Premiers pas à l'ESE avec la PSSI

Le document est fait à partir de :

Politique générale de Sécurité de l'Information - PGSI - 20180701.pdf

Politique SSI opérationnelle - Laboratoires - 20180701.pdf

Politique SSI opérationnelle - Services – 20180701

PSSIC v2018.1 (détaillée)_20180925

Charte de sécurité des Systèmes d'Information du CNRS

Nicolas Moulonguet

PGSI :

La PGSI (Politique Générale des Systèmes d'Information) du CNRS couvre l'ensemble des unités du CNRS, unités propres et unités mixtes. L'ESE est concerné par la PGSI du CNRS. L'information peut être de nature administrative ou scientifique.

Chaque utilisateur des systèmes d'information doit prendre connaissance de la Charte de Sécurité des Systèmes d'Information du CNRS (Charte SSI) qui fixe les principes de sécurité que chacun doit connaître. La Charte est dans l'Intranet du site Web de l'ESE, avec le Règlement intérieur. Elle est aussi accessible en bas de la page d'accueil.

Cette Charte a été écrite en 2013 mais elle est parfaitement d'actualité en 2023.

Remarque : un utilisateur ne peut pas connecter aux réseaux locaux de l'Entité – quelle que soit la nature de ces réseaux (filaires ou non filaires) - des matériels autres que ceux confiés ou autorisés par la direction ou l'Entité. Suivant cette phrase, les ordinateurs portables personnels sont interdits sur le réseau.

PSSI :

L'ESE est concerné par la PSSI (Politique de Sécurité des Systèmes d'Information) opérationnelle **PSSI-CNRS-Laboratoires.**

La mise en œuvre de la PSSI opérationnelle par l'unité débute par l'identification du niveau de sécurité requis par ses activités - elle utilisera pour cela une grille de classification (3 niveaux de sécurité allant de * à ***) et une méthode définies dans la PSSI opérationnelle.

Le directeur d'unité définit un plan d'action SSI (Sécurité des Systèmes d'Information) pluriannuel pour la mise en œuvre de la PSSI qui concerne son unité, qui prend en compte les ressources budgétaires et humaines nécessaires.

Dans le cas de l'ESE, unité mixte, une des tutelles est identifiée comme pilote de la SSI : CNRS, Université Paris Saclay, AgroParisTech ?

Le pilote SSI sollicite l'ensemble des acteurs locaux (Responsables SSI des parties, équipes informatiques des partenaires, etc.) lors de la formalisation du plan d'action SSI qui est rédigé en application de la PSSI opérationnelle définie pour l'unité.

Le directeur d'unité nomme un chargé de la SSI (CSSI) qui est intégré à l'ensemble des chaînes fonctionnelles SSI des tutelles : Nicolas Moulonguet.

Tout incident SSI est signalé à l'ensemble des chaînes fonctionnelles SSI des tutelles.

Dans le cas où le pilote de la SSI n'est pas le CNRS, de façon à ne pas dégrader le niveau de couverture du risque prévu par la PSSI opérationnelle du CNRS pour cette unité, les règles issues de la PSSI opérationnelle et de la charte SSI du CNRS sont intégrées et mises en cohérence avec la PSSI et la Charte SSI définie par le pilote. Si le pilote choisi est Université Paris Saclay, ce que je propose, la PSSI opérationnelle et la charte SSI de l'Université doit s'accorder avec ceux du CNRS. Questionner l'Université Paris Saclay sur ce point.

Le Directeur d'Unité (DU) est responsable de la sécurité des systèmes d'information dans son unité. Le CSSI assiste son Directeur d'Unité dans l'exercice de ses responsabilités en matière de SSI et en particulier il remonte les incidents SSI vers la ou les chaînes fonctionnelles concernées. Le détail des missions est défini dans la PSSI opérationnelle de l'unité.

Les mesures de prévention doivent être complétées par un dispositif permettant la détection et la réaction en cas d'atteinte à la sécurité des SI du CNRS (ces atteintes sont nommées incidents SSI). L'activité des systèmes d'information est donc en permanence analysée afin de détecter toute activité anormale pouvant relever d'une atteinte à la sécurité des SI.

La détection et l'analyse des incidents SSI passe notamment par l'enregistrement de l'activité des systèmes d'information. Ces enregistrements sont appelés journaux ou traces. Les Politiques de Sécurité des Systèmes d'Information (PSSI) opérationnelles d'unité détaillent les mesures relatives à la production, la conservation et l'analyse des traces. Ces mesures sont définies dans le respect de la loi et des dispositions réglementaires internes. La Charte de la Sécurité des Systèmes d'Information du CNRS informe les utilisateurs de l'existence de ce dispositif.

Les incidents de sécurité des SI sont remontés au RSSIC (Responsable de la Sécurité des Systèmes d'Information Central) du CNRS suivant les mesures détaillées dans les Politiques de Sécurité des Systèmes d'Information (PSSI) opérationnelles d'unité. Le RSSIC informe en tant que de besoin le DGD-R (Direction Générale Déléguée aux Ressources), le FSD (Fonctionnaire de Sécurité et de Défense), la DAJ (Direction des Affaires Juridiques), le DPD (Délégué à la Protection des Données), les partenaires concernés et les autorités compétentes au plan national (ministère de tutelle, ANSSI, etc.)

Chaque unité doit produire et conserver les documents et enregistrements permettant de surveiller, contrôler la gestion de la SSI.

PSSI CNRS Laboratoires (Politique Sécurité des Systèmes d'Information opérationnelle applicable aux laboratoires du CNRS) **:**

La PSSI est un document de 157 pages de règles sous forme de fiches concernant la politique, l'organisation, la protection des documents et des informations, les ressources humaines, la sécurité physique, l'exploitation des SI, l'authentification et le contrôle d'accès, le développement des SI, la gestion des incidents, la continuité d'activité, et la conformité.

Lorsque la PSSI n'est pas pilotée par le CNRS, les règles de cette PSSI devront être intégrées dans la PSSI définie par le pilote.

L'ESE – UMR8079 est concernée par la PSSI Laboratoires.

Le Directeur d'Unité (DU) est responsable de la sécurité des SI mis en œuvre dans son unité et il nomme un chargé de SSI (CSSI) qui l'assiste en la matière : Nicolas Moulonguet. Le DU s'appuie sur le CSSI pour mettre en application cette PSSI dans son unité.

Un CSSI peut être chargé de la SSI pour plusieurs unités si les différents directeurs d'unité concernés donnent leur accord pour ce faire : se mettre en relation avec GQE et EGCE pour éventuellement partager un seul CSSI à l'IDEEV.

Le DU, dans le cadre du dialogue de gestion, s'assure de l'attribution des moyens et ressources nécessaires à l'application de cette PSSI et de la mise en œuvre de l'organisation, des procédures, des dispositifs nécessaires à l'application de la PSSI.

En l'absence de CSSI, le Directeur d'Unité remplit, par défaut, les fonctions attribuées au CSSI dans cette politique.

<u>Mise en œuvre de la PSSI :</u>

Pour le laboratoire :

Le DU s'appuie sur le CSSI pour :

- identifier, à l'aide de la méthode décrite par la règle « POL-1 », le niveau de couverture des risques – la couverture des risques croissant de *, **, *** - qu'il convient de fixer pour son unité et sélectionne l'ensemble des règles PSSI qui correspondent à ce niveau (pour un niveau les règles de niveau inférieur sont applicables) ;

- formaliser un plan d'action SSI permettant de mettre en application ces règles en lien avec le responsable informatique en charge des infrastructures et équipements utilisés par l'unité.

Le plan d'action SSI prend en compte les ressources budgétaires et humaines nécessaires à sa mise en œuvre et est examiné lors du dialogue de gestion.

Pour les systèmes d'information conçus par le laboratoire :

Chaque projet de système d'information conçu sous la responsabilité d'un laboratoire du CNRS doit intégrer la sécurité comme un besoin fonctionnel dès l'étape de cadrage du projet suivant les règles définies dans la PSSI.

Le représentant de la maîtrise d'ouvrage du système considéré est responsable de la gestion des risques SSI afférents à la mise en œuvre de ce système et de l'approbation officielle des risques résiduels avant mise en production du système :

- Définition de la direction responsable de l'approbation des risques : DU de la structure,

- Définition des modalités de la décision d'approbation des risques : cf. règles PSSI,

- Définition des pièces du dossier sécurité pour l'approbation des risques : cf. règles PSSI.

Dans le cas où l'étape de cadrage détecte que le système d'information nécessite une homologation au sens du Référentiel Général de Sécurité de l'administration française :

- Définition de l'autorité administrative responsable de l'homologation : le Délégué Régional dont dépend le laboratoire,

- Définition des autorités d'homologation en fonction des cas : le DU représentant de la MOA du système d'information considéré ayant délégation de signature du DR pour cette fonction,

- Définition des comités d'homologation compétents en fonction des cas : le Délégué Régional dont dépend le laboratoire + le DU représentant de la MOA du système d'information considéré + CPO du système considéré + CSSI du laboratoire + le RSSI de la DR,

- Définition des modalités de la décision d'homologation : cf. règles PSSI,

- Définition des pièces du dossier sécurité pour l'homologation : cf. règles de la PSSI,

- Contrôle et renouvellement de l'homologation : cf. règles de la PSSI.

Suivi de la mise en œuvre de la PSSI :

Le suivi de la mise en œuvre de cette PSSI dans l'unité est réalisé par le DU.

Au plan national, le suivi de la mise en œuvre de la PSSI est organisé par le RSSI du CNRS conformément à la PGSI.

Les modalités de suivi sont adaptées en fonction du niveau de couverture des risques fixé pour l'unité.

Pour les unités dont le niveau de couverture des risques est fixé à ***, le DU devra transmettre chaque année au RSSI du CNRS, via le RSSI de DR, un rapport – dont le modèle défini au niveau national - permettant de juger du niveau d'application des règles de sécurité des SI dans l'unité.

Application pratique de la PSSI :

Conformément à la PSSI opérationnelle, le directeur :

- définit le niveau de couverture des risques – la couverture des risques croissant de *, **, *** - qu'il fixe pour son unité et sélectionne l'ensemble des règles PSSI qui correspondent à ce niveau (au niveau n, les règles de niveau inférieur sont applicables) ;

- formalise un plan d'action SSI permettant de mettre en application ces règles en lien avec le responsable informatique en charge des infrastructures et équipements utilisés par l'unité.

Définition du niveau de couverture des risques (* à ***) :

- Dans le cas où l'unité est déclarée protégée au titre de la PPST[1] et inclut au moins une ZRR[2], l'unité doit bénéficier d'une couverture des risques SSI au niveau ***.

- Dans le cas où l'unité inclut des SI ou manipule des informations dont le niveau de sensibilité est « critique » suivant la classification définie dans cette PSSI, l'unité doit bénéficier d'une couverture des risques SSI au niveau *** au minimum (Pour l'évaluation de la sensibilité d'un SI se reporter à la fiche PDI-3-implémentation).

- Dans le cas où l'unité est déclarée protégée au titre de la PPST, l'unité doit bénéficier d'une couverture des risques SSI au niveau ** au minimum.

- Dans le cas où l'unité est une structure de type administratif (DR, unité du Siège, etc.), l'unité doit bénéficier d'une couverture des risques SSI au niveau ** au minimum. **(ce n'est pas le cas)**

- Dans tous les autres cas, l'unité doit bénéficier d'une couverture des risques SSI au niveau * au minimum.

Pour avancer, il faut répondre à 3 questions, après avoir défini le SI :

L'Unité est-elle déclarée protégée au titre de la PPST ?

L'unité inclut-elle au moins une ZRR ? Il n'y a pas de ZRR à l'ESE. Comme il n'y a pas de ZRR à l'ESE, d'après la note 1, l'ESE n'est pas déclarée protégée au titre de la PPST.

Quelle est la sensibilité du SI ?

Pour réaliser l'évaluation de la sensibilité du SI, il convient de le cartographier, c'est-à-dire recenser les différents actifs et estimer ensuite leur niveau de sensibilité.

[1] Protection du Patrimoine Scientifique et Technique. La protection contre l'espionnage technologique est l'objectif premier du dispositif. Le dispositif PPST offre une protection juridique et administrative fondée notamment sur le contrôle des accès, physiques comme virtuels, aux informations sensibles détenues au sein de zones protégées, appelées zones à régime restrictif (ZRR), qui constituent des espaces définis à l'intérieur desquels se déroulent des activités de recherche ou de production à protéger en raison de l'intérêt qu'elles présentent pour la nation.

[2] Zone à Régime Restrictif.

Définition des actifs SI de l'Unité : Geslab, Réséda, Agate-Tempo, Dialog, Sirhus, Simbad, Notilus, Etamine, Zimbra, Sympa. (vérifier que toutes le SI est couvert par ses applications).

La sensibilité d'un actif sera déterminée en fonction :

- du niveau de besoin de sécurité des informations et des processus liés à cet actif suivant les 4 critères SSI classiques (Disponibilité, Intégrité, Confidentialité, Auditabilité) ;

- du type et niveau d'impact potentiel en cas d'atteinte à la qualité d'un des 4 critères SSI classiques (Disponibilité, Intégrité, Confidentialité, Auditabilité)

Pour donner un exemple, si l'Unité n'est pas déclarée protégée au titre de la PPST, qu'elle n'inclut pas au moins une zone ZRR, et que le niveau de sensibilité du SI est Faible, Moyen, voire Important en termes de Disponibilité, Intégrité, Confidentialité et Auditabilité, l'Unité doit bénéficier d'une couverture des risques au niveau *.

Sécurité en termes de Disponibilité, Intégrité, Confidentialité, Auditabilité du SI à l'ESE :

Pour Agate-Tempo, par exemple :

Le SI peut être indisponible entre 24 heures et une semaine (Niveau Moyen).

Le SI peut être altéré pendant une période de 24 heures à une semaine et le contenu rétabli sans délais dès l'identification de l'altération (Niveau Moyen).

Le SI est accessible à un groupe restreint d'agents du CNRS et de partenaires authentifiés (Niveau Important).

Aucun besoin d'auditabilité sur le SI (Niveau 0).

Impacts en termes de Disponibilité, Intégrité, Confidentialité, Auditabilité du SI à l'ESE :

Pour Agate-Tempo, par exemple :

Impact humain (Aucun impact).

Impact sur l'image (Aucun impact).

Impact financier (Aucun impact).

Impact légal (Aucun impact).

Impact sur le fonctionnement (Aucun impact).

Impact sur le potentiel scientifique et technique (Aucun impact).

Ces niveaux de sécurité et d'impacts sont à vérifier avec Sandrine Dessaints, Nathalie Frascaria et Nathalie Lecat.

La définition des niveaux pour les besoins de sécurité et les impacts sont donnés en Annexe.

Annexes techniques

Echelle des niveaux de besoin DICA :

Niveau	Besoin de disponibilité
0 - Aucun	L'actif peut être perdu définitivement
1 - Faible	L'actif peut être indisponible entre une semaine et un mois
2 - Moyen	L'actif peut être indisponible entre 24 heures et une semaine
3 - Important	L'actif peut être indisponible jusqu'à 24 heures
4 - Critique	L'actif doit être disponible en temps réel

Niveau	Besoin d'intégrité
0 - Aucun	L'actif n'a pas besoin d'être intègre même si l'altération est détectée
1 - Faible	L'actif peut être altéré pendant une période d'une semaine à un mois et le contenu rétabli dès que possible après identification de l'altération Exemple d'application : les contrôles visuels et des sauvegardes régulières sont suffisantes
2 - Moyen	L'actif peut être altéré pendant une période de 24 heures à une semaine et le contenu rétabli sans délais dès l'identification de l'altération Exemple d'application : des contrôles planifiés sur des éléments clés et des sauvegardes quotidiennes sont suffisants
3 - Important	L'actif peut-être altéré jusqu'à 24 heures et le contenu rétabli sans délais dès l'identification de l'altération Exemple d'application : des dispositifs automatiques de scellements et des sauvegardes quotidiennes sont nécessaires
4 - Critique	L'actif doit être rigoureusement intègre Exemple d'application : des dispositifs automatiques de scellements, des procédures de réaction en temps réel et des sauvegardes sur une période très courte sont nécessaires

Niveau	Besoin de confidentialité
0 - Aucun	L'actif est accessible à tous, publié sur Internet
1 - Faible	L'actif est accessible à tous les agents du CNRS et aux partenaires
2 - Moyen	(Diffusion interne) L'actif est accessible à un large groupe d'agents du CNRS et de partenaires authentifiés
3 - Important	(Diffusion restreinte) L'actif est accessible à un groupe retreint d'agents du CNRS et de partenaires authentifiés Exemple d'application : il existe une procédure formelle d'habilitation et les accréditations sont revues périodiquement
4 - Critique	(Diffusion restreinte) L'actif est très sensible et uniquement accessible par certains agents du CNRS authentifiées Exemple d'application : il existe une procédure formelle d'habilitation et les accréditations sont revues périodiquement. Les accès applicatifs et physiques nécessitent des dispositifs d'authentification forte.

Niveau	Besoin d'auditabilité
0 - Aucun	Aucun besoin d'auditabilité sur l'actif
1 - Faible	Auditabilité permettant uniquement de retrouver la date et l'horaire des connexions des utilisateurs
2 - Moyen	Auditabilité permettant de retrouver l'auteur, la date et l'horaire des actions
3 - Important	Auditabilité permettant de retrouver l'auteur, la date, l'horaire et les détails des actions
4 - Critique	Auditabilité probante et opposable permettant de retrouver l'auteur, la date, l'horaire et les détails des actions

Type d'impacts et échelles de niveaux d'impact.

Niveau	Impact humain
0 - Aucun	Aucun impact
1 - Faible	Non Applicable
2 - Moyen	Atteinte potentielle à l'intégrité physique ou psychique ou atteinte potentielle aux données à caractère personnel d'au moins une personne
3 - Important	Atteinte à l'intégrité physique ou psychique ou atteinte aux données à caractère personnel non sensibles d'au moins une personne
4 - Critique	Atteinte à la vie ou atteinte aux données à caractère personnel sensibles d'au moins une personne

Niveau	Impact sur l'image
0 - Aucun	Aucun impact
1 - Faible	Mention négative sur les canaux internes du CNRS
2 - Moyen	Mention négative limitée sur les canaux externe au CNRS
3 - Important	Mention négative dans la presse spécialisée et/ou atteinte limitée à la réputation du CNRS
4 - Critique	Mention négative dans la presse grand public et/ou atteinte de grande ampleur à la réputation du CNRS

Niveau	Impact financier
0 - Aucun	Aucun impact
1 - Faible	Perte financière de l'ordre de 0,1% du budget de l'entité
2 - Moyen	Perte financière de l'ordre de 1% du budget de l'entité
3 - Important	Perte financière de l'ordre de 10% du budget de l'entité
4 - Critique	Perte financière supérieure à 10% du budget de l'entité

Niveau	Impact sur le fonctionnement
0 - Aucun	Aucun impact
1 - Faible	Le nombre de jours de travail perdus est de l'ordre de 0,1% du nombre de jours travaillés de l'entité
2 - Moyen	Le nombre de jours de travail perdus est de l'ordre de 1% du nombre de jours travaillés de l'entité Ou la désorganisation conduit à des défauts limités de prise de décision, de gestion et/ou de sécurisation
3 - Important	Le nombre de jours de travail perdus est de l'ordre de 10% du nombre de jours travaillés de l'entité. Ou la désorganisation conduit à des défauts de prise de décision, de gestion et/ou de sécurisation
4 - Critique	Le nombre de jours de travail perdus est supérieur à 10% du nombre de jours travaillés de l'entité Ou la désorganisation conduit à l'incapacité de prise de décision, de gestion et/ou de sécurisation

Niveau	Impact légal
0 - Aucun	Aucun impact
1 - Faible	Non-respect de la réglementation interne
2 - Moyen	Non-respect de la réglementation interne, accompagné d'avertissements ou de sanctions internes
3 - Important	Engagement de la responsabilité civile
4 - Critique	Engagement de la responsabilité pénale

Niveau	Impact sur le potentiel scientifique et technique
0 - Aucun	Aucun impact
1 - Faible	Atteinte pouvant aboutir à une perte de compétitivité limitée à l'entité
2 - Moyen	Atteinte pouvant aboutir à une perte de compétitivité pour le CNRS sans risque de perte de compétitivité significative pour la Nation Ou atteinte pouvant faciliter l'activisme sans risque de déstabilisation de l'État
3 - Important	Atteinte pouvant aboutir à une perte de compétitivité pour la Nation (fraction relativement faible du PIB) Atteinte pouvant aboutir à l'affaiblissement de la capacité de défense nationale (de façon partielle et peu importante) Ou atteinte pouvant faciliter la prolifération ou le terrorisme (de façon partielle et peu importante) Ou atteinte pouvant faciliter l'activisme avec risque important de déstabilisation de l'État
4 - Critique	Atteinte pouvant aboutir à une perte de compétitivité pour la Nation (fraction significative du PIB) Atteinte pouvant aboutir à l'affaiblissement de la capacité de défense nationale (de façon significative) Ou atteinte facilitant la prolifération ou le terrorisme (de façon significative) Ou atteinte pouvant faciliter l'activisme avec risque majeur de déstabilisation de l'État

Evaluation du niveau de sensibilité en fonction des besoins et impacts :

Niveau de sensibilité		Max du niveau d'impact redouté				
		0 - Aucun	1 - Faible	2 - Moyen	3 - Important	4 - Critique
Max du niveau de besoin DICA	0 - Aucun	Pas sensible	Peu sensible	Sensible	Très sensible	Critique
	1 - Faible	Peu sensible	Peu sensible	Sensible	Très sensible	Critique
	2 - Moyen	Sensible	Sensible	Sensible	Très sensible	Critique
	3 - Important	Très sensible	Très sensible	Très sensible	Très sensible	Critique
	4 - Critique	Critique	Critique	Critique	Critique	Critique

Résultat de l'Audit :

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Disponibilité	3	3	3	3	3	3	3	3	3	3	3	3	3	3		
Intégrité	4	4	3	3	4	3	3	3	3	3	4	3	3	3		
Confidentialité	4	4	3	3	4	3	3	3	3	3	4	3	3	3		
Auditabilité	4	4	3	3	4	3	3	3	3	3	4	3	3	2		
I. humain	2	2	2	2	2	2	2	2	2	2	3	3	3	3		
I. image	2	2	2	2	2	2	2	2	2	2	2	2	2	3		
I. financier	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
I. légal	4	1	1	1	1		1	1	1	1	4	1	2	0		
I. fonctionnement	4	1	1	4	1	1	1	4	1	1	4	1	1	0		
I. potentiel sci. et Tech.	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
	1	Geslab						11	Sifac							
	2	Réséda						12	Sigefor							
	3	Agate-tempo						13	Ariane							
	4	Dialog						14	Web							
	5	Sirhus						15	Notilus							
	6	Simbad						16	Cirrus							
	7	Etamine														
	8	Zimbra														
	9	Sympa														
	10	Nouba														

		Max du niveau de besoin DICA	Max de niveau d'impact redouté	Niveau de sensibilité résultant
1	Geslab	4	4	Critique
2	Réséda	4	2	Critique
3	Agate-tempo	3	2	Très sensible
4	Dialog	3	4	Critique
5	Sirhus	4	2	Critique
6	Simbad	3	2	Très sensible
7	Etamine	3	2	Très sensible
8	Zimbra	3	4	Critique
9	Sympa	3	2	Très sensible
10	Nouba	3	2	Très sensible
11	Sifac	4	4	Critique
12	Sigefor	3	3	Très sensible
13	Ariane	3	3	Très sensible
14	Web	3	3	Très sensible
15	Notilus			
16	Cirrus			