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

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 du système d'information par les personnels du vice-rectorat de la Nouvelle-Calédonie
Charte des administrateurs du vice-rectorat de la Nouvelle-Calédonie.
PGS 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 de sécurité des systèmes d'information (PSSI) de l'académie de Caen
Gestion de crise pour les RSSI

SOMMAIRE

I. Préambule

Ce document constitue la politique de sécurité système d'information pour le vice-rectorat de la Nouvelle-Calédonie. Cette politique de SSI est conforme et consécutive à la PSSI de l'Etat. Elle est adaptée à l'organisation, aux enjeux, aux besoins, aux menaces et aux risques du vice-rectorat de la Nouvelle-Calédonie, direction générale des enseignements.

I.1. Champ d'application de la PSSI au vice-rectorat de la Nouvelle-Calédonie, direction générale des enseignements

Conformément à la politique générale de sécurité de l 'information du vice-rectorat, le champ d'application de la PSSI du vice-rectorat de la Nouvelle-Calédonie se décompose en plusieurs périmètres fonctionnels :

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

La PSSI du vice-rectorat s'appuie et intègre les exigences de :

- 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 se conforme pour le bon fonctionnement des environnements numériques de travail (ENT), des télés services, du réseau d'accès et de consolidation des intranets de l'Éducation nationale ou réseau RACINE,
- les obligations légales.

Enfin, elle tient compte des systèmes d'information propres aux différents sites du vice-rectorat.

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

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 territoriales afin que celles-ci puissent d'une part assumer leurs compétences sur les espaces numériques de travail ainsi que l'entretien et la maintenance des infrastructures en EPENC (Loi sur la refondation de l'école – Loi Peillon) et, d'autre part, gérer les droits pour les élèves ou leur famille relatifs à l'action sociale.

La protection des informations, données et systèmes d'information requiert la mobilisation de tous les acteurs du vice-rectorat de la Nouvelle-Calédonie et le concours de ses partenaires et fournisseurs.

Conformément aux exigences de la politique système d'information de l'Etat du RGS (référentiel général de sécurité), la politique de sécurité du système d'Information (PSSI) du vice-rectorat prend en compte :

- tous les aspects qui peuvent avoir une influence sur la protection des moyens de traitement des données numériques tant d'un point de vue technique (matériels, logiciels, réseaux, etc.) que non technique (organisations, infrastructure, personnel, etc.) ;
- tous les risques et menaces, d'origine humaine ou naturelle, accidentelle ou délibérée qui peuvent provoquer des pertes de disponibilité, d'intégrité ou de confidentialité des informations, des données et des systèmes d'information associés ;
- l'intégration de la protection des données numériques tout au long du cycle de vie des systèmes d'information (depuis l'étude d'opportunité jusqu'à la fin de vie du système).

Le champ d'application de la PSSI du vice-rectorat de la Nouvelle-Calédonie couvre :

- les moyens (matériels, logiciels et structurels) assurant la mise en état opérationnel du système d'information du vice-rectorat de la Nouvelle-Calédonie ;

- les agents du vice-rectorat de la Nouvelle-Calédonie, en qualité d'utilisateurs ou d'informaticiens, quels que soient leurs secteurs d'activité ;
- les partenaires, fournisseurs et intervenants externes ayant accès aux données et systèmes numériques du vice-rectorat de la Nouvelle-Calédonie ou devant se connecter au système d'information (SI) du vice-rectorat de la Nouvelle-Calédonie, ou hébergeant ou gérant des ressources, systèmes ou données du vice-rectorat de la Nouvelle-Calédonie ;
- les utilisateurs des télés services.

En outre, ne sont pas inclus dans le périmètre de cette politique :

La protection des systèmes numériques personnels des agents de l'académie dès lors qu'ils ne sont pas connectés au système d'information ou qu'ils ne permettent pas de traiter des données numériques placées sous la responsabilité du vice-rectorat de la Nouvelle-Calédonie ;

La protection des systèmes numériques personnels des partenaires de l'académie dès lors qu'ils ne sont pas connectés au système d'information ou qu'ils ne permettent pas de traiter des données numériques traitées placées sous la responsabilité du vice-rectorat de la Nouvelle-Calédonie ;

La politique de sécurité du système d'information (PSSI) concerne l'ensemble des entités utilisatrices, ou chargées de la conception, du développement, de l'exploitation des données et des systèmes numériques. Les pratiques qui en découlent prennent en compte les spécificités des différents métiers, notamment aux plans réglementaire et technique.

I.2. Cible de sécurité en terme de maturité

Le niveau de sécurité que le vice-rectorat vise à mettre en œuvre s'appuie sur l'utilisation des recommandations de l'ANSSI (agence nationale de la sécurité des systèmes d'information – France) qui propose une démarche intitulé « Maturité SSI ».

La sécurité des systèmes d'information doit être gérée en adéquation avec ses enjeux spécifiques SSI.

Au regard des enjeux de sécurité pour le vice-rectorat de la Nouvelle-Calédonie, le niveau cible de maturité à atteindre est 4 (processus contrôlé) sur l'échelle de 6 présentée par l'ANSSI.

La cible de niveau 4 signifie que le vice-rectorat de la Nouvelle-Calédonie doit mettre en œuvre :

- **la gouvernance** adaptée permettant de prendre les décisions au niveau adéquat de responsabilité et de responsabiliser tous les acteurs en matière de sécurité des données et des systèmes numériques ;
- **la définition des objectifs opérationnels** de sécurité en adéquation avec les risques identifiés (méthode d'appréciation des risques à définir et à formaliser avec le chef de projet des risques opérationnels) ;
- **la formalisation de documents guides et manuels techniques** spécifiques de sécurité et des procédures associées ;
- **une démarche incluant des contrôles permanents** en vue d'améliorer les dispositifs opérationnels (tableaux de bord, audits de contrôle, revue documentaire, appréciation régulière des risques, …) ;
- **les recommandations émises dans les normes ISO 27001 et ISO 27002** qui introduisent un processus d'amélioration continue et des bonnes pratiques en matière de SSI et qui font références dans le domaine. A noter que l'usage de ces normes est imposé par l'ANSSI dans le cadre du RGS ;
- **les règles structurantes de la politique de sécurité système d'information de l'Etat.**

La PSSI décrit les directives et les règles qui permettent au vice-rectorat de la Nouvelle-Calédonie de répondre à l'objectif défini et prend en compte les risques à apprécier notamment en conformité avec l'obligation qui incombe à l'organisme au titre de l'article 3 du décret « RGS » n° 2010-112 du 2 février 2010.

I.3. Une logique d'amélioration continue :

L'amélioration continue de la politique de sécurité et de la performance globale du dispositif de gouvernance de la sécurité système d'information est un objectif en soi.
Elle est fondée sur l'analyse de son efficience ainsi que des modalités de traitement des risques liés aux SI.

Parmi les sources permettant d'appréhender les axes d'amélioration figurent :

- les évolutions des standards ;
- l'évolution des textes règlementaires ;
- l'apparition de nouveaux enjeux pour le vice-rectorat de la Nouvelle-Calédonie ;

- l'apparition de nouvelles menaces, vulnérabilités ou risques ;
- les résultats des audits et contrôles périodiques et permanents et les indicateurs liés au suivi des dysfonctionnements majeurs de sécurité (incidents de sécurité, cas graves de non-respect de la PSSI, ...).

I.4. Structure du référentiel documentaire SSI du vice-rectorat

La politique sécurité système d'information du vice-rectorat de la Nouvelle-Calédonie constitue un des composants du référentiel documentaire sécurité des systèmes d'information du vice-rectorat de la Nouvelle-Calédonie.

Le référentiel SSI de l'académie est structuré selon le schéma d'ensemble ci-dessous.

Référentiel documentaire SSI du vice-rectorat de la Nouvelle-Calédonie		
Population plus particulièrement ciblée	**Document**	**Objectifs et orientations**
Signée par l'AQSSI, concerne tous les utilisateurs du SI	**La charte éthique pour la SSI**	**« Démontre » l'engagement de la direction.** **Synthèse de l'orientation stratégique et organisationnelle**
Le management et plus particulièrement les divisions métiers	**La politique générale de sécurité système d'Information**	**Orientation stratégique et organisationnelle**
Le management, les représentants des maitrises d'ouvrage, la DSI et l'équipe SSI	**La politique de sécurité système d'information**	**Orientation fonctionnelle définissant les grands principes à respecter**
Les administrateurs de SI	**La charte administrateurs**	**Orientation règlementaire et comportementale**
Les utilisateurs du SI	**La charte utilisateurs**	**Orientation règlementaire et comportementale**
Les techniciens du SI	**Les guides et manuels SSI**	**Orientation technique**

La politique de sécurité système d 'information du vice-rectorat de la Nouvelle-Calédonie est une étape entre :

- d'une part la charte éthique pour la sécurité système d'information et la politique générale de sécurité qui décrivent les grandes orientations dans ce domaine et,
- d'autre part les plans d'action et le fonctionnement opérationnel, (chartes et guides et manuels).

I.5. La charte éthique pour la SSI et la politique générale de sécurité SI

La charte éthique pour la sécurité des systèmes d'information et la politique générale de sécurité des systèmes d'information décrivent l'ensemble des principes fondateurs et structurants gouvernant la définition des moyens réglementaires, organisationnels ou techniques à mettre en œuvre.

Elles sont des instruments de cohérence pour l'ensemble du vice-rectorat de la Nouvelle-Calédonie.

Ces documents à orientation stratégique s'arrêtent, 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.

Ils sont des éléments stables, structurants et permanents du vice-rectorat de la Nouvelle-Calédonie.

Ils sont proposés par le RSSI, validés par le DSI et approuvés par l'AQSSI.

I.6. La politique de sécurité des systèmes d'information

La PSSI traduit la politique de protection :

- dans différents domaines d'action, fonction de cibles particulières que sont les types d'acteurs à qui sont destinés les messages et règles à respecter,
- dans un contexte donné caractérisé par les types d'activité du vice-rectorat de la Nouvelle-Calédonie, par les technologies disponibles et les systèmes d'information employés, par le cadre réglementaire en vigueur, etc.,
- en décrivant les règles fonctionnelles à mettre en œuvre.

La PSSI est ainsi plus détaillée et sert de base à l'élaboration de plans d'action, au fonctionnement opérationnel de la SSI au vice-rectorat de la Nouvelle-Calédonie et à la conduite d'audit de contrôle.

Elle regroupe, sous la forme d'un ensemble de directives, les règles fonctionnelles standards qui doivent impérativement être mises en application pour garantir, de manière cohérente et efficace, la protection des systèmes d'information du vice-rectorat de la Nouvelle-Calédonie pour l'ensemble des missions « gestion » et « pédagogie ».

Ces règles sont conçues et maintenues en tenant compte de l'état de l'art de la sécurité des systèmes d'information (SSI) pour chacun des domaines traités et intègrent :

- les objectifs, directives et règles définis dans la PSSI de l'Etat,
- les recommandations émanant des instances de référence en la matière, (Agence Nationale Sécurité Système d'Information),
- les exigences liées aux normes de sécurité, ISO 2700x, …

Ces directives et règles sont validées par le DSI après consultation éventuelle des parties prenantes (division des personnels, cellule juridique, divisions métiers, …), portées par le RSSI, puis diffusées à l'ensemble des services concernés pour mise en œuvre.

Le non-respect des directives et des règles doit être soumis à un processus dérogatoire, présenté dans la directive Organisation et gouvernance.

I.6.1. Rappel des grands principes stratégiques à décliner dans la PSSI

La politique de sécurité des systèmes d'information du vice-rectorat de la Nouvelle-Calédonie doit contribuer à la protection des valeurs essentielles formalisées dans la politique générale de sécurité de l'information :

- la garantie de disponibilité et de qualité du service public d'enseignement ;
- l'éducation à la citoyenneté ;
- l'égalité des chances ;
- l'engagement du vice-rectorat de la Nouvelle-Calédonie 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.

La protection de ces valeurs essentielles est mise en cohérence avec dix les principes stratégiques définis dans la PSSI de l'Etat :

Les dix principes stratégiques

P1	**Lorsque la maîtrise des SI l'exige, l'administration fait appel à des opérateurs de confiance.**
P2	**Tout SI de l'Etat doit faire l'objet d'une analyse de risques adaptée aux enjeux, dans une démarche d'amélioration continue.**
P3	**Les moyens financiers et humains consacrés à la SSI doivent être planifiés, quantifiés et identifiés.**
P4	**Des moyens d'authentification forte des agents doivent être mis en place. L'usage de la carte à puce doit être privilégié.**
P5	**Les opérations de gestion et d'administration des SI de l'état doivent tracées et contrôlées.**
P6	**La protection des SI doit être assurée par l'application de règles précises. Ces règles font l'objet de la PSSI du vice-rectorat et sont consécutives à la PSSI de l'Etat.**
P7	**Chaque agent de l'Etat doit être informé de ses droits et devoirs et formé et sensibilisé à la cyber sécurité. Les mesures doivent être connues de tous.**
P8	**Les administrateurs de SI doivent appliquer après formation les règles élémentaires d'hygiène informatique.**
P9	**Les produits et services acquis par les administrations doivent faire l'objet d'une évaluation et d'une attestation préalable de leur niveau de sécurité.**
P10	**Les informations considérées comme sensibles en raison de leurs besoins en confidentialité, intégrité, traçabilité ou disponibilité sont hébergées sur le territoire national.**

I.7. Les chartes, guides et manuels

Les chartes, guides et manuels définissent concrètement les comportements à respecter ou les paramétrages d'implémentation consécutifs aux règles fonctionnelles de la politique de sécurité des systèmes d'information du vice-rectorat de la Nouvelle-Calédonie de Nouvelle-Calédonie.

Ces documents de « support » ou « d'opportunité » (guides méthodologique, bonnes pratiques, préconisations, guides et procédures de mises en œuvre et configurations …) favorisent :

- un déploiement cohérent des dispositifs de sécurité ;
- une administration, une surveillance, un contrôle et une utilisation conformes des dispositifs du SI ;
- les bons comportements généraux complémentaires à l'utilisation du SI et une optimisation des coûts.

I.8. Les rôles et responsabilités en matière du SI

La non application de la politique de sécurité du système d'information (PSSI) constitue une menace pour :

- le bon fonctionnement du vice-rectorat de la Nouvelle-Calédonie ;
- la protection de ses valeurs essentielles ;
- le respect des principes stratégiques définis dans la PSSI de l'Etat ;
- pour la qualité des services rendus aux usagers.

A ce titre, la responsabilité du vice-rectorat de la Nouvelle-Calédonie peut être engagée. Le délégataire de cette responsabilité est le vice-recteur.

En conséquence, des moyens organisationnels et des règles doivent être mis en œuvre pour s'assurer du respect des objectifs de sécurité et des procédures opérationnelles qui en découlent. Cette organisation s'applique à l'ensemble des divisions du vice-rectorat de la Nouvelle-Calédonie.

II. Introduction

La PSSI du vice-rectorat de la Nouvelle-Calédonie concerne l'ensemble :

- des personnes physiques (divisions, cadres fonctionnels, personnels techniques, utilisateurs, sous-traitants, … ;
- des personnes morales (du vice-rectorat de la Nouvelle-Calédonie, partenaires, sous-traitants, …)

Les 10 principes stratégiques à la base de la PSSI de l'Etat et repris dans la PSSI du vice-rectorat de la Nouvelle-Calédonie sont traduits en 13 familles d'objectifs à atteindre.

Chaque famille d'objectifs fait l'objet d'une directive formalisant les règles à respecter.

Liste des directives	Chapitre de la PSSI du vice-rectorat	Objectifs
1. Politique, organisation, gouvernance	**3**	• Mettre en place une organisation adéquate, garantissant la prise en compte préventive et réactive de la sécurité
2. Ressources humaines	**4**	• Faire des personnes les maillons forts des SI du vice-rectorat de la Nouvelle-Calédonie.
3. Gestion des biens	**5**	• Tenir à jour une cartographie détaillée et complète des SI. • Qualifier l'information de façon à adapter les mesures de protection.
4. Intégration de la SSI dans le cycle de vie des SI	**6**	• Apprécier, traiter et communiquer sur les risques relatifs à la sécurité des SI.
5. Sécurité physique	**7**	• Inscrire la sécurisation physique des SI dans la sécurisation physique des locaux et dans les processus associés. • Dimensionner les protections physiques des centres informatiques en fonction des enjeux liés à la concentration des moyens et données abritées. • Dimensionner les protections physiques des centres informatiques en fonction des enjeux liés à la concentration des moyens et données abritées.
6. Sécurité des réseaux	**8**	• Utiliser les infrastructures nationales, en respectant les règles de sécurité qui leurs sont attachées. • Maîtriser les interconnexions de réseaux locaux • Configurer de manière adéquate les équipements de réseaux actifs. • Ne pas porter atteinte à la sécurité du SI par le déploiement d'accès non supervisés. • Maîtriser le déploiement, la configuration et l'usage des réseaux sans fil. • Configurer les mécanismes de commutation et de routage pour se protéger des attaques. • Tenir à jour une cartographie détaillée et complète des réseaux et interconnexions
7. Architecture des SI	**9**	• Appliquer les principes de défense en profondeur à l'architecture matérielle et logicielle des centres informatiques.
8. Exploitation des SI	**10**	• Appliquer les principes de défense en profondeur à l'architecture matérielle et logicielle des centres informatiques.

9. Sécurité du poste de travail	**11**	• Durcir les configurations des postes de travail en protégeant les utilisateurs. • Paramétrer les imprimantes et copieurs multifonctions afin de diminuer leur surface d'attaque. • Sécuriser la téléphonie pour protéger les utilisateurs contre des attaques malveillantes • Contrôler régulièrement la conformité des paramétrages de sécurité appliqués aux postes de travail.
10. Sécurité du développement des systèmes	**12**	• Reconnaître la sécurité comme une fonction essentielle, et la prendre en compte dès la conception des projets. • Mener les développements logiciels selon une méthodologie de sécurisation du code produit. • Accompagner le développement sécurisé d'applications à risques par des contre-mesures minimisant l'impact d'attaques nouvelles
11. Traitement des incidents	**13**	• Partager l'information (alertes, incidents) dans le respect des règles de prudence et mutualiser les opérations de remise en état, de façon à lutter efficacement contre les attaques.
12. Continuité d'activité	**14**	• Se doter de plans de continuité d'activité, et les tester.
13. Conformité, audit, inspection, contrôle	**15**	• Effectuer des contrôles (audits, inspections) et des exercices réguliers de façon à mesurer les progrès accomplis et corriger les manquements.

Chaque famille d'objectifs fait l'objet d'une directive décrivant des règles fonctionnelles. Les règles permettent de contribuer à la réalisation de chaque objectif énoncé.

Les règles reprises ou légèrement adaptées de la PSSI de l'Etat sont reconnaissables par leurs identifications issues de la PSSI de l'Etat. Elles sont considérées comme règles « mère ». Quand un complément de règles s'avère nécessaire, afin d'être en cohérence avec le contexte du vice-rectorat, la règle « mère » est complétée d'une règle fille. Dans ce cas un numéro d'occurrence de règle fille est ajouté à l'identification de la règle mère.

Exemple :

N° Directive. N° règle EXEMPLE - SSI : Règle SSI adaptée de la PSSI E pour être en cohérence avec le contexte académique.
Responsable : X conduit l'action
Contributeur : Y participe à l'action
Procédure ou documentation AAAA à écrire
La règle DOIT être expliquée en toute transparence.

N° Directive. N° règle EXEMPLE – SSI : Règle SSI écrite par le vice-rectorat de la Nouvelle-Calédonie pour compléter la règle issue de la PSSI de l'Etat.
Responsable : X conduit l'action
Contributeur : N participe à l'action
Procédure ou documentation à écrire
Des formations expliquant les enjeux de la SSI et les règles relatives à ces enjeux DOIVENT faire l'objet de formations spécifiques SSI, obligatoires pour l'ensemble des utilisateurs. **Des contrôles d'appropriation des règles doivent être organisés régulièrement.**

III. Organisation et gouvernance

Objectif 1 : Organisation de la SSI

Mettre en place une organisation adéquate, garantissant la prise en compte préventive et réactive de la sécurité

III.1. L'organisation SSI

3.1. ORG - SSI : Organisation de la SSI
Responsable : L'AQSSI
Contributeur : Le RSSI
Une organisation dédiée à la SSI DOIT être mise en place au vice-rectorat de la Nouvelle-Calédonie. **Cette organisation doit être établie selon les directives du HFD conformément aux principes de l'IGI1300, (Instruction Générale Interministérielle sur la protection du secret de la défense nationale).** **Cette organisation définit les responsabilités internes à l'égard des tiers, les modalités de coordination avec les autorités externes ainsi que les modalités d'application des mesures de protection.** **Des procédures d'applications sont écrites et portées à la connaissance de tous.**

III.1.1. Principe fondateur

L'organisation de la sécurité présentée ci-après a été définie à partir du principe de séparation des pouvoirs :

- l'expression des enjeux et besoins de sécurité relève des divisions métiers et de leurs maîtrises d'ouvrage ;
- la conception et la communication de la PSSI relèvent du RSSI.
- la mise en application, l'intégration des règles dans les solutions d'architecture relèvent de la DSI.
- l'engagement de responsabilité des personnes physiques ou morales à respecter les règles ;
- le contrôle et l'audit relèvent :
  - de la division métier responsable de ses propres contrôles ;
  - du RSSI et de son adjoint ;
  - de la direction de l'audit chargée du contrôle interne.

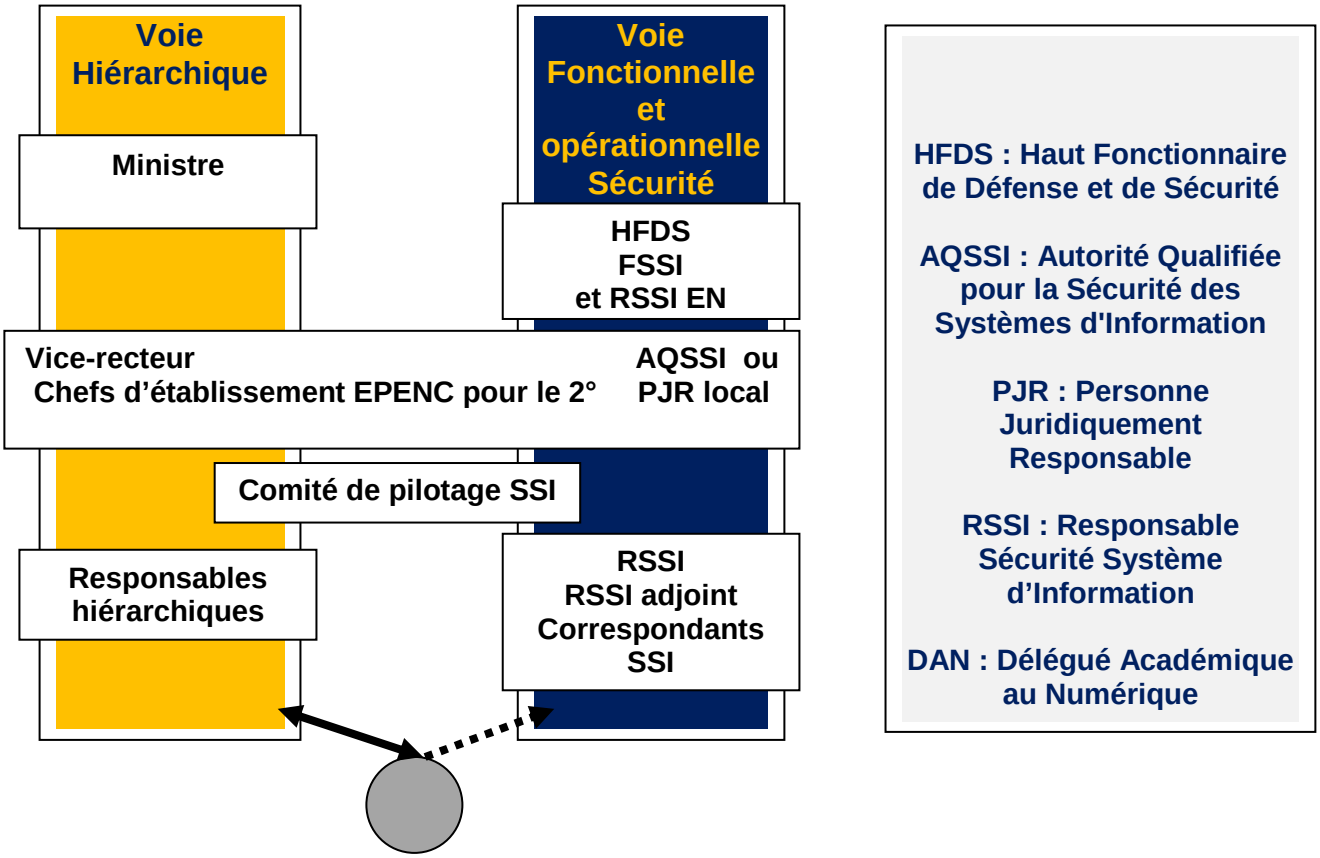
Les principes de gouvernance et les règles communes formalisés dans ce cadre garantissent l'efficacité de la sécurité du système d'information du vice-rectorat de la Nouvelle-Calédonie, tout en donnant les moyens de capitaliser sur l'ensemble des actions de sécurité des entités et de partager les bonnes pratiques. Dans une optique de progrès et un souci d'optimisation, ce partage assure ainsi une amélioration des services.

La définition et la mise en œuvre de la politique de sécurité des systèmes d'information s'appuient sur deux voies principales qui coexistent et collaborent : la voie hiérarchique et une voie fonctionnelle et opérationnelle. Ces voies se déclinent nationalement et académiquement et sont conformes à la directive interministérielle N° 901/DISSI/SCSSI le 2 mars 1994 portant sur la recommandation pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense.

III.1.2. Les acteurs SSI au niveau du ministère

3.2. Acteurs ORG - ACT - SSI : Identification des acteurs SSI
Responsables : Les HFD, FSSI et AQSSI
Contributeur : Le RSSI
L'organisation SSI de l'Etat déclinée au niveau du vice-rectorat de la Nouvelle-Calédonie DOIT s'appuyer sur des acteurs clairement identifiés. Ces acteurs responsables en matière de SSI pour la protection du secret de défense, désignés et les agents chargés de les assister dans cette mission sont référencés dans un annuaire interministériel dans l'IGI 1300. Cette chaine fonctionnelle s'appuie, pour chaque ministère, sur le HFD, assisté par un fonctionnaire de sécurité des SI (FSSI).

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



III.2. Les acteurs SSI aux niveaux du ministère et de l'académie

Fonction SSI	Rôle
Le Haut Fonctionnaire de Défense et de sécurité **(HFDS)**	**Le haut fonctionnaire de défense et de sécurité** Dans un esprit de défense globale chaque ministère a son propre HFDS, nommé par le ministre. Le décret n° 2007-207 du 19 février 2007 fixe les attributions du HFDS : • il est le conseiller du ministre pour toutes les questions relatives à la défense et aux situations d'urgence affectant la défense, la sécurité et la vie de la nation ; • il assure anime et coordonne la préparation des mesures de défense : plans de défense, sécurité de défense, protection du secret ; • il exerce son autorité, dans le cadre de ses attributions, sur l'ensemble des services du ministère où il est affecté ; • il anime la politique de sécurité des systèmes d'information et contrôle l'application de celle-ci ;
Le Fonctionnaire de Défense pour la Sécurité Système d'Information **(FSSI)**	**Le fonctionnaire de défense pour la sécurité système d'information** Il est en charge de la sécurité des systèmes d'information auprès du HFDS.
L'Autorité Qualifiée pour la Sécurité système d'Information **(AQSSI)**	**L'autorité qualifiée pour la sécurité système d'information** Il assure la responsabilité globale de la sécurité des systèmes d'information sur son périmètre. Les autorités qualifiées sont les autorités responsables de la sécurité des systèmes d'information dans les administrations centrales et les services déconcentrés de l'Etat, ainsi que dans les établissements publics visés à l'article 3 de la recommandation interministérielle 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. Sous le contrôle du HFDS et du FSSI, l'AQSSI est chargée de : • faire définir une politique de SSI adaptée au vice-rectorat de la Nouvelle-Calédonie et d'en fixer les objectifs ; • s'assurer que les dispositions contractuelles et réglementaires sur la sécurité des systèmes d'information sont appliquées aux différents niveaux et selon les structures propres à l'organisme ou à l'entreprise ; • faire élaborer les consignes et les directives internes ; • s'assurer que les contrôles internes de sécurité sont régulièrement effectués ; • faire organiser la sensibilisation et la formation du personnel aux questions de sécurité ; • mettre en œuvre les procédures prescrites pour le contrôle des personnes ainsi que pour l'homologation des produits et des installations ; dans les administrations et services déconcentrés de l'Etat, ainsi que dans les établissements publics visés à l'article 3, de ministre désigne les autorités qualifiées aux niveaux convenables (directions, services, établissements...). Compte tenu de l'obligation et de la nécessité d'appliquer la PSSI de l'Etat, l'AQSSI a décidé :

	• d'accorder les moyens budgétaires, humains, techniques, pour formaliser et mettre en application les directives de la politique de sécurité du système d'Information (PSSI) décrite dans le présent document ; • de s'impliquer dans les décisions de management ; • de soutenir la démarche engagée ; • de désigner un responsable de la SSI, le RSSI.
Les chefs des EPENC **(Chefs. EPENC)**	**Les chefs des EPENC** Les directions 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 des événements notables ayant compromis la SSI. Pour cela, les personnels de direction des EPENC s'appuient sur le RSSI et le DAN (délégué au numérique) et l'équipe d'assistance informatique. L'application des dispositions de protection des SI relève de la responsabilité de cette chaîne fonctionnelle.
Le Responsable de la Sécurité des Systèmes d'Information **(RSSI)**	**Le responsable de la Sécurité des Systèmes d'Information** Il assiste l'AQSSI. Il a la responsabilité du management de la sécurité des données et des systèmes numériques. Le RSSI s'appuie sur un adjoint RSSI placé sous l'autorité du DSI et exerçant des fonctions d'administrateur systèmes et réseaux. A ce titre, il anime les actions de la SSI au sein du vice-rectorat de la Nouvelle-Calédonie dans sa globalité : • le RSSI coordonne la mise en œuvre, l'application et l'évolution de la politique de sécurité système d'information. Il assure l'assistance à maîtrise d'ouvrage des divisions métiers sur le thème de la protection des données et des systèmes numériques ; • il promeut la démarche globale de sécurité et participe aux actions de sensibilisation à la sécurité pour les acteurs. Il peut, si nécessaire, et à des fins d'audit en particulier, faire appel à des experts ou recourir à des organismes externes spécialisés ; • le RSSI définit la stratégie en matière de gestion des risques sur les données et les systèmes numériques et notamment la politique spécifique décrivant, le référentiel SSI et les métriques prévus dans ce cadre ; • il est le garant du processus de gestion des risques (l'établissement du contexte, l'identification, l'estimation et l'évaluation des risques, le traitement des risques, l'acceptation des risques, la surveillance et la communication des risques) (et, à ce titre, actualise annuellement la cartographie des risques sur les données et les systèmes numériques ; • la démarche conduite par le RSSI permet de mettre en évidence les principales situations à risques et de définir un plan de prévention des risques cohérent avec les enjeux du vice-rectorat de la Nouvelle-Calédonie et les objectifs de sécurité à maintenir ;

	• le RSSI s'assure, avant leurs déploiements, de la conformité à la PSSI des choix techniques effectués par les maitrises d'œuvre. • Lors de la mise en place ou le remplacement de tout(s) nouveau(x) matériel(s) ou application(s), le RSSI est systématiquement consulté pour avis et conseil. Les demandes d'avis et de conseil sont formulés (par écrit) par les équipes techniques concernées ; • le RSSI évalue périodiquement l'efficacité de la SSI par rapport aux objectifs du vice-rectorat de la Nouvelle-Calédonie et aux risques à traiter. • l'efficacité de l'application de la PSSI est examinée de manière indépendante par le RSSI, un auditeur interne habilité, ou par un organisme spécialisé ; • le RSSI est le secrétaire du Comité de Sécurité du Système d'Information (CSSI).
L'adjoint au Responsable de la Sécurité des Systèmes d'Information **(Adjoint au RSSI)**	L'adjoint au Responsable de la Sécurité des Systèmes d'Information Il assiste le RSSI et le remplace en cas d'absence. L'adjoint au responsable de la sécurité des systèmes d'information est un agent de la division des services informatiques (DSI) du vice-rectorat de la Nouvelle-Calédonie ayant des fonctions d'administrateurs systèmes et réseaux il est placé directement sous l'autorité du responsable de la sécurité des systèmes d'information. Il a principalement un rôle d'administrateur technique pour les questions de sécurité des systèmes d'information. Il est notamment en charge de gérer les clefs de sécurité (OTP, Chorus, …) , les certificats et d'effectuer si nécessaire le recueil des éléments de preuves (logs, journaux, …). Il veille à la bonne application de la politique académique de la sécurité des systèmes d'information. Cela se traduit par : - des actions de sensibilisation auprès de tous les personnels ; - l'animation d'un réseau de correspondants de sécurité notamment par une veille technologique et la publication de bulletins de sécurité ; - l'aide à la mise en place de plans de secours adaptés ; - le traitement des incidents remontés et leur valorisation ; - l'évaluation et le contrôle du niveau de sécurité dans nos établissements.

Le délégué académique au numérique **(DAN)**	**Le délégué académique au numérique** Le délégué académique au numérique (DAN) est le conseiller du vice-recteur et des chefs d'établissement pour la mise en œuvre de la SSI relative au numérique éducatif. Sous l'autorité du vice-recteur, il contribue à l'intégration de la SSI et à l'application de la PSSI dans le projet académique déclinant les orientations de la stratégie numérique nationale et coordonne les réseaux d'acteurs concernés. Il pilote en liaison avec le RSSI, la mise en œuvre de la PSSI du vice-rectorat de la Nouvelle-Calédonie du service public du numérique éducatif et en évalue les résultats. En liaison avec le Secrétaire Général et les inspecteurs d'académie, dans les domaines liés au numérique pour l'éducation, il est en charge des relations avec les collectivités territoriales et assure l'animation d'une instance de gouvernance académique. Il joue un rôle de prescripteur en matière de formation SSI « au » et « par » le numérique en collaboration avec le responsable académique de formation, les corps d'inspection. Il contribue à intégrer la SSI dans la mise en place des partenariats permettant au vice-rectorat de la Nouvelle-Calédonie d'être acteur dans la production : • de référentiels SSI ; • d'outils SSI pédagogiques ; • d'outils méthodologiques SSI ; • de la sécurité des ressources ou services numériques en lien avec les EPENC et les entreprises de la filière du numérique éducatif.
Le chef de la division des services informatiques **(DSI)**	**Le chef de la division des services informatiques** Le DSI est le maitre d'œuvre de la SSI et il est chargé : • d'intégrer dans les architectures du SI les architectures les directives et règles de sécurité • de maintenir et de garantir, selon les modalités prévues, la disponibilité et le bon fonctionnement des moyens et ressources informatiques ; • de s'assurer que les moyens techniques déployés pour assurer la protection des informations sont correctement gérés dans le respect des bonnes pratiques et des démarches qualité en vigueur ; • de réaliser, de déployer et d'administrer les moyens techniques de sécurité dans le respect des bonnes pratiques en vigueur

Le Correspondant Informatique et Libertés **(CIL)**	**Le correspondant informatique et libertés** Désigné par l'AQSSI, il a en charge de veiller à l'application de la loi « Informatique et Libertés » au sein du vice-rectorat de la Nouvelle-Calédonie. Il exerce, en totale indépendance, les actions suivantes : • l'établissement, la mise à jour et la publication de la liste des traitements automatisés des données à caractère personnel ; • les recommandations préalables à toute mise en œuvre de traitements de données à caractère personnel ; • l'alerte en cas de manquement à la loi ; • la définition de la stratégie de gestion des données à caractère personnel en accord avec les normes déontologiques et professionnelles applicables au sein du vice-rectorat de la Nouvelle-Calédonie dans le respect de la procédure de validation auprès de l'AQSSI et de la cellule juridique ; • l'appréciation systématique des événements redoutés et les menaces concernant la protection de la vie privée ; • la mise sous contrôle des risques et la maîtrise des activités de collecte et de traitement des données à caractère personnel conformément aux exigences légales, aux normes déontologiques et professionnelles ; • la construction et la diffusion de la culture de la maîtrise des risques liées à la gestion des données à caractère personnel ; • l'élaboration, l'actualisation et l'autorité pour faire respecter les principes et les règles d'application de la politique de conformité des données à caractère personnel ; • l'établissement et maintien d'une relation privilégiée de collaboration avec la CNIL.
La division de la logistique et des lycées (DLL)	**La division de la logistique et des lycées** Sous la responsabilité du Secrétaire Général, la division de la logistique et des lycées est un opérateur qui participe à la sécurité physique des biens et des personnes. A ce titre, la DLL applique les règles de la PSSI sur instruction du RSSI et coordonne l'ensemble des tâches de la sécurité physique des locaux et des matériels du système d'information. Sa mission inclut notamment: • un reporting régulier des actions engagées au niveau de la sécurité physique et du niveau de conformité aux politiques et directives à destination du RSSI ; • une présentation au CSSI des actions engagées et du niveau de conformité aux directives spécifiques de sécurité physique ; • une coordination opérationnelle lors des phases d'analyse et de choix de solutions techniques et des phases de déploiement des solutions validées par le CSSI ; • un pilotage et un suivi des actions d'audits techniques et des appréciations des risques physiques et environnementaux (analyses de risques, audit des locaux et des sites, audits des équipements, etc.) ; • l'alerte du RSSI en cas d'identification ou de survenance de risques majeurs qui peuvent avoir un impact direct ou indirect sur la protection des informations du vice-rectorat de la Nouvelle-Calédonie.

Le Secrétaire Général
 	
(RPCA)
	Le Secrétaire Général est responsable du plan de continuité d'activité (RPCA)
	
	Le secrétaire général est le coordinateur PCA au niveau du vice-rectorat de la Nouvelle-Calédonie et assure les missions suivantes :
	
	• il rédige et propose, pour validation par la direction, la Politique Générale du Plan de Continuité d'Activité (PGPCA) et ses évolutions, s'assure qu'elle couvre les risques majeurs et extrêmes et veille à son application. Il est chargé de la diffusion de cette PGPCA auprès de toutes les entités concernées ;
	• il s'assure de la mise en œuvre des plans d'actions dans le domaine PCA. Ces plans d'actions sont constitués sur la base des plans d'actions élaborés par les métiers et les activités de support (maîtrise d'œuvre système d'information, ressources humaines, communication, logistique et sécurité). Le RPCA assure le reporting sur l'avancement de ces plans d'actions au CSSI ;
	• il prépare, en collaboration avec le RPSI, les travaux du CSSI pour le volet PCA, et s'assure de la mise en application de toutes les décisions prises par le CSSI ;
	• il s'assure que les responsabilités liées au PCA décrites dans la politique sont clairement attribuées et prises en charge et que l'ensemble des activités et des infrastructures sont ainsi couvertes. Dans ce cadre, il doit notamment s'assurer :
	  ◦ que l'évaluation des risques et des besoins pour la continuité d'activité liées aux processus est effectivement réalisée par les métiers ;
	  ◦ que les organisations et procédures adéquates sont mises en œuvre pour assurer la gestion des crises de toute nature ;
	  ◦ que les solutions mises en œuvre par la maîtrise d'œuvre informatique répondent aux exigences des besoins exprimés par les métiers ;
	  ◦ il apporte, en complément de la maîtrise d'ouvrage, un support aux divisions et aux pilotes de processus pour tout ce qui relève du PCA (méthodologies, organisations, sensibilisation et formation, etc.) ;
	• il déclenche, s'il l'estime nécessaire ou sur demande du CSSI, des contrôles pour vérifier la bonne mise en œuvre et l'efficacité des mesures dans le domaine du PCA. En cas de non-conformité, il s'assure de la mise en œuvre des mesures correctrices ; il traite les demandes de dérogation à la PGPCA et les fait remonter, si elles sont structurantes, au CSSI ;
	• il définit et pilote le processus de mise à jour et de révision des plans de continuité ;
	• il sensibilise le personnel de l'organisme au processus PCA ;
	• il planifie des tests et exercices réguliers conjointement avec ses correspondants métiers ;
	• il prépare un tableau de bord PCA et effectue le maintien en condition opérationnelle du PCA ;
	• il assure le secrétariat de la Cellule de crise décisionnelle (CCD).
	
	• Il s'assure que les obligations du fonctionnaire définies dans la loi n°83-634 ou dans la jurisprudence notamment en matière de secret professionnel, d'obligation de discrétion et de devoir de réserve, sont respectées.

Le Responsable du Plan de Secours Informatique **(RPSI)**	**Le responsable du plan de secours informatique (RPSI)** Placé sous la responsabilité du DSI, le Responsable du plan de secours Informatique est en charge du suivi de la mise en œuvre opérationnelle des dispositifs de secours informatiques. Il rend compte au RPCA de l'organisme des activités qui lui incombent. Il définit et coordonne toutes les opérations de conception, de maintenance, de tests et de l'exploitation des moyens informatiques mutualisés et/ou dédiés à un métier qui seront utilisés dans le cadre du plan de secours informatique. Il s'assure que la conformité de ces moyens avec les exigences de la politique générale PCA et avec les besoins de continuité des activités exprimés par les maîtrises d'ouvrages est respectée. Il s'assure également que les directives de la PSSI sont appliquées dans le cadre du plan de secours Informatique et signale sans délai au RSSI toute impossibilité d'application de règles de sécurité.
Le Chef de Projet Informatique **(CPI)**	**Le chef de projet informatique (CPI)** Placé sous la responsabilité du DSI, le Chef de Projet Informatique (CPI) est en charge de prévoir la prise en compte de la sécurité : • lors de la conception générale d'un nouveau SI, (application ou architecture), pour identifier et formaliser, sur indication du Chef de Projet Utilisateur – CPU les besoins et objectifs généraux de sécurité ; • lors de la conception détaillée, pour affiner les objectifs de sécurité et identifier le niveau de risque maximum que le CPU se déclare prêt à accepter ; • lors de la réalisation du système, pour décrire concrètement les mesures de sécurité et la manière de les appliquer dans l'environnement effectif d'utilisation ; • à la fin de la phase de développement et au plus tard avant la phase d'exploitation, pour faire prononcer la décision d'homologation. Conformément aux exigences du RGS et au guide « GISSIP » élaborés par l'ANSSI, il formalise, en collaboration avec le CPU), le dossier de sécurité du projet informatique qui sera soumis à l'Autorité d'Homologation (AH).
Le Chef de Projet Utilisateur **(CPU)**	**Le chef de projet utilisateur (CPU)** Placé sous la responsabilité d'un chef de division métier, le Chef de Projet Utilisateur (CPU) est en charge de prévoir la prise en compte de la sécurité : • lors de la conception générale, pour identifier, avec le Chef de Projet Informatique – CPI, les besoins et objectifs généraux de sécurité ; • lors de la conception générale, pour identifier, avec le Chef de Projet Informatique – CPI, les risques résiduels et les communiquer au métier pour décision; • à la fin de la phase de développement et au plus tard avant la phase d'exploitation, pour valider les dispositifs de sécurité prévus par la maitrise d'œuvre. Conformément aux exigences du RGS et du guide GISSIP réalisés par l'ANSSI, il élabore, en collaboration avec le CPI, le dossier de sécurité du projet informatique qui sera soumis à l'Autorité d'Homologation (AH).

III.3. Les autres acteurs impliqués dans la SSI

Fonction	Rôle pour la SSI
La division du personnel **(DP)**	**La division du personnel** La division du personnel, par sa responsabilité concernant les aspects contractuels pour les agents du vice-rectorat de la Nouvelle-Calédonie, a en charge de prévenir la DSI des mouvements des agents du vice-rectorat de la Nouvelle-Calédonie au nom de la sécurité des systèmes d'information.
La cellule Juridique **(JUR)**	**La cellule juridique** La cellule juridique doit être particulièrement vigilante afin d'inclure les clauses de sécurité dans les documents: contrats, marchés, prestations, fiches de procédure, etc. Elle alerte, sans délai, le CIL en cas de non-conformité à la loi « informatique et libertés » et aux principes de la politique interne de protection des données à caractère personnel.
Les responsables métiers **(RM)**	**Les responsables métiers** Les responsables métiers ont la responsabilité : • de s'assurer que tout nouveau projet fait bien l'objet d'une étude formalisant les besoins, les risques, les objectifs de sécurité par le CPU ; • d'exprimer des exigences de sécurité à destination des maîtrises d'œuvre (Informatique, Sureté, Sécurité Physique, Archives, Moyens Généraux, etc.) ; • de valider les demandes de droit d'accès à une ressource du système d'Information du vice-rectorat de la Nouvelle-Calédonie (applications hébergées sur le système d'information, espaces de partage, etc. • le traitement de cette validation peut être délégué, la délégation doit être formalisée et signée de la direction concernée ; • de valider les risques résiduels identifiés par le CPU ; • de mettre en application les règles consécutives à la PSSI au cours de leurs tâches quotidiennes et de s'assurer que les agents respectent les règles relatives à la classification, les bonnes pratiques et la charte d'utilisation des ressources du SI ; • d'identifier et de gérer les risques portant sur leur périmètre ; • d'identifier les non-conformités aux règles de sécurité.
Les agents et sous-traitants de l'académie **(USER)**	**Les agents de l'académie et les sous-traitants utilisateurs du SI** Tout agent ou sous-traitant ayant un accès au système d'information et aux données du vice-rectorat de la Nouvelle-Calédonie est responsable du respect des règles de sécurité des outils du SI mis à sa disposition et des données qu'il manipule. Il se doit de se conformer à la charte de sécurité d'utilisation des outils du SI et du bon usage des ressources système d'information du vice-rectorat de la Nouvelle-Calédonie et de rendre compte des incidents de sécurité dont il est témoin (exemple : vol de documents, de postes utilisateur, notification de divulgation de données à caractère personnel, etc.). Pour cela, la procédure de notification des incidents doit être connue de tous.

	Tout agent est également soumis au secret professionnel, à l'obligation de discrétion et au devoir de réserve. Il doit donc, à ce titre, s'assurer de la bonne application et du respect des directives de protection qui lui incombent.
Les administrateurs de SI **(ADMIN SI)**	**Les administrateurs de SI** Les administrateurs de SI sont des agents ou des prestataires de la division des services informatiques (DSI) et des cellules mixtes DSI/Métiers assurant des missions : • de conception ; • d'exploitation ; • de maintenance ; • de maintien en condition opérationnelle ; des ressources informatiques, et d'assistance aux utilisateurs (CPU –chef de projet utilisateurs-, CPI –chef de projet Informatique-, administrateur, développeur, etc.). Ils sont soumis au code de déontologie des informaticiens du vice-rectorat de la Nouvelle-Calédonie et à ce titre s'engagent individuellement à contribuer à la protection du SI du vice-rectorat de la Nouvelle-Calédonie.

3.3. ORG - RSSI : Désignation du responsable SSI.
Responsable : L'AQSSI
Contributeur : Le Secrétaire Général (SG), le DSI
L'autorité qualifiée en sécurité des systèmes d'information (AQSSI) DOIT s'appuyer sur un ou plusieurs (RSSI), chargés de l'assister dans le pilotage et la gestion de la SSI. **Des correspondants locaux SSI DOIVENT être désignés dans les établissements et à la DSI, afin de constituer des relais du RSSI.** **Le RSSI DOIT faire valider les mesures d'application par le DSI qui les fait approuver par l'AQSSI.**

3.4. ORG - RESP : Formalisation des responsabilités.
Responsables : L'AQSSI
Contributeur : Le RSSI
Note de répartition des responsabilités à écrire, (DSI, SSI, CSSI, …)
Une note d'organisation fixant la répartition des responsabilités et rôles en matière de SSI DOIT être proposée par le RSSI, validée par le DSI et approuvée par l'AQSSI. Cette note sera intégrée au livrable PSSI.

III.3.1. Principe fondateur de la répartition des missions SSI entre le RSSI et le DSI

La division des services informatiques (DSI) et le RSSI coordonnent la mise en œuvre de la PSSI. Les missions, l'organisation et l'animation et les missions respectives sont décrites ci-après. L'adjoint du RSSI est un personnel de la DSI.

Répartitions des missions SSI entre le RSSI et le DSI

Missions	RSSI	DSI pour la SSI
Pilotage	Organiser puis contrôler le déploiement de la PSSI, à s'assurer que les risques majeurs sont sous contrôle et à évaluer l'efficacité de l'action SSI du vice-rectorat de la Nouvelle-Calédonie : • définir la stratégie SSI, élaborer et actualiser les directives, procédures et guides ; • exercer une veille afin de recenser les nouvelles obligations légales et règlementaires ayant une incidence sur l' « action sécurité », les meilleures pratiques et d'identifier les nouvelles menaces ; • orienter la définition des plans de traitement des risques liés à des faiblesses de sécurité puis suivre leur déroulement ; • accompagner la DSI dans la démarche de classification des ressources SI et de cartographie des risques ; • contrôler l'application des directives et échanger avec la direction de l'audit ; • suivre les non-conformités et gérer les dérogations éventuelles et suivre les risques résiduels induits ; • alerter en cas de situation majeur de risque ; • gérer les articulations avec la protection des données à caractère personnel ; • établir le tableau de bord SSI ; • collecter et analyser les résultats produits par les activités de contrôle et de reporting pour définir et mettre en œuvre les plans d'amélioration continue des processus SSI ; • accompagner la mise en œuvre d'un dispositif de suivi des dépenses sécurité.	Intégrer techniquement les règles fonctionnelles de la SSI dans les architectures : • formaliser et promouvoir la prise en compte de la sécurité dans les projets SI : • participer à la démarche de maîtrise des risques avec l'aide de la filière SSI : • en classifiant les ressources du SI ; • en contrôlant la cohérence des plans de traitement ; • en contrôlant les risques résiduels. • alimenter le dispositif de pilotage de la SSI.
Opérationnel	Accompagner les acteurs DSI en charge de la mise en œuvre des mesures de sécurité préventives, dissuasives et réactives : • assister les métiers et leurs maitrises d'ouvrage dans le cadre des projets • jouer un rôle de prescripteur et assister la DSI ou le Chef d'établissement d'EPENC dans l'élaboration des procédures d'administration et d'exploitation des dispositifs de sécurité et dans le contrôle de leur robustesse ; • assister les établissements scolaires • mener les campagnes de sensibilisation à la SSI à destination des divisions métiers, des utilisateurs et des informaticiens • assurer une assistance dans les opérations de crise relatives à la SSI	Accompagner la mise en place des solutions de sécurité ayant un impact sur le fonctionnement des divisions métiers. Mettre en place et maintenir les dispositifs de détection, de surveillance et de réaction à incident de sécurité

	• selon les besoins, exercer des missions particulières telles que :
	  • la supervision directe de la mise en place d'outils dédiés à la SSI ;
	  • le rôle d'Autorité de Certification pour la délivrance de certificats électroniques et de moyens personnels d'authentification forte ;
	  • le rôle de maîtrise d'ouvrage dans le cadre des projets ou programmes SI à forte composante sécurité ;
	• gérer les relations avec les organismes officiels et de tutelle ou les associations qui traitent de la SSI en se coordonnant avec la protection des données à caractère personnel.	

Support	Permettre aux intervenants en charge de la mise en œuvre et du contrôle de la PSSI de réaliser les actions qui leur incombent. Participer à la mise en œuvre d'une politique active et cohérente de formation SSI Accompagner la rédaction des contrats établis avec les tiers	Mettre en place et maintenir les dispositifs de détection, de surveillance et de réaction à incident de sécurité

III.3.2. Le besoin d'arbitrage, de suivi et d'homologation

III.3.2.1. Le besoin d'arbitrage

Les contraintes inhérentes aux mesures de sécurité sont susceptibles (ou ressenties) d'aller à l'encontre d'objectifs d'efficacité» ou de productivité communément admis :

- certaines interdictions techniques de sécurité brident les services que veulent mettre en œuvre certaines directions de projet,
- la prise en compte de la sécurité dans les projets est identifiée comme un facteur potentiel de ralentissement.

Dans tous les cas il y a plusieurs « conflits » potentiels :

- entre la maîtrise d'ouvrage en charge du projet et la maîtrise d'œuvre DSI,
- entre la maîtrise d'ouvrage et éventuellement la maîtrise d'œuvre associée et la SSI,
- entre les maîtrises d'ouvrage,
- entre les utilisateurs et la SSI, …

La mise en œuvre de la politique de sécurité doit anticiper ces difficultés et prévoir la mise en place de comité SSI de suivi et arbitrage : Le Comité de Sécurité du Système d'Information (CSSI).

III.3.2.2. Le besoin de suivi

Pour surmonter ces difficultés et réaliser ses missions, le Responsable de la Sécurité du Système d'Information (RSSI) s'appuie sur un Comité de Sécurité du Système d'Information (CSSI), lequel, présidé par l'AQSSI, se réunit une fois par an pour :

- passer en revue les difficultés éventuelles de mise en application directives de la politique de sécurité du système d'information (PSSI) et les responsabilités globales ;
- sur indication du RSSI, surveiller l'évolution de l'exposition aux menaces qui pèsent sur les données et les systèmes numériques ;
- suivre les incidents de sécurité remontés par le RSSI;
- valider et approuver les initiatives renforçant la sécurité des données et des systèmes numériques ;

- suivre et vérifier l'avancement des travaux décidés au titre du(es) plan(s) de sécurité élaboré(s) avec les responsables des maitrises d'œuvre (DSI, Moyens généraux, …) ;
- identifier les écarts et coordonner les mesures de sécurité entre les différents métiers ; homologuer les dispositifs SSI dans les ressources du système d'information.

III.3.2.3. Le besoin d'homologation

La politique de sécurité système d'information de l'Etat et le décret « RGS » n° 2010-112 du 2 février 2010 (Chapitre II : Fonctions de sécurité des systèmes d'information) imposent au vice-rectorat la création d'une Autorité d'Homologation (AH).

Le CSSI assure cette mission pour l'académie pour tous les nouveaux projets placés sous sa responsabilité.

Cette autorité d'homologation - le CSSI - atteste formellement auprès des utilisateurs de son système d'information que celui-ci est protégé conformément aux besoins et objectifs de sécurité fixés. ;

Dans le cas d'un télé service, cette attestation est rendue accessible aux usagers selon les mêmes modalités que celles prévues à l'article 4 de l'ordonnance du 8 décembre 2005 susvisée pour la décision de création du télé service.

Cette « attestation formelle » correspond à une « homologation de sécurité du système d'information. Celle-ci est obligatoire et constitue un préalable à la mise en service opérationnelle de tout système d'information.

La décision d'homologation, ou « attestation formelle », est l'engagement par lequel l'autorité d'homologation – le CSSI atteste, au nom de l'organisme, que le projet a bien pris en compte les contraintes opérationnelles de sécurité établies au départ, que les exigences de sécurité sont bien déterminées et satisfaites, que les risques résiduels sont maîtrisés et acceptés, et que le système d'information est donc apte à entrer en service.

Afin que sa décision soit motivée et justifiée, le CSSI s'appuie sur un dossier de sécurité, formalisé par la maitrise d'œuvre du projet de SI.

III.3.2.4. Le processus d'homologation

L'homologation permet à l'AQSSI en s'appuyant sur des experts, (RSSI, DSI, …) de s'informer et d'attester aux utilisateurs d'un SI que les risques qui pèsent sur eux, sur les informations qu'ils manipulent et sur les services rendus sont connus et maîtrisés.

3.5. ORG-PROCESSU-HOMOLOG
Responsables : Les RSSI, le DSI et l'AQSSI
Contributeurs : Le DAN et / ou les CPU et CPI
La démarche d'homologation EST OBLIGATOIRE et est donc un préalable à l'instauration de la confiance dans les SI.

Il s'agit d'un processus d'information et de responsabilisation qui aboutit à une décision, prise par l'AQSSI.

Cette décision constitue un acte formel par lequel il :

- atteste de sa connaissance du système d'information et des mesures de sécurité (techniques, organisationnelles ou juridiques) mises en œuvre ;
- accepte les risques qui demeurent, qu'on appelle risques résiduels.

Le processus d'homologation est le suivant :

- le dossier de sécurité est formalisé par le chef de projet informatique de la DSI en collaboration avec les responsables de la maitrise d'ouvrage, les chefs de projet utilisateur concernés et les équipes techniques de la DSI ;
- le RSSI, qui assure le secrétariat du CSSI, fait la première validation du dossier de sécurité remis par le Chef de projet de la DSI. Dans le cas ou des modifications doivent être apportées, le Chef de projet informatique de la DSI dispose d'un délai raisonnable défini par le RSSI pour compléter le dossier de sécurité et apporter les réponses aux éventuelles questions ;

- une fois validé par le RSSI, le CSSI est saisi de la demande d'homologation (par le RSSI ou la DSI) et formalise une attestation officielle de « pré-homologation » par écrit, signée par tous les membres ou par l'AQSSI ;
- l'attestation définitive d'homologation ne sera formalisée qu'après déploiement de la version de pré-production du projet et avant mise en production définitive. Pour obtenir cette homologation définitive, un rapport de tests, de validation ou de contrôle des dispositifs prévus dans le dossier de sécurité sera remis au RSSI pour validation et au CSSI pour homologation ;
- l'attestation formelle est mise à disposition des usagers au travers des moyens techniques de communication en vigueur.

La démarche d'homologation doit être adaptée aux enjeux de sécurité du système, notamment au contexte d'emploi, à la nature des données contenues, ainsi qu'aux utilisateurs :

- dans les cas de systèmes complexes ou à fort enjeu de sécurité, il est souhaitable que le responsable s'entoure d'experts techniques et fonctionnels (la commission d'homologation). Il peut déléguer la prise de décision à l'un de ses représentants qui présidera ce comité d'experts ;
- dans le cas de systèmes simples, le responsable peut mettre en place des procédures simplifiées associant un nombre plus limité d'acteurs.

III.3.2.5. L'organisation du CSSI

3.6. ORG - RESP : Organisation d'un Comité de suivi et d'homologation SSI.
Responsable : L'AQSSI
Contributeurs : Le DSI et le RSSI

Un comité de pilotage et suivi SSI DOIT être organisé.
Présidé par le RSSI ce comité dispose d'un mode de fonctionnement fondé sur un travail collaboratif visant à assurer un déploiement harmonieux de la PSSI dans les différentes entités ou services du vice-rectorat de la Nouvelle-Calédonie.
 	
A ce titre, le Comité de pilotage SSI DOIT :
• **être garant du référentiel, (charte éthique pour la SSI, PGSI, PSSI, chartes, guides et manuels SSI), fait élaborer et instruire par le RSSI les évolutions des directives ou des règles qui le composent ;**
• **identifier les priorités en termes de mise en conformité avec la PSSI et de couverture des risques puis de valider le plan d'action qui en découle ;**
• **éclairer les éléments d'arbitrage relatifs à la SSI dans le cadre des projets SI transverses ou des projets SI ;**
• **suivre les événements liés à la SSI (incidents, demandes de dérogations, non-conformités…) susceptibles d'induire un risque majeur pour le vice-rectorat de la Nouvelle-Calédonie ;**
• **effectuer une veille permettant d'anticiper les évolutions à apporter à la stratégie du vice-rectorat de la Nouvelle-Calédonie en matière de SSI (nouvelles exigences des métiers, menaces, solutions, obligations légales ou contractuelles…).**
• **définir un socle commun de contrôles et d'indicateurs permettant de s'assurer que la PSSI est respectée et que les risques majeurs sont maîtrisés ;**
• **exploiter les résultats des contrôles et des reportings afin d'engager les actions d'amélioration nécessaires ;**
• **émettre un avis sur les demandes de dérogation à la PSSI ;**
• **gérer les articulations avec les autres filières qui concourent à la politique de maîtrise des risques de l'académie (protection des données à caractère personnel ;**
• **le CSSI présidé par le RSSI tient lieu de comité d'homologation permettant de décider d'une homologation, attestant que le SI est bien protégé conformément aux objectifs de sécurité.**
 	
L'autorité du comité d'homologation DOIT être désignée par l'AQSSI.
• **Le Comité de pilotage pour la SSI DOIT se réunir au minimum une fois par an. Il est composé de :**
  • **l'AQSSI ;**
  • **du Secrétaire Général ;**
  • **le chef de la division des services informatiques (DSI) ;**
  • **le correspondant informatique et libertés (CIL) ;**
  • **le responsable de la sécurité des systèmes d'information (RSSI) ;**
  • **l'adjoint au responsable de la sécurité des systèmes d'information (RSSI adjoint)**

- **le responsable de la sécurité physique (DLL) ;**
- **le responsable du plan de continuité d'activité (RPCA) ;**
- **le délégué académique au numérique (DAN).**

- **Les membres invités du CSSI sont, en fonction de l'ordre du jour**
  - **les secrétaires généraux adjoints.**
- **Le secrétaire du CSSI est le responsable de la sécurité des systèmes d'information.**

Selon les sujets traités, des représentants des fonctions de contrôle ou des métiers ainsi que des experts internes ou externes peuvent être invités.
L'ordre du jour est établi par le RSSI et DOIT fait l'objet systématique d'un compte rendu.
A noter que le comité de pilotage peut être amené à se réunir, en cas d'événement exceptionnel, à la demande de l'un de ses membres.

En complément de cette instance, des groupes de travail, dont la constitution varie selon les sujets abordés et regroupant un ensemble d'experts internes et externes, peuvent être ponctuellement constitués afin de mener des réflexions ciblées sur les directives, méthodes, standards ou outils.

Ces groupes de travail DOIVENT être de préférence animés par un membre du Comité de pilotage SSI, faire l'objet de comptes rendus et être à l'origine d'un livrable à destination du Comité de pilotage SSI.

III.3.3. La Cellule de Crise Décisionnelle (CCD)

Les menaces qui pèsent sur le vice-rectorat en matière d'usage des SI peuvent, si elles sont avérées et réalisées, provoquer des incidents ou des sinistres majeurs pour les services publics rendus ou pour les activités internes (par exemple : cyber-attaque, attaque virale massive, intrusion dans les systèmes centraux, fuite d'information sensible, panne informatique, etc.).

3.7. ORG - RESP : Organisation d'une Cellule de Crise Décisionnelle (CCD).

Responsables : L'AQSSI

Contributeurs : Le DSI, le CIL, le Secrétaire Général, la cellule juridique et le RSSI

Une Cellule de Crise Décisionnelle DOIT être créée au sein de l'académie pour pouvoir réagir rapidement en cas de sinistre système d'information majeur, environnemental ou physique impactant fortement les missions de l'académie ou en cas de violation importante des informations sensibles, notamment relevant de la loi dite « informatique & libertés ».

Cette Cellule de Crise Décisionnelle DOIT être activée par les acteurs en charge de la sécurité des données et des systèmes d'information ou de la continuité d'activité (RPCA, RSSI, DSI) ou par les chefs de divisions métiers concernés par le sinistre, dès les premières phases de déclenchement des sinistres majeurs afin de prendre les décisions stratégiques qui s'imposent.

Lorsque la CCD est activée, la ou les Cellules de Crise Opérationnelles - CCO - mettent en application les décisions de la CCD et font un reporting régulier du suivi des tâches opérationnelles visant à stopper le sinistre et à rétablir le service rendu.

La CCD est composée à minima :
- **du Secrétaire Général (SG) ;**
- **des Secrétaires Généraux adjoints (SGA);**
- **du chef de la division des services informatiques (DSI) ;**
- **du chef de la cellule juridique et des marchés ;**
- **du correspondant informatique et libertés ;**
- **le responsable de la sécurité des systèmes d'information (RSSI) ;**
- **de l'adjoint au responsable de la sécurité des systèmes d'information (RSSI adjoint)**
- **du responsable de la sécurité physique (DLL) ;**
- **du responsable du plan de continuité d'activités (RPCA) ;**
- **du responsable de la communication et de l'information (RCI) ;**
- **du délégué académique au numérique (DAN).**

Les procédures d'activation et de suivi de la crise sont formalisées par le RPCA en collaboration avec le RSSI et sont validées par le CSSI. L'AQSSI et le RPCA assurent respectivement la présidence et le secrétariat de la cellule de crise décisionnelle.

III.3.4. Les Cellules de Crise Opérationnelles (CCO)

3.8. ORG - RESP : Organisation d'une Cellule de Crise Opérationnelle (CCO).
Responsable : Le DSI
Contributeur : Le RSSI et la CCD
Plusieurs Cellules de Crise Opérationnelles DOIVENT être définies notamment au niveau des maitrises d'œuvres informatiques (DSI) et de sécurité physique (Moyens généraux) qui en définissent les missions, les participants et les procédures. Composée d'experts internes, la Cellule de Crise Opérationnelle (CCO) est en charge : • d'activer et de suivre les processus de gestion des incidents et, le cas échéant, de gestion de crise en cas de déclenchement du Plan de Continuité d'Activité (PCA) ; • d'analyser la situation des sinistres et d'évaluer les impacts sur les activités de l'organisme ; • d'alerter la CCD si la situation nécessite des décisions importantes notamment de déclenchement de repli utilisateur, de secours informatiques et/ou de communications externes ; • de coordonner les actions opérationnelles visant à rétablir les services rendus dans les meilleurs délais ; • d'informer la CCD de toute situation pouvant impacter le fonctionnement normal des services ; • de s'assurer que les dispositifs prévus pour gérer les incidents et les situations de crise ne génèrent pas de non-conformités majeures aux obligations légales et aux politiques de sécurité en vigueur.

III.3.5. Fréquence d'activation des instances de décisions

Le tableau ci-dessous précise la fréquence des réunions des différentes instances de la gouvernance de la SSI :

Instance de gouvernance	Fréquence des réunions	Responsable de coordination
Comité de Sécurité (CSSI)	1 réunion par an	RSSI
Réunion opérationnelle sécurité informatique au sein de la DSI	1 réunion par mois	DSI
Réunion du Comité d'Homologation et des Libertés (Autorité d'homologation)	Dès qu'une attestation d'homologation doit être formalisée.	RSSI
Cellule de Crise Décisionnelle (CCD)	Dès le déclenchement d'une crise importante (cyber-attaques, pannes informatiques majeures, intrusions, etc.)	Membre de la CCD désirant activer la cellule de la crise

III.4. Les responsabilités SSI vis-à-vis des tiers

3.9. ORG - TIERS : Gestion contractuelle des tiers.
Responsables : Le RSSI
Contributeurs : Le DAN, les divisions effectuant des achats ou les chefs d'établissement,
Formalisation des clauses SSI dans les contrats

Le RSSI DOIT coordonner les actions permettant l'intégration des clauses liées à la SSI dans tout contrat ou convention impliquant un accès par des tiers à des informations ou des ressources du système d'information.

La rédaction du contrat d'externalisation ou de sous-traitance DOIT stipuler :

- **l'engagement du prestataire à respecter les obligations légales SSI ;**
- **le respect du référentiel SSI du vice-rectorat, (PGSI, PSSI, chartes, guides et manuels) ;**
- **l'auditabilité : le vice-rectorat DOIT pouvoir à tout moment réaliser des audits sur tout ou partie des éléments composant le service mis en externalisation. Ce droit de regard DOIT pouvoir être réalisé par le vice-rectorat lui-même ou par un tiers désigné par le vice-rectorat. Seules les contraintes liées à l'aspect concurrentiel peuvent être opposées au vice-rectorat de la part du prestataire ;**
- **la réversibilité : en cas de fin de contrat, soit normale parce que le contrat est arrivé à terme, soit anticipée, parce que de graves dysfonctionnements ont été constatés, le vice-rectorat DOIT avoir la garantie avant la signature du contrat que le prestataire mettra tout en œuvre pour lui assurer une continuité de service que ce soit pour permettre au vice-rectorat de reprendre le fonctionnement de son informatique en interne, ou que ce soit pour la transmettre à un autre prestataire ;**
- **le maintien de la propriété du vice-rectorat sur :**
  - **tous les logiciels ou matériels dont le vice-rectorat a payé les licences ;**
  - **tous les développements effectués pour le compte du vice-rectorat ;**
  - **toutes les procédures manuelles ou électroniques liées à l'exécution du service ;**
  - **toutes les documentations produites par le prestataire dans le cadre de l'exécution du service.**
- **la protection contre les actions de contrefaçon ;**
- **la formation à la sécurité du personnel du prestataire ;**
- **la confidentialité du contrat et de ses annexes et de tous les documents, informations et données, quel qu'en soit le support, que les parties échangent à l'occasion de l'exécution du contrat ;**
- **le suivi du contrat de service avec des indicateurs précis ;**
- **l'obligation générale de conseil, d'information et de recommandation du prestataire en termes de qualité de service et mise à l'état de l'art.**

En outre le contrat DOIT préciser, dans ses clauses particulières ou annexes :

- **le niveau de service attendu et les niveaux de service inacceptables ;**
- **les indicateurs pouvant servir de mesure du niveau de service et le processus d'obtention de ces indicateurs ;**
- **les procédures à suivre en cas d'incident de sécurité ou de non tenue du niveau de service attendu ;**
- **le processus de gestion des anomalies et de suivi de la résolution des problèmes détectés ;**
- **les services attendus en période de gestion de crise, notamment en ce qui concerne la disponibilité du personnel et/ou la mise à disposition de personnel complémentaire ;**
- **le contrat DOIT préciser le périmètre de ce qui est auditable chez le prestataire. Il DOIT préciser également que l'audit éventuel pourra être effectué par toute personne mandatée par le vice-rectorat.**

III.5. L'application des mesures de sécurité au sein du vice-rectorat

3.10. ORG - APP - INSTR : Application de l'instruction interministérielle SSI.
Responsable : Le RSSI
Contributeurs : Le DSI
Formalisation d'un plan d'action SSI annuel
Le RSSI DOIT planifier les actions de la mise en application de la PSSI du vice-rectorat.

3.11. ORG - APP - DOCS : Formalisation des documents d'application.
Responsable : Le RSSI
Contributeurs : Le DSI
Mise à jour de l'ensemble du référentiel SSI de l'académie
Le RSSI DOIT formaliser et tenir à jour les documents d'application validés par la DSI et approuvés par l'autorité qualifiée, permettant la mise en œuvre des mesures du Référentiel SSI dans l'académie. **Le référentiel SSI de l'académie est formalisée dans une structure documentaire à trois niveaux :** • **la politique générale de sécurité système d'information en constitue le premier niveau. Il est le document de référence, en termes stratégique SSI. La charte éthique constitue une synthèse de la politique générale de sécurité système d'information ;** • **la PSSI constituée de directives et de règles fonctionnelles constitue le second niveau du référentiel documentaire SSI. Elle définit les règles de sécurité structurantes par thème ;** • **des chartes, guides, standards et procédures opérationnelles complètent la PSSI et constituent le troisième niveau de la politique. Il s'agit de déclinaisons, dans des environnements techniques et organisationnels spécifiques, des politiques de niveau supérieur.**

III.6. Le besoin d'une gestion des dérogations au sein du vice-rectorat de la Nouvelle-Calédonie

III.6.1. Principes généraux

Le processus de traitement des dérogations DOIT être déclenché suite à l'émission par un intervenant soumis à la PSSI de l'académie d'une demande de « **non-conformité temporaire** ».

Il est donc totalement indépendant du contexte dans lequel est faite cette demande. Ceci signifie que la demande peut être déclenchée :

- dans le cadre d'une activité projet, d'une opération quotidienne d'exploitation ou d'utilisation du SI, de la résolution d'un incident, …
- que l'émetteur ou l'initiateur de la demande soit un utilisateur, un administrateur ou un exploitant, le responsable ou le représentant d'une division métier, un chef de projet, une maîtrise d'œuvre ou une maîtrise d'ouvrage,…

3.12. ORG - GEST- DEROG : Gestion des dérogations.
Responsables : Le RSSI
Contributeurs : Le DSI et l'AQSSI
Les règles suivantes DOIVENT être respectées : • une dérogation ne DOIT être accordée pour une année maximum. Arrivée à échéance, si elle s'avère encore nécessaire, elle DOIT faire l'objet d'une demande de renouvellement selon le même processus que celui correspondant au traitement de la demande initiale. • les demandes de dérogation peuvent contenir des informations sensibles relatives notamment aux vulnérabilités qu'elles induisent. A ce titre, elles DOIVENT faire l'objet d'une classification qui impose la mise en œuvre de mesures de protection adaptées en fonction du niveau et ce, tout au long de leur instruction. La classification en confidentialité DOIT être au minimum de niveau 2 cf. 5.8 GDB-QUALIF-SENSI : Qualification des informations. • les demandes de dérogation DOIVENT être enregistrées et conservées : o demande validée : durée de conservation égale au minimum à la période de validité de la directive sur laquelle porte la demande ; o demande non validée : durée de stockage minimum égale à un an.

III.6.2. Description du processus de gestion des demandes de dérogations

3.13. ORG - DEMAN- DEROG : Emission ou mise à jour d'une demande de dérogation.
Responsable : le RSSI et l'émetteur de la demande
Contributeurs : Le RSSI, le DSI et l'AQSSI
Une demande de dérogation peut, sauf règle spécifique limitant cette possibilité à des populations précises, être émise par tout collaborateur qui évalue avoir besoin, dans le cadre de sa fonction, d'agir temporairement d'une façon non-conforme avec une ou plusieurs directives ou règles de sécurité en vigueur au vice-rectorat de la Nouvelle-Calédonie. Toute demande de dérogation DOIT comporter les informations nécessaires à la prise de décision et à son suivi, à savoir : • l'état de la demande : « demande initiale », « 1er renouvellement », « 2ème renouvellement » … • une justification détaillée des contraintes ou des bénéfices attendus rendant nécessaire la demande de dérogation (besoins métiers, nouvelle activité, exigence contractuelle…), ainsi que la durée de validité souhaitée, (Cette durée ne peut pas être supérieure à 12 mois) ; • la liste des actifs ou des services classifiés sur lesquels porte la demande ; • une analyse même macroscopique des risques induits ; • les mesures compensatoires ou palliatives, permettant de limiter autant que possible les risques induits par le non-respect de la politique sécurité système d'information du vice-rectorat de la Nouvelle-Calédonie; • le plan de remédiation, qui sera mis en place pour supprimer, à terme, les contraintes justifiant la demande de dérogation et revenir à une situation conforme à la PSSI du vice-rectorat de la Nouvelle-Calédonie ; Toute demande de dérogation à la PSSI du vice-rectorat de la Nouvelle-Calédonie doit être adressée par courrier confidentiel si possible chiffré au RSSI. Le RSSI DOIT : • s'assurer que les « bonnes parties prenantes » ont bien été impliquées ; • accuser réception de la demande en précisant au demandeur les modalités de son traitement ; • vérifier de la complétude des informations que la demande est censée comporter et solliciter un supplément éventuel d'informations auprès de l'émetteur ; • s'assurer du bienfondé de la demande en regard des besoins la justifiant ; • examiner la demande en regard : • des directives ou règles sur lesquelles porte la demande ; • des besoins la justifiant et des risques induits ; En fonction de cette analyse, il a la possibilité :

- de demander des informations complémentaires notamment sur les risques encourus et les mesures conservatoires prises ou à prendre ;
- de consulter les demandes de dérogation comparables émises antérieurement ;
- de déléguer le traitement de la demande au niveau national ;
- en cas de réserve ou de doute, d'entamer un processus de consultation / concertation avec le CSSI ;
- déterminer la nécessité ou non de transmettre la demande au CSSI.
- de traiter la demande à son niveau ou d'escalader au niveau CSSI ou national.

III.6.3. Description du processus d'arbitrage des demandes de dérogations

3.14. ORG - ARBIT- DEROG : Arbitrage des demandes de dérogation.
Responsables : Le RSSI
Contributeurs : Le DSI, le CSSI et l'AQSSI
A cette étape, l'organe décisionnel DOIT être : • le RSSI national ; • ou le CSSI selon l'estimation du RSSI. L'avis rendu peut être de deux natures : • « accord » ; • « refus ». Dans le cas d'un accord, la demande ne DOIT être accordée pour une durée excédant 12 mois. Eventuellement, l'accord peut être donné sous conditions. Dans le cas s'un refus, une explication quant aux motivations de la décision ou aux aménagements à apporter à la demande doit être fournie en accompagnement. Quelle que soit la configuration du processus décisionnel, il est OBLIGATOIRE que l'émetteur et le RSSI du vice-rectorat de la Nouvelle-Calédonie et le RSSI national soient tenus informés de la décision finale.

III.6.4. Traitement des dérogations à échéance

3.15. ORG - ECHEAN- DEROG : Traitement des dérogations à échéance
Responsables : Le RSSI
Contributeurs : Le DSI, le CSSI et l'AQSSI
A l'approche de son échéance, toute demande de dérogation DOIT être réévaluée en prévision de l'expiration de sa durée de validité. Cette réévaluation DOIT être (théoriquement) initialisée par l'émetteur. Dans le cas contraire, le RSSI DOIT émettre une relance auprès de l'émetteur. Dans l'hypothèse où l'émetteur réaffirme la nécessité de maintenir la dérogation, il doit respecter le processus initial en précisant les raisons entrainant le besoin de renouvellement. Dans l'hypothèse contraire, se reporter à l'activité suivante « Avis de fin de dérogation ». En fonction de la situation, les informations figurant sur la demande initiale DOIVENT être actualisées (nouvelle date d'échéance, mesures palliatives complémentaires, niveau de risque induit, enregistrement de la clôture…).

III.6.5. Avis de fin de dérogation

3.16. ORG - FIN- DEROG : Fin de dérogation
Responsables : Le RSSI
Contributeurs : Le DSI, le CSSI et l'AQSSI
A l'issue de l'activité de « traitement des dérogations à échéance » ou des activités de suivi et de contrôle, le RSSI doit signifier l'avis de fin de dérogation et mettre en place, un dispositif permettant de s'assurer que les actions autorisées dans le cadre de la dérogation ont été supprimées.

III.6.6. Suivi et contrôle des dérogations

3.17. ORG - SUIVI – DEROG : Suivi et Contrôle des dérogations
Responsables : Le RSSI
Contributeurs : Le DSI, le CSSI et l'AQSSI
Une fois par an, le RSSI réalise une revue des dérogations accordées, refusées ou clôturées afin : • d'exploiter tout renseignement permettant d'améliorer la sécurité en regard de la nature des dérogations accordées ou de leur caractère répétitif ; • d'accélérer le processus de clôture ou de suspendre les dérogations accordées, par exemple en cas de risque imminent ; • de s'assurer de la mise en œuvre des plans de remédiation ou des mesures palliatives ; • de détecter les évolutions éventuelles à apporter à la politique de sécurité système d'information du vice-rectorat de la Nouvelle-Calédonie ; • de détecter les améliorations à apporter aux processus de traitement des dérogations en regard des retours d'expérience.

IV. Ressources humaines

Objectif 2 : Ressources humaines.

Faire des personnes les maillons forts des SI du vice-rectorat de la Nouvelle-Calédonie.

IV.1. Les utilisateurs

4.1. RH- SSI : Charte d'application SSI.

Responsable : Le RSSI

Contributeur : Le chef de la DSI, le chef de la DP et la cellule juridique

L'académie sous la responsabilité du RSSI DOIT se munir d'une charte d'utilisation des informations et ressources du SI.
La charte régissant l'usage du système d'information par les personnels du vice-rectorat de la Nouvelle-Calédonie SI, DOIT récapituler les engagements de responsabilité et les principes structurants l'utilisation sécurisée des ressources du SI.

La charte DOIT être opposable juridiquement et si possible, intégrée au règlement intérieur.

Le personnel permanent ou non permanent DOIT être informé de droits et devoirs dans le cadre de l'usage des SI de l'académie.

4.2. RH- SSI : Information et sensibilisation, responsabilisation sur les droits et devoirs SSI.

Responsable : Le RSSI

Contributeur : Le chef de la DSI, le chef de la DP et la cellule juridique

Ecriture d'un guide utilisateur et conception d'une formation/sensibilisation pour les différents utilisateurs

L'information / sensibilisation SSI à tout le personnel DOIT inclure et expliquer les sujets suivants :

Devoirs et comportements généraux	Manipulation de l'information	Utilisation des outils SI

IV.2. Le personnel manipulant des informations ou ressources sensibles

4.3. RH- MOTIV : Choix et sensibilisation des personnes tenant des postes clés impactant la SSI

Responsables : Le RSSI

Contributeurs : Le DSI en coopération avec la DP et la cellule juridique

Une attention particulière DOIT être portée au recrutement des personnes tenant des postes clés pour le bon fonctionnement de la SSI :

- **RSSI,**
- **correspondants SSI,**
- **administrateurs de SI,**
- **auditeurs,**
- **…**

Dans le cas où des personnes ont à manipuler des informations ou des ressources particulièrement sensibles une qualification pour accréditation par un organisme tiers, (ANSSI par exemple) DOIT être mise en œuvre.

IV.3. Les administrateurs de SI

4.4. RH- MOTIV SSI : Charte d'administration des SI.
Responsable : Le RSSI
Contributeurs : Le DSI en coopération avec la DP
Le vice-rectorat de la Nouvelle-Calédonie sous la responsabilité du RSSI DOIT se munir d'une charte d'administration des SI. **La charte d'administration des SI des ressources et informations du SI, DOIT récapituler les engagements de responsabilité et les principes structurants l'administration sécurisée des ressources du SI.** **La charte d'administration DOIT être opposable juridiquement et si possible, intégrée au règlement intérieur ou annexée au fiche de poste d'administrateurs de SI.**

4.5. RH- MOTIV : Sensibilisation et formation des administrateurs de SI
Responsable : Le RSSI
Contributeur : Le DSI
Conception d'une formation pour administrateurs de SI
Les administrateurs de SI DOIVENT être régulièrement sensibilisés aux droits et devoirs liés à leur fonction et DOIVENT engager leur responsabilité à respecter les règles SSI liées à l'administration, la supervision et le contrôle. L'information / sensibilisation SSI aux administrateurs DOIT inclure et expliquer les sujets suivants : **Les bonnes pratiques d'administration de SI :** • **la protection des enjeux ;** • **l'organisation SSI ;** • **l'identification des obligations légales et des règles à respecter pour les administrateurs ;** o **l'authentification ;** o **la responsabilité disciplinaire / contractuelle ;** o **le devoir de remontée d'incidents ;** o **la responsabilité civile ;** o **la loi informatique et libertés ;** o **les formalités auprès de la CNIL ;** o **la lutte contre la cybercriminalité ;** o **le respect de la propriété intellectuelle ;** o **le régime juridique de la cryptologie ;** o **le devoir de traces ;** o **le contrôle ;** o **l'investigation ciblée ;** o **la preuve.**

IV.4. Les responsables hiérarchiques

4.6. RH- SSI : Information et sensibilisation, responsabilisation sur les bonnes pratiques de gestion des collaborateurs dans le contexte SSI.
Responsable : Le RSSI
Contributeur : Le DSI
Conception d'une formation SSI pour managers
En complément de la sensibilisation pour le personnel, une information / sensibilisation SSI au management doit inclure et expliquer les sujets suivants : • **les obligations légales SSI ;** • **les responsabilités du management ;** • **les enjeux et la classification ;** • **les risques ;** • **les bonnes pratiques de management pour la SSI :** o **la gestion des habilitations ;** o **l'affectation du personnel à des tâches particulièrement sensibles ;** o **la gestion de la discipline ;** o **la gestion du personnel stratégique ;** o **la gestion des sous-traitants ;** o **la gestion des opérations externalisées.** o **les règles à faire appliquer ;** o **le contrôle.**

4.7. RH- SSI : Gestion des collaborateurs affectés à des taches sensibles.
Responsable : Les responsables métier (RM) hiérarchiques
Contributeurs : DP et RSSI
Lors de l'affectation de personnel à des tâches particulièrement sensibles, les responsables hiérarchiques DOIVENT prendre soin, lors du choix des personnes auxquelles de telles tâches sont confiées : • **de s'assurer de la totale adhésion de ces personnes aux objectifs de la fonction et aux tâches qui en découlent,** • **d'éviter de placer ces personnes dans des situations de conflit d'intérêts de par leur situation familiale ou autre,** • **d'éviter de les mettre dans des situations de fragilité où elles pourraient subir des pressions qu'elles ne se sentiraient pas aptes à supporter.** **Lors de ces choix, les responsables hiérarchiques managers DOIVENT s'appuyer sur la division du personnel et sur le RSSI.** **Lors de l'affectation à des tâches sensibles de personnes n'appartenant pas au ministère ou au vice-rectorat de la Nouvelle-Calédonie, une habilitation par un organisme officiel peut apporter une réponse satisfaisante.**

4.8. RH- SSI : Fautes professionnelles
Responsable : Les responsables hiérarchiques
Contributeur : Le RSSI
Les actions menées de manière consciente et volontaire et/ou sans autorisation ou motif valable dans l'intérêt du vice-rectorat de la Nouvelle-Calédonie DOIVENT être considérées comme formellement prohibées et donc comme des fautes professionnelles : • **la pénétration ou la tentative de pénétration dans un système d'information sans autorisation** • **la mise à disposition de tiers d'informations classifiées sensibles en confidentialité ou toute action tendant à faciliter cette mise à disposition, sans autorisation officielle et explicite.** • **la neutralisation ou la mise hors circuit d'un système de sécurité, matériel ou logiciel.** • **l'utilisation de logiciels sans licences officiellement et régulièrement acquises.** **L'appel à la dissuasion réclame, outre les mesures techniques d'audit et de contrôle, que les abus détectés DOIVENT être sanctionnés.**

IV.4.1. Précisions

A l'inverse, l'absence de sanction est généralement considérée comme une vulnérabilité forte car elle incite à l'action malveillante

IV.5. Les mouvements de personnel

4.9. RH- MOUV : Gestion des arrivées, des mutations et des départs.
Responsable : Le RSSI
Contributeurs : La DP, le DSI et les responsables hiérarchiques
Conception de la procédure de gestion des mouvements de personnels
Une procédure permettant de gérer les arrivées, les mutations et les départs des collaborateurs dans les SI DOIT être formalisée et strictement appliquée. **Cette procédure DOIT couvrir au minimum :** • **la gestion révocation des comptes et des droits d'accès aux SI, y compris pour les partenaires et les prestataires externes ;** • **la gestion du contrôle d'accès aux locaux ;** • **la gestion des équipements mobiles ;** • **la gestion du contrôle des habilitations.**

IV.6. Le personnel non permanent

4.10. RH- NPERM : Gestion du personnel non permanent.
Responsable : Le RSSI
Contributeurs : La DP, le DSI et les responsables hiérarchiques
Les règles de la PSSI et de la charte utilisateur DOIVENT s'appliquer à tout personnel non permanent d'un SI. **Les dispositions contractuelles préexistantes régissant l'emploi de ce personnel DOIVENT être amendées si nécessaire.** **Pour tout personnel non permanent, un tutorat par un agent permanent DOIT être mis en place, afin de l'informer de ces règles et d'en contrôler l'application.**

4.11. RH- NPERM : Gestion du personnel non permanent.
Responsable : Le RSSI
Contributeurs : La DP, le DSI et les responsables hiérarchiques
Conception de la plaquette de synthèse SSI d'accueil pour les nouveaux arrivés
Une plaquette de synthèse des bonnes pratiques et règles SSI DOIT être remis à l'accueil des personnels non permanents.

V. Gestion des biens

Objectif 3 : Cartographie des SI.
Tenir à jour une cartographie détaillée et complète des SI.
Objectif 4 : Qualification et protection de l'information.
Qualifier l'information de façon à adapter les mesures de protection

La mise en œuvre des règles édictées au sein de cette directive vise principalement à :

- identifier les ressources sensibles du SI et définir des priorités d'actions ;
- alimenter les démarches d'analyse de risque (vision des enjeux et des priorités), d'intégration de la sécurité dans les projets SI (approche des exigences de sécurité), et de mise en œuvre de plans de continuité d'activité (analyse d'impacts), et faciliter ainsi leur déroulement ;
- améliorer la pertinence du discours de sensibilisation et obtenir une meilleure adhésion des parties prenantes ;
- définir des mesures de protection immédiates adaptées aux enjeux des activités.

5.1. GDB- INVENT : Inventaire des ressources SI.

Responsable : Le DSI

Contributeur : Le RSSI

Formalisation de l'inventaire cartographique des ressources SI

La DSI DOIT établir et maintenir à jour un inventaire des ressources du SI.

Cet inventaire, sous la forme d'une base de données DOIT être mis à disposition du RSSI, ainsi que du FSSI et de l'ANSSI en cas de besoin de coordination opérationnelle.

L'inventaire DOIT lister :

- **les ressources matérielles et logicielles utilisées ainsi que leurs versions exactes.**
- **toute ressource doit avoir un propriétaire (la direction métier utilisatrice de la ressource) ayant notamment pour responsabilité l'expression de la sensibilité des informations associées à cette ressource.**

5.2. GDB- CARTO: Cartographie.

Responsable : Le DSI

Contributeur : Le RSSI

Formalisation de l'inventaire cartographique des ressources SI classifiées

La cartographie DOIT préciser les centres informatiques, les architectures des réseaux (sur lesquels sont identifiés les points névralgiques et la sensibilité des informations manipulées) et qualifie le niveau de sécurité attendu.

Cette cartographie DOIT être maintenue à jour et DOIT être mise à disposition du RSSI, ainsi que du FSSI et de l'ANSSI en cas de besoin de coordination opérationnelle

V.1. Principe fondateur

Le principe fondamental est que les moyens et les mesures de sécurité sont appliqués aux éléments à protéger, en fonction de leur importance pour l'activité du vice-rectorat de la Nouvelle-Calédonie.

Les éléments à protéger sont principalement les informations, mais aussi les ressources utilisées pour le traitement de l'information : ressources telles que les serveurs, les réseaux, les postes de travail etc. ou les programmes de traitement, logiciels et progiciels, mais également les téléphones, les fax, les modems ou les PABX, les messageries vocales, etc.

Les raisons d'une telle règle sont doubles :

- D'une part les moyens affectés à la sécurité ne sont pas infinis et il faut donc les utiliser au mieux, c'est-à-dire en protégeant d'abord ce qui a le plus d'importance pour le vice-rectorat de la Nouvelle-Calédonie.
- D'autre part la sécurité entraîne généralement des contraintes et ces contraintes ne doivent affecter que des éléments qui le justifient.

.

On entend par ressources du SI les applications, les données, les moyens techniques nécessaires au fonctionnement des applications et au traitement des données (matériel, système d'exploitation, système de gestion de base de données et réseaux locaux, …), les environnements d'exploitation (bâtiments et locaux hébergeant les ressources) ainsi que les compétences requises pour leur conception, leur fonctionnement, leur maintenance et leur utilisation.

V.1.1. Définition de la sensibilité d'une information ou d'une ressource

La sensibilité d'une information ou d'une ressource est évaluée en fonction de l'impact qu'aurait sur le vice-rectorat de la Nouvelle-Calédonie la divulgation, la dégradation, la modification indue ou l'indisponibilité de cette information ou de cette ressource.

L'évaluation de la sensibilité d'une information ou d'une ressource est ce que l'on appelle la classification de cette information ou de cette ressource.

5.3. GDB – CARTO : Cartographie et classification de la sensibilité
Responsable : Le DSI sur expression des besoins des divisions métier
Contributeur : Le RSSI
Formalisation de l'inventaire cartographique des ressources SI classifiées
Chaque ressource du SI DOIT se voir attribuer une classification qui traduit son niveau de sensibilité, pour chacun des critères de sécurité retenus par le vice-rectorat de la Nouvelle-Calédonie, en fonction des types et niveaux d'impacts induits par toute atteinte à ces critères.

5.4. GDB – CLASS : Choix des critères de sécurité pour la classification.
Responsable : Le DSI sur expression des besoins des divisions métier
Contributeur : Le RSSI
Conformément à la politique générale de sécurité des SI du vice-rectorat de la Nouvelle-Calédonie, les critères à retenir pour la classification d'une information ou d'une ressource, au nombre de quatre, DOIVENT être les suivants : • **Disponibilité(D) : aptitude du SI à garantir l'exécution des traitements et l'accès aux informations dans des conditions prédéfinies.** • **Intégrité(I) : aptitude du SI à assurer que les informations sont inaltérables dans le temps et dans l'espace.** • **Confidentialité(C) : aptitude du SI à protéger les informations sensibles de toute divulgation non autorisée.** • **Preuve (P) : aptitude du SI à fournir des « pistes d'audit » et les éléments de preuve correspondant aux actions réalisées.**

5.5. GDB – CLASS 4: Classification (Choix des types d'impacts pour la classification)
Responsable : Le DSI sur expression des besoins des divisions métier
Contributeur : Le RSSI
En conformité avec la politique générale de sécurité système d'information du vice-rectorat de la Nouvelle-Calédonie, les types d'impacts à retenir pour la classification d'une ressource DOIVENT être les suivants : • **éducatif / opérationnel : impact sur le métier et l'incapacité à remplir la mission ;** • **financier: impacts financiers directs et indirects résultant notamment d'une dégradation du résultat, d'une perte de part de marché, de pénalités, de dommages et intérêts…** • **image: dégradation de l'image et de la réputation (publications dans les médias locaux, nationaux voire internationaux…) ;** • **social: atteinte à l'intégrité des personnes ou dégradation du climat social ;** • **juridique: conséquences induites par le non-respect des lois et règlements (contentieux, responsabilités civiles ou pénales) ;** **Pour chaque type d'impact, un seuil est défini, sur une échelle allant de 0 (impact le moins important) à 4 (impact le plus grave).**

V.1.2. Précisions sur les impacts

Les impacts à retenir pour la classification des informations ou ressources sont à évaluer à partir des dommages potentiels sur les valeurs essentielles du vice-rectorat de la Nouvelle-Calédonie présentées dans la PGSI :

- la garantie de disponibilité et de qualité du service public d'enseignement ;
- l'éducation à la citoyenneté ;
- l'égalité des chances ;
- l'engagement du vice-rectorat de la Nouvelle-Calédonie 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'état ;
- 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.

La Perte de :	Entraine des dommages sur les valeurs essentielles du vice-rectorat de la Nouvelle-Calédonie	Synthétisés sur les 4 axes d'impact
Disponibilité Intégrité Confidentialité Preuve	• l'engagement du vice-rectorat de la Nouvelle-Calédonie 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'état ; • 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.	EDUCATIF OPERATIONNEL FINANCIER JURIDIQUE IMAGE SOCIAL PERSONNEL

Grille de niveaux d'impacts avec des exemples d'impact pour chaque critère :

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	Coût supérieur au budget	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	Coût de 10 à 100 % du budget	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	Coût de 1 à 10 % du budget	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	Coût inférieur à 1% du budget	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					

***L'évaluation des impacts juridiques DOIT tenir compte des lois et règlements notamment la règlementation relative à la protection de la vie privée et la protection des données à caractère personnels.**

V.1.3. Précisions relatives à l'attribution des profils de classification

La démarche de classification consiste à attribuer une valeur qui correspond à l'impact des situations de risque potentielles susceptibles d'affecter les « biens informationnels » et les « biens ressources analysées » selon les quatre critères considérés.
Chaque ressource se voit donc attribuer, pour chacun des critères P, D, I, C un niveau de sensibilité qui correspond au niveau maximum d'impact atteint pour le critère considéré.

A titre d'exemple, les niveaux de sensibilité d'une ressource seraient déterminés comme suit :

- niveau de sensibilité en Preuve et contrôle = EO (3), FI (1), IM (2), S(2), JR (1) = Preuve(3)
- niveau de sensibilité en Disponibilité = EO (1), FI (2), IR (3), SP (3), JR (3) = Disponibilité (3)
- niveau de sensibilité en Intégrité = EO (4), FI (3), IR (1), SP(3), JR (4) = Intégrité (4)
- niveau de sensibilité en Confidentialité = EO (1), FI (2), IM (2), S(1), JR (2) = Confidentialité (2)

Le « profil de classification » de la ressource résulte de ces niveaux de sensibilité :
"Profil de classification" = D(3), I(4), C(2), P(3)

V.1.4. La sensibilité des informations et ressources entraînent des besoins

IMPACT \ BESOIN		Preuve 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

V.1.5. Cas Particulier de la disponibilité :

L'évaluation de la sensibilité d'une ressource vis-à-vis de la disponibilité est fonction de la durée de l'indisponibilité.

Ce n'est pas une valeur absolue (la ressource « peut » ou « ne peut pas » être disponible), mais relative (la ressource peut être indisponible « pour une durée maximum X). Par conséquent, il convient de définir le seuil de tolérance à l'indisponibilité.

5.6. GDB – CLASS : DMIA et PIT
Responsable : Le DSI sur expression des besoins des divisions métier
Contributeur : Le RSSI
Formalisation de l'inventaire cartographique des ressources SI classifiées
Pour chaque ressource à classifier, le seuil de tolérance DOIT être précisé, ce dernier étant constitué des deux valeurs décrites ci-dessous. • **Le délai maximal d'indisponibilité admissible (DMIA) : Définit la durée maximum pendant laquelle une entité (ou un projet) peut ne pas accéder à une ressource du SI sans en subir d'impact significatif. La valeur est numérique et exprimée en nombre de minutes, d'heures ou en jours ;** • **La perte d'information tolérée (PIT) ou Perte de Données Tolérées : Définit le degré maximum de perte d'informations acceptable par une entité (ou un projet) avant qu'elle (ou qu'il) ne commence à subir des impacts significatifs. La valeur est numérique et d'unité variable à adapter en fonction de la nature des données et du contexte (exemples : nombre d'heures ou de jours de données perdues, volume maximum de données manquantes exprimé en pourcentage, …).**

V.1.6. Cas Particulier de la confidentialité : le droit d'en connaitre et l'habilitation d'accès

5.7. GDB – CLASS : Confidentialité et habilitations
Responsable : Le DSI sur expression des besoins des divisions métier
Contributeur : Le RSSI
Formalisation de la procédure d'habilitation
Des procédures d'habilitation d'accès DOIVENT couvrir l'attribution, l'actualisation et le contrôle des droits d'accès aux informations (la liste de diffusion) ou aux ressources les habilitations) SI.

En théorie, la démarche de classification des ressources du SI se situe en aval de la démarche de classification des informations (ou des processus métiers). Dans l'hypothèse où cette dernière a été effectuée, la classification des ressources héritera des profils de classification des informations traitées sans qu'il soit nécessaire de calculer à nouveau les impacts métiers.
Toutefois, une ressource pouvant traiter plusieurs informations, il conviendra de s'assurer que le niveau de classification de la ressource ne soit pas inférieur à celui de l'information présentant le niveau de classification le plus élevé.

V.2. Qualification et protection de l'information

5.8. GDB- QUALIF – SENSI : Qualification des informations
Responsable : Les divisions métiers
Contributeur : Le RSSI
La sensibilité de toute information DOIT être évaluée. **Le marquage systématique des documents en fonction du niveau de sensibilité en confidentialité DOIT être effectué :** • **4 : SECRET** • **3 : CONFIDENTIEL** • **2 : DIFFUSION RESTREINTE** • **1 : DIFFUSION INTERNE** • **0 : Non classifié** **Pour les niveaux 4, 3 et 2 une liste des personnes ou des fonctions habilitées à en connaitre DOIT être définie avec le niveau de classification.** **Une classification complémentaire pourra être apportée :** • **PERSONNEL** • **PROFESSIONNEL** • **SYSTEME D'INFORMATION** • **SECURITE DE L'INFORMATION**

5.9. GDB- PROT – IS : Protection des informations
Responsable : Les divisions métiers
Contributeur : Le RSSI
L'utilisateur DOIT protéger les informations qu'il est amené à manipuler dans le cadre de ses fonctions, selon leurs sensibilités en disponibilité, intégrité confidentialité et preuve et tout au long de leur cycle de vie, depuis la création du brouillon jusqu'à son éventuelle destruction. **Les étapes du cycle de vie sont :** • **conception / marquage ;** • **identification enregistrement ;** • **transmission ;** • **copie ;** • **impression ;** • **accès ;** • **stockage / archivage ;** • **destruction.**

Les règles sont détaillées dans le guide de manipulation des informations sensibles.

VI. Intégration de la SSI dans le cycle de vie des SI

Objectif 5 : Risques
Apprécier, traiter et communiquer sur les risques relatifs à la sécurité des SI.
Objectif 6 : Maintien en condition de sécurité
Gérer dynamiquement les mesures de protection tout au long de la vie du SI.
Objectif 7 : produits et services qualifiés ou certifiés.
Utiliser des produits et services dont la sécurité est évaluée et attestée selon des procédures reconnues par l'ANSSI, afin de renforcer la protection des SI.
Objectif 8 : maîtrise des prestations.
Veiller aux exigences de sécurité lorsqu'il est fait appel à de la prestation par des tiers.

Les règles édictées s'inscrivent dans les principes généraux de gestion des risques du vice-rectorat de la Nouvelle-Calédonie et respectent l'état de la normalisation notamment les recommandations de la norme ISO 27005.

Elles sont complétées ou viennent compléter les règles édictées au sein des directives :

- Organisation et gouvernance,
- Gestion des biens.

VI.1. Gestion des risques et homologation de sécurité

6.1. INT – HOMOLOG – SSI
Responsable : L'autorité comité d'homologation CSSI
Contributeurs : DSI, CPI, RSSI et CPU
Tout SI 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 atteste formellement que le SI est protégé conformément aux objectifs de sécurité fixés.** **La décision DOIT être prise par l'autorité d'homologation, au niveau national ou désignée par l'AQSSI pour le niveau académie** **Cette décision DOIT s'appuyer sur une analyse de risques adaptée aux enjeux et besoins classifiés du SI et préconise les conditions d'emploi.**

VI.2. Gestion des risques

Les règles de l'analyse de risque portent sur 6 axes permettant de répondre à la problématique adressée :

- **Evaluation des risques (identification et estimation)**
- **Traitement des risques**
- **Acceptation des risques**
- **Communication des risques**
- **Suivi des risques**

VI.3. Actualisation des cartographies de risques

6.2. INT – ANRISQ 2 – SSI
Responsable : L'autorité comité d'homologation CSSI
Contributeurs : DSI, CPI, RSSI et CPU
Formalisation d'une fiche analyse de risques
Les propriétaires (utilisateurs métiers) de ressources (ou de services) du SI classifiés comme sensibles, DOIVENT identifier les scénarii de risque qui résulteraient d'une défaillance ou d'une inadéquation des dispositifs de sécurité mis en œuvre pour protéger ces ressources. Chaque scénario de risque DOIT être caractérisé par deux critères : • une menace potentielle; La potentialité est liée en premier lieu à la probabilité ou fréquence d'apparition de la menace. • les types d'impacts directs (pertes) ou indirects (interruption d'une activité, remise en cause d'un projet, utilisation du SI pour favoriser une fraude…) qu'engendrerait le scénario de risque s'il se produisait ;

6.3. INT – ANRISQ – SSI
Responsable : L'autorité comité d'homologation
Contributeurs : DSI, CPI, RSSI et CPU
Formalisation d'une fiche analyse de risques
Les résultats d'une analyse des risques DOIVENT être présentés sous la forme d'une «matrice de hiérarchisation des risques». Il s'agit d'une vision de synthèse devant permettre de situer l'ensemble des scénarii de risque analysés et de les comparer entre eux selon les deux axes - potentialité et impacts. Ainsi, il est possible de visualiser : • les risques globalement acceptables (impact négligeable et fréquence faible) ; • les risques nécessitant un arbitrage (impact ou fréquence élevés) ; • les risques à traitement prioritaire (impact et fréquence élevés).

La grille ci-dessous propose une méthode pour obtenir ce niveau de risque. Elle peut et doit être adaptée en fonction des contextes.

Vraisemblance / Potentialité / Impact	1	2	3	4
4	3	3	4	4
3	2	2	3	4
2	1	2	2	3
1	1	1	1	2

La métrique standard de potentialité est décrite ci-dessous :

Vraisemblance Potentialité	Description
1	Très improbable ne surviendra probablement jamais
2	Possible, bien qu'improbable
3	Probable, devrait arriver un jour
4	Très probable, surviendra sûrement à court terme

La métrique standard de l'impact est une cotation sur une échelle de 4 niveaux décrite ci-dessous :

Impact	Description
1	Impact insignifiant au niveau du vice-rectorat de la Nouvelle-Calédonie
2	Impact significatif, causant du tort au vice-rectorat
3	Impact grave, sans cependant menacer la vie du vice-rectorat
4	Impact extrêmement grave, menaçant le vice-rectorat ou l'une de ses activités

Gravité (combinaison impact / vraisemblance potentialité)	Description
1	**Risque tolérable** S'il se concrétisait, ce risque aurait peu de conséquences sur les activités du vice-rectorat de la Nouvelle-Calédonie. Il n'est pas obligatoirement utile de mettre en œuvre des moyens de protection complexe ou onéreux pour réduire ce risque.
2	**Risque supportable** S'il se concrétisait, ce risque aurait des conséquences sur les activités du vice-rectorat de la Nouvelle-Calédonie, mais pourrait être supporté sans problème majeur. Il est cependant important de mettre en œuvre des moyens de protection pour limiter ce risque.
3	**Risque insupportable** Un maximum de moyens doit être prévu pour limiter ce risque, qui aurait des conséquences très importantes sur les activités du vice-rectorat de la Nouvelle-Calédonie
4	**Risque inadmissible** Tout doit être mis en œuvre pour que ce risque n'arrive jamais, car il aurait alors des conséquences critiques sur les activités du vice-rectorat de la Nouvelle-Calédonie.

VI.4. Traitement des risques

6.4. INT – TRAITRISQ – SSI
Responsable : L'autorité comité d'homologation
Contributeurs : DSI, CPI, RSSI et CPU
Formalisation d'un fiche risque initiaux et risques résiduels
Dans le prolongement de l'évaluation des risques, un plan de traitement DOIT être établi et faire ressortir les niveaux de risques résiduels. **Pour les « nouveaux SI sensibles » et les « maintenances importantes de SI sensibles en production », les actions prioritaires de réduction DOIVENT être réalisées avant la mise en production.** **Pour les SI sensibles existants, l'analyse des risques DOIT aboutir à la définition d'un plan de traitement dont les priorités seront fixées par le propriétaire de la ressource et validées selon un processus d'acceptation formel.**

Les options de traitement sont les suivantes :

Evitement	**Consiste à se soustraire au risque et à ses conséquences.**
Transfert	**Consiste à déplacer en tout ou partie les conséquences du risque vers un tiers qui est jugé plus apte à en assurer le traitement.**
Réduction	**Consiste à atténuer l'impact d'un risque et/ou diminuer la probabilité d'occurrence.**
Acceptation	**Consiste à accepter le risque et le suivre.**

Les mesures de sécurité doivent démontrer en réduisant les vulnérabilités sur les ressources parmi les entités organisationnelles ou techniques qu'elles réduisent les impacts ou les potentialités pour transformer les risques initiaux identifiés lors de l'analyse de risques en risques résiduels.

Exemple :

Vraisemblance / Potentialité / Impact	1	2	3	4
4	3	3	4	4
3	2		3 : R1	4
2	1 : R2	2 : R2	2	3
1	1	1	1 : R1	2

- Le Risque initial R1 de gravité initiale 3 grâce à l'application de la mesure devient un risque résiduel de gravité 1, exemple l'effacement des médias mis au rebut limite la potentialité de récupération de données.
- Le Risque initial R2 de gravité initiale 2 grâce à la mise en en œuvre d'une zone de confinement par le cloisonnement limite l'impact d'une prise de contrôle malveillante d'une ressource.

VI.5. Acceptation des risques.

6.5. INT – ACCERISQ – SSI
Responsable : CSSI
Contributeurs : DSI, CPI, RSSI et CPU
Un processus d' « acceptation des risques » DOIT obligatoirement être enclenché à la suite de toute démarche d'analyse de risque, quel que soit le contexte de réalisation de cette analyse (ex. : démarche de cartographie, élaboration d'un projet, émission d'une demande de dérogation, respect d'une exigence dans le cadre de la mise en place d'un projet SI, processus régulier d'évaluation d'une application, etc.). Ce processus doit impliquer le métier (ou sa maîtrise d'ouvrage par délégation), la fonction SI et la filière SSI, et tenir compte des acteurs touchés par d'éventuels impacts collatéraux.

L'autorité d'homologation réunit toutes les parties prenantes (le représentant métier ou leur maîtrise d'ouvrage, les dépositaires des ressources, les tiers pouvant subir des impacts collatéraux…) afin d'évaluer le risque dans son ensemble.

Les avis émis par les différentes instances ou représentants consultés sont généralement de trois natures :

- « accord » ;
- « accord avec réserve », dans ce cas, une explication quant à la nature de la réserve doit être fournie en accompagnement ;
- « avis défavorable », là aussi, une explication de l'avis doit obligatoirement être fournie en accompagnement.

Il convient de stocker ces avis (selon une durée à déterminer et un processus sécurisé) et d'en assurer le suivi**.**

6.6. INT – COMRISQ – SSI
Responsable : L'autorité comité d'homologation CSSI
Contributeurs : DSI, CPI, RSSI et CPU
Les risques DOIVENT être communiqués aux parties concernées afin de permettre à chaque acteur d'assumer ses responsabilités.

VI.5.1. Principe fondateur de l'acceptation des risques

Un « risque accepté » décrit le positionnement du vice-rectorat de la Nouvelle-Calédonie face à un risque et est caractérisé par la conjonction des 3 éléments suivants :

- connaissance de l'existence d'un risque associé à une défaillance de sécurité des SI par les décideurs ;
- mesure du risque par les intervenants autorisés, en fonction d'un référentiel (critères, calcul et seuils d'impact, etc.) opposable ;
- arbitrage et autorisation d'assumer les conséquences du risque, en tenant compte des mesures de réduction, selon les principes de délégation en vigueur. La direction doit avoir conscience des risques encourus et des risques résiduels.

VI.6. Suivi des risques

6.7. INT – SUIRISQ – SSI
Responsable : L'autorité comité d'homologation CSSI
Contributeurs : DSI, CPI, RSSI et CPU
Les risques résiduels et, d'une manière plus spécifique, les risques ayant fait l'objet d'une réserve ou d'un avis défavorable DOIVENT être suivis. Les cartographies réalisées DOIVENT faire l'objet d'un archivage. Par ailleurs, un rapport reflétant l'avancement des cartographies de risques DOIT être mis en place en suivant la ligne hiérarchique et du RSSI.

VI.7. Actualisation des cartographies de risques.

6.8. INT – ACTRISQ – SSI
Responsable : L'autorité comité d'homologation CSSI
Contributeurs : DSI, CPI, RSSI et CPU
Les risques identifiés et évalués DOIVENT être révisés selon une périodicité prédéfinie à l'issue de la cartographie de risques initiale (réalisée dans le cadre d'un projet de nouveau SI ou conduite sur un SI existant).

VI.8. Maintien en condition de sécurité des SI

6.9. INT – SSI : Intégration de la SSI dans les projets
Responsable : L'autorité comité d'homologation CSSI
Contributeurs : DSI, CPI, RSSI et CPU
La SSI doit être prise en compte dans toutes les phases des projets, sous le contrôle d'homologation, de la conception et de la spécification du SI jusqu'à sa fin de vie.

Les règles édictées sont structurées selon 5 axes permettant de répondre à la problématique adressée :

- **Prise en compte de la sécurité dans les projets SI**
- **Sécurité des études et des développements de SI**
- **Sécurité de la mise en production des SI**
- **Sécurité de la maintenance des SI**
- **Documentation des SI**

VI.8.1. Prise en compte de la sécurité dans les projets SI

6.10. INT – SSI : Intégration de la SSI dans les projets et formalisation de la fiche projet
Responsable : L'autorité comité d'homologation
Contributeurs : DSI, CPI, RSSI et CPU
Formalisation d'une fiche projet type
Le processus de conduite des projets SI DOIT systématiquement intégrer la prise en compte des exigences (besoins et objectifs) de sécurité inhérentes au produit cible, qu'il s'agisse d'un développement spécifique réalisé en interne ou par un prestataire du vice-rectorat de la Nouvelle-Calédonie, du choix d'un progiciel ou de la mise en œuvre d'un service d'infrastructure. Les livrables issus de la mise en application de cette démarche d'intégration de la sécurité dans les projets DOIVENT être consolidés au sein du « dossier sécurité » du projet.

La prise en compte de la sécurité dans les projets SI a pour principaux objectifs :

- de permettre aux métiers et à leurs maîtrises d'ouvrage (MOA) d'appréhender et d'énoncer les besoins de sécurité de leurs SI pour tous les critères à prendre en compte - DICP - (disponibilité, intégrité, confidentialité, preuve et contrôle) et de leur fournir les éléments d'arbitrage des choix concernant les dispositifs de sécurité ;
- de fournir aux maîtrises d'œuvre (MOE) des expressions de besoins « calibrées » pour la sécurité des SI dont ils ont la charge, et de leur permettre de proposer des solutions appropriées pour pallier les vulnérabilités et satisfaire aux exigences exprimées par leurs « clients » ;
- d'être en mesure de vérifier la mise en œuvre effective des dispositifs de sécurité requis et d'avoir une vision précise des risques résiduels.

Le RSSI peut être sollicité par les maitrises d'ouvrage et la maîtrise d'œuvre de projets SI afin de leur fournir l'assistance requise à la mise en application de la méthode d'intégration native de la SSI dans les projets.

6.11. INT – SSI : Expression des besoins de sécurité du SI.

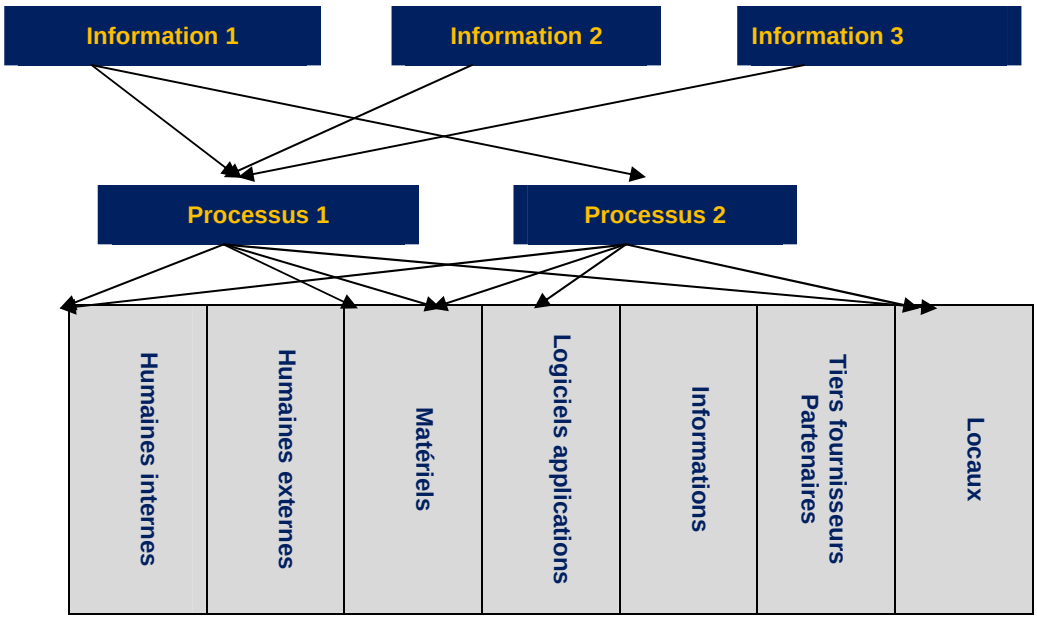
Responsable : CPU

Contributeurs : AQSSI, DSI, CPI et RSSI

Formalisation d'une fiche projet type

L'expression des besoins (en disponibilité, intégrité, confidentialité et preuve) de sécurité DOIT être formellement définie lors de l'étude des besoins fonctionnels du futur SI.
Etablie au regard des situations de risques pouvant être envisagées par le métier commanditaire du projet et du niveau de sensibilité du SI qui en découle, cette expression des besoins de sécurité doit porter sur les exigences de disponibilité du SI, de confidentialité des informations, d'intégrité des traitements et des données, et sur la nécessité d'éventuels éléments de preuve et de contrôle (critères D.I.C.P.).

L'héritage de la classification des ressources du système d'information :



Les ressources du système héritent de la classification des informations consolidées dans les processus puis dans les ressources

- **Le métier DOIT classifier l'information pour chaque processus les niveaux DICP dépendent du processus.**
- **La confidentialité est intrinsèque à l'information et ne dépend pas du processus.**
- **Le responsable métier DOIT consolider la classification des informations dans les processus.**
- **Le chef de projet maitrise d'œuvre DOIT consolider la classification dans les ressources du SI.**

Conformément aux règles de la classification présentées dans le chapitre gestion des biens, le chef de projet informatique avec le représentant métier DOIVENT respecter les règles de la classification GDB – CLASS 5: DMIA et PIT et GDB – CLASS 5: Confidentialité et habilitations.

6.12. INT – SSI : Réponses aux besoins de sécurité du SI.
Responsable : CPI
Contributeurs : AQSSI, DSI, RSSI et CPU
Les mesures de sécurité proposées pour le futur SI (qu'il s'agisse d'un développement spécifique réalisé en interne ou par un prestataire, du choix d'un progiciel ou de la mise en œuvre d'un service d'infrastructure) DOIVENT : • **être suffisantes pour ne pas dégrader le niveau de sécurité du SI au sein duquel il doit s'intégrer ;** • **satisfaire aux règles édictées dans les différentes directives de la PSSI du vice-rectorat de la Nouvelle-Calédonie ;** • **être expressément associées aux besoins de sécurité exprimés par la maîtrise d'ouvrage MOA afin de lui permettre d'analyser le niveau de sécurité proposé pour chacun des critères D.I.C.P. et d'identifier les risques résiduels avant toute décision de mise en œuvre.**

6.13. INT – SSI : Réponses aux besoins de sécurité du SI.
Responsable : Autorité d'homologation CSSI
Contributeur : CPU
Conformément à la règle : INT – HOMOLOG – SSI, la mise en œuvre effective des mesures de sécurité prévues au sein du SI DOIT donner lieu à une homologation technique et fonctionnelle de sécurité permettant de valider le niveau de sécurité atteint à l'issue du déroulement des plans de tests, de mesurer les écarts avec les niveaux de sécurité attendus et de qualifier les risques résiduels en préalable à toute mise en production. **Conformément aux règles INT – SUIRISQ7 – SSI et INT – ACTRISQ8 – SSI, un dispositif de suivi des risques résiduels identifiés à l'issue de la recette de sécurité du projet doit être mis en place afin de mettre en œuvre les mesures connexes à la sécurité du SI permettant de limiter les dysfonctionnements, et d'anticiper la prise en compte de ces risques dans le cadre des prochaines évolutions du SI.**

VI.8.2. Sécurité des études et des développements de SI

Les règles concernant les conditions de sécurité dans lesquelles doivent être réalisées les activités liées à la conception, au développement et à l'intégration d'un nouveau système d'information, conformément à la PSSI de l'Etat et à sa déclinaison académique sont définies dans la directive : Sécurité du développement des systèmes.

VI.8.3. Sécurité de la mise en production des SI

VI.8.3.1. Test et recette des systèmes d'information.

La notion de « nouvelle version » d'une application ou d'un service d'infrastructure s'applique à la fois à la version initiale du SI, à ses évolutions fonctionnelles et aux mises à niveau des composants sur lesquels il repose (ex : nouvelle version d'un système de gestion de bases de données).

6.14. INT – SSI : Test et recette des SI.
Responsable : L'autorité d'homologation CSSI .
Contributeurs : Le DSI, le chef de projet informatique et le RSSI
Tout nouvelle version d'une application (spécifiquement développée ou reposant sur un progiciel) ou d'un service d'infrastructure DOIT être soumise, en préalable à sa mise en production, à une recette formelle reposant sur un plan de tests défini conjointement par la MOE et la MOA. **Les scénarios de test DOIVENT permettre de valider, outre la conformité fonctionnelle du SI au cahier des charges établi et l'absence de toute régression en regard des versions antérieures, le fonctionnement effectif des composants de sécurité du système d'information dans un contexte représentatif de l'environnement dans lequel il sera mis en exploitation.**

Il convient de fixer la nature et la complexité des tests en fonction de la criticité des différents composants de l'application et de l'importance des dispositifs de sécurité mis en œuvre.

Au niveau fonctionnel, une attention particulière pourra par exemple être portée sur les services de sécurité suivants :

- contrôle des restrictions d'accès à certaines fonctionnalités et - ou à certaines données ;
- traces et imputabilité de certaines opérations sensibles ;
- contrôle de la validité des données en entrée, en sortie, …

Au niveau technique, il pourra s'agir de vérifier par exemple :

- le fonctionnement des dispositifs de chiffrement de données ou de flux et des solutions recouvrement associées ;
- le basculement vers les dispositifs de secours technique ;
- les interfaces avec des dispositifs de sécurité connexes : remontées d'alertes, propagation d'authentification, …

VI.8.3.2. Préparation de la mise en exploitation des SI.

6.15. INT SSI : Préparation de la mise en exploitation des SI.
Responsable : Le DSI
Contributeurs : Le CPI et le RSSI
Formalisation des spécifications SSI pour l'exploitation
La fonction responsable de la production informatique du nouveau SI DOIT vérifier l'existence des spécifications requises à la prise en charge des aspects liés à la SSI dans le cadre des opérations d'exploitation. **Il s'agit notamment des procédures d'installation des dispositifs de sécurité, des principes de supervision et d'administration de la sécurité, des politiques de sauvegarde, d'archivage et de restauration, des principes d'escalade conduisant au basculement vers une éventuelle solution de secours technique.** **Si besoin, un transfert de compétences DOIT être organisé entre le projet et les équipes de production informatique pour une prise en charge efficace des dispositifs de sécurité du nouveau SI.**

Les éléments relatifs à la sécurité à définir, documenter et transmettre à l'exploitant en préalable à la mise en production peuvent concerner, par exemple, en regard des sujets évoqués ci-dessus :

- le périmètre de supervision de la sécurité dévolu respectivement aux équipes sécurité et aux équipes de production : analyse des traces, surveillance des tentatives d'accès infructueuses récurrentes… ;
- le périmètre d'administration des dispositifs de sécurité à prendre en charge ou non par les exploitants : gestion des clés de chiffrements, gestion des traces, gestion des accès en télémaintenance et des interventions « à chaud » en environnement de production, … ;
- la politique de sauvegarde (types de sauvegardes, fréquence, nombre de versions, supports et stockage, externalisation, rétention) et modalités de restauration ;
- la politique d'archivage : liste des éléments archivés, durée de conservation, outils, périodicité, stockage, … ;
- la description du processus d'escalade vers le dispositif de secours technique dans le cadre du PRA (plan de reprise d'activité) et des plans de test associés.

VI.8.3.3. Préparation du déploiement des SI.

6.16. INT SSI : Préparation du déploiement des SI.
Responsable : Le CPI
Contributeur : Le DSI
Formalisation des spécifications SSI pour le déploiement
Les modalités de déploiement des applications et des services d'infrastructure DOIVENT être intégrées au processus de gestion du changement. **Elles DOIVENT prendre en compte, outre la formation des utilisateurs aux conditions d'usage de l'application :** • **tous les éléments requis pour un fonctionnement efficace et conforme des mesures de sécurité agissant au niveau des utilisateurs du système d'information (procédures d'utilisation des dispositifs de sécurité, règles de sécurité à respecter, procédures de reprise d'activité en cas d'incident majeur, information sur les dispositifs de traçabilité…) ;** • **toutes les consignes et procédures de sécurité devant être appliquées par les services de support aux utilisateurs.**

VI.8.3.4. Validation des mises en production.

6.17. INT SSI : Validation des mises en production.
Responsables : Le CPU
Contributeur : Le DSI et le RSSI
Les nouvelles versions des applications ou des services d'infrastructure NE DOIVENT ETRE PASSEES en production qu'à l'issue d'une acceptation formelle du responsable métier et/ou du CPU.

L'acceptation de la mise en production des applications est prononcée à l'issue des validations des recettes fonctionnelles et techniques par les MOA et MOE respectivement concernées, qui intègrent une vérification systématique de la mise en place des mesures de sécurité requises.

VI.8.4. Sécurité de la maintenance des systèmes d'information

VI.8.4.1. Demandes de modifications.

6.18. INT SSI : Demandes de modifications.
Responsable : Le CPU
Contributeur : Le DSI et le RSSI
Formalisation d'une procédure de demande de modification
Toute demande de modification d'une application ou d'un service d'infrastructure DOIT être formalisée et auditable, et faire l'objet d'une procédure permettant de vérifier, outre les impacts sur le système fonctionnel global, l'absence de dégradation de la sécurité du système d'information et la mise en conformité réglementaire. **Les demandes de modification fonctionnelle d'un SI, qu'il s'agisse de maintenance corrective ou évolutive, DOIVENT être validées par le RSSI.**

Les demandes de modification auprès de la DSI et du CPI sont émises par le Responsable Métier concerné ou sa MOA qui sont en charge de solliciter, en cas de contraintes légales ou réglementaires applicables, les instances appropriées (telles que les autorités de tutelle et de contrôle du traitement des données à caractère personnel, des données financières, …etc.).

VI.8.4.2. Demandes de modifications d'un progiciel.

6.19. INT SSI : Demandes de modifications d'un progiciel.
Responsable : Le CPI
Contributeur : Le DSI et le RSSI
En complément des règles applicables à toute demande de modification d'une application, lorsque celle-ci s'applique à un progiciel, IL EST NECESSAIRE d'obtenir du fournisseur un avis formel quant à l'absence d'impact de l'évolution requise sur le bon fonctionnement du logiciel ou des dispositifs de sécurité associés, et une confirmation de l'intégration de cette nouvelle version dans les prestations de maintenance souscrites.

La prise en charge globale de la nouvelle version par le fournisseur de progiciel implique, à l'issue de la réalisation des développements requis, la rédaction de la documentation associée, la mise à jour des procédures de maintenance et, éventuellement, la révision des contrats de garantie afférents.

VI.8.4.3. Gestion des modifications.

6.20. INT SSI : Gestion des modifications.
Responsable : Le CPI
Contributeur : Le DSI et le RSSI
La mise en œuvre des modifications DOIT être réalisée en intégrant la possibilité d'un retour à la version antérieure de l'application en cas d'anomalie et faire l'objet des mêmes contrôles que les développements initiaux. **Elle DOIT donner lieu à la mise à jour de la documentation fonctionnelle et technique de l'application concernée.**

La capacité à opérer un retour arrière, en cas de dysfonctionnement de la nouvelle version de l'application ou de régression fonctionnelle, repose en particulier sur une gestion en configuration rigoureuse des différents composants de l'application (sauvegarde et stockage des codes sources, structures des bases de données, compilateurs, environnements systèmes…).

VI.8.4.4. Maintenance « à chaud ».

6.21. INT SSI : Maintenance « à chaud ».
Responsable : Le CPU utilisera la procédure
Contributeurs : Le CPI, le DSI et le RSSI
Formalisation de la procédure de maintenance par le RSSI
En cas de nécessité d'opérations exceptionnelles de maintenance « à chaud », c'est-à-dire d'actions directes sur les ressources en production (traitements ou données), une procédure particulière DOIT être appliquée. **La demande d'intervention DOIT être formellement et conjointement validée par un représentant habilité du domaine métier concerné et par le responsable de l'environnement d'exploitation. Le RSSI DOIT en être informé.** **La procédure appliquée DOIT garantir la possibilité d'un retour arrière à tout moment, la traçabilité et l'imputabilité de l'ensemble des opérations de maintenance et le maintien en condition opérationnelle des dispositifs de sécurité à l'issue de l'intervention.**

Il convient de limiter les opérations de maintenance « à chaud » à des cas exceptionnels nécessités par exemple par la correction d'une anomalie dans les plus brefs délais (erreur sur un traitement, blocage d'une opération).

Les mesures conservatoires pour un retour arrière reposent essentiellement sur la sauvegarde préalable et la restauration du système en l'état antérieur à l'opération de maintenance.

Il convient que la piste d'audit des opérations de maintenance regroupe les autorisations délivrées, l'horodatage du début et de la fin des travaux, la nature et le bilan des interventions, une copie des données et/ou des traitements impactés avant et après la maintenance, et une validation de la remise en place des dispositifs de sécurité (ex : restriction des accès, filtrage des flux, …).

VI.8.4.5. Télémaintenance.

6.22. INT SSI : Télémaintenance.
Responsable : Le CPU
Contributeurs : Le CPI, le DSI et le RSSI
La MOA DOIT être impliquée dans le processus de décision de mise en place d'un service de télémaintenance, et être informée par la MOE des risques associés.

VI.8.5. Documentation des SI

6.23. INT SSI : Gestion de la documentation.
Responsable : Tous les acteurs impliqués dans le projet.
Une documentation complète de chaque nouveau SI, portant sur ses aspects fonctionnels (dossiers de spécifications, manuel d'utilisation) et techniques (dossiers de réalisation, procédures d'exploitation), DOIT être élaborée et mise à jour en regard des cycles d'évolution du SI. **Cette documentation DOIT intégrer, au sein du « dossier sécurité », l'ensemble des éléments liés à la sécurité du SI.**

Conformément à la règle GDB- PROT – IS : Protection des informations: Qualification et protection de l'information, la documentation doit être stockée de façon à être accessible par l'ensemble des acteurs ayant à en connaitre et en adéquation avec son niveau de classification.

VII. Sécurité physique des informations et ressources du SI

Objectif 9 : Sécurité physique des locaux abritant les SI
Inscrire la sécurisation physique des SI dans la sécurisation physique des locaux et dans les processus associés.
Objectif 10 : Sécurité physique des centres informatiques
Dimensionner les protections physiques des centres informatiques en fonction des enjeux liés à la concentration des moyens et données abritées.
Objectif 11 : sécurité du SI de sûreté.
Traiter de manière globale la sécurité des systèmes d'information et de communication qui assurent la sûreté d'un site.

VII.1. Principe fondateur

Les exigences de sécurité physique à satisfaire pour protéger les ressources du SI du vice-rectorat de la Nouvelle-Calédonie sont consécutives à la définition de zones de sécurité distinguées en fonction de la sensibilité des ressources qu'elles contiennent et du niveau de sécurité requis.

VII.2. Règles générales

1.1. PHY-ZONES : Découpage des sites en zones de sécurité
Responsable : Le RSSI
Contributeurs : La DSI et la DLL
Un découpage des sites en zones de sécurité DOIT être effectué, en liaison avec le RSSI, les correspondants locaux SSI et les services en charge de l'immobilier, de la sécurité et des moyens généraux. Pour chaque zone de sécurité, des critères précis d'autorisation d'accès DOIVENT être établis.

1.2. PHY-CI-LOC : Découpage du centre informatique en zones de sécurité
Responsable : RSSI
Contributeurs : La DSI et la DLL
Un découpage du centre informatique en zones physiques de sécurité DOIT être effectué, en liaison avec le RSSI et les services en charge de l'immobilier, de la sécurité et des moyens généraux.

1.3. PHY-CI-HEBER : Convention de service en cas d'hébergement tiers.
Responsable : RSSI
Contributeur : Le DSI
Formalisation de convention de service type
Dans le cas où un tiers gère tout ou partie des locaux du centre informatique, une convention de service, définissant les responsabilités mutuelles en matière de sécurité, DOIT être établie entre ce tiers et le vice-rectorat de la Nouvelle-Calédonie.

Les règles édictées portent sur 3 aspects liés à la problématique adressée :

- **Identification des zones de sécurité physique ;**
- **Sécurité des accès physiques aux différentes zones de sécurité ;**
- **Protection contre les risques divers ou environnementaux.**

Ces règles s'appliquent à tous les sites sur lesquels sont situées les ressources des SI du vice-rectorat de la Nouvelle-Calédonie, qu'il s'agisse d'installations permanentes ou temporaires.

Elles sont complétées par les règles édictées au sein de la directive « Gestion des biens ».

VII.3. Identification des zones de sécurité physique

Ces zones sont repérées par un code couleur :

Zones blanches	**Niveau de classification 0** • Information classées en confidentialité : « Public » • Information ou ressource classée en DIT : « besoin faible »	Elles correspondent à des parties ou zones de sites du vice-rectorat de la Nouvelle-Calédonie pour lesquelles aucune mesure de sécurité physique n'est exigée. Il peut s'agir de zones destinées à accueillir du public, sans contrainte, ou de zones ne contenant aucune information ni aucun équipement sensible.
Zones vertes	**Niveau de classification 1** • Information classées en confidentialité : « Diffusion interne » • Information ou ressource classée en DIT : « besoin peu sensible ».	Elles correspondent à des lieux contenant certains équipements ou informations sensibles, qui requièrent la mise en place de mesures de sécurité physique.
Zones jaunes	**Niveau de classification 2** • Information classées en confidentialité : « Diffusion restreinte » • Information ou ressource classée en DIT : « besoin important ».	Locaux techniques abritant des équipements d'alimentation et de distribution d'énergie, ou des équipements de réseau et de téléphonie requérant un niveau de sécurité physique renforcé, du fait qu'elles contiennent certains équipements ou informations plus sensibles.
Zones rouges	**Niveaux de classification 3 ou 4** • Information classées en confidentialité : « Confidentiel ou Secret ». • Information ou ressource classée en DIT : « besoin stratégique, vital ou critique ».	Elles requièrent un niveau de sécurité physique renforcé, du fait qu'elles contiennent certains équipements ou informations vitaux.

Les principaux types de dispositifs de sécurité physique à mettre en œuvre sont gradués selon le type de zone à sécuriser d'une part, et en fonction du niveau classification des ressources concernées pour les différents critères de sécurité, d'autre part.

1.4. PHY-ZONES : Principe général d'attribution des zones de sécurité.
Responsable : Le RSSI.
Contributeurs : La DSI et la DLL
Le type de zone de sécurité physique au sein de laquelle doit être située une ressource du SI du vice-rectorat de la Nouvelle-Calédonie DOIT être effectuée en regard du niveau de sensibilité de cette ressource (exprimé par son niveau de classification), et de la nature de l'équipement ou du local considérés.

Le niveau de classification d'une ressource du SI, représentatif de sa sensibilité (ou criticité) en termes de sécurité, est positionné pour chacun des critères D.I.C.P. (disponibilité, intégrité, confidentialité, preuve et contrôle), selon les principes édictés au sein de la directive « Gestion des biens ».

Le principe général de zonage décliné au sein des règles de cette directive est le suivant :

- ressource classifiée au niveau 4 ou 3 (*) : positionnée en zone rouge ;
- ressource classifiée au niveau 2, (*) : positionnée en zone jaune ;
- ressource classifiée au niveau 1, (*) : positionnée en zone verte ;
- ressource classifiée au niveau 0, (*) : positionnée en zone blanche.

(*) Quel que soit le critère de sécurité concerné (D.I.C.P).

VII.4. Sécurité des accès physiques aux différentes zones de sécurité

1.5. PHY – ZONES : Sécurité des accès physiques aux différentes zones de sécurité	
Responsable : Le RSSI	
Contributeurs : La DSI et la DLL	

Zones blanches	**Il s'agit de zones destinées à accueillir du public, sans contrainte, ou de zones ne contenant aucune information ni aucun équipement sensible.**
	• **Le contrôle individuel des accès piétons (principe d'unicité de passage) peut par exemple être mis en œuvre :**
	  ◦ **au moyen de portes automatiques, garantissant que deux personnes ne puissent entrer simultanément ou successivement en n'utilisant par exemple qu'un seul badge.**
	  ◦ **ou par l'intermédiaire d'un gardien assurant le filtrage individuel des accédants.**
	• **Le contrôle des accès véhicules peut être réalisé selon divers moyens tels que :**
	  ◦ **un dispositif de vidéosurveillance ou de gardiennage pour l'autorisation des accès des personnels, incluant le contrôle de l'autorisation effective de tous les passagers ;**
	  ◦ **le stationnement sur un parking extérieur des véhicules visiteurs ou leur contrôle individuel par un gardien (après le processus d'accueil) ;**
	  ◦ **la vérification par un gardien des véhicules utilitaires ;**
	  ◦ **…etc.**
	• **Tout accès réseau installé dans une zone d'accueil du public DOIT être filtré ou isolé du reste du réseau du vice-rectorat de la Nouvelle-Calédonie**
	• **Le traitement d'informations sensibles au sein de zones d'accueil est à éviter. Si un tel traitement est strictement nécessaire, il DOIT rester ponctuel et exceptionnel. Des mesures particulières DOIVENT alors être adoptées :**
	  ◦ **Protection audiovisuelle**
	  ◦ **Protection des informations stockées sur les supports.**

Zones vertes	**La circulation des visiteurs et des prestataires occasionnels à l'intérieur d'une zone verte DOIT être contrôlée :** **- soit directement, par accompagnement de la personne ;** **- soit indirectement, par un contrôle des temps de déplacement.**
Zones jaunes	**Les règles suivantes DOIVENT être respectées en complément de celles applicables aux zones vertes.** **PHY- CI-CTRLACC : L'accès aux zones internes (autorisées uniquement au personnel du centre informatique ou aux visiteurs accompagnés) et restreintes (autorisées aux seules personnes habilitées ou aux visiteurs accompagnés) DOIT reposer sur un dispositif de contrôle d'accès physique. Ce dispositif doit s'appuyer sur des produits qualifiés, lorsqu'ils sont disponibles et bénéficier d'un maintien en condition de sécurité rigoureux.** **PHY-CI-MOYENS : la délivrance des moyens d'accès physique DOIT respecter un processus formel permettant de s'assurer de l'identité de la personne, s'appuyant sur le processus d'arrivée et de départ du personnel. Le personnel autre que celui explicitement autorisé et habilité, mais néanmoins appelé à intervenir dans les zones sensibles intervient systématiquement et impérativement sous surveillance permanente.** **PHY-CI-TRACES : une traçabilité des accès par les visiteurs externes aux zones restreintes jaune et rouge DOIT être mise en place.** **Ces traces sont conservées un an dans le respect de la législation pour la protection des données à caractère personnel.** **Un registre des détenteurs des moyens d'accès à chaque zone jaune DOIT être tenu à jour.** **Les responsables ou propriétaires des locaux techniques dédiés aux équipements du SI situés en zone jaune DOIVENT réaliser une revue annuelle de la pertinence des autorisations d'accès octroyées et provoquer, si besoin, la restitution des moyens d'accès non requis.** **La possession effective des moyens d'accès par leurs détenteurs DOIT également être vérifiée lors de cette revue annuelle.** **Le câblage réseau DOIT être protégé contre les dommages et les interceptions des communications qu'ils transmettent.** **Les panneaux de raccordements et les salles des câbles DOIVENT être placés en dehors des zones d'accueil du public.**
Zones rouges	**Les règles suivantes DOIVENT être respectées en complément de celles applicables aux zones jaunes.** **Une zone rouge NE DOIT PAS être accessible directement depuis une zone blanche, et en aucun cas directement depuis l'extérieur d'un site du vice-rectorat de la Nouvelle-Calédonie. L'approche d'une zone rouge doit être contrôlée en permanence.** **Les fenêtres des bâtiments d'une zone rouge donnant vue sur l'extérieur DOIVENT être équipées de brise-vue occultant toute visibilité depuis l'extérieur sur l'intérieur de la zone sécurisée.** **Toutes les fenêtres des étages inférieurs des bâtiments d'une zone rouge (rez-de-chaussée et premier étage) DOIVENT être spécifiquement protégées contre l'effraction. Plus généralement, les dispositifs de protection mécanique des issues (huisseries, portes, fenêtres, serrures, verrous, …) doivent être résistants à l'effraction.** **La protection des fenêtres des étages bas peut être obtenue au moyen de la pose de barreaux suffisamment rapprochés ou d'un vitrage antieffraction (avec maintien des fenêtres fermées).** **L'ouverture des issues d'une zone rouge, usuelles ou de secours, y compris les fenêtres, DOIT être contrôlée et journalisée en permanence.** **L'ouverture des issues d'une zone rouge, usuelles ou de secours, y compris les fenêtres, doit**

	être contrôlée et signalée en temps réel à un centre de surveillance (interne ou externe) permanente. **Les accès à toute zone rouge DOIVENT être contrôlés, en entrée et sortie, au moyen d'un double dispositif : lecteur de carte et vérification d'un code personnel, associés à un système de vidéosurveillance.** **Toute zone rouge DOIT être équipée d'un dispositif permettant de détecter toute intrusion en dehors des heures de présence du personnel.** **Ces accès DOIVENT être strictement limités aux seules personnes préalablement autorisées.** **Un registre des détenteurs des moyens d'accès à chaque zone rouge DOIT être tenu à jour.** **Les responsables des locaux techniques dédiés aux équipements du SI situés en zone rouge DOIVENT réaliser une revue semestrielle de la pertinence des autorisations d'accès octroyées, et provoquer, si besoin, la restitution des moyens d'accès non requis.** **La possession effective des moyens d'accès par leurs détenteurs DOIT également être vérifiée lors de cette revue semestrielle.** **Sur les zones hébergement des SI particulièrement sensibles, des contrôles réguliers anti-piégeages (dépoussiérage) DOIVENT être effectués régulièrement. Il peut être fait appel à des services spécialisés.**

VII.5. Protection contre les risques divers ou environnementaux

VII.5.1. Protection de l'alimentation électrique

1.6. PHY-CI - ENERGIE : Alimentation secteur
Responsable : La DLL
Contributeurs : La DSI, le RSSI
L'alimentation secteur des équipements DOIT être conforme aux règles de l'art de façon à se prémunir des atteintes à la sécurité des personnes et équipements liées à un défaut électrique.

1.7. PHY-CI – ENERGIE : Entretien des installations électriques
Responsable : la DLL
Contributeurs : La DSI, le RSSI
Les installations d'alimentation en énergie électrique des centres informatiques DOIVENT être dimensionnées en tenant compte du plan de développement du centre informatique et disposer d'une réserve de puissance. **Elles DOIVENT être aménagées de façon à minimiser les risques de perturbation électrique.** **Elles DOIVENT comprendre un dispositif permettant de réguler la tension électrique (onduleur) délivrée aux équipements informatiques.** **Tous les composants des installations d'alimentation en énergie électrique DOIVENT être régulièrement contrôlés et entretenus par du personnel compétent.**

1.8. PHY-CI – ENERGIE : Secours de l'alimentation électrique.
Responsable : la DLL
Contributeurs : La DSI, le RSSI
En cas de défaillance des circuits normaux d'alimentation en énergie électrique dans les centres informatiques importants et/ou traitant des ressources classifiées au niveau 3 ou 4 pour le critère de disponibilité, des systèmes de secours DOIVENT être prévus et leur fonctionnement effectif régulièrement testé.

1.9. PHY-CI – ENERGIE : Gestion des coupures d'alimentation
Responsable : la DLL
Contributeurs : La DSI, le RSSI
En cas de défaillance des circuits normaux d'alimentation en énergie électrique des équipements non secourus et traitant des ressources classifiées au niveau 3 ou 4 pour les critères de disponibilité, d'intégrité ou de preuve, un dispositif de contrôle de la coupure électrique DOIT être mis en œuvre afin de prévenir tout dommage consécutif à l'arrêt brutal de l'équipement.

1.10. PHY-CI – ENERGIE : Protection des équipements contre la foudre.
Responsable : la DLL
Contributeurs : La DSI, le RSSI
Outre la protection contre la foudre des bâtiments au moyen de paratonnerres, les moyens de traitement informatique et les équipements de télécommunication DOIVENT être spécifiquement protégés contre les effets de la foudre. **Pour être efficaces, les dispositifs de protection (parafoudre, …) DOIVENT être placés au plus près possible des appareils à protéger.**

1.11. PHY-CI – ENERGIE : Protection contre les champs électromagnétiques
Responsable : la DLL
Contributeurs : La DSI, le RSSI
Les ordinateurs, les supports magnétiques et les câbles de communication se rapportant à des ressources classifiées au niveau 3 ou 4 pour le critère de disponibilité ne doivent pas être exposés à un niveau de parasites électromagnétiques (d'origine naturelle ou artificielle) supérieur aux limites spécifiées par leurs constructeurs.

VII.5.2. Protection contre l'incendie

1.12. PHY-CI - INC : Lutte contre l'incendie
Responsable : La DLL
Contributeurs : La DSI, le RSSI
L'installation de matériel de protection contre le feu est obligatoire. **Les mesures de confinement mises en œuvre, qui visent à limiter la propagation d'un incendie, reposent notamment sur des cloisons (ou murs) et des portes coupe-feu, et DOIVENT prendre en compte les faux-planchers, les faux-plafonds, de même que les passages de câbles (électricité, informatique, télécoms, …).** **Des procédures de réaction à un incendie DOIVENT être définies et régulièrement testées.** **Les salles techniques DOIVENT être propres.** **Aucun carton, papier ou autre sources potentielle de départ de feu ne DOIT être entreposé dans ces locaux.** **Il DOIT être strictement interdit de fumer dans ces locaux.**

1.13. PHY-CI – INC : Dispositifs de détection et d'extinction d'incendie.
Responsable : la DLL
Contributeurs : La DSI, le RSSI
Les zones dans lesquelles sont situées des ressources classifiées à un niveau égal ou supérieur à 3 pour le critère de disponibilité DOIVENT être équipées de moyens de détection et d'extinction automatique d'incendie conformes aux normes requises par les compagnies d'assurance. **Au sein des zones rouges ou lorsque la classification des ressources concernées atteint le niveau 4, ces moyens DOIVENT être reliés à un poste central de surveillance permanente.** **Tous les dispositifs de détection et d'extinction automatique d'incendie DOIVENT être entretenus et contrôlés au moins deux fois par an.**

VII.5.3. Protection contre les voies d'eau

1.14. PHY-CI - EAU : Lutte contre les voies d'eau
Responsable : la DLL
Contributeurs : La DSI, le RSSI
Une étude sur les risques dus aux voies d'eau DOIT être réalisée. **Cette étude DOIT notamment prendre en compte le risque de fuite sur un collecteur d'eau douce.**

1.15. PHY-CI – EAU : Protection contre les dégâts des eaux.
Responsable : la DLL
Contributeurs : La DSI, le RSSI
Les zones où sont situées ressources classifiées au niveau 3 ou supérieur pour le critère de disponibilité DOIVENT être équipées de dispositifs de détection d'eau et d'humidité. **Dans ces zones, ainsi que dans les bandothèques, le passage de canalisations d'eau DOIT être évité. En cas d'impossibilité (exemple : matériels à refroidissement liquide), le parfait état des conduites et de leur isolement DOIT être assuré et régulièrement contrôlé.** **Les vannes d'arrêt des canalisations traversant éventuellement ces zones ou situées à proximité doivent être placées hors des salles informatiques ou télécoms, dans des locaux protégés, leur emplacement devant être clairement signalé.** **Les dispositifs de détection et d'évacuation d'eau DOIVENT être périodiquement contrôlés par des personnels compétents et faire l'objet d'une maintenance régulière.**

VII.6. Contrôle des dispositifs de sécurité des accès physiques

1.16. PHY-SI - SUR : Sécurisation du SI de sûreté
Responsable : RSSI
Contributeurs : La DSI et la DLL
L'emploi de produits de sûreté labellisés, quand ils existent, DOIVENT être recommandés.

1.17. PHY – SI- SUR : Surveillance et maintenance des dispositifs de sécurité des accès physiques.
Responsable : RSSI
Contributeurs : La DSI et la DLL
Tous les dispositifs de surveillance et de contrôle des accès physiques, (SI de sûreté) DOIVENT être vérifiés et entretenus périodiquement par du personnel compétent. **L'arrêt ou le dysfonctionnement de tout équipement de sûreté des accès physiques DOIVENT être automatiquement détectés localement et déclencher une action immédiate, par l'intermédiaire d'une alerte transmise si possible en temps réel vers un centre de surveillance disposant des consignes et des procédures requises à une réaction appropriée.**

1.18. PHY – SI- SUR : Contrôle et test de la conformité de fonctionnement des dispositifs de sûreté des accès physiques.
Responsable : RSSI
Contributeurs : La DSI et la DLL
Un test exhaustif du fonctionnement effectif de tous les contrôles devant être mis en œuvre pour sécuriser les accès physiques aux différentes zones protégées DOIT être réalisé régulièrement.

1.19. PHY – SI- SUR : Contrôle de l'administration et de l'utilisation des dispositifs de sécurité des accès physiques.
Responsable : le RSSI
Contributeurs : La DSI et la DLL
Les accès et tentatives d'accès physiques aux zones jaunes, orange et rouges DOIVENT être journalisés, conservés et analysés de même que toutes les opérations d'administration des dispositifs de sûreté des accès physiques. **Dans le cas où les dispositifs de sécurité déployés reposent sur des micro-ordinateurs, la configuration tant matérielle que logicielle de ces postes informatiques DOIT également être contrôlée.**

VIII. Sécurité des réseaux

Objectif 12 : Sécurité des réseaux nationaux
Utiliser les infrastructures nationales, en respectant les règles de sécurité qui leurs sont attachées.
Objectif 13 : Usage sécurisé des réseaux locaux
Maîtriser les interconnexions de réseaux locaux. Configurer de manière adéquate les équipements de réseaux actifs.
Objectif 14 : Aspects spécifiques
Ne pas porter atteinte à la sécurité du SI par le déploiement d'accès non supervisés.
Objectif 15 : Usage sécurisé des réseaux sans fil
Maîtriser le déploiement, la configuration et l'usage des réseaux sans fil.
Objectif 16 : Sécurité des mécanismes de commutation et de routage
Configurer les mécanismes de commutation et de routage pour se protéger des attaques.
Objectif 17 : Cartographie réseau
Tenir à jour une cartographie détaillée et complète des réseaux et interconnexions

VIII.1. Sécurité du réseau national inter académique

8.1. RES- HEBER_PHY_RESEAU : Hébergement physique des composants réseau
Responsable : RSSI
Contributeurs : Le DSI, la DLL
Conformément à la directive sécurité physique du SI, les locaux hébergeant les équipements réseaux et sécurité sensibles (c'est-à-dire dont le profil de classification fait apparaître un niveau de sensibilité supérieur ou égal à 3 quel que soit le critère étudié) DOIVENT : • **être hébergés en zone jaune ou en zone rouge ;** • **disposer d'un contrôle d'accès physique (y compris pour les accès aux panneaux de brassage et aux câbles) ;** • **offrir des conditions opérationnelles d'hébergement conformes à celles recommandées par le constructeur, à l'état de l'art technique et aux exigences règlementaires ;** • **offrir si nécessaire un secours d'énergie garantissant une disponibilité des équipements en cas de coupure d'électricité.**

8.2. RES-MAITRISE : Systèmes autorisés sur le réseau national
Responsables : RSSI
Contributeurs : Le DSI
Seules les équipes informatiques à gérer et configurer un équipement DOIVENT être habilitées à connecter au réseau national un équipement.

8.3. RES-MAITISE : Déploiement des équipements réseau.
Responsable : DSI
Contributeur : Le RSSI
Les équipements réseau DOIVENT être déployés et mis à jour selon les configurations standardisées respectant les règles édictées au niveau national, afin notamment : • **de limiter leurs surfaces d'attaques logiques ;** • **d'encadrer l'administration des équipements, en particulier la gestion des accès et des traces ;** • **de mettre en œuvre une surveillance permanente des incidents de sécurité.** **Les ressources physiques n'étant pas sous le contrôle du vice-rectorat de la Nouvelle-Calédonie ne DOIVENT pas être connectées au réseau sans l'accord du RSSI.**

8.4. RES-INTERCO : Interconnexion avec des réseaux externes
Responsable : Le DSI
Contributeur : Le RSSI
Toute interconnexion entre les réseaux locaux et un réseau externe (réseau d'un tiers, Internet, …) DOIT être réalisée via les infrastructures nationales.

8.5. RES-ENTERSOR : Mettre en place un filtrage réseau pour les flux sortants et entrants
Responsables : Le DSI
Contributeur : Le RSSI
Dans l'optique de réduire les possibilités offertes à un attaquant, les connexions des machines du réseau interne vers l'extérieur DOIVENT être filtrées.

8.6. RES-ENTERSOR : Les configurations standardisées des équipements réseau sont spécifiées par la fonction SI.
Responsable : Le DSI
Contributeur : Le RSSI
Les points suivants DOIVENT être pris en compte : • **limitation des services techniques activés à ceux strictement nécessaires ;** • **utilisation de protocoles sécurisés pour l'administration des équipements (notamment via des mécanismes de chiffrement des séquences d'authentification et des échanges) ;** • **limitation des informations techniques contenues dans les bannières d'accueil des équipements ;** • **implémentation de la qualité de service.**

8.7. RES-PROT : Protection des informations
Responsable : Le DSI
Contributeur : Le RSSI
Les accès à Internet DOIVENT passer obligatoirement à travers les passerelles nationales. **Dès lors que des informations sensibles doivent transiter sur des réseaux non maitrisés, ces informations DOIVENT être chiffrées.**

VIII.2. Sécurité des réseaux locaux

8.8. RES- CLOIS : Cloisonner le SI en sous réseaux de niveaux de sécurité homogènes
Responsable : Le DSI
Contributeur : Le RSSI
Par analogie avec le cloisonnement physique d'un bâtiment, le SI DOIT être segmenté selon des zones présentant chacune un niveau de sécurité homogène.

8.9. RES_CLOIS : Classification et cloisonnement
Responsable : Le DSI
Contributeur : Le RSSI
Une segmentation logique (VLAN étanche) ou physique des réseaux locaux DOIT être mise en place en fonction du niveau de classification des systèmes connectés. **Cette segmentation DOIT respecter les principes suivants :** **Les systèmes numériques classifiés à un niveau 3 et 4 ne DOIVENT PAS être connectées sur des segments de réseau supportant des systèmes numériques classifiés au niveau 1 ou 2.** **Les systèmes numériques classifiés à un niveau 1 ne DOIVENT PAS être raccordées sur des segments supportant des systèmes numériques classifiés aux niveaux 2, 3 et 4 ;** **Des firewalls physiques ou logiques DOIVENT isoler les segments supportant des systèmes numériques classifiés aux niveaux 2 et 3 des autres segments. Pour certaines applications, lorsque le RSSI juge que la segmentation logique n'offre pas un niveau de sécurité suffisant, il DOIT imposer la mise en place d'une segmentation physique ;** **Des segments physiques dédiés DOIVENT être mis en œuvre pour les systèmes numériques utilisés pour la téléphonie IP, la vidéosurveillance les locaux et la surveillance des systèmes numériques.**

Dans le cas où une segmentation physique du réseau est nécessaire pour le raccordement de systèmes numériques classifiés aux niveaux 3 ou 4, le RSSI DOIT soumettre au CSSI la solution technique envisageable ainsi que les contraintes sur l'architecture technique opérationnelle.

Le CSSI décide alors du maintien de l'architecture VLAN ou le rajout de segment physique dédié au regard des enjeux de sécurité et des contraintes internes.

8.10. RES- INTERGEO : Interconnexion des sites géographiques locaux du vice-rectorat de la Nouvelle-Calédonie
Responsable : Le DSI
Contributeur : Le RSSI, le DAN
L'interconnexion au niveau local de réseaux locaux du vice-rectorat de la Nouvelle-Calédonie ne DOIT être possible que si la proximité géographique le justifie et sous réserve de la mise en place de connexions dédiées à cet effet et de passerelles validées par l'autorité d'homologation et / ou par le HFDS.

8.11. RES- RESS : Cloisonnement des ressources en cas de partage de locaux ;
Responsable : Le DSI
Contributeur : Le RSSI, le DAN
Dans le cas où un établissement partage des locaux avec des entités externes, des mesures de cloisonnement des ressources informatiques ou réseaux DOIVENT être mises en place. **Si le cloisonnement n'est pas physique, les mesures prises DOIVENT être validées par le ou les HFDS concernés.**

VIII.3. Aspects spécifiques

8.12. RES- INTERNET-SPECIFIQUE : Cas particulier des accès spécifiques à Internet dans l'académie
Responsables : Le DSI et ou le DAN
Contributeur : Le RSSI
Les accès spécifiques à Internet ne DOIVENT être mis en place que sur des dérogations dûment justifiées et sur des machines isolées physiquement et séparées du réseau de l'entité, après validation de l'autorité d'homologation.

8.13. RES- INTERNET-SPECIFIQUE : Contrôle des accès spécifiques dans l'académie
Responsables : Le DSI et ou le DAN
Contributeur : Le RSSI
En aucun cas la navigation sur Internet ne DOIT être autorisée sans authentification / contrôle d'accès.

VIII.4. Sécurité des réseaux sans fil

8.14. RES- SSFIL : Mise en place de réseaux sans fil
Responsable : Le DSI
Contributeur : Le RSSI
Le déploiement de réseaux sans fil DOIT faire l'objet d'une analyse de risques spécifique. Les protections intrinsèques complémentaires, validées par le HFDS concerné, DOIVENT être prises dans le cadre de la défense en profondeur. En particulier, une segmentation du réseau DOIT être mise en place de façon à limiter à un périmètre déterminé les conséquences d'une intrusion via la voix radio. A défaut de mise en œuvre de mesures spécifiques, le déploiement de réseaux sans fil sur des SI manipulant des données sensibles (2, 3, 4) DOIT être proscrit.

8.15. RES- INTERNET-SPECIFIQUE : Contrôle des accès spécifiques dans l'académie
Responsable : Le DSI
Contributeur : Le RSSI et ou le DAN
En aucun cas la navigation sur Internet ne DOIT être autorisée sans authentification / contrôle d'accès.

VIII.5. Sécurisation des mécanismes de commutation et de routage

8.16. RES- COUCHBAS : Implanter des mécanismes de protection contre les attaques sur les couches basses.
Responsable : Le DSI
Contributeur : Le RSSI
Une attention particulière DOIT être apportée à l'implantation des protocoles de couches basses, de façon à se prémunir des attaques usuelles par saturation ou empoisonnement de cache mémoire. Cela concerne par exemples, les protocoles ARP ou ICMP.

8.17. RES- ROUTDYN : Surveiller les annonces de routage
Responsable : Le DSI
Contributeur : Le RSSI
Lorsque l'utilisation de protocoles de routage dynamiques est nécessaire, celle-ci DOIT s'accompagner de la mise en place d'une surveillance des annonces de routage, et de procédures permettant de réagir rapidement en cas d'incidents.

8.18. RES- ROUTDYN - IGP: Configurer les protocoles IGP de manière sécurisée
Responsable : Le DSI
Contributeur : Le RSSI
Les protocoles de routage dynamique de type IGP DOIVENT être activés exclusivement sur les interfaces nécessaires à la construction de la topologie du réseau et désactivés sur le reste des interfaces. **La configuration des protocoles de routage dynamique DOIT systématiquement s'accompagner d'une authentification, exemple Message- digest-key.**

8.19. RES- ROUTDYN - EGP: Configurer les protocoles EGP de manière sécurisée
Responsable : Le DSI
Contributeur : Le RSSI
Lors de la mise en place d'une session EGP avec un réseau extérieur sur un média partagé, cette session DOIT s'accompagner d'une authentification, exemple Message- digest-key.

8.20. RES-SECRET : Modifier systématiquement les éléments d'authentification par défaut des équipements et services réseau.
Responsable : Le DSI
Contributeur : Le RSSI
Les dispositifs d'authentification par défaut DOIVENT être impérativement modifiés (mots de passe, certificats, ...) **Les dispositions nécessaires DOIVENT être prises auprès des fournisseurs de façon à pouvoir modifier les certificats installés par défaut.**

8.21. RES- DURCI: Durcir les configurations des équipements de réseaux
Responsable : Le DSI
Contributeur : Le RSSI
Les équipements de réseaux doivent faire l'objet d'un durcissement spécifique comprenant la désactivation des interfaces et services inutiles.

VIII.6. Cartographie réseau

8.22. RES- CARTO : Elaborer les documents d'architecture technique et fonctionnelle
Responsable : Le DSI
Contributeur : Le RSSI
L'architecture réseau du SI DOIT être décrite et formalisée à travers des schémas d'architecture et des configurations, maintenus au fil des évolutions apportées au SI. **Les documents d'architecture DOIVENT être classifiés au minimum au niveau 2 et font donc l'objet d'une protection adaptée.** **La cartographie réseau DOIT s'insérer dans la cartographie des SI.**

8.23. RES- CARTO1 : Inventaire des équipements réseau.
Responsable : Le DSI
Contributeur : Le RSSI
Un inventaire des équipements réseau DOIT être établi, pour les réseaux « Voix » et les réseaux « Données ». **Cet inventaire DOIT comprendre :** • **le propriétaire de l'équipement ;** • **les sites géographiques reliés pour les équipements d'interconnexion : correspondants, rattachements organisationnels ;** • **les logiciels de base installés dans les équipements de réseau : types et versions de firmwares,** • **le plan d'adressage ;** • **la cartographie du réseau.**

8.24. RES- CARTO2 : Classification des équipements réseau.
Responsable : Le DSI
Contributeur : Le RSSI
Une classification des équipements réseau connectés aux réseaux du vice-rectorat de la Nouvelle-Calédonie DOIT être établie conformément à la directive Gestion des biens.

Chaque équipement du réseau doit avoir un profil de classification, en théorie déduit des profils de classification des informations circulant sur ces équipements ou des ressources (systèmes, postes de travail, applications, etc.) connectées à l'équipement.

Le « propriétaire » de l'équipement doit inscrire, ou faire inscrire, le profil de classification dans l'inventaire des équipements réseau.

Une attention particulière doit être apportée à la mise en cohérence du niveau de sécurité fourni tout au long des chaînes de liaison (ensemble de ressources mobilisées par une application) avec le niveau requis par les applications.

IX. Architecture des SI

Objectif 18 : Architecture sécurisée des centres informatiques

Appliquer les principes de défense en profondeur à l'architecture matérielle et logicielle des centres informatiques.

IX.1. Principe structurant

L'intégration de la sécurité en phase de conception d'une architecture répond à 2 impératifs :

- garantir le niveau de sécurité consécutif aux besoins classifiés exprimés et requis par les métiers ;
- garantir un niveau de sécurité en adéquation avec l'environnement dans lequel cette architecture sera déployée ;

Le niveau de risque pesant sur une architecture dépend :

- des informations que celle-ci traite ou héberge et qui peuvent susciter l'intérêt d'attaquants potentiels ;
- de la facilité avec laquelle cette architecture est attaquable ;
- de l'environnement dans lequel cette architecture est exploitée.

Les menaces peuvent prendre différentes formes :

- actes de malveillance (fraude, vols, divulgation d'information, attaque par déni de service…) ;
- erreurs, et manque de maîtrise (départ de personnes clés par exemple) ;
- sinistres (incendie, dégâts des eaux, panne technique…) ;
- événements naturels non maîtrisables (inondation, tornades, phénomènes sismiques, foudre…) ;
- défaillances techniques, (pannes, dysfonctionnements, internes ou externes au SI…) ;

L'identification de la nature et de la provenance d'une menace (et donc des scénarios possibles d'attaques) doit permettre de qualifier les principes techniques à mettre en œuvre pour sécuriser l'architecture cible.

9.1. ARCHI-HEBERG : Principes d'architecture de la zone d'hébergement
Responsable : Le DSI
Contributeur : Le RSSI
D'une manière générale, l'architecture des infrastructures des centres informatiques DOIT être conçue de façon à satisfaire l'ensemble des besoins de disponibilité, intégrité, confidentialité et traçabilité. **Le principe de défense en profondeur DOIT être respecté, en particulier pour la mise en œuvre de « zones démilitarisées », d'environnements de sécurité en zone d'hébergement, de machines virtuelles ou physiques dédiées, de réseaux locaux virtuels (VLAN) appropriés d'un filtrage strict des flux applicatifs et d'administration.**

IX.1.1. Précisions

IX.1.1.1. La zone d'hébergement

La zone d'hébergement est un ensemble de points de connexion géographiquement proches permettant l'accès de ressources au réseau du vice-rectorat de la Nouvelle-Calédonie.
La zone d'hébergement abrite un certain nombre de zones réseaux :

- une zone de sécurité,
- des zones démilitarisées utilisées pour la communication avec l'extérieur de la zone d'hébergement.

IX.1.1.2. Les zones démilitarisées

Une zone tampon est une zone hébergeant des ressources dont le rôle est d'assurer la protection d'une zone de sécurité, par le filtrage ou la maîtrise des flux échangés entre cette zone contrôlée et l'extérieur.

IX.1.1.3. Les zones de sécurité

Une zone de sécurité regroupe l'ensemble des ressources que sont les postes de travail, services, applications et utilisateurs sous contrôle de l'organisation SSI du vice-rectorat de la Nouvelle-Calédonie. Elle peut elle-même contenir des zones de sécurité supplémentaires permettant de regrouper des ressources par profils de classification similaires.

Pour être hébergé dans la zone de sécurité, tout élément doit être connu et accepté de l'organisation SSI du vice-rectorat de la Nouvelle-Calédonie.

9.2. ARCHI-HEBERG : Validation de la connexion d'une ressource physique à une zone d'hébergement.
Responsable : Le RSSI
Contributeur : Le DSI
Toute nouvelle ressource physique connectée à une zone d'hébergement doit avoir fait l'objet d'une analyse pour les aspects sécurité. Cette analyse doit notamment : • **permettre de vérifier la conformité de la ressource à la PSSI du vice-rectorat de la Nouvelle-Calédonie;** • **comporter une étude des nouveaux risques que la connexion de la nouvelle ressource fait peser sur l'existant.** **Cette analyse ne DOIT pas nécessairement être renouvelée pour chaque nouvelle ressource si celle-ci est, d'un point de vue de la sécurité, comparable à une autre ressource connectée au réseau et ayant déjà fait l'objet d'une recette.**

9.3. ARCHI-HEBERG : Autorisation de la connexion de ressources physiques externes au réseau.
Responsable : Le RSSI et ou le DAN
Contributeur : Le DSI
Les ressources physiques n'étant pas sous le contrôle du vice-rectorat de la Nouvelle-Calédonie ne DOIVENT pas être connectées au réseau sans l'accord de la filière SSI.

9.4. ARCHI-HEBERG : Cloisonnement au sein des zones d'hébergement.
Responsable : Le DSI
Contributeur : Le RSSI
Les ressources sensibles (DICP supérieur ou égal à 3) DOIVENT être hébergées dans des zones de sécurité supplémentaires.

Est considérée comme sensible toute ressource présentant un niveau de classification supérieur ou égal à 3, quel que soit le critère étudié.

On veillera à ne pas mélanger au sein d'une même zone de sécurité des ressources de profils de classification différents.

On anticipera la mise en place de ces zones de sécurité en séparant au niveau réseau des ressources de types différents.

9.5. ARCHI-HEBERG : Gestion des flux entre zones d'hébergement de l'académie
Responsable : Le DSI
Contributeur : Le RSSI
Les flux circulant entre deux zones d'hébergement de sécurité distinctes par exemple une zone gestion et une zone pédagogie DOIVENT : • **soit transiter par une zone tampon dont l'objet est de limiter les risques pesant sur le domaine de sécurité,» ;** • **soit faire l'objet d'un traitement spécifique (filtrage, cloisonnement dans une zone de sécurité dédiée, etc.), et d'une documentation appropriée.** **Par ailleurs, ces flux DOIVENT faire l'objet d'une analyse de risques communiquée aux autorités de chacun des domaines de sécurité concernés.**

9.6. ARCHI-HEBERG : Gestion des flux entre les zones d'hébergement du vice-rectorat de la Nouvelle-Calédonie et l'extérieur
Responsable : Le DSI
Contributeur : Le RSSI
Toute mise en place de nouveaux flux entre le réseau de l'académie contenant une ou plusieurs zones d'hébergement et l'extérieur de l'académie DOIT être précédée d'une analyse de risques systématique. Cette analyse de risques DOIT proposer les mesures de sécurité adaptées à la sécurisation de ces nouveaux flux. **Tout accès depuis le réseau interne de l'académie vers l'extérieur ne pouvant pas passer par une zone démilitarisée DOIT être autorisé par le RSSI eu égard aux risques encourus.** **Tout accès depuis l'extérieur vers une ressource du réseau interne d'une zone d'hébergement de l'académie DOIT obligatoirement comporter un passage dans une zone démilitarisée.** **Dans le cas où une authentification forte des utilisateurs externes et un tunnel chiffré de communication entre eux et la zone tampon sont mis en œuvre, un accès direct sera autorisé depuis la zone démilitarisée uniquement vers les ressources du réseau interne nécessaires en fonction du profil de l'utilisateur et de la typologie des accès.** **En l'absence d'authentification forte ou de tunnel chiffré, un traitement complet applicatif du flux dans la zone démilitarisée tampon SERA OBLIGATOIRE et aucun flux vers des ressources hébergées sans protection en zone de sécurité ne sera autorisé.** **Dans le cas où l'accès depuis la zone tampon vers des ressources hébergées au sein du réseau interne reste nécessaire, les flux ne seront autorisés qu'avec mise en œuvre des mesures suivantes :** • **les flux sortants ne DEVRONT pas être reproduits à l'identique par rapport au flux entrants dans la zone tampon ;** • **les ressources internes devront obligatoirement être hébergées dans une zone de sécurité supplémentaire du réseau interne. Les flux sortants depuis cette zone de sécurité supplémentaire seront limités au strict nécessaire de manière à éviter tout risque de rebond.**

9.7. ARCHI-STOCKCI : Architecture de stockage et de sauvegarde
Responsable : Le DSI
Contributeur : Le RSSI
Le réseau de stockage/sauvegarde pour les besoins des centres informatiques DOIT reposer sur une architecture dédiée à cet effet.

9.8. ARCHI-PASS : Passerelles Internet
Responsable : Le DSI et ou le DAN
Les interconnexions Internet DOIVENT passer obligatoirement par les passerelles nationales homologuées.

X. Exploitation des SI

Objectif 19 : Protection des informations sensibles
Définir et mettre en œuvre des mesures de protection renforcées pour les informations sensibles.
Objectif 20 : Surveillance et configuration des ressources informatiques
Durcir les configurations des ressources informatiques et surveiller les interventions opérées sur celles-ci.
Objectif 21 : Autorisation et contrôle d'accès logique aux ressources
Authentifier les usagers et contrôler leurs accès aux ressources des SI de l'Etat, en fonction d'une politique explicite d'autorisations.
Objectif 22 : Sécurisation de l'exploitation
Fournir aux administrateurs les outils nécessaires à l'exercice des tâches SSI et configurer ces outils de manière sécurisée.
Objectif 23 : Défense des systèmes d'information
Défendre les SI nécessite une vigilance de tous et des actions permanentes.
Objectif 24 : Exploitation sécurisée des centres informatiques
Exploiter de manière sécurisée les centres informatiques en s'appuyant sur des procédures adaptées et sur la maîtrise des outils de supervision.

X.1. Protection des informations sensibles

10.1 EXP-PROT-INF : Protection des informations en confidentialité et en intégrité
Responsable : Le RSSI
Contributeur : Le DSI
Formalisation d'un guide de protection des informations sensibles
Des mesures doivent être mises en œuvre afin de garantir la protection des informations sensibles en confidentialité et en intégrité. A défaut d'utilisation d'un réseau homologué, ces informations doivent être chiffrées et ou signées/scellées à l'aide d'un moyen de chiffrement labellisé.

Toutes les règles de protection de la disponibilité, de l'intégrité, de la confidentialité et de la traçabilité sont présentées dans la directive gestions des biens.

X.2. Sécurité des ressources informatiques

X.2.1. Protection physique des socles systèmes

Les matériels sur lesquels sont installés les socles systèmes doivent être situés dans des zones de protection adaptées et bénéficier des mesures de sécurité physique requises, en conformité avec les règles édictées au sein de la directive et des règles associées sécurité physique du SI, en termes de :

- sécurité des accès physiques ;
- protection contre les risques environnementaux (fourniture des servitudes essentielles, sécurité incendie, protection contre les dégâts des eaux).

La protection du câblage de ces matériels doit également être assurée afin de prévenir tout dommage physique ou l'interception d'informations.

X.2.2. Traçabilité des interventions de maintenance

10.2 EXP- TRAC : Traçabilité des interventions sur le SI
Responsable : Le DSI
Contributeur : Le RSSI
Les interventions de maintenance sur les ressources SI du vice-rectorat de la Nouvelle-Calédonie DOIVENT être tracées par la DSI et ces traces DOIVENT être accessibles au RSSI pendant au moins un an.

10.3 EXP – TRAC : Journal de maintenance
Responsable : Le RSSI
Contributeur : Le DSI
Un journal de toutes les interventions de maintenance d'équipement de réseau (matériel et logiciel), indiquant les modifications effectuées ou solutions apportées et l'identifiant de l'intervenant DOIT être tenu à jour.

X.2.3. Durcissement des configurations

10.4 EXP- CONFIG : Configuration des ressources SI
Responsable : Le DSI
Contributeur : Le DSI
Les systèmes d'exploitation et les logiciels DOIVENT faire l'objet d'un durcissement. **Les configurations et mises à jour DOIVENT être appliquées dans le strict respect des guides et procédures en vigueur au vice-rectorat de la Nouvelle-Calédonie ou dans le ministère.**

10.5 EXP – CONFIG : Durcissement des configurations des ressources SI
Responsable : Le DSI
Contributeur : Le DSI
La configuration des socles systèmes DOIT limiter les surfaces d'attaque logique : • **prise en compte des vulnérabilités (failles) de configuration publiées ;** • **restriction des fonctionnalités, protocoles et services aux stricts besoins nécessaires.** **Les composants matériels inutiles ou considérés comme dangereux en regard de la sensibilité du socle système DOIVENT être désinstallés, désactivés ou spécifiquement protégés.**

X.2.4. Documentation et base de données des configurations

10.6 EXP- DOC-CONFIG : Documentation des configurations des ressources SI
Responsable : Le DSI
Contributeur : Le RSSI
Formalisation et mise à jour de la configuration des ressources SI
La configuration des ressources SI DOIT être documentée et mise à jour à chaque changement notable.

10.7 EXP- DOC_CONFIG : Base d'information des systèmes
Responsable : Le DSI
Contributeur : Le RSSI
Formalisation et mise à jour de la configuration des ressources SI
Une base d'informations des socles systèmes doit être alimentée et maintenue à jour, afin d'être en mesure de maîtriser le niveau de sécurité des équipements déployés au sein des SI du vice-rectorat de la Nouvelle-Calédonie, avec les éléments suivants : • **le responsable désigné de chaque socle système ;** • **la liste des logiciels de base installés dans leur version en cours (système d'exploitation, SGBD, utilitaires, …) ;** • **les applications associées au socle système et leur propriétaire ;** • **la référence des spécifications de configuration appliquées sur le socle système.**

X.2.5. Gestion des autorisations et contrôle d'accès logique aux ressources du SI

Les règles de sécurité relatives au domaine particulier de la gestion des accès logiques aux SI visent à :

- limiter les risques d'erreur ou de malveillance consécutifs à des accès injustifiés ou illicites au SI afin de préserver l'intégrité, la confidentialité et la disponibilité des données du vice-rectorat de la Nouvelle-Calédonie ;
- faciliter l'imputabilité des accès au SI et la justification des opérations réalisées en leur sein.

X.2.5.1. Le contrôle d'accès logique

10.8 EXP- ID-AUTH : Identification, authentification et contrôle d'accès logique
Responsable : Le DSI
Contributeur : Le RSSI
Formalisation de la procédure d'autorisation
L'accès à toute ressource non publique DOIT nécessiter une identification individuelle de l'utilisateur. **Dans le cas de l'accès à des données sensibles, des moyens d'authentification forte DOIVENT être utilisés.** **A cette fin, l'usage d'une carte à puce DOIT être privilégié.** **Le contrôle d'accès DOIT être géré et s'appuyer sur un processus formalisé en cohérence avec la gestion des ressources humaines.**

10.9 EXP- ID-PERS : Identification personnelle des utilisateurs
Responsable : Le DSI
Contributeur : Le RSSI
Chaque utilisateur du SI du vice-rectorat de la Nouvelle-Calédonie, acteur interne ou externe (collaborateur, prestataire, stagiaire), permanent ou temporaire, DOIT être identifiable de façon strictement personnelle, selon un dispositif permettant d'établir un lien unique, fiable et pérenne avec cette personne physique. Par conséquent : • **chaque utilisateur SI se voit attribuer un (ou plusieurs) identifiant(s) strictement personnel(s) ;** • **l'utilisation par un usager d'un identifiant personnel appartenant à un autre utilisateur est interdite (même avec son accord) ;** • **le partage d'un même identifiant par plusieurs utilisateurs n'est pas autorisé, à l'exception des cas spécifiques et exceptionnels aux organisations de travail, pour lesquels des dispositions particulières doivent être établies, documentées et validées par le RSSI, et sous réserve que l'utilisation de ces identifiants « collectifs » soit strictement limitée aux réseaux opérés par l'académie ;** • **les « identifiants par défaut » associés à des comptes fournis lors de l'installation initiale des systèmes (comptes « invités », comptes « anonymes », …) et qui ne sont pas absolument indispensables à leur fonctionnement doivent être supprimés ou désactivés, leur utilisation étant interdite.**

10.10 EXP- DROITS : Droits d'accès aux ressources
Responsable : Le DSI
Contributeurs : Le RSSI et le CPU ou le DAN
Formalisation et mise à de la configuration des ressources SI
Après avoir déterminé le niveau de sensibilité ; le besoin de diffusion et de partage des ressources, les droits d'accès aux ressources DOIVENT être gérés suivant les principes suivants : • **le besoin d'en connaitre, chaque utilisateur n'est autorisé à accéder qu'aux ressources pour lesquelles on lui accorde explicitement le bénéfice de l'accès ;** • **le moindre privilège, chaque utilisateur accède aux ressources avec le minimum de privilèges lui permettant de conduire les actions explicitement autorisées pour lui.**

10.11 EXP- PROFILS : Gestion des profils d'accès aux applications
Responsables : Le DSI
Contributeurs : Le DSI ou le DAN avec les CPU ou les RM
Les applications manipulant des informations sensibles DOIVENT permettre une gestion fine par profils d'accès. **Les principes suivant DOIVENT s'appliquer :** • **établir un lien entre un utilisateur identifiable en tant que personne physique et un ensemble défini et limité d'accès autorisés aux ressources du SI, ce lien étant établi, sauf impossibilité, via un ou plusieurs profils d'accès prédéterminés ;** • **savoir à quoi peut accéder un utilisateur et d'être en mesure de justifier et d'actualiser ces autorisations ;** • **du besoin d'en connaitre ;** • **du moindre privilège ;** • **de la séparation des droits non cumulables.**

10.12 EXP-PROFILS-AFF-Affectation des profils d'accès aux applications
Responsable : DSI
Contributeurs : Le RSSI et le CPU ou le DAN
La gestion des profils d'accès au SI de l'académie doit : • **être réalisée sous la seule et unique autorité d'un responsable désigné au sein du métier concerné ;** • **respecter les principes de moindre privilège et de séparation des tâches ;** • **donner lieu à une revalidation périodique de la pertinence et de la compatibilité des droits par profil et des profils cumulables.**

X.2.5.2. Précisions

La personne habilitée à valider les demandes d'accès est en général la fonction responsable de l'entité à laquelle est rattaché l'utilisateur concerné.

Dans le cas où la demande d'habilitation porte sur des accès privilégiés (permettant de réaliser des opérations à risque ou d'atteindre des ressources sensibles du SI), celle-ci doit aussi être soumise à l'approbation du responsable désigné au sein du métier concerné par chacune des ressources accédées.

Lorsque la demande concerne un tiers, tel qu'un prestataire ou un partenaire du vice-rectorat de la Nouvelle-Calédonie, le responsable habilité au sein du vice-rectorat de la Nouvelle-Calédonie doit la valider et vérifier l'existence d'un contrat qualifiant les termes et les conditions de l'accès au SI du vice-rectorat de la Nouvelle-Calédonie.

L'attribution des droits d'accès au SI doit se limiter aux besoins strictement nécessaires aux activités de l'utilisateur, et respecter les règles d'exclusion établies conjointement par les responsables des métiers concernés (faisant mention des droits d'accès non cumulables).

Enfin, la limite de validité des droits d'accès temporaires (accordés par exemple aux personnels en contrat à durée déterminée, aux prestataires, aux intérimaires, aux stagiaires, …) doit être définie lors de la demande d'accès ou fixée par défaut par la fonction SI en accord avec les métiers, la durée maximum de validité des droits d'accès temporaires étant de 1 an.

X.2.5.3. Point de vigilance

Le principe de séparation des pouvoirs (requis notamment par certains contextes métiers tels que la finance ou la comptabilité informatisée implique celui de séparation des tâches opérées au sein du SI et se traduit par l'interdiction du cumul de certains droits d'accès incompatibles au sein du SI compte tenu des activités qu'ils permettent de réaliser.

Par conséquent, il convient, lors de l'octroi des habilitations d'accès à une ressource du SI (ex : une application métier), de vérifier si la personne physique bénéficiaire dispose de différents "comptes" sur cette ressource.

En effet, ceci pourrait lui permettre, compte tenu du cumul des droits d'accès associés à ces différents comptes, de réaliser des opérations en contradiction avec le principe de séparation des tâches.

Ce principe de séparation des tâches s'applique également aux activités liées à la gestion des habilitations d'accès.

La mise en œuvre des autorisations d'accès (création, modification, suspension ou suppression d'une habilitation d'accès) doit être réalisée par :

- une fonction différente de celle qui opère l'administration du contenu des profils d'accès, ou, en l'absence de ces profils d'accès, de celle qui déclare l'utilisateur au sein du SI ;
- une personne différente de celle qui émet la demande d'accès.

X.2.6. Processus d'autorisation

10.13 EXP- PROC-AUTH : Autorisation d'accès des utilisateurs
Responsables : RH, responsable métier et RSSI
Contributeurs : Le DSI et le CPU ou le DAN
Formalisation et mise à de la configuration des ressources SI
Toute action d'autorisation d'accès d'un utilisateur à une ressource SI, qu'elle soit locale ou nationale DOIT s'inscrire dans le cadre d'un processus d'autorisation formalisé qui s'appuie sur le processus d'arrivée et de départ du personnel.

10.14 EXP- REVUE –AUTH : Revue des autorisations d'accès
Responsable : Le RSSI
Contributeurs : Le RSSI et le CPU ou le DAN
Une revue des autorisations d'accès DOIT être réalisée annuellement sous le contrôle du RSSI et avec l'appui du correspondant SSI.

10.15 EXP- PROC-AUTH : Mise en œuvre des autorisations d'accès des utilisateurs
Responsables : Le DSI ou le DAN
Contributeurs : Le RSSI
Formalisation et mise à de la configuration des ressources SI
Aucun accès effectif aux SI ne doit être autorisé avant validation expresse de la demande par un responsable habilité (en respectant le principe de séparation des pouvoirs). **Le processus de validation des habilitations d'accès doit prendre en compte :** • **la conformité des droits d'accès requis avec les principes de moindre privilège et les règles de séparation des tâches ;** • **la nécessité éventuelle de limiter dans le temps la validité des accès octroyés ;** • **la restriction si besoin de ces accès en fonction de critères calendaires ou de localisation de l'accédant.** **La mise en œuvre des autorisations d'accès (création, modification, suspension ou suppression d'une habilitation d'accès) DOIT être réalisée par :** • **une fonction différente de celle qui opère l'administration du contenu des profils d'accès, ou, en l'absence de ces profils d'accès, de celle qui déclare l'utilisateur au sein du SI ;** • **une personne différente de celle qui émet la demande d'accès.**

X.2.7. Gestion des authentifiants

10.16 EXP- CONF-AUTH : Confidentialité des informations d'authentification
Responsables : Tous
Contributeurs : Le RSSI ou le DAN
Les informations d'authentification, (mots de passe d'accès aux SI, des clés privées liées aux certificats électroniques, etc.) DOIVENT être considérées comme des données sensibles (niveau 3 en confidentialité).

10.17 EXP- GEST-PASS : Gestion des mots de passe
Responsables : Tous
Contributeurs : Le RSSI et le DSI ou le DAN
Les utilisateurs ne doivent pas stocker leurs mots de passe en clair, (par exemple) dans un fichier sur leurs postes de travail. Les mots de passe ne doivent pas transiter en clair sur les réseaux.

10.18 EXP- INIT-PASS : Initialisation des mots de passe
Responsable : Le DSI
Contributeurs : Le RSSI et ou le DAN
Chaque compte utilisateur DOIT être crée avec un mot de passe initial aléatoire et unique. Si les circonstances l'imposent un mot de passe plus simple mais à usage unique peut être envisagé.

10.19 EXP- POL-PASS : Politique des mots de passe
Responsables : Tous
Contributeurs : Le RSSI et le CPU ou le DAN
Les règles de gestion et de protection des mots de passe donnant accès aux applications et infrastructures nationales, telles qu'édictées par les maîtrises d'ouvrage DOIVENT être respectées. Pour les ressources dont la politique des mots de passe est gérée localement, les recommandations de l'ANSSI DOIVENT être appliquées pour tous les comptes.

10.20 EXP- POL-PASS : Politique des mots de passe
Responsable : Le RSSI
Contributeurs : Le DSI et le CPI ou le DAN
Formalisation du guide de gestion des mots de passe
La taille minimale des authentifiants utilisateurs, DOIT être fixée à 12 caractères minimum composés de lettre majuscules, minuscules, de chiffres et de caractères spéciaux. Des moyens mnémotechniques sont utilisés afin que les mots de passe ne soient pas écrits et des consignes à destination des utilisateurs sont mentionnées dans la charte informatique. Le changement des mots de passe est régulier, tous les 3 mois minimum sur recommandation de l'ANSSI ; La taille des mots de passe administrateur DOIT être fixée à un minimum de 16 caractères composés de lettres, chiffres et caractères spéciaux. La fréquence minimale de changement de ces mots de passe est fixée à 6 mois maximum. Pour les comptes administrateurs des systèmes numériques supportant des données classifiées au niveau C3, la fréquence de changement des mots de passe est fixée à 3 mois ; Lorsque le renouvellement d'un mot de passe est nécessaire (en cas d'oubli par exemple), les systèmes, obligent l'utilisateur à changer le mot de passe générique.

10.21 EXP- QUAL-PASS : Contrôle systématique de la qualité des mots de passe
Responsable : Le RSSI
Contributeurs : Le DSI ou le DAN
Des moyens techniques permettant d'imposer la politique des mots de passe, (par exemple) pour s'assurer du respect de l'obligation relative à l'usage des caractères spéciaux) DOIVENT être mis en place. A défaut un contrôle périodique des paramètres techniques relatifs aux mots de passe DOIT être réalisé.

10.22 EXP- QUAL-PASS : Prévention des conséquences de divulgation des authentifiants
Responsable : Le RSSI
Contributeurs : Le DSI ou le DAN et tous les utilisateurs
Des dispositions DOIVENT être prises afin de limiter les conséquences de la divulgation d'authentifiant permettant l'accès au SI du vice-rectorat de la Nouvelle-Calédonie : • information aux utilisateurs de la nécessité de modifier immédiatement leur code secret (mot de passe, code pin) dès lors que la divulgation ou compromission en est suspectée ; • mise en place d'une procédure permettant de rendre inopérants les supports physiques d'authentification en cas de perte ou de vol, ceci dans les délais les plus brefs ; • en cas de compromission d'un système : application d'une procédure de restauration d'un système intègre, et modification ou réinitialisation de la totalité des codes secrets gérés au niveau de ce système. Les utilisateurs sont responsables de la protection des authentifiants qui leur sont confiés, et qui ne DOIVENT être ni partagés, ni communiqués ou prêtés à un tiers

X.2.8. Recommandations

- Avoir des mots de passe de 12 caractères minimum, si possible de 16 caractères.
- Utiliser des caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux).
- Ne pas utiliser de mot de passe ayant un lien avec soi (noms, dates de naissance…).
- Le même mot de passe ne doit pas être utilisé pour des accès différents.
- Changer de mot de passe régulièrement.

X.2.9. Gestion des authentifiants d'administration

10.23 EXP- SEQ-ADMIN : Séquestre des authentifiants « administrateur »
Responsable : Le DSI
Contributeurs : Le DSI ou le DAN
Les authentifiants permettant l'administration des ressources du SI DOIVENT être placés sous séquestre et tenus à jour, dans un coffre ou une armoire fermée à clé. **Tout accès d'administration à une ressource SI DOIT pouvoir être tracé et permettre de remonter à la personne ayant ce droit.** **Les informations d'authentification bénéficiant d'un moyen de protection physique, (notamment carte à puce) n'ont par défaut pas besoin d'être l'objet d'opérations de séquestre de la part d'autres personnels que l'authentifié lui-même.**

10.24 EXP- POL- ADMIN : Politique des mots de passe administrateur
Responsable : Le DSI
Contributeurs : Le DSI ou le DAN
Chaque administrateur DOIT disposer d'un mot de passe propre à l'administration.

10.25 EXP- DEP- ADMIN : Gestion du départ d'un administrateur
Responsables : RSSI et DSI
En cas départ d'un administrateur disposant de privilèges sur des composants du SI, les comptes individuels dont il disposait DOIVENT être immédiatement désactivés. **Les éventuels mots de passe d'administration dont il avait connaissance DOIVENT être changés.**

X.2.10. Précisions sur la responsabilité des utilisateurs et administrateurs pour les mots de passe

Il est essentiel que les utilisateurs et administrateurs soient alertés, lors du choix de leur mot de passe, des règles à appliquer pour en assurer la robustesse.
Le respect de ces principes implique que les dispositifs d'authentification fournissent les fonctionnalités contraignant les utilisateurs à définir et modifier eux-mêmes leurs mots de passe, et ce à travers une procédure intégrant leur réauthentification préalable.
Concernant la composition des mots de passe, la notion de « complexité » implique l'interdiction :

- d'utiliser des termes triviaux (ex : nom propre, identifiant, prénom, nom commun…).
- l'utilisation de caractères non imprimables (caractère de contrôle par exemple) doit être proscrite, en raison des problèmes de transmission qu'ils sont susceptibles de générer et des interférences possibles avec certains utilitaires système.

X.2.11. L'utilisation des certificats

10.26 EXP- CERTIFS : Utilisation de certificats électroniques
Responsable : Le correspondant SSI de la DSI
Contributeurs : Le DSI, le RSSI
L'utilisation de certificats électroniques doit respecter les règles édictées par le RGS.

X.2.12. Précisions sur les certificats

L'utilisation de ces certificats numériques est conforme à la norme X509 de classe 3 fournis par une autorité de certification habilitée ou certifiée par l'ANSSI.

10.27 EXP- CERTIFS : Gestion des certificats électroniques
Responsables : Le correspondant SSI de la DSI
Contributeurs : Le DSI, le RSSI
Une politique spécifique de sécurité relative à la gestion des clés publiques DOIT être formalisée par le RSSI en collaboration avec les équipes techniques de la DSI. Cette politique DOIT appliquer les directives de l'ANSSI énoncées dans le RGS et ses annexes. Le RSSI DOIT tenir à jour la liste des systèmes utilisant les mécanismes d'authentification basés sur les certificats numériques

X.3. Exploitation sécurisée des ressources du SI

X.3.1. Administration des SI

10.28 EXP- RESTR-DROITS : Restriction des droits
Responsable : Le DSI
Contributeurs : Le RSSI ou le DAN
Sauf exception dûment motivée et validée par le RSSI, les utilisateurs ne DOIVENT pas avoir de droits d'administration.

10.29 EXP- PROT - ADMIN : Protection des accès aux outils d'administration
Responsables : Le RSSI et le correspondant SSI de la DSI
Contributeurs : Le DSI
L'accès aux outils et interfaces d'administration DOIT être strictement limité aux personnes habilitées selon une procédure formelle d'autorisation d'accès.

10.30 EXP- HABILIT- ADMIN : Habilitation des administrateurs
Responsables : Le RSSI et le CSSI
Contributeurs : Le DSI ou le DAN
L'habilitation des administrateurs DOIT s'effectuer selon une procédure validée par l'autorité d'homologation. Le nombre de personnes habilitées pour les opérations d'administration DOIT être connu et validé par l'autorité d'homologation.

10.31 EXP- GEST-ADMIN : Gestion des actions d'administration
Responsables : Le DSI
Contributeurs : Le RSSI ou le DAN
Les opérations d'administration DOIVENT être tracées de manière à pouvoir gérer au niveau individuel l'imputabilité des actions d'administration.

10.32 EXP- SEC-FLUXADMIN : Sécurisation des flux d'administration
Responsables : Le DSI
Contributeurs : Le RSSI ou le DAN
Les opérations d'administration sur les ressources locales du vice-rectorat de la Nouvelle-Calédonie DOIVENT s'appuyer des protocoles sécurisés. Un réseau dédié à l'administration des équipements, ou au moins un réseau logiquement séparé de celui des utilisateurs, DOIT être utilisé. Les postes administrateur DOIVENT être dédiés et ne doivent pas accéder à Internet.

10.33 EXP- CENTRAL : Centraliser la gestion du SI
Responsable : Le DSI
Contributeurs : Le RSSI ou le DAN
Afin de gérer efficacement un grand nombre de postes utilisateurs ou d'équipements réseau, les administrateurs DOIVENT utiliser des outils centralisés, permettant l'automatisation de traitements quotidiens et offrant une vision globale et pertinente sur le SI.

10.34 EXP- SECX-DIST : Sécurisation des outils de prise de main à distance
Responsables : Le DSI
Contributeurs : Le RSSI ou le DAN
Conception de la formation pour administrateurs
La prise de main à distance d'une ressource SI locale ne DOIT être réalisable que par les agents autorisés par l'équipe locale chargée des SI, sur les ressources de leur périmètre. Les administrateurs DOIVENT être sensibilisés et formés au respect des obligations légales et bonnes pratiques structurant l'administration des SI, à leurs droits et leurs devoirs définis et rappelés dans la charte d'administration des SI.

X.3.2. Administration des domaines

10.35 EXP-DOM-POL : Définir une politique de gestion des comptes du domaine
Responsable : Le RSSI
Contributeurs : Le DSI ou le DAN
Formalisation de la politique de gestion des comptes du domaine
Une politique explicite de gestion des comptes du domaine DOIT être documentée.

10.36 EXP-DOM-PASS : Configurer la stratégie des mots de passe des domaines
Responsable : Le RSSI
Contributeurs : Le DSI ou le DAN
Formalisation de la politique de gestion des mots de passe
La politique de gestion des mots de passe DOIT être conçue de façon à protéger contre les attaques par essais successifs de mots de passe. Une complexité minimale dans le choix des mots de passe DOIT être imposée aux utilisateurs.

10.37 EXP-DOM-NOMENCLAT : Définir et appliquer une nomenclature des comptes du domaine.
Responsables : Le RSSI
Contributeurs : Le DSI ou le DAN
La gestion des comptes DOIT s'appuyer sur une nomenclature adaptée, afin de pouvoir distinguer selon leur usage : comptes d'utilisateur standard, comptes d'administration (domaine, serveurs, postes de travail) et comptes de service.

10.38 EXP-DOM-RESTADMIN : Restreindre au maximum l'appartenance aux groupes d'administration du domaine
Responsable : Le DSI
Contributeurs : Le RSSI ou le DAN
L'appartenance aux groupes du domaine administrateurs du vice-rectorat de la Nouvelle-Calédonie et administrateurs du domaine n'est nécessaire que dans de très rares cas. **Les opérations les plus courantes DOIVENT être effectuées avec des comptes du domaine membres des groupes locaux d'administration des ordinateurs ou ayant une délégation d'administration.**

10.39 EXP-DOM-SERV : Maîtriser l'utilisation des comptes de service.
Responsables : Le DSI et le CPI
Contributeurs : Le RSSI ou le DAN
Les comptes de service ont la particularité d'avoir généralement leurs mots de passe inscrits en dur dans des applications ou dans des systèmes. Afin de pouvoir être en mesure de changer ces mots de passe en urgence, leur utilisation DOIT être maitrisée.

10.40 EXP-DOM-LIMITSERV : Limiter les droits des comptes de service
Responsables : Le DSI et ou le CPI
Contributeurs : Le RSSI ou le DAN
Les comptes de service DOIVENT faire l'objet d'une restriction des droits, en suivant le principe du moindre privilège.

10.41 EXP-DOM-OBSOLET : Désactiver les comptes du domaine obsolètes
Responsable : Le DSI
Contributeurs : Le RSSI ou le DAN
Il est OBLIGATOIRE de désactiver immédiatement, voire de supprimer, les comptes obsolètes, que ce soient des comptes d'utilisateur (administrateur, de service ou utilisateur standard) ou des comptes de machine.

10.42 EXP-DOM-ADMINLOC : Améliorer la gestion des comptes d'administrateur locaux
Responsable : Le DSI
Contributeurs : Le RSSI ou le DAN
Afin d'empêcher la réutilisation des empreintes d'un compte utilisateur local d'une machine à une autre, il est OBLIGATOIRE soit : • **utiliser des mots de passe différents pour les comptes locaux d'administration,** • **interdire la connexion à distance via ces comptes.**

X.3.3. Envoi en maintenance et mise au rebut

10.43 EXP-MAINT-EXT : Maintenance externe.
Responsable : Le DSI
Contributeur : Le RSSI, le CIL ou le DAN
Les données non chiffrées DOIVENT être effacées avant l'envoi en maintenance externe de toute ressource informatique. Les opérations de chiffrement doivent faire appel à des produits qualifiés. L'effacement des données sensibles doit s'appuyer sur des produits qualifiés, ou respecter des procédures établies en concertation avec l'ANSSI.

Les moyens mis en œuvre dans le cadre de ces procédures, validées par le RSSI, ont pour objectif de réduire les risques de fuites d'information.

- L'effacement des données sur les supports doit être réalisé au moyen d'un outil et selon des procédures approuvés par le CSSI permettant d'éviter la reconstitution des informations supprimées.

La destruction des supports physiques peut être confiée à un prestataire dont la fiabilité sera reconnue par le CSSI.

10.44 EXP-MIS-REB : Mise au rebut
Responsable : Le DSI
Contributeurs : Le RSSI ou le DAN
Lorsqu'une ressource informatique est amenée à quitter définitivement le vice-rectorat de la Nouvelle-Calédonie les données présentes sur les disques durs ou la mémoire intégrée DOIVENT être effacées de manière sécurisée. **L'effacement des données sensibles DOIT s'appuyer sur des produits qualifiés, ou respecter des procédures établies en concertation avec l'ANSSI.**

X.3.4. Lutte contre les codes malveillants

10.45 EXP-PROT-MALV : Protection contre les codes malveillants
Responsable : Le DSI
Contributeurs : Le RSSI ou le DAN
Des logiciels de protection contre les codes malveillants, appelés communément antivirus, DOIVENT être installés sur l'ensemble des serveurs d'interconnexion, serveurs applicatifs et postes de travail de l'entité. **Ces logiciels de protection DOIVENT être distincts pour ces trois catégories au moins, et le dépouillement de leurs journaux DOIT être corrélé.**

10.46 EXP-GES-ANTIVIR : Gestion des événements de sécurité de l'antivirus
Responsable : Le DSI
Contributeurs : Le RSSI ou le DAN
Les événements de sécurité de l'antivirus DOIVENT être remontés sur un serveur académique pour analyse statistique et gestion des problèmes a posteriori (exemples : serveur constamment infecté, virus détecté et non éradiqué par l'antivirus, etc.).

10.47 EXP-MAJ-ANTIVIR : Mise à jour de la base de signatures
Responsable : Le DSI
Contributeurs : Le RSSI ou le DAN
Les mises à jour des bases antivirales et des moteurs d'antivirus DOIVENT être déployées automatiquement sur les serveurs et les postes de travail par un dispositif prescrit par la DSI et la DANE.

10.48 EXP-NAVIG : Configuration du navigateur Internet
Responsable : Le DSI
Contributeurs : Le RSSI ou le DAN
Le navigateur déployé par l'équipe locale chargée des SI sur l'ensemble des serveurs et des postes de travail nécessitant un accès Internet ou Intranet DOIT être configuré de manière sécurisée (désactivation des services inutiles, nettoyage du magasin de certificats, etc.).

10.49 EXP-INT- VIRUS : Interdiction de manipulation des codes malveillants
Responsables : Tous
Contributeurs : Le RSSI ou le DAN
L'introduction (développement, décompilation, copie, téléchargement), la propagation ou l'exécution volontaires de tout code malveillant au sein du SI du vice-rectorat de la Nouvelle-Calédonie SONT INTERDITS. Toute dérogation exceptionnelle et ponctuelle à cette règle est soumise à l'accord formel préalable et au contrôle de la filière SSI.

X.3.4.1. Sensibilisation à la lutte contre les codes malveillants

10.50 EXP-SENSI-VIRUS : Sensibilisation à la lutte contre les codes malveillants.
Responsable : Le DSI
Contributeurs : Le RSSI ou le DAN
Conception de la formation sensibilisation SSI
Les utilisateurs des SI du vice-rectorat de la Nouvelle-Calédonie DOIVENT être sensibilisés et responsabilisés à la problématique des codes malveillants. Ils doivent être informés : • des bonnes pratiques et des règles d'usage à appliquer pour s'en protéger ; • des comportements de vigilance à adopter ; • de la conduite à tenir en cas d'incident de ce type.

X.3.5. Mise à jour des systèmes et des logiciels

10.51 EXP-POL-COR : Définir et mettre en œuvre une politique de suivi et d'application des correctifs de sécurité.
Responsable : Le RSSI
Contributeur : Le DSI
Le maintien dans le temps du niveau de sécurité d'un SI impose une gestion organisée et adaptée des mises à jour de sécurité. **Un processus de gestion des correctifs propre à chaque système ou applicatif DOIT être défini, et adapté suivant les contraintes et le niveau d'exposition du système.**

10.52 EXP-COR-SEC : Déploiement des correctifs de sécurité
Responsable : Le DSI
Contributeur : Le RSSI
Les correctifs de sécurité des ressources informatiques locales DOIVENT être déployés par l'équipe locale chargée des SI en s'appuyant sur les préconisations et outils proposés par les services centraux.

10.53 EXP-OBSOLET : Assurer la migration des systèmes obsolètes
Responsables : Le DSI
Contributeur : Le RSSI
L'ensemble des logiciels utilisés sur le système d'information DOIT être dans une version pour laquelle l'éditeur assure le support, et tenu à jour. En cas de défaillance du support, il convient d'en étudier l'impact et de prendre les mesures adaptées.

10.54 EXP-ISOL : Isoler les systèmes obsolètes restants
Responsables : Le DSI
Contributeurs : Le RSSI ou le DAN
Il est nécessaire d'isoler les systèmes obsolètes, gardés volontairement pour assurer un maintien en condition opérationnelle des projets, et pour lesquels une migration n'est pas envisageable. **Chaque fois que cela est possible, cette isolation DOIT être effectuée au niveau du réseau (filtrage strict), des éléments d'authentification (qui ne doivent pas être communs avec le reste du SI) et des applications (pas de ressources partagées avec le reste du SI).**

X.3.6. Journalisation

10.55 EXP-JOUR-SUR : Journalisation des alertes
Responsable : Le DSI
Contributeurs : Le RSSI ou le DAN
Chaque système DOIT disposer de dispositifs de journalisation permettant de conserver une trace des événements de sécurité. Ces traces doivent être conservées de manière sûre.

10.56 EXP-POL-JOUR : Définir et mettre en œuvre une politique de gestion et d'analyse des journaux de traces.
Responsable : RSSI
Contributeurs : Le DSI
Formalisation de la politique d'analyse des journaux de trace
Une politique de gestion et d'analyse des journaux de traces des événements de sécurité DOIT être définie par le RSSI, validée par l'autorité qualifiée, et mise en œuvre. **Le niveau de sécurité d'un système d'information dépend en grande partie de la capacité de ses exploitants et administrateurs à détecter les erreurs, dysfonctionnements et tentatives d'accès illicites survenant sur les éléments qui le composent.**

10.57 EXP-CONT –ACCE-TRACES : Contrôle des accès aux traces informatiques.
Responsable : Le RSSI
Contributeur : Le DSI
L'accès aux traces informatiques DOIT être restreint aux seules personnes habilitées en regard de leur mission : Responsables de la SSI, administrateurs du SI, ou tout autre acteur nommément désigné et formellement autorisé. **Ces personnes sont tenues à une obligation de confidentialité concernant les informations contenues dans les traces informatiques.**

10.58 EXP-PROT-TRACES : Protection des traces informatiques.
Responsable : Le RSSI
Contributeur : Le DSI
Les traces informatiques DOIVENT être protégées contre tout événement d'origine accidentelle ou malveillante susceptible de porter atteinte à leur disponibilité ou à leur intégrité. **Dans cet objectif, les ressources sur lesquelles reposent les dispositifs de journalisation DOIVENT être classifiées en fonction de la sensibilité des traces que celles-ci génèrent, et les mesures de sécurité appropriées DOIVENT être mises en œuvre.** **Les traces concernant des événements associés aux équipements de sécurité DOIVENT présenter un caractère infalsifiable et être quotidiennement sauvegardées.** **Dans tous les cas les dispositifs de journalisation DOIVENT être placés sous surveillance (ou supervision) permanente.**

X.3.7. Points de vigilance

Les autorisations d'accès aux traces doivent être justifiées en regard de l'usage pour lequel elles ont été générées :

- prévention et analyse des incidents de sécurité ou des dysfonctionnements du SI,
- justification de certaines opérations,
- contrôle des conditions d'utilisation des ressources du SI, …

Dans la mesure où les traces contiennent des informations indirectement nominatives (permettant d'identifier l'auteur de l'événement journalisé), la préservation de leur confidentialité, et par conséquent le contrôle des accès autorisés, est un point essentiel au respect des obligations légales en matière de protection des informations à caractère personnel.

10.59 EXP-CONS-JOUR : Conservation des journaux.
Responsable : Le DSI
Les journaux des événements de sécurité DOIVENT être conservés sur douze mois glissants, hors contraintes légales et réglementaires particulières imposant des durées de conservation spécifiques.

L'état de conservation et l'existence de moyens d'exploitation des traces informatiques doivent permettre leur restitution et leur utilisation pendant toute la période de rétention définie.

10.60 EXP-CONTENU-TRACE : Contenu des traces informatiques.
Responsables : RSSI et DSI
Le contenu des traces informatiques DOIT être défini en fonction de la nature des événements journalisés et des finalités d'usage associées. **Au minimum, les traces informatiques DOIVENT contenir les données permettant :** • **d'imputer l'événement journalisé (action ou tentative d'action sur le SI) à son origine (personne physique, équipement technique, programme informatique, …) ;** • **de dater cet événement ;** • **de le qualifier pour en comprendre la nature, en termes de :** o **type d'opération (ex : envoi d'un mail),** o **paramètres significatifs de l'action (ex : destinataires du mail),** o **résultat de l'opération (ex : réussite ou échec).** **En aucun cas les traces NE DOIVENT mentionner le contenu de secrets, mots de passe, ou toute autre information dont la confidentialité doit être préservée.**

X.3.8. Précisions sur les traces

En synthèse, le contenu des traces doit répondre au minimum au « principe QQQ » (Qui ? Quand ? Quoi ?).
Par ailleurs, l'exigence de datation des traces implique la mise en place d'un dispositif d'horodatage fiable et précis, reposant sur une base de temps normalisée et homogène pour l'ensemble des traces enregistrées.
Cette base de temps devra de préférence être fournie par un tiers de confiance extérieur au vice-rectorat de la Nouvelle-Calédonie.

Le contenu spécifique de chaque type de trace est spécifié par la fonction SI, et peut, par exemple, en fonction des domaines journalisés, fournir les informations suivantes :

- **pour les traces des opérations d'administration du SI :**
  - l'identifiant de l'administrateur,
  - l'adresse du poste de l'administrateur,
  - la date/heure/mn et durée des actions,
  - les commandes envoyées aux équipements et leur statut,
  - les problèmes éventuels et les causes d'erreur ;
- **pour les traces des échanges avec Internet :**
  - l'adresse de l'émetteur et du (des) destinataire(s),
  - la date/heure/mn et durée des transactions,
  - les sites demandés et sites consultés,
  - les téléchargements effectués,
  - les problèmes éventuels et les causes d'erreur ;
- **pour les traces liées à l'usage de la messagerie :**
  - l'adresse de l'émetteur et du (des) destinataire(s),
  - la date/heure/mn d'envoi ou de réception,
  - la volumétrie associée,
  - les résultats des contrôles anti spam et antivirus,
  - les problèmes éventuels et les causes d'erreur.

X.3.9. Défense des systèmes d'information

10.61 EXP-GES-DYN : Gestion dynamique de la sécurité
Responsable : Le RSSI
Contributeurs : Le DSI
L'équipe en charge de la SSI DOIT procéder, notamment via l'analyse des journaux, à la surveillance des comportements anormaux au sein du système d'information, et à la surveillance des flux d'entrée et de sortie du système d'information.

X.3.10. Gestion des matériels informatiques fournis à l'utilisateur

10.62 EXP-MAIT-MAT : Maîtrise des matériels
Responsables : Le DSI et tous les utilisateurs
Contributeurs : Le RSSI ou le DAN
Les postes de travail - y compris dans le cas d'une location - sont fournis à l'utilisateur, gérés et configurés sous la responsabilité du vice-rectorat de la Nouvelle-Calédonie. La connexion d'équipements non maîtrisés, non administrés ou non mis à jour par l'académie (qu'il s'agisse d'ordi phones, d'équipements informatiques nomades et fixes ou de supports de stockage amovibles) sur des équipements et des réseaux professionnels EST INTERDITE.

10.63 EXP-PROT-VOL : Rappel des mesures de protection contre le vol
Responsables : Tous les utilisateurs
Contributeurs : Le RSSI ou le DAN
Les postes fixes bénéficient des mesures de protection physique offertes au titre de la directive de sécurité physique de la présente politique de sécurité système d'information du vice-rectorat de la Nouvelle-Calédonie. Chaque utilisateur DOIT veiller à la sécurité des supports amovibles (clés USB et disques amovibles), notamment en les conservant dans un endroit sûr. Il est recommandé de chiffrer les données contenues sur ces supports. Les supports contenant des données sensibles DOIVENT être stockés dans des meubles fermant à clef.

10.64 EXP-DECLAR-VOL : Déclarer les pertes et vols
Responsables : Tous
Contributeurs : Le RSSI ou le DAN
Toute perte ou vol d'une ressource d'un système d'information DOIT être déclarée au RSSI.

10.65 EXP-REAFFECT : Réaffectation de matériels informatiques
Responsables : Le RSSI et la DP
Contributeurs : Le DSI ou le DAN
Formalisation de la procédure de gestion des ressources et des mouvements de personnel
Une procédure de gestion des postes et supports dans le cadre de départs de personnel ou de réaffectations à de nouveaux utilisateurs DOIT être mise en place et validée par le RSSI. Elle DOIT définir les conditions de recours à un effacement des données.

X.3.11. Nomadisme

10.66 EXP-NOMAD-SENS : Déclaration des équipements nomades aptes à traiter des informations sensibles
Responsable : CSSI
Contributeurs : Le RSSI ou le DAN
L'autorité d'homologation du SI valide les usages possibles des équipements nomades vis-à-vis du traitement des informations sensibles ; les usages non explicitement autorisés sont interdits.

10.67 EXP-ACC-DIST : Accès à distance au système d'information de l'organisme
Responsable : DSI
Contributeurs : Le RSSI ou le DAN
Les utilisateurs distants DOIVENT s'authentifier sur le réseau de l'entité en utilisant une méthode conforme à l'annexe B3 du RGS.

Pour les postes de travail nomades, les mesures de sécurité renforcées suivantes sont prévues (en complément des mesures précédemment énoncées) :

- seule une authentification forte permet l'accès aux applications et au système (système OTP) ;
- un logiciel de connexion à distance via un VPN est installé.

X.3.12. Sécurisation des imprimantes et copieurs multifonctions manipulant des informations sensibles

10.68 EXP-IMP-SENS : Impression des informations sensibles
Responsable : DSI
Contributeurs : Le RSSI ou le DAN
Formalisation du Guide d'utilisation des informations sensibles
Les impressions d'informations sensibles DOIVENT être effectuées selon une procédure prédéfinie, garantissant le contrôle de l'utilisateur, du déclenchement de l'impression jusqu'à la récupération du support imprimé. **Les règles sont définies dans la directive Gestion des biens.**
10.69 EXP-IMP-2 : Sécurité des imprimantes et copieurs multifonctions
Responsable : DSI
Contributeurs : Le RSSI ou le DAN
Les imprimantes et copieurs multifonctions sont des ressources informatiques à part entière qui doivent être gérées en tant que telles. Elles ne DOIVENT pas pouvoir communiquer avec l'extérieur.

X.4. Exploitation des centres informatiques

X.4.1. Sécurité des ressources informatiques

Les règles suivantes sont présentées selon le modèle qui structure l'architecture des applications selon trois Tiers (Présentation – Application – Données).

Les socles techniques déployés dans chaque tiers – en particulier les règles de sécurité à appliquer – sont précisés dans un cadre de cohérence technique ministériel (CCT).

10.70 EXP-CI-OS : Systèmes d'exploitation
Responsable : DSI
Contributeurs : Le RSSI ou le DAN
Les systèmes d'exploitation déployés DOIVENT faire l'objet d'un support valide de la part d'un éditeur ou d'un prestataire de service. Seuls les services et applications nécessaires sont installés, de façon à réduire la surface d'attaque. **Une attention particulière DOIT être apportée aux comptes administrateurs.**

10.71 EXP-CI-LTP : Logiciels en Tiers Présentation
Responsable : DSI
Contributeurs : Le RSSI ou le DAN
La mise en œuvre d'une configuration renforcée EST OBLIGATOIRE sur les logiciels déployés pour le tiers présentation (ex : serveur Web, Reverse Proxy).

10.72 EXP-CI-LTA : Logiciels en Tiers Application
Responsable : DSI
Contributeurs : Le RSSI et le CPI
Des règles de développement sécurisé, et les configurations des logiciels en Tiers Application DOIVENT être fixées et appliquées. Elles sont détaillées dans le cadre de cohérence technique (CCT).

10.73 EXP-CI-LTD : Logiciels en Tiers données
Responsable : DSI
Contributeurs : Le RSSI, le CPU et le CPI
Des règles très strictes (restrictions d'accès, interdictions de connexions, gestion des privilèges) s'appliquent aux logiciels en tiers données. Ces règles DOIVENT être détaillées dans le cadre de cohérence technique (CCT).

10.74 EXP-CI-PROTFIC : Passerelle d'échange de fichiers
Responsable : DSI
Contributeur : Le RSSI
Les échanges de fichiers entre applications DOIVENT privilégier les protocoles sécurisés (SSL/TLS, FTPS...).

10.75 EXP-CI-MESSTECH : Messagerie technique
Responsable : DSI
Contributeur : Le RSSI
Pour satisfaire les besoins d'exploitation et de supervision des infrastructures et des applications, une messagerie dite technique peut être déployée en zone de Back-office du centre informatique. Cette messagerie technique ne DOIT être en aucun cas utilisée directement par un utilisateur.

10.76 EXP-CI-FILT : Filtrage des flux applicatifs
Responsable : Le DSI
Contributeurs : Le RSSI
De façon à garantir un niveau de sécurité satisfaisant face aux attaques informatiques, des mécanismes de filtrage et de cloisonnement DOIVENT être mis en œuvre.

10.77 EXP-CI-ADMIN : Flux d'administration
Responsable : Le DSI
Contributeurs : Le RSSI
D'une manière générale, il convient de différencier deux types de flux d'administration : • les flux d'administration de l'infrastructure (réservés aux agents du centre informatique) d'une part, • les flux d'administration des applications métier (réservés à la direction métier) d'autre part. L'attribution des droits d'administration DOIT respecter cette différenciation, et les 2 types de flux d'administration doivent être dans la mesure du possible cloisonnés.

10.78 EXP-CI-DNS : Service de noms de domaine – DNS technique
Responsable : Le DSI
Contributeurs : Le RSSI et le CPI
Dans le cas du déploiement d'un serveur de noms de domaines pour les besoins techniques internes au centre informatique, on utilisera les extensions sécurisées DNSSEC.

10.79 EXP-CI-EFFAC : Effacement de support
Responsable : Le RSSI
Contributeurs : Le DSI et ou le DAN
Le reconditionnement et la réutilisation des disques durs pour un autre usage (ex : réattribution d'une machine/serveur) NE SONT AUTORISES qu'après une opération d'effacement sécurisé des données.

10.80 EXP-CI-DESTR : Destruction de support
Responsable : Le RSSI
Contributeurs : Le DSI et ou le DAN
La fin de vie d'un support ou d'un matériel embarquant un support de stockage (imprimante, routeur, commutateur…) DOIT s'accompagner d'une opération de destruction avant remise au constructeur.

10.81 EXP-CI-TRAC : Traçabilité / imputabilité
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
Afin d'assurer une cohérence dans les échanges entre applications ainsi qu'une traçabilité pertinente des événements techniques et de sécurité, les centres d'exploitation DOIVENT employer une référence de temps commune (service NTP, Network Time Protocol).

10.82 EXP-CI-SUPERVIS : Supervision.
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
Un cloisonnement entre les flux de supervision (remontée d'informations) et les flux d'administration (commandes, mises à jour) DOIT être mis en place.

10.83 EXP-CI-AMOV : Accès aux périphériques amovibles
Responsable : Le RSSI ou le DAN
Contributeurs : Le DSI
L'accès aux supports informatiques amovibles DOIT faire l'objet d'un traitement adapté, plus particulièrement lorsqu'ils ont été utilisés pour mémoriser de l'information sensible ou lorsqu'ils sont utilisés pour des opérations d'exploitation. Voir la directive et les règles associées Gestion des biens.

10.84 EXP-CI-ACCRES : Accès aux réseaux
Responsable : RSSI
Contributeurs : Le DSI et ou le DAN
Dans un centre informatique, le contrôle physique des accès réseaux, l'attribution des adresses IP, le filtrage des informations et l'usage de dispositifs spécifiques (machines virtuelles, cartes d'administration à distance, etc.) font l'objet de procédures sécurisées.
10.85 EXP-CI-AUDIT : Audit/contrôle
Responsable : RSSI
Contributeurs : Le RSSI et le CPI
Le RSSI DOIT piloter des audits réguliers du système d'information relevant de sa responsabilité.

Les règles de contrôle de conformité sont détaillées dans la directive Conformité, audit, inspection et contrôle.

XI. Sécurité du poste de travail

Objectif 25 : Sécurisation du poste de travail
Durcir les configurations des postes de travail en protégeant les utilisateurs.
Objectif 26 : Sécurisation des copieurs multifonctions
Paramétrer les imprimantes et copieurs multifonctions afin de diminuer leur surface d'attaque.
Objectif 27 : Sécurisation de la téléphonie.
Sécuriser la téléphonie pour protéger les utilisateurs contre des attaques malveillantes
Objectif 28 : Contrôles de la conformité des postes de travail.
Contrôler régulièrement la conformité des paramétrages de sécurité appliqués aux postes de travail.

XI.1. Sécurisation des postes de travail

XI.1.1. Mise à disposition du poste

Le poste de travail représente très fréquemment sinon l'unique, du moins le principal point d'entrée depuis l'interne du vice-rectorat de la Nouvelle-Calédonie aux SI du ministère, du vice-rectorat de la Nouvelle-Calédonie, des partenaires et de l'Internet.

Il permet d'accéder aux informations localisées sur le poste lui-même, et à l'ensemble des ressources mises à disposition des différents utilisateurs à travers les réseaux du vice-rectorat de la Nouvelle-Calédonie. Il doit donc être protégé par des mesures adaptées au contexte d'usage.

11.1. PDT-GEST : Fourniture et gestion des postes de travail
Responsable : Le DSI
Contributeurs : Le RSSI et ou le DAN
Les postes de travail utilisés dans le cadre professionnel DOIVENT être fournis et gérés par l'équipe locale chargée des SI.

11.2. PDT –ATRIBUT Attribution et déploiement des postes de travail
Responsable : Le DSI
Contributeurs : Le RSSI et RH
Formalisation de la procédure de gestion des ressources et des mouvements de personnel
L'attribution d'un poste de travail à un utilisateur au sein du vice-rectorat de la Nouvelle-Calédonie doit faire l'objet d'une demande formelle, validée par la hiérarchie, selon une procédure auditable.

11.3. PDT-CONFIG : Formalisation de la configuration des postes de travail
Responsable : Le DSI
Contributeurs : Le RSSI et ou le DAN
Formalisation de la procédure de configuration des postes de travail
Une procédure formalisée de configuration des postes de travail est établie au vice-rectorat de la Nouvelle-Calédonie, conformément aux directives nationales existantes.

XI.1.2. Sécurité physique des postes de travail

11.4. PDT-VEROUIL-FIXE : Verrouillage de l'unité centrale des postes fixes
Responsables : le DSI et RSSI
Contributeurs : Tous les utilisateurs concernés
Lorsque l'unité centrale d'un poste fixe est peu volumineuse, donc susceptible d'être facilement emportée, elle DOIT être protégée contre le vol par un système d'attache (par exemple un câble antivol).

11.5. PDT-VEROUIL-PORT : Verrouillage des postes portables
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
Un câble physique de sécurité DOIT être fourni avec chaque poste portable. Les utilisateurs DOIVENT être sensibilisés à son utilisation.

XI.1.3. Réaffectation du poste et récupération d'informations

11.6. PDT-REAFFECT : Réaffectation du poste de travail
Responsable : Le DSI
Contributeurs : Le RSSI et ou le DAN
Formalisation du Guide des informations sensibles
Une procédure SSI définit les règles concernant le traitement à appliquer aux informations ayant été stockées ou manipulées sur les postes réaffectés

XI.1.4. Gestion des privilèges sur les postes de travail

11.7. PDT-PRIVIL : Privilèges des utilisateurs sur les postes de travail
Responsable : Le RSSI
Contributeurs : Le DSI et ou le DAN avec les RM
La gestion des privilèges des utilisateurs sur leurs postes de travail DOIT suivre le principe du « moindre privilège » : chaque utilisateur ne DOIT disposer que des privilèges nécessaires à la conduite des actions relevant de sa mission.

11.8. PDT-PRIV : Utilisation des privilèges d'accès « administrateur »
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
Les privilèges d'accès « administrateur » DOIVENT être utilisés uniquement pour les actions d'administration le nécessitant

11.9. PDT-ADM-LOCAL : Gestion du compte « administrateur local ».
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
L'accès au compte « administrateur local » sur les postes de travail DOIT être strictement limité aux équipes en charge de l'exploitation et du support sur ces postes de travail.

XI.1.5. Protection des informations

11.10. PDT-STOCK : Stockage des informations
Responsables : Le DSI, le DAN et le RSSI
Contributeurs : Tous les utilisateurs
Dans la mesure du possible, les données traitées par les utilisateurs doivent être stockées sur des espaces réseau, eux-mêmes sauvegardés selon les exigences des entités et en accord avec les règles de sécurité en vigueur. Les règles sont détaillées dans la directive protection des biens.

11.11. PDT-SAUV-LOC : Sauvegarde / synchronisation des données locales
Responsable : Le DSI
Contributeurs : Le RSSI et ou le DAN
Dans le cas où des données doivent être stockées en local sur le poste de travail, des moyens de synchronisation ou de sauvegarde DOIVENT être fournis aux utilisateurs.

11.12. PDT-PART-FIC : Partage de fichiers
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
Le partage de répertoires ou de données hébergées localement sur les postes de travail ne DOIT pas être autorisé.

11.13. PDT-SUPPR-PART : Suppression des données sur les postes partagés
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
Les données présentes sur les postes partagés (portable de prêt, par exemple) DOIVENT être supprimées entre deux utilisations, dès lors que les utilisateurs ne disposent pas du même besoin d'en connaître

11.14. PDT-CHIFF-SENS : Chiffrement des données sensibles
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
Une solution de chiffrement labellisée DOIT être mise à disposition des utilisateurs et des administrateurs afin de chiffrer les données sensibles stockées sur les postes de travail, les serveurs, les espaces de travail, ou les supports amovibles. Voir les règles dans la directive Gestion des biens.

11.15. PDT-AMOV : Fourniture de supports de stockage amovibles
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
Les supports de stockage amovibles (clés USB et disque durs externes, notamment) DOIVENT être fournis aux utilisateurs par l'équipe locale chargée des SI.

XI.1.6. Nomadisme

11.16. PDT-NOMAD-ACCESS : Accès à distance aux systèmes d'information du vice-rectorat de la Nouvelle-Calédonie
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
Les accès à distance aux SI du vice-rectorat de la Nouvelle-Calédonie (accès dits « nomades ») DOIVENT être réalisés via les infrastructures nationales. Lorsque l'accès à distance utilise d'autres infrastructures, l'usage de réseaux privés virtuels (VPN) de confiance est nécessaire.

11.17. PDT-NOMAD-PAREFEU : Pare-feu local
Responsable : Le DSI
Contributeurs : Le RSSI et ou le DAN
Un pare-feu local conforme aux directives nationales DOIT être installé sur les postes nomades.

11.18. PDT-NOMAD-STOCK : Stockage local d'information sur les postes nomades
Responsable : Tous les utilisateurs de postes nomades
Contributeurs : Le RSSI et ou le DAN
Le stockage local d'information sur les postes de travail nomades DOIT être limité au strict nécessaire. Les informations sensibles DOIVENT être obligatoirement chiffrées par un moyen de chiffrement labellisé.

11.19. PDT-NOMAD-FILT : Filtre de confidentialité.
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
Pour les postes de travail nomades manipulant des données sensibles, un filtre de confidentialité DOIT être fourni et être positionné sur l'écran dès lors que le poste est utilisé en dehors du vice-rectorat de la Nouvelle-Calédonie.

11.20. PDT-NOMAD-CONNEX : Configuration des interfaces de connexion sans fil
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
La configuration des interfaces de connexion sans fil DOIT interdire les usages dangereux de ces interfaces.

11.21. PDT-NOMAD-DESACTIV : Désactivation des interfaces de connexion sans fil
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
Des règles de configuration des interfaces de connexion sans fil (Wifi, Bluetooth, 3G…), DOIVENT interdire les usages non maîtrisés et empêcher les intrusions via ces interfaces, ces règles DOIVENT être définies et appliquées. **Les interfaces sans fil ne DOIVENT être activées qu'en cas de besoin.**

XI.1.7. Sécurisation des imprimantes et copieurs multifonctions

11.22. PDT-MUL-DURCISS : Durcissement des imprimantes et copieurs multifonctions
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
Les imprimantes et copieurs multifonctions hébergés localement au vice-rectorat de la Nouvelle-Calédonie DOIVENT faire l'objet d'un durcissement en termes de sécurité : • **changement des mots de passe initialement fixés par le « constructeur »,** • **désactivation des interfaces réseau inutiles,** • **suppression des services inutiles, chiffrement des données sur le disque dur lorsque cette fonctionnalité est disponible,** • **configuration réseau statique.**

11.23. PDT-MUL-SECNUM : Sécurisation de la fonction de numérisation
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
Lorsqu'elle est activée, la fonction de numérisation sur les copieurs multifonctions hébergés dans l'académie DOIT être sécurisée. **Les mesures de sécurité suivantes DOIVENT notamment être appliquées :** • **envoi de documents uniquement à destination d'une adresse de messagerie interne au vice-rectorat de la Nouvelle-Calédonie,** • **envoi uniquement à une seule adresse de messagerie.**

XI.2. Sécurisation de la téléphonie

11.24. PDT-TEL-MINIM : Sécuriser la configuration des autocommutateurs
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
Les autocommutateurs doivent être maintenus à jour au niveau des correctifs de sécurité. **Leur configuration doit être durcie.** **La définition et l'affectation des droits d'accès et des privilèges aux utilisateurs (transfert départ-départ, entrée en tiers, interphonie, autorisation de déblocage, renvoi sur numéro extérieur, substitution, substitution de privilège, interception d'appel dirigé, etc.) DOIVENT faire l'objet d'une attention particulière.** **Une revue de la programmation téléphonique DOIT être organisée périodiquement.**

11.25. PDT-TEL-CODES : Codes d'accès téléphoniques
Responsable : RSSI
Contributeurs : Le DSI et ou le DAN
Les utilisateurs DOIVENT être sensibilisés au besoin de modifier le code d'accès de leur téléphone et de leur messagerie vocale.

11.26. PDT-TEL-DECT : Limiter l'utilisation du DECT
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
Les communications réalisées au travers du protocole DECT sont susceptibles d'être interceptées, même si les mécanismes d'authentification et de chiffrement que propose ce protocole sont activés. Il est recommandé d'attribuer des postes téléphoniques filaires aux utilisateurs dont les échanges sont les plus sensibles.

XI.2.1. Contrôles de conformité

11.27. PDT-CONF-VERIF : Utiliser des outils de vérification automatique de la conformité.
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
Un outil de vérification régulière de la conformité des éléments de configuration des postes de travail DOIT être mis en place, afin d'éviter une dérive dans le temps de ces éléments de configuration.

XII. Sécurité du développement des systèmes

Objectif 29 : Prise en compte de la sécurité dans le développement des SI.

Reconnaître la sécurité comme une fonction essentielle, et la prendre en compte dès la conception des projets

Objectif 30 : Prise en compte de la sécurité dans le développement des logiciels.

Mener les développements logiciels selon une méthodologie de sécurisation du code produit.

Objectif 31 : Sécurisation des applications à risques.

Accompagner le développement sécurisé d'applications à risques par des contre-mesures minimisant l'impact d'attaques nouvelles.

XII.1. Développement des systèmes

12.1. DEV-INTEGR-SECLOC : Intégrer la sécurité dans les développements locaux

Responsable : Les DSI, CPU et CPI, puis l'autorité d'homologation le CSSI

Contributeurs : Le RSSI et ou le DAN

Toute initiative locale de développement informatique DOIT respecter les exigences nationales en matière de SSI, concernant la prise en compte de la sécurité dans les projets et les développements informatiques.

Le service à l'origine du projet DOIT se porter garant de l'application du référentiel général de sécurité, et de l'application d'une démarche d'homologation du système.

12.2. DEV-SOUS-TRAIT : Intégrer des clauses SSI dans les contrats de sous-traitance de développement informatique

Responsable : Le RSSI

Contributeurs : Le DSI et ou le DAN

Formalisation des clauses contractuelles SSI

Lors de l'écriture d'un contrat de sous-traitance de développement, plusieurs clauses relatives à la SSI DOIVENT être intégrées :

- **formation obligatoire des développeurs sur le développement sécurisé et sur les vulnérabilités classiques ;**
- **utilisation obligatoire d'outils permettant de minimiser les erreurs introduites durant le développement (outils gratuits d'analyse statique de code, utilisation de bibliothèques réputées pour leur sécurité, etc.) ;**
- **production de documentation technique décrivant l'implantation des protections développées (gestion de l'authentification, stockage des mots de passe, gestion des droits, chiffrement, etc.) ;**
- **respect de normes de développement sécurisé, qu'elles soient propres au développeur, publiques ou propres au commanditaire ;**
- **obligation pour le prestataire de corriger, dans un temps raisonnable et pour un prix défini, les vulnérabilités introduites durant le développement et qui lui sont remontées, en incluant automatiquement les corrections des autres occurrences des mêmes erreurs de programmation.**

XII.2. Développements logiciels et sécurité

12.3. DEV-FUITES : Limiter les fuites d'information
Responsables : Tous
Contributeurs : Le RSSI et ou le DAN
Les fuites d'informations techniques sur les logiciels utilisés permettent aux attaquants de déceler plus facilement d'éventuelles vulnérabilités. Il est impératif de limiter fortement la diffusion d'informations au sujet des produits utilisés, même si cette précaution ne constitue pas une protection en tant que telle.

12.4. DEV-LOG-ADHER : Réduire l'adhérence des applications à des produits ou technologies spécifiques
Responsable : DSI
Contributeurs : Le RSSI et ou le DAN
Le fonctionnement d'une application s'appuie sur un environnement logiciel et matériel. **En phases de conception et de spécification technique, il est nécessaire de s'assurer que les applications n'ont pas une trop forte adhérence vis-à-vis des environnements sur lesquels elles reposent.** **En effet, l'apparition de failles sur un environnement a de fait un impact sur la sécurité des applications qui en dépendent.** **En plus du maintien en condition de sécurité propre à l'application, il est donc nécessaire de pouvoir faire évoluer son environnement pour garantir sa sécurité dans la durée.**

12.5. DEV-LOG-CRIT : Instaurer des critères de développement sécurisé
Responsables : DSI et CPI
Contributeurs : Le RSSI et ou le DAN
Une fois passées les phases de définition des besoins et de conception de l'architecture applicative, le niveau de sécurité d'une application dépend fortement des modalités pratiques suivies lors de sa phase de développement. Voir les règles de la directive Gestion des biens.

12.6. DEV-LOG-CYCLE : Intégrer la sécurité dans le cycle de vie logiciel
Responsables : Les RM, CPU, CPI, l'autorité d'homologation le CSSI
Contributeurs : Le RSSI et ou le DAN
La sécurité DOIT être intégrée à toutes les étapes du cycle de vie du projet, depuis l'expression des besoins jusqu'à la maintenance applicative, en passant par la rédaction du cahier des charges et les phases de recette.

12.7. DEV-LOG-WEB : Améliorer la prise en compte de la sécurité dans les développements Web.
Responsables : Le DSI et le CPI
Contributeurs : Le RSSI et ou le DAN
Les développements Web (et les développements en PHP en particulier) font l'objet de problèmes de sécurité récurrents qui ont conduit à la constitution de référentiels de sécurité. **Ces référentiels ont pour objectif de fixer des REGLES DE BONNES PRATIQUES à l'usage des développeurs. Ce sont des règles d'ordre générique ou pouvant être spécifiques à un langage (PHP, ASP, NET, etc.).**

12.8. DEV-LOG-PASS : Calculer les empreintes de mots de passe de manière sécurisée
Responsables : Le DSI et le CPI
Contributeurs : Le RSSI et ou le DAN
Lorsqu'une application doit stocker les mots de passe de ses utilisateurs, il est important de mettre en œuvre des mesures permettant de se prémunir contre les attaques documentées : attaques par dictionnaire, attaques par tables arc-en-ciel, attaques par force brute, etc.

XII.3. Applications à risques

12.9. DEV-FILT-APPL : Mettre en œuvre des fonctionnalités de filtrage applicatif pour les applications à risque
Responsable : Le DSI
Contributeurs : Le RSSI et ou le DAN
Devant les applications à risques, il est recommandé de faire usage d'une solution tierce de filtrage applicatif.

XIII. Traitement des incidents

Objectif 32 : Chaînes opérationnelles.

Partager l'information (alertes, incidents) dans le respect des règles de prudence et mutualiser les opérations de remise en état, de façon à lutter efficacement contre les attaques.

La présente directive aborde les règles relatives au domaine particulier du traitement des incidents qui est une exigence majeure pour le vice-rectorat de la Nouvelle-Calédonie et le ministère.

Son objectif général est de décrire l'ensemble des règles à respecter pour :

- s'assurer que les incidents sont détectés au plus tôt et traités au bon niveau de l'organisation de façon à limiter leurs impacts pour le vice-rectorat de la Nouvelle-Calédonie ;
- favoriser le partage d'expériences et tirer les enseignements permettant d'améliorer la sécurité de façon continue.

Ces règles sont, dans leur ensemble, génériques et indépendantes des contextes techniques, géographiques ou des activités métier afin d'assurer leur applicabilité au sein des différentes entités du vice-rectorat de la Nouvelle-Calédonie.

XIII.1. Précisions

Rapporté au domaine de la SSI, il s'agit de tout événement constaté remettant en cause la sécurité ou le fonctionnement normal d'une ressource du SI (ou d'un service fourni par la fonction SI) et susceptible de porter atteinte à sa disponibilité ou à son intégrité, à la confidentialité d'une information sensible ou à la fourniture d'éléments de preuve qui pourraient s'avérer nécessaires (obligation légale, saisine, opérations sensibles pour les métiers…).

Par extension, doit être considérée comme incident de sécurité toute violation à la politique de sécurité des SI du vice-rectorat de la Nouvelle-Calédonie.

Généralement, un incident se caractérise par 3 éléments :

- une ou plusieurs causes (défaillance d'un processus, acte délibéré…) ;
- les éléments constitutifs de l'événement (descriptif de ce qui est survenu) ;
- les effets (impacts et conséquences).

XIII.2. Chaînes opérationnelles

13.1. TI-OPS-SSI : Chaînes opérationnelles SSI
Responsable : RSSI
Contributeur : Le DAN
Les chaînes opérationnelles des ministères concourent à l'effort national de cyber sécurité. **Les alertes et les incidents DOIVENT être selon des procédures testées lors d'exercices.** **La coordination des compétences est organisée à l'échelon ministériel. Les situations d'urgences peuvent faire appel à des mesures définies préalablement dans le cadre des plans gouvernementaux.**

XIII.3. Traitement des alertes de sécurité émises par les instances nationales (ANSSI)

13.2. TI-MOB : Mobilisation en cas d'alerte
Responsable : RSSI
Contributeur : Le DAN
En cas d'alerte de sécurité identifiée au niveau national, le RSSI s'assure de la bonne application des exigences formulées par les instances nationales, dans les meilleurs délais.

XIII.4. Remontée des incidents de sécurité rencontrés

13.3. TI-QUAL-TRAIT : Qualification et traitement des incidents
Responsable : RSSI
Contributeur : Le DAN
La chaîne fonctionnelle SSI DOIT être informée par la chaîne opérationnelle de tout incident de sécurité, et contribue si nécessaire à la qualification de l'incident et au pilotage de son traitement.

13.4. TI-INC-REM : Remontée des incidents
Responsable : RSSI
Tout incident de sécurité, même apparemment mineur, dont l'impact dépasse ou est susceptible de dépasser le SI du vice-rectorat de la Nouvelle-Calédonie ou du ministère, DOIT faire l'objet d'un compte-rendu, via la chaîne SSI, au Centre opérationnel de la sécurité des systèmes d'information (COSSI) de l'ANSSI. La remontée d'incidents par les chaînes opérationnelles ministérielles participe à la posture permanente de vigilance. Cette remontée est immédiate pour les incidents dont la portée est susceptible de dépasser à court terme le périmètre de l'entité ou du ministère, et pour les incidents correspondant à des signalements spécifiques, notamment de la part de l'ANSSI. La remontée prend la forme d'une synthèse mensuelle pour les autres incidents. Les critères et procédures précis de remontée d'incidents sont élaborés sous le pilotage de la chaîne fonctionnelle SSI, en lien avec la chaîne opérationnelle. Le vice-rectorat de la Nouvelle-Calédonie DOIT maintenir à jour un historique clair des suites liées à l'escalade de chaque incident, afin de capitaliser les enseignements associés à la résolution (ou non) de ces incidents. L'aspect difficile de la caractérisation des attaques (ambiguïté de la source, du dommage, du moyen, de la finalité) rend nécessaire les échanges d'informations interministériels - même sur des « signaux faibles » - ainsi que la coordination continue des actions.

XIV. Continuité d'activité

Objectif 33 : Gestion de la continuité d'activité.

Se doter de plans de continuité d'activité, et les tester.

XIV.1. Gestion de la continuité d'activité des SI

L'objectif est de décrire l'ensemble des règles à respecter pour limiter l'impact de tout choc extrême, événement d'origine naturelle, accidentelle ou criminelle, susceptible de perturber, voire d'interrompre, le fonctionnement normal des ressources du SI sur lesquelles s'appuient les métiers.

La notion de « choc extrême » correspond à des sinistres graves tels que la destruction complète d'un bâtiment ou l'inaccessibilité d'une zone étendue.

La capacité à résister à des « chocs extrêmes » est une caractéristique essentielle de la continuité des activités informatiques.

Elle est fondée sur les principes suivants :

- redondance des éléments totale ou partielle, adaptée en fonction de leur niveau de criticité en termes de disponibilité ;
- répartition géographique distante des ressources de production et de secours diminuant les impacts d'un sinistre environnemental majeur ;
- pour les équipements considérés comme « vitaux », existence d'un secours de deuxième niveau.

14.1. PCA-MINIS : Définition du plan ministériel de continuité d'activité des SI
Responsable : FSSI
Contributeurs : les RSSI, DSI, RPCA, RPSI
Chaque ministère DOIT définir un plan de continuité d'activité ministériel des SI permettant d'assurer, en cas de sinistre, la continuité d'activité des SI.

XIV.1.1. Définition du plan de continuité d'activité des systèmes d'information d'une entité

14.2. PCA-LOCAL : Définition du plan local de continuité d'activité des SI
Responsables : DSI et RSSI
Contributeurs : Les RPCA et RPSI
Le DSI ou le RSSI DOIT définir la structure et les attendus du plan de continuité d'activité des SI permettant d'assurer effectivement, en cas de sinistre, la continuité d'activité.

14.3. PCA –STRATEGIE : Définition des stratégies de continuité.
Responsables : DSI et RSSI
Contributeurs : Les RPCA et RPSI
Le DSI ou le RSSI DOIT définir une stratégie de continuité de fonctionnement de ses ressources SI qui tienne compte : • **des seuils de tolérance des activités à une indisponibilité des ressources ou services informatiques ;** • **des scénarii de crise susceptibles d'affecter le fonctionnement des ressources ou services informatiques supportant les activités les plus critiques.**

XIV.1.1.1. Point de vigilance

Les démarches de classification, présentées dans la directive Gestion des biens fournissent les éléments permettant d'apprécier la criticité des activités et leurs seuils de tolérance à une indisponibilité partielle ou totale des services informatiques selon deux critères :

- **Le Délai Maximal d'Indisponibilité Admissible (DMIA) :**

  Il définit la durée maximum pendant laquelle une activité courante ou une activité en mode projet peuvent ne pas accéder à une ressource ou à un service informatique sans en subir d'impact significatif. La valeur est numérique et exprimée en nombre de minutes, d'heures ou en jours ;

- **La Perte de Données Tolérées(PDT), ou Perte d'Information Tolérée (PIT) :**
  Elle définit le degré maximum de perte d'informations acceptable par une activité ou un projet avant qu'ils ne commencent à subir des impacts significatifs. La valeur est numérique et d'unité variable à adapter en fonction de la nature des données et du contexte (exemples : nombre d'heures ou de jours de données perdues, volume maximum de données manquantes exprimé en pourcentage, …).

  En complément à ces deux critères, il peut être nécessaire de déterminer le Niveau Minimum de Service Requis (NMSR) dans l'hypothèse où le service initial ne peut être fourni à l'identique (exemple : nombre d'utilisateurs minimum à connecter aux ressources informatiques de secours, …).

Les scénarii de crise à étudier sont de deux natures :

- **Les scénarii directement imputables à une indisponibilité des ressources du SI :**
  (défaillance du réseau de télécommunication, défaillance d'un élément technique critique, altération ou perte de données, destruction ou inaccessibilité d'un centre informatique, défaillance d'un prestataire IT critique...) ;

- **Des scénarii qui ne sont pas imputables à un dysfonctionnement du SI :**
  Qui nécessitent la mise en œuvre (ou l'accroissement) de ressources informatiques particulières (exemples : crise sanitaire impliquant le travail à distance, sinistres impliquant la mise en œuvre de moyens informatiques de secours sur des sites de repli utilisateurs…).

Dans ce cadre, il convient de mesurer l'impact de la défaillance des prestataires et fournisseurs de ressources du SI (ou de services informatiques essentiels), d'étudier leur capacité à limiter cet impact en regard des scénarii de crise qui les concernent et de prendre les dispositions complémentaires techniques ou contractuelles qui s'imposent.

Les contrats doivent être aménagés en ce sens.

14.4. PCA – CHOIX –SOL : Choix des solutions de continuité
Responsables : DSI et RSSI
Contributeurs : Les RPCA et RPSI
Les solutions DOIVENT répondre aux scénarii de crise à couvrir et respecter les seuils de tolérance (RTO, RPO) des activités critiques. **Leur choix DOIT mettre en regard le niveau de risque encouru, le niveau de couverture, une estimation des coûts des solutions envisagées ainsi que le niveau de risque résiduel qui en découle**

XIV.1.1.2. Précisions

En fonction de la stratégie arrêtée, une solution de continuité doit être définie pour chaque « couple » service informatique (ou ensemble de services) / scénario de crise (ou ensemble de scénarii de crise appelant la mise en œuvre de solutions similaires).

Le choix des solutions permettant d'assurer la continuité de fonctionnement des ressources ou services informatiques essentiels s'effectue en analysant les différentes activités et composants permettant d'assurer le développement, la maintenance et l'exploitation des dites ressources (ou services) et en identifiant les zones de vulnérabilités ou de ruptures possibles :

- serveurs de données ;
- serveurs hébergeant les applications ;
- infrastructures réseaux locaux et distants ;
- collaborateurs et prestataires nécessaires au développement, à la maintenance et à l'exploitation des SI les plus sensibles, et postes de travail associés avec montée en charge ;
- matériels spécifiques (portables, consoles d'administration…) ;
- sites hébergeant les collaborateurs ou prestataires concernés ;
- documents nécessaires (annuaires, documentation technique, procédures, éléments contractuels...) ;
- informations complémentaires nécessaires (mots de passe…) ;
- etc.

Le délai de remise à disposition d'une ressource ou d'un service informatique dépend de la disponibilité de l'ensemble des moyens humains et techniques nécessaires à son bon fonctionnement.

14.5. PCA-CHOIX_ VALI RR : Validation du niveau de risque résiduel.
Responsables : DSI et RSSI
Contributeurs : Les RPCA, RPSI et les RM
Conformément à la Directive Gestion des biens, un processus « d'acceptation des risques » DOIT obligatoirement être enclenché à la suite de toute démarche d'élaboration (ou d'actualisation) d'un plan de continuité et favoriser la recherche d'un consensus avec les divisions métier.

Le processus d'acceptation des risques doit impliquer l'ensemble des parties prenantes dans le périmètre d'étude et faire ressortir formellement :

- les écarts entre les seuils de tolérance et les niveaux de services susceptibles d'être fournis ;
- les scénarii de crise non pris en compte ou partiellement couverts ;
- les causes (impossibilité technique, éléments économiques…) justifiant ces éléments ;
- les mesures de contournements envisagées, notamment par les divisions métiers.

A cet effet, il est fortement recommandé de mettre en place un comité de pilotage qui aura en charge :

- de valider la stratégie et de procéder aux arbitrages ;
- d'assurer la cohérence et l'harmonisation des actions menées dans ce domaine ;
- de suivre les plans d'actions ultérieurs suite aux tests, aux contrôles ou aux audits (internes ou externes).

XIV.1.2. Mise en œuvre du plan local de continuité d'activité des SI

14.6. PCA-SUIVILOCAL : Suivi de la mise en œuvre du plan de continuité d'activité local des SI (PCA des SI)
Responsable : RSSI
Contributeurs : Les RPCA et RPSI
Le RSSI du vice-rectorat de la Nouvelle-Calédonie DOIT s'assurer de la bonne mise en œuvre des dispositions prévues dans le plan de continuité d'activité des systèmes d'information.

14.7. PCA-PROC : Mise en œuvre des dispositifs techniques et des procédures opérationnelles
Responsable : CPI et RPSI
Contributeurs : Le DSI, le RSSI et le RPCA
Les équipes informatiques DOIVENT mettre en œuvre les dispositifs techniques et les procédures opérationnelles contribuant à la continuité des SI, en assurent la supervision au quotidien et la maintenance dans le temps.

14.8. PCA – MEO -SOL : Mise en œuvre des solutions de continuité.
Responsable : RPCA
Contributeurs : Le DSI, le RSSI et le RPSI
Chaque plan de continuité doit comporter, en tant que de besoin : • un volet organisationnel présentant les conditions du déclenchement de sa mise en œuvre (organisation, matrice de responsabilités…) et les articulations avec le dispositif de gestion de crise ; • un volet informatique (description des solutions de secours, plan de reprise des moyens informatiques et de télécommunication) ; • un volet fonctionnel (procédures mises en œuvre par les divisions métier, transfert des équipes informatiques…) ; • un volet présentant le plan de retour à la situation nominale ou aux conditions initiales de fonctionnement ; • ses conditions de tests; • les conditions de gestion des changements susceptibles de modifier la solution envisagée.

14.9. PCA – FORM -SOL : Formation des intervenants aux procédures de continuité.
Responsables : DSI et RSSI
Contributeurs : Les RPCA et RPSI
Les intervenants (utilisateurs, exploitants…) DOIVENT être informés et formés aux procédures permettant la mise en œuvre des solutions de continuité pour lesquelles ils ont un rôle à jouer.

14.10. PCA- DOC – DOC : Documentation de référence des solutions de continuité
Responsables : DSI et RSSI
Contributeurs : Les RPCA et RPSI
La documentation relative à la mise en œuvre des solutions de continuité DOIT être structurée, maintenue à jour et conservée dans un lieu sécurisé adapté à son niveau de classification. **Elle DOIT être facilement accessible aux intervenants concernés.**

La documentation de référence décrit l'organisation et l'ordonnancement général des actions à réaliser ainsi que les modes opératoires pour mettre en œuvre les solutions prévues : procédures organisationnelles (éléments (coordonnées, rôles et responsabilités, suppléants, astreintes, relations contractuelles avec les tiers impliqués…) permettant l'activation des dispositifs de secours ou la mise en place des sites de repli, …) et techniques (procédures de bascule sur les ressources de secours et procédures de reprise).

Les procédures contenues dans les plans de secours doivent être simples, exhaustives, et compréhensibles par des acteurs qui, quel que soit leur niveau de compétence, seront potentiellement soumis à un stress important.

Par ailleurs, les modalités de mobilisation du personnel et de la documentation associée doivent être conformes à la réglementation en vigueur (concernant la protection des données à caractère personnel en particulier).

14.11. PCA – ROBUST -SOL : Robustesse des solutions de continuité
Responsables : DSI et RSSI
Contributeurs : Les RPCA et RPSI
Le niveau de robustesse de chaque solution doit être évalué en termes de : • **capacité des équipements de secours à assurer une charge opérationnelle suffisante ;** • **capacité des solutions à résister à des « chocs extrêmes » (sinistres graves) ;** • **livraison des matériels de remplacement dans des délais compatibles avec les impératifs de continuité ;** • **niveau de mutualisation des ressources de secours et nombre d'adhérents ;** • **durée d'utilisation possible des moyens de secours.**

14.12. PCA-SAUVE : Protection de la disponibilité des sauvegardes
Responsable : Le DSI
Contributeurs : Les RPCA, RPSI, le RSSI et le DAN
Les sauvegardes de données ne DOIVENT pas être soumises aux mêmes risques de sinistres que les données sauvegardées.

14.13. PCA – SAUVE - ORG : Organisation des sauvegardes
Responsable : Le DSI
Contributeurs : Le RSSI et ou le DAN
Les configurations des équipements (système, réseau, télécommunication), les logiciels de base, les applications et les données de production DOIVENT faire l'objet de sauvegardes de production et de recours distinctes.

XIV.1.2.1. Point de vigilance

Les sauvegardes dites de recours ne sont utilisées que dans le cadre des plans de continuité étudiés (tests ou sinistres) ou, à titre exceptionnel, dans le cas où les sauvegardes de production ne seraient pas exploitables.

On les distingue des sauvegardes de production car généralement ces dernières :

- sont conservées sur site et peuvent être détruites en cas de sinistre majeur ;
- font l'objet de manipulations plus ou moins fréquentes susceptibles de les altérer.

14.14. PCA – GEST-SAUV : Gestion des sauvegardes de recours.
Responsables : Le DSI
Contributeurs : Le RSSI et ou le DAN
Les sauvegardes de recours DOIVENT être externalisées en un lieu distinct et suffisamment distant du site de production pour ne pas subir les dommages d'un sinistre pouvant l'impacter. **Elles DOIVENT être accessibles en permanence selon des procédures strictes et protégées en regard du niveau de sensibilité des informations qu'elles contiennent.**

14.15. PCA-PROT : Protection de la confidentialité des sauvegardes
Responsable : Le DSI
Contributeurs : Le RSSI et ou le DAN
Les sauvegardes DOIVENT être traitées de manière à garantir leur confidentialité et leur intégrité.

XIV.1.3. Maintien en conditions opérationnelles du plan local de continuité d'activité des SI

14.16. PCA-EXERC : Exercice régulier du plan local de continuité d'activité des SI
Responsables : Le DSI et le RSSI
Contributeurs : Le RPSI et ou le DAN
Le RSSI du vice-rectorat de la Nouvelle-Calédonie DOIT organiser des exercices réguliers, afin de tester le plan local de continuité d'activité des SI.

XIV.1.3.1. Précisions

Les tests et exercices doivent plus particulièrement permettre de vérifier que :

- les informations sont disponibles et à jour ;
- le processus d'escalade, permettant l'information des parties prenantes, est efficace ;
- les prises de décision peuvent s'opérer ;
- les intervenants ont connaissance de leurs rôles ;
- les dispositifs de secours sont opérationnels.

Les tests unitaires, ou globaux techniques (n'impliquant pas les utilisateurs), ou impliquant les utilisateurs, ainsi que les exercices, doivent reposer sur des scénarii variés (prévus, impromptus, bascule ou non de la production…) et couvrir des périmètres techniques ou fonctionnels différents (reprise sur les sites de repli des équipes informatiques, tests de connexions, restauration des environnements systèmes et réseaux, réaction des fournisseurs ou des acteurs internes, répétitions complètes ou partielles impliquant les Métiers…).

Pour les tests ou exercices globaux, une étude de risque préalable peut être nécessaire comme prérequis.

Chaque test et chaque exercice doivent faire l'objet de la tenue d'une main courante et d'un bilan détaillé afin de déterminer ce qui a bien fonctionné et ce qui nécessite une amélioration - modification.

Tout incident doit faire l'objet d'un suivi, au même titre que les incidents de production.

Les plans doivent être testés au moins une fois par an et après chaque modification majeure de l'environnement organisationnel, technique, humain par rapport auquel les dispositifs de continuité des activités informatiques ont été conçus.

XIV.1.3.2. Cas particulier des restaurations à partir des sauvegardes de secours:

Pour être réputée utilisable, une sauvegarde de recours doit être validée, chaque validation devant faire l'objet de la tenue d'une main courante et d'un bilan détaillé afin de déterminer ce qui a bien fonctionné et ce qui nécessite, dans le dispositif de sauvegarde, une amélioration - modification.

La capacité de l'organisation à rapatrier les sauvegardes localisées sur le site de secours doit être également évaluée (coordination avec le dépositaire de la sauvegarde interne ou externe). Les procédures de restauration et modes opératoires doivent être disponibles sur le site de secours.

Les résultats des restaurations doivent être consignés dans un document de suivi.

14.17. PCA-MISAJOUR : Mise à jour du plan local de continuité d'activité des SI
Responsable : RSSI
Contributeurs : Le RSSI et ou le DAN
Le RSSI DOIT assurer le maintien à jour du plan local de continuité d'activité des SI.

XIV.1.3.3. Précisions

Tout besoin d'amélioration - modification détecté lors des tests ou des exercices, ou lors des revues de changements, doit rapidement être répercuté sur les solutions de continuité mises en œuvre, les documentations afférentes devant être mises à jour en même temps que celles de production.

Les intervenants doivent être tenus informés de toute modification apportée au titre du maintien en condition opérationnelle.

XV. Conformité, audit, inspection et contrôle

Objectif 34 : Contrôles réguliers.

Effectuer des contrôles (audits, inspections) et des exercices réguliers de façon à mesurer les progrès accomplis et corriger les manquements.

XV.1. Contrôles

Afin de s'assurer de la conformité des dispositifs opérationnels avec les directives internes, les obligations légales et les bonnes pratiques en vigueur, le RSSI organise régulièrement, au moins une fois par an, des audits de contrôle visant à mettre en évidence les non-conformités.

La fonction sécurité a une mission importante de contrôle de l'état de la sécurité et d'alerte de l'AQSSI en cas de risque majeur.

XV.1.1. Indicateurs d'application de la PSSI du vice-rectorat de la Nouvelle-Calédonie

15.1. CONTR-SSI : Contrôles locaux
Responsable : RSSI
Contributeur : Le DAN
La conformité à la PSSI du vice-rectorat de la Nouvelle-Calédonie, à la PSSI ministérielle et à la PSSI de l'Etat DOIT être vérifiée par des contrôles réguliers. **Le RSSI DOIT conduire des actions locales d'évaluation de la conformité à la PSSI du vice-rectorat de la Nouvelle-Calédonie et contribuent à la consolidation, dans un bilan annuel, de l'état d'avancement de sa mise en œuvre.**

Une feuille de synthèse indiquant pour chaque règle dans chaque directive si elle est appliquée, en dérogation (jusqu'à quand) ou l'objet d'un plan d'action (avec la date d'aboutissement) doit être gérée et tenue à jour par le RSSI.

En fonction de ces éléments, des indicateurs d'application de la PSSI du vice-rectorat de la Nouvelle-Calédonie sont définis et incorporés au tableau de bord.

15.2. CONTR-BILAN-SSI : Bilan annuel
Responsable : Le FSSI
Contributeurs : Le RSSI
Chaque ministère établit un bilan annuel mesurant sa maturité SSI globale. L'ANSSI consolide l'ensemble de ces bilans. Le document de synthèse est soumis au Premier ministre

XV.2. Confidentialité des documents de reporting, de pilotage et d'audit de la sécurité

15.3. CONTR-CONF-AUDIT : Classification des documents ayant trait à la sécurité
Responsable : Le RSSI
Contributeurs : Le DSI et ou le DAN
Les rapports d'audits, indicateurs, tableaux de bord et synthèses sur l'état de la sécurité établis localement par le RSSI seront classifiés au moins au niveau 3 en confidentialité. **Avec l'approbation du supérieur hiérarchique du rédacteur, les plans d'action peuvent n'être classifiés qu'au niveau 2.**

XV.2.1. Contrôles indépendants

15.4. CONTR - CONTROLE - INDE : Contrôles indépendants
Responsable : Le RSSI
Contributeurs : Le DSI et ou le DAN
Formalisation de la procédure de contrôle
Les contrôles indépendants mais homologués par l'ANSSI peuvent être inclus dans le plan de contrôle pour : • **des contrôles de conformité technique des systèmes opérationnels pour s'assurer de la mise en œuvre correcte des mesures de sécurité concernant les matériels ou les logiciels** • **des tests d'intrusion** • **des tests de comportement des utilisateurs** • **etc.** **Le contenu de ces contrôles, la manière de les conduire et les relations avec les entités contrôlées DOIT faire l'objet d'une procédure détaillée par le RSSI.**

XVI. Glossaire

Sigle / terme / abréviation	Designation
AH	Autorité d'Homologation
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.
CCD	Cellule de Crise Décisionnelle
CCO	Cellule de Crise Opérationnelle
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.
CSSI	Comité de Sécurité du Système d'Information.
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.
CIL	Correspondant Informatique et Libertés.
CIO	Centre d'Information et d'Orientation
CPI	Chef de projet informatique (MOE)
CPU	Chef de projet utilisateur (MOA)
DAN	Délégué académique au numérique
DICP	Disponibilité, Intégrité, Confidentialité, Preuve et contrôle
DLL	Division de la logistique et des lycées
DMIA	Délai maximal d'indisponibilité admissible
DP	Division du personnel
DSI	Division des services informatiques
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.
NMSR	Niveau Minimum de Service Requis
OSSI	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
PGPCA	Politique Générale du Plan de Continuité d'Activité
PGSI	Politique Générale de Sécurité de l'Information
PIT	Perte d'information tolérée
PS I	Politique Sécurité de l'Information
PJR	Personne Juridiquement Responsable
PSSI	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
RCI	Responsable de la communication et de l'information
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).
RPCA	Responsable du Plan de Continuité d'Activité
RPSI	Responsable du Plan de Secours Informatique
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
RPCA	Responsable du plan de continuité d'activité
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.