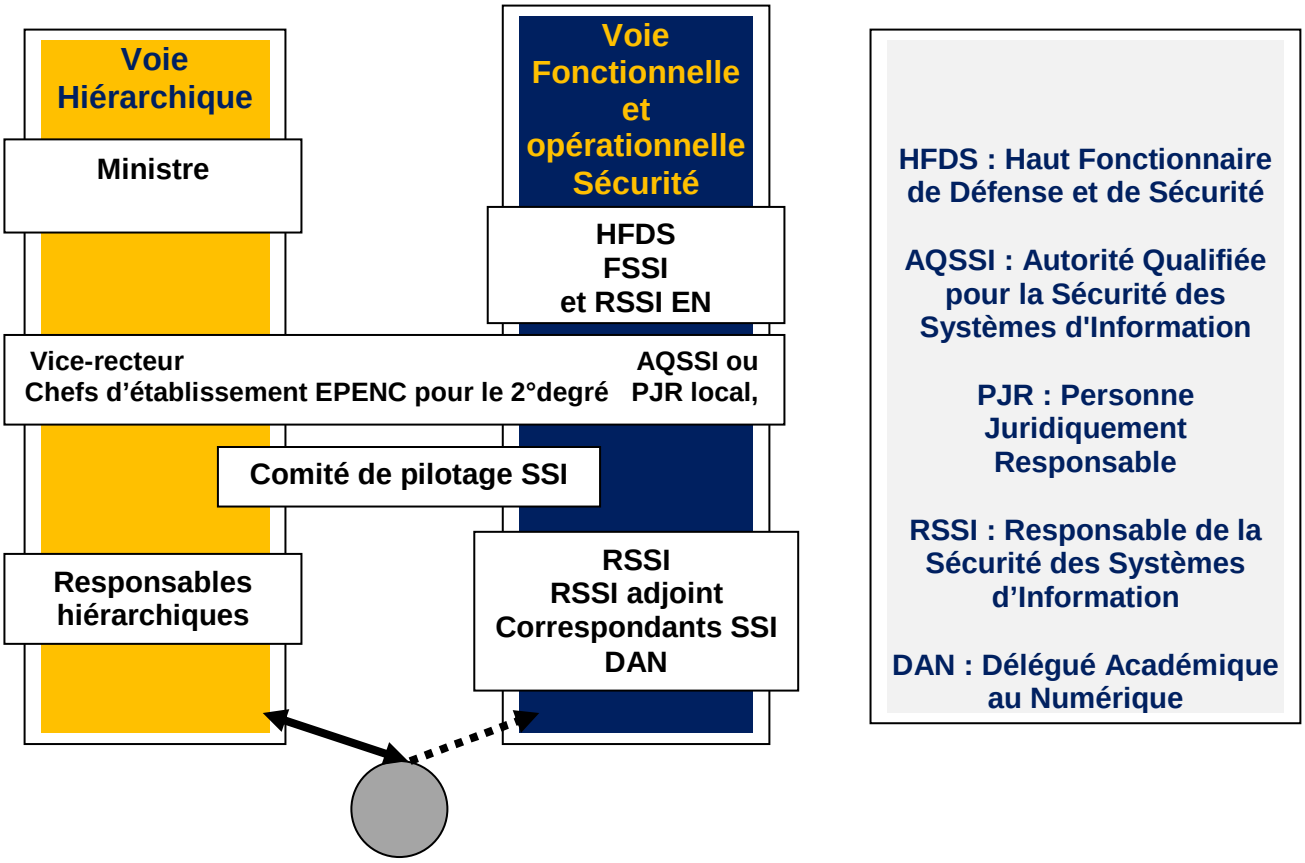
V. l'organisation

La définition et la mise en œuvre de la politique de sécurité des systèmes d'information s'appuient sur deux voies SSI qui coexistent et collaborent :

- une voie hiérarchique ;
- une voie fonctionnelle et opérationnelle de la SSI.

Ces voies se déclinent nationalement et académiquement et sont conformes à la directive interministérielle n° 901/DISSI/SCSSI du 2 mars 1994 portant sur la recommandation pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense et l'article 86 de l'instruction générale interministérielle 1300 sur la protection du secret de la défense nationale.

Figure 1 : Synoptique des chaînes fonctionnelle / opérationnelle SSI et hiérarchique



V.1. Rôles de la chaîne fonctionnelle et opérationnelle

V.1.1. Articulation avec la voie hiérarchique

La directive interministérielle N° 901/DISSI/SCSSI du 2 mars 1994 prescrit en particulier que : « Les autorités qualifiées pour la sécurité des systèmes d'information (AQSSI) sont les autorités responsables de la sécurité des systèmes d'information dans les administrations centrales et les services déconcentrés de l'État, ainsi que dans les établissements publics visés à l'article 3 et dans les organismes et entreprises ayant conclu avec l'administration des marchés ou des contrats visés par ce même article. Leur responsabilité ne peut pas se déléguer ».

Pour le niveau académique, conformément au schéma directeur de la sécurité des systèmes d'information, le vice-recteur est fonctionnellement désigné comme AQSSI.

À cet égard, le vice-recteur, en tant qu'AQSSI du vice-rectorat est chargé de :

- définir une politique de sécurité des systèmes d'information adaptée à sa structure et d'en fixer les objectifs ;
- s'assurer que les dispositions contractuelles et réglementaires sur la sécurité des systèmes d'information sont bien appliquées ;
- élaborer les consignes et les directives internes ;
- s'assurer que les contrôles internes de sécurité sont régulièrement effectués ;
- sensibiliser et organiser la formation du personnel aux questions de sécurité ;
- informer le fonctionnaire de sécurité des systèmes d'information (FSSI) auprès du haut fonctionnaire de défense et de sécurité (HFDS) des événements notables ayant compromis la sécurité des systèmes d'information ;

Dans le cadre du référentiel général de sécurité, le vice-recteur garantit que les systèmes d'information du vice-rectorat offrent un environnement de sécurité conforme aux exigences d'exploitation des télé services homologués.

Pour mener à bien cette politique de sécurité, il désigne et s'appuie sur un responsable de la sécurité des systèmes d'information (RSSI). Celui-ci assume du point de vue de la circulaire interministérielle N° 901/DISSI/SCSSI du 2 mars 1994 le rôle d'agent de sécurité des systèmes d'information (ASSI).

À ce titre, le RSSI assure la gestion et le suivi des moyens de sécurité des systèmes d'information se trouvant sur le ou les sites où s'exercent sa responsabilité.

Pour le niveau établissement, les personnels de direction des EPENC sont les personnes juridiquement responsables pour la sécurité des systèmes d'information de leur établissement.

À cet égard, les personnels de direction des EPENC sont chargés de :

- appliquer la politique de sécurité des systèmes d'information définie par le vice-recteur ;
- s'assurer que les dispositions contractuelles et réglementaires sur la sécurité des systèmes d'information sont bien appliquées ;
- élaborer les consignes et les directives internes ;
- s'assurer que les contrôles internes de sécurité sont régulièrement effectués ;
- sensibiliser et organiser la formation du personnel et des élèves aux questions de sécurité ;
- informer le RSSI du vice-rectorat de la Nouvelle-Calédonie, direction générale des enseignements des événements notables ayant compromis la sécurité des systèmes d'information.

Pour cela, les personnels de direction des EPENC s'appuient sur les techniciens et le correspondant sécurité des systèmes d'information de la DSI du vice-rectorat de la Nouvelle-Calédonie.

L'application des dispositions de protection des systèmes d'information relève de la responsabilité de cette chaîne fonctionnelle.

V.1.2. Rôle du RSSI dans la voie fonctionnelle et opérationnelle

Pour conduire la politique de sécurité des systèmes d'information et faciliter sa mise en œuvre, le RSSI s'appuie sur une chaîne opérationnelle interne spécialisée en SSI. Cette chaîne s'inscrit elle-même dans la chaîne opérationnelle animée par le RSSI de l'éducation nationale.

La chaîne opérationnelle de sécurité des SI du vice-rectorat est composée du RSSI, de son adjoint (agent de la DSI) et des correspondants de la sécurité des systèmes d'information.

En ce qui concerne les EPENC, les techniciens de la DSI du vice-rectorat sont fonctionnellement désignés comme OSSI.

Pour le niveau académique, le RSSI et le correspondant sécurité des systèmes d'information assistent le vice-recteur dans la définition de la politique de sécurité de systèmes d'information. Ils assurent sa mise en œuvre et son suivi conformément aux directives données par le vice-recteur.

En particulier, ils assurent les missions suivantes :

- le suivi de l'état de sécurité des unités du vice-rectorat (documents de PSSI, identification des OSSI, bilans de sécurité, appréciation des besoins…) ;
- suivi de la mise en œuvre des dispositions de SSI définies au niveau national,
- remontées des dysfonctionnements vers le FSSI et le RSSI de l'Éducation nationale ;
- contacts avec les responsables de la sécurité des systèmes d'information d'autres tutelles, notamment les collectivités territoriales ;
- conduite d'actions de formation et d'information à destination des différents acteurs;
- conseil et soutien à l'AQSSI, aux chefs de service et d'établissements ;
- participation aux exercices d'alerte et à la gestion de crise ;
- participation à des travaux menés au niveau national (groupes de travail, réunions de coordinations, actions de formation).

Pour le niveau local :

- les OSSI des équipes de proximité assistent les personnels de direction des établissements dans l'exercice de leurs missions.

VI. Principes méthodologiques

La politique générale de sécurité détermine les principes structurants, les moyens et procédures nécessaires et suffisants à garantir le niveau de protection attendu.

Les principes structurants de la politique générale de sécurité sont développés dans des documents complémentaires.

L'objectif est l'établissement progressif ainsi que le maintien à niveau de documents de référence :

- une politique de sécurité des systèmes d'information définissant les règles fonctionnelles,
- des plans de mise en œuvre pour décliner les règles fonctionnelles de la PSSI, découlant des principes structurants de la politique générale,
- des politiques techniques de sécurité,
- des procédures techniques et organisationnelles.

Dans la pratique, cet établissement et ce maintien à niveau sous entendent l'obligation de :

- formaliser les niveaux d'enjeux,
- déterminer, quantifier et qualifier les véritables risques courus,
- arbitrer les niveaux d'enjeux et de besoins, les risques, les mesures de sécurité en fonction des contraintes tant économiques qu'organisationnelles.
- suivre de façon périodique le niveau de sécurité atteint.

Pour ce faire, les principes méthodologiques retenus par le vice-rectorat sont présentés dans les paragraphes suivants.

VI.1. La démarche SSI : une amélioration continue

Le vice-rectorat de la Nouvelle-Calédonie met en œuvre une démarche d'amélioration continue qui répond non seulement aux exigences du référentiel général de sécurité mais aussi au souci de maintenir la qualité du service public. Cette démarche consiste à garantir une sécurité appropriée, continue et pérenne du « patrimoine informationnel » et des ressources système d'information. Elle prend en compte les évolutions permanentes :

- des enjeux et besoins,
- des menaces et des risques,
- des exigences de la PSSI de l'État et du RGS,
- des ressources humaines ou techniques,
- des usages.

Elle réévalue de manière continue :

- les niveaux de sécurité effective et adéquate,
- la politique de sécurité du système d'information.

VI.2. Les enjeux : répertoire des ressources

Un répertoire cartographique de l'ensemble des informations et ressources est établi et maintenu à jour. Ce répertoire comprend, pour chaque ressource, l'impact que peut entrainer un événement redouté sur les valeurs à préserver :

- une atteinte faiblement significative, significative, importante ou critique de la disponibilité des informations et des ressources associées ;

Propriété du vice-rectorat de la Nouvelle-Calédonie – Reproduction interdite sans autorisation préalable

- une atteinte faiblement significative, significative, importante, ou critique de l'intégrité des informations et des ressources associées ;
- une atteinte faiblement significative, significative, importante, ou catastrophique de la confidentialité des informations et des ressources associées ;
- une atteinte faiblement significative, significative, importante ou critique de la perte de preuve ou d'imputabilité des informations et des ressources associées.

VI.3. La formalisation des enjeux par les impacts

Afin de simplifier l'analyse des enjeux, l'évaluation des dommages consécutifs aux atteintes de perte de disponibilité, intégrité, confidentialité et preuve seront synthétisés selon cinq axes d'impacts :

- Éducatif,
- Social,
- Juridique,
- Image,
- Financier.

Les quatre niveaux d'atteinte potentielle, redoutés permettent de formaliser quatre niveaux de besoin.

Exemples de niveaux d'impacts

Niveaux d'impact	Éducatif / Opérationnel EO	Financier FI	Juridique* JR	Social/ Personne SP	Image/ Réputation IR
4 Majeur	Mauvaise affectation des élèves suite à un dysfonctionnement du SI	Le niveau d'impact doit être apprécié par la division financière	Condamnation et Interdiction de l'exploitation d'un système d'information par décision judiciaire	Mécontentement de tous les candidats à un concours national	Affectation de l'image dans un media national
3 Important	Accès internet indisponible pour tous les établissements	Le niveau d'impact doit être apprécié par la division financière	Mise en demeure par la CNIL pour non-respect des obligations légales	Mécontentement de quelques candidats à un concours national (ex : Capes)	Affectation de l'image dans un media local, suite à un retard de paiement des bourses aux familles
2 Significatif	Propagation d'un virus en établissement	Le niveau d'impact doit être apprécié par la division financière	Saisine par des usagers du tribunal administratif suite à une erreur sur un système d'information	Mécontentement de l'ensemble des candidats à un concours académique	Défiguration d'un site Web
1 Faible	Indisponibilité du poste de travail d'un enseignant ou d'un agent	Le niveau d'impact doit être apprécié par la division financière	Non-respect des dates fixées par la réglementation	Mécontentement de quelques candidats à un concours(ex : professeur des écoles)	Indisponibilité temporaire d'un site Web
0 Non significatif					

Pour chacun des critères, quatre niveaux de classification sont définis par ordre croissant de sensibilité, conformément au tableau ci-dessous.

IMPACT \ BESOIN		Traçabilité impossibilité de vérifier ou d'identifier, voire de prouver un événement	Disponibilité indisponibilité dans les délais requis pour l'exécution d'une opération	Intégrité modification erronée ou illicite	Confidentialité divulgation ou perte
4	Extrêmement grave mettant en danger une activité majeure du vice-rectorat	BESOIN STRATEGIQUE ou VITAL	BESOIN STRATEGIQUE ou VITAL	BESOIN STRATEGIQUE ou VITAL	SECRET
3	Grave ne compromettant pas une activité majeure du vice-rectorat	BESOIN CRITIQUE ou IMPORTANT	BESOIN CRITIQUE ou IMPORTANT	BESOIN CRITIQUE ou IMPORTANT	CONFIDENTIEL
2	Significatif sur les missions du vice-rectorat, d'une de ses entités, ou son image	BESOIN SENSIBLE	BESOIN SENSIBLE	BESOIN SENSIBLE	DIFFUSION RESTREINTE
1	Peu significatif pouvant générer une nuisance faible ou un peu gênante	BESOIN FAIBLE	BESOIN FAIBLE	BESOIN FAIBLE	DIFFUSION INTERNE
0	Impact non significatif	BESOIN NORMAL	BESOIN NORMAL	BESOIN NORMAL	PUBLIC

L'objectif de ce recueil et de ces estimations d'impact, effectués sous contrôle des directions métier de l'académie est de fournir une base « métier, orientée niveaux d'enjeux » à l'identification des risques techniques ou humains.

VI.4. Les besoins de sécurité, origine des plans de mesures

Les mesures de sécurité mises en œuvre par le vice-rectorat de la Nouvelle-Calédonie répondent aux besoins de sécurité analysés conformément aux enjeux. Les plans d'actions pour mettre en œuvre ces mesures tiennent compte des priorités définies pour les besoins.

Les besoins de sécurité sont de deux ordres :

1. Certains besoins sont considérés comme intangibles, à satisfaire indépendamment des enjeux exprimés. Ils correspondent au simple état de l'art, à la satisfaction d'exigences légales ou à une décision de principe du vice-rectorat de la Nouvelle-Calédonie.

2. Au-delà des exigences de sécurité « de base », l'analyse des enjeux fait apparaître des scénarios de risques spécifiques à certaines ressources et a priori non couverts par les exigences de sécurité de base. La détermination et la hiérarchisation de ces scénarios de risque conduisent à proposer des mesures de sécurité supplémentaires aux simples exigences.

Pour répondre à ces besoins, le vice-rectorat de la Nouvelle-Calédonie définit deux grandes priorités de gestion SSI :

- La première priorité concerne les exigences de sécurité intangibles.
- La deuxième priorité concerne les règles de sécurité relatives aux enjeux.

VII. Risques majeurs du vice-rectorat

Le ministère de l'éducation nationale a mené une analyse de risque sur trois académies afin d'identifier les principaux risques ayant un impact significatif sur les systèmes d'information académiques. Face à ces risques majeurs, il est nécessaire de définir les objectifs de sécurité pour limiter leurs impacts, sachant que le risque «zéro », n'existe pas.

L'importance des données à caractère personnel et des budgets que gère le vice-rectorat ainsi que la sensibilité d'un grand nombre d'opérations de gestion reposant sur son système d'information confèrent un caractère stratégique à la protection de ces données et des processus informatiques.

Le vice-rectorat considère que les atteintes à ces derniers peuvent avoir des conséquences intolérables sur le plan humain, sur la bonne exécution de ses missions, sur le plan financier où sur l'image de l'institution elle-même. L'attractivité que peuvent revêtir certaines données, voire certains processus ajoutent aux risques encourus.

Voici les principaux risques identifiés :

- **perte des moyens de télécommunication** : suite à la défaillance de l'accès Internet, les applications nationales accédées par le grand public ou les enseignants (Web services) ne sont plus accessibles ;
- **saturation du système informatique** : un attaquant ou un groupe d'attaquants réalise un déluge de requêtes fictives sur un serveur d'inscription à un concours, empêchant les candidats de s'inscrire ;
- **abus de droit** : un membre du personnel profite de ses droits d'accès aux applications, par exemple sur la gestion des affectations, pour modifier les données d'un personnel dans le but soit de le favoriser soit de le desservir ;
- **information sans garantie d'origine** : un membre du personnel d'une académie reçoit par messagerie électronique une demande de renseignement (ex : sur une orientation, une affectation), par un individu se faisant passer pour la personne concernée ;
- **piégeage du logiciel** : un portable infecté par un virus informatique est connecté au réseau interne du vice-rectorat (vice-rectorat, EPENC, CIO, SELCK, …) et s'y propage.

Les processus de gestion suivants sont particulièrement sensibles :

- **processus des examens et concours ;**
- **processus de la scolarité (notamment dans son volet affectation) ;**
- **processus de gestion des ressources humaines pour les volets paye et les bases de gestion de personnels.**

La criticité des éléments de support technique reflète pour sa part l'emploi systématisé de la messagerie tant en terme de communication interne qu'externe.

VIII. Objectifs principaux de sécurité du vice-rectorat

Afin de faire face aux risques identifiés, le vice-rectorat s'est fixé un ensemble d'objectifs de sécurité. Ces objectifs de sécurité ont pour finalité de couvrir les risques et sont à la base des règles de sécurité qui seront appliquées par le vice-rectorat pour protéger les éléments essentiels de son système d'information.

La sécurité du système d'information prend en compte le contexte fonctionnel et organisationnel du vice-rectorat. Elle revêt donc un caractère stratégique car elle a comme finalités de :

- protéger les données à caractère personnel des élèves et des personnels ;
- généraliser l'utilisation des technologies de l'information dans le cadre de l'administration électronique ;
- assurer la confiance en celles-ci ;
- contribuer à l'image de marque de l'établissement ;
- être en conformité avec la réglementation ;
- maîtriser les risques et lutter contre la malveillance informatique.

Pour cela, le vice-rectorat se fixe un ensemble d'objectifs de sécurité dont les principaux sont précisés ci-après :

- toute malveillance ou négligence pesant sur les applications sensibles ainsi que sur les systèmes les hébergeant doit être détectée. Pour tout système, il doit être possible de détecter en temps réel ou a posteriori un comportement anormal, de retracer les opérations réalisées et d'identifier les auteurs ;
- les traces des opérations doivent être exploitables y compris si elles sont générées par des systèmes différents ;
- il doit exister une gestion active des habilitations au sein des systèmes pour le traitement des informations en fonction des besoins d'accès et de modification ;
- il doit être possible de restaurer tout ou une partie d'un système, d'une application, d'un ensemble de données et d'une trace en cas de sinistre, de panne ou de négligence ;
- l'organisation doit protéger les équipements et supports contre l'accès physique par des personnes non autorisées. Elle intègre une politique préventive contre la saturation et les pannes des équipements (informatiques, climatisation, énergie, communication) ;
- la politique anti-virus doit empêcher l'introduction et la diffusion dans les systèmes de tout code malveillant ;
- le personnel doit adhérer à la démarche sécurité et les rôles et responsabilités doivent être clairement identifiés et connus de chacun. Les personnels ayant accès à des informations sensibles doivent être sensibilisés et identifiés.

Propriété du vice-rectorat de la Nouvelle-Calédonie – Reproduction interdite sans autorisation préalable

IX. Politique de Sécurité des Systèmes d'Information (PSSI)

La sécurité du système d'information nécessite la définition d'une politique de sécurité des systèmes d'information, conçue à partir des éléments stratégiques, structurants et formalisés dans la PGS.

La politique de sécurité est un cadre de référence qui définit et organise les meilleures pratiques à retenir et à appliquer en matière de sécurité des systèmes d'information.

La politique de sécurité des systèmes d'information est définie de la manière suivante :
« L'ensemble des lois, règlements et pratiques qui régissent la façon de gérer, protéger et diffuser les biens, en particulier les informations sensibles, au sein d'une académie et lors de ses communications avec d'autres systèmes d'information ».

Elle est conforme à la politique de sécurité des systèmes d'information de l'Etat (circulaire N° 5725/SG du premier ministre du 17 Juillet 2014).

La PSSI relève d'une vision stratégique au vice-rectorat de la Nouvelle-Calédonie et traduit un engagement fort du vice-recteur. 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 partenaires (provinces).

Au sein des EPENC, il n'est pas nécessaire de décliner la PSSI en cas de strict respect des préconisations du vice-rectorat. La déclinaison au sein des EPENC pour prendre en compte des particularités propres, est envisageable sous condition de conformité avec les préconisations du vice-rectorat. La mise en œuvre d'une PSSI propre devra faire l'objet d'une communication au RSSI du vice-rectorat.

Propriété du vice-rectorat de la Nouvelle-Calédonie – Reproduction interdite sans autorisation préalable

X. Politique de Sécurité des Systèmes d'Information en établissement

La définition et l'application de la politique de sécurité des systèmes d'information doivent tenir compte de la situation du statut des établissements scolaires (collèges et lycées) en EPENC. Cf. délibération n°77 du 28 septembre 2015 relative aux EPENC.

La politique de sécurité des systèmes d'information d'un EPENC doit être conforme à la politique de sécurité des systèmes d'information du vice-rectorat définie par le vice-recteur. En cas de stricte observance de la PSSI du vice-rectorat, l'EPENC n'a aucune obligation de décliner formellement une PSSI.

Toutefois en cas de besoins spécifiques, l'établissement peut décliner sa propre PSSI sous condition de conformité avec les préconisations du vice-rectorat.
Cette PSSI peut toutefois être commune à plusieurs unités relevant d'un cadre commun partageant les mêmes structures. Inversement, dans le cas de cités scolaires 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.
La mise en place d'une PSSI fournit à l'EPENC une approche méthodique et systématique pour garantir une sécurité homogène de son système d'information.
À partir de la PSSI du vice-rectorat, l'EPENC définit sa propre PSSI adaptée à ses besoins internes. Celle-ci doit intégrer les politiques nationales et académiques, tutelle principale en matière de SSI, ainsi que celle de la collectivité territoriale de rattachement.
L'élaboration d'une PSSI spécifique à une EPENC résulte d'un dialogue entre les différents acteurs du système d'information : instances décisionnelles, responsables d'équipes pédagogiques administratives de l'EPLE, coordinateurs TICE, intervenants extérieurs, prestataires de services.
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'établissement peut ou doit investir dans la sécurisation de son SI.

La PSSI d'un EPENC relève de l'initiative du chef d'établissement en sa qualité de PJR.
Une fois validée en conseil d'administration, la PSSI doit être transmise au RSSI qui vérifiera la conformité de ce document avec les politiques nationales et académiques, notamment pour ce qui concerne la protection du cercle de confiance RACINE. Il pourra, le cas échéant, effectuer un audit technique du site concerné.

Propriété du vice-rectorat de la Nouvelle-Calédonie – Reproduction interdite sans autorisation préalable

XI. Application de la PSSI au sein d'un EPENC

XI.1. Principe général

L'application de la politique de sécurité des systèmes d'information doit tenir compte du statut des EPENC.

Le RSSI assure une coordination académique avec les RSSI des collectivités et leur responsable de la sécurité s'il existe. En l'absence de dispositions contractuelles formelles, les présents principes de coordination doivent guider les relations entre le MEN et les autres tutelles.

Le chef d'établissement, en sa qualité d'AQSSI, a la charge d'arrêter la politique de SSI dans son unité. Celle-ci doit être conforme à la présente politique académique de la SSI, mais le strict respect des préconisations académiques en matière d'infrastructures le dispense de la formaliser.

Le système d'information de l'EPENC fait partie du système d'information du ministère de l'Éducation nationale. Si une PSSI spécifique est adoptée, elle satisfera notamment les points suivants :

- la priorité donnée à la préservation des accès au système d'information du ministère de l'Éducation nationale (administration, gestion...) ;
- l'articulation interne au ministère de l'Éducation nationale des responsabilités opérationnelles et fonctionnelles en matière de SSI et en particulier la responsabilité du chef d'établissement.

XI.2. En cas d'incident

Les incidents sur le système d'information de l'établissement doivent remonter par la voie fonctionnelle de la tutelle principale, 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 un EPENC, il y a lieu d'informer le RSSI près du vice-recteur qui appréciera l'opportunité de convoquer la cellule de crise académique et, si nécessaire, de saisir la cellule nationale.

Inversement, l'EPENC sera informé par la chaîne hiérarchique de l'académie et par la chaîne opérationnelle SSI 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'académie par le vice-recteur, le RSSI et les responsables informatiques concernés.

XI.3. En cas de litige

Les éventuelles divergences sont à traiter au niveau du comité de pilotage, de la coordination locale, voire du vice-recteur ; les éventuels arbitrages sont à soumettre à la voie fonctionnelle SSI (vice-recteur, RSSI national, FSSI, HFDS).

XII. Gestion d'incidents

XII.1. Principe général

Les incidents sur le système d'information remontent par la voie fonctionnelle, 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, il y a lieu d'informer le RSSI du vice-rectorat de la Nouvelle-Calédonie qui appréciera l'opportunité de convoquer la cellule de crise académique et, si nécessaire, de saisir la cellule nationale.
La mise en œuvre des plans de posture (VIGIPIRATE) ou d'intervention (PIRANET) est déclinée au sein du vice-rectorat de la Nouvelle-Calédonie par le vice-recteur, le RSSI et les responsables informatiques concernés.

XII.2. Procédure de gestion d'incidents

Une procédure de gestion des incidents est diffusée sur le site du vice-rectorat. Elle donne aux administrateurs, aux OSSI les directives nécessaires pour réagir à bon escient et transmettre l'information.
Le signalement des incidents à la chaîne opérationnelle devrait être systématique. Il convient de prévenir les incidents SSI à l'adresse de courriel ci-dessous :

incident-ssi@ac-noumea.nc

L'information des autorités hiérarchiques et du RSSI (et de son adjoint) est obligatoire lorsque l'incident peut mettre en cause l'entité dans son fonctionnement, sa sécurité, sa discipline interne, son image. Elle est impérative si l'incident est susceptible d'implications juridiques.

L'opportunité d'une information directe du FSSI près du HFDS est appréciée au regard de la gravité de l'incident et/ou du caractère sensible de l'entité concernée. Elle relève de l'appréciation du RSSI national.

Il appartient à l'EPENC d'informer la collectivité territoriale de rattachement et le cas échéant de se concerter avec celle-ci.
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 sont considérés comme des incidents de SSI et traités selon le même principe.

XII.3. En cas de litige

Les éventuelles divergences sont traitées par le comité de pilotage. Les éventuels arbitrages sont soumis à la voie fonctionnelle et opérationnelle de la SSI (vice-recteur, RSSI national, FSSI, HFDS).

Propriété du vice-rectorat de la Nouvelle-Calédonie – Reproduction interdite sans autorisation préalable

XIII. Glossaire

Sigle / terme / abréviation	Designation
API (RACINE)	Accès postes isolés
AQSSI	Autorité qualifiée pour la Sécurité des Systèmes d'Information
Audit	Examen méthodique d'une situation relative à un produit, un processus ou une organisation, et des enregistrements qui ont été réalisés à cet effet, en vue de vérifier la conformité, passée et présente, de cette situation aux dispositions préétablies, et l'adéquation de ces dernières à l'objectif recherché (selon plusieurs définitions International Standard Organization).
Besoin	Identification des informations et des traitements de l'information sensibles, associée à l'expression des enjeux relatifs à leur protection en termes de disponibilité, intégrité, confidentialité et authenticité.
Classification	Détermination qu'une information ou qu'une ressource nécessite, dans l'intérêt de l'entité, un niveau spécifique de protection contre la divulgation, l'altération, la destruction ou la perte de preuve.
Confidentialité	Caractère réservé d'une information, dont l'accès est limité aux personnes, entités ou processus autorisés à la connaître ou à y avoir accès. Propriété d'une information qui n'est pas rendue disponible ni divulguée à des personnes, entités ou processus non autorisés. (ISO 7498-2).
Critères d'évaluation	Au sein du vice-rectorat, les critères d'évaluation de la sensibilité et donc de classification sont la Disponibilité, l'Intégrité, la Confidentialité et la Preuve.
Disponibilité	Propriété d'une information d'être accessible et utilisable à la demande, pour une entité ou un processus autorisés. (ISO 7498-2). Propriété d'un système, d'un matériel ou d'un logiciel, d'être apte à remplir ses fonctions dans des conditions définies d'horaires, de délais et de performances.
CIO	Centre d'Information et d'Orientation
EPENC	Etablissement Public d'Enseignement de la Nouvelle-Calédonie
EPLE	Établissement Public Local d'enseignement
FSD	Fonctionnaire Sécurité de Défense
IA	Inspecteur d'Académie
FSSI	Fonctionnaire à la Sécurité de Système d'Information
HFDS	Haut fonctionnaire de Défense et de Sécurité
IA IPR	Inspecteur d'Académie – Inspecteur Pédagogique Régional
IEN	Inspecteur Éducation Nationale
MEN	Ministère de l'Éducation Nationale
Menaces	Action ou évènement pouvant porter préjudice à la SSI. Généralement les actions considérées sont le fait d'attaquants, dont la motivation et les capacités doivent être évalués. Elles comprennent : le vol de supports ou de documents, l'atteinte à la disponibilité des systèmes, les écoutes, etc. Les évènements considérés sont généralement le résultat d'incidents, dont la probabilité d'occurrence et la gravité doivent être évaluées. Les incidents comprennent : l'incendie, les pollutions, les pannes ou destructions matérielles, etc.
O S S I	Opérateur de Sécurité des Systèmes d'Information
Patrimoine Informationnel	Ensemble des acteurs, des composants techniques, supports et informations propriétés du vice-rectorat ou qui lui sont confiés
P G S I	Politique Générale de Sécurité de l'Information
P S I	Politique Sécurité de l'Information
PJ R	Personne Juridiquement Responsable
P S S I	Politique de Sécurité des Systèmes d'Information ou Référentiel

RACINE	Réseau d'Accès et de Consolidation des Intranets Éducation
RENATER	Réseau National de Technologie de l'Enseignement et de la Recherche
Risque	Présence d'une vulnérabilité de sécurité, pouvant être exploitée pour la réalisation potentielle d'une menace et ayant un impact sur les enjeux relatifs aux activités de l'organisation concernée. Les enjeux impactés et la potentialité de la menace donnent une mesure du risque. La potentialité de la menace dépend de la facilité d'exploitation de la vulnérabilité et de la motivation de l'attaquant (ou probabilité d'occurrence de l'incident).
Sensibilité d'une information ou d'une ressource	Valeur attribuée à une information ou à une ressource (agent, système, matériel, logiciel, etc.) pour chacun des critères de Disponibilité, Intégrité, Confidentialité et Preuve, par sa classification.
Système d'Information	Ensemble des moyens destinés à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information
RSSI	Responsable de la Sécurité des Systèmes d'Information, Sécurité de l'Information
TICE	Technologies de l'information et de la communication pour l'enseignement
Traçabilité	Propriété d'une information de pouvoir être un élément de trace, voire de preuve de traitements effectués ou d'occurrence d'événements.
Trace	Données archivées et informations disponibles pour audit, afin de détecter une faille de sécurité ou de prouver que les procédures de sécurité ont été suivies correctement et intégralement
Vulnérabilité	Une vulnérabilité est une faiblesse du système d'information qui peut être exploitée pour la réalisation d'une menace.