PSSI ESE applicable suivant la PSSI CNRS.[1]

Politique :

POL-1 implémentation de la règle (23/01/2017)
Sensibilité : *

Politique : ***Les règles de la PSSI opérationnelle de l'unité sont définies après détermination du niveau de couverture des risques applicable.***

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 ***)*

Il convient de considérer successivement les cas suivants :
• Dans le cas où l'unité est déclarée protégée au titre de la PPST et inclut au moins une ZRR, 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.
• 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.
• 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.
• Dans tous les autres cas, l'unité doit bénéficier d'une couverture des risques SSI au niveau * au minimum.

NOTA : Pour l'évaluation de la sensibilité d'un SI se reporter à la fiche PDI-3-implémentation

En attendant un éclaircissement du second cas, la sensibilité * est retenue pour l'ESE, c'est-à-dire le niveau élémentaire.

Sélection des règles applicables

La liste des règles applicables dans les unités du CNRS sont regroupées suivant les chapitres de la norme internationale ISO 27002 qui fait référence pour les pratiques SSI (il s'agit de la version 2005 de la norme, depuis il a été publié la version 2013).

Ces règles sont publiées dans la liste : https://extra.core-cloud.net/collaborations/RSSI-CNRS/Lists/PSSI%20rgles/AllItems.aspx
Ces règles sont regroupées suivant 3 niveaux de couverture des risques SSI :

[1] Dans ce document, tout n'est pas reporté de la PSSI CNRS. En cas d'interrogation, se reporter à la PSSI CNRS.

- Niveau * : niveau élémentaire
- Niveau ** : niveau standard
- Niveau *** : niveau fort

Le DU formalise dans un document :
- Le niveau de couverture des risques déterminé pour son unité
- La liste des règles applicables

Formalisation du plan d'action

À l'issue de l'étape précédente, le DU dispose de la liste des règles applicables pour son unité. Pour chaque règle une fiche détaille les mesures à mettre en œuvre :
- une fiche explicative détaille ce qui doit être fait ou apporte des précisions sur ce qui doit être fait, cette fiche est nommée <N° de la règle>-implémentation ;
- 0 à n fiches techniques détaillent éventuellement le « comment » en fonction des plates-formes techniques et des différents matériels ;
- 0 à n fiches donnent éventuellement des exemples de mise en œuvre.

Les fiches détaillées correspondant à ces règles sont regroupées dans la bibliothèque : https://extra.core-cloud.net/collaborations/RSSI-CNRS/PSSI%20documents/Forms/AllItems.aspx

Le DU doit maintenant :
- pointer les règles qui sont déjà mises en œuvre ;
- évaluer le niveau de mise en œuvre en pourcentage d'application ;
- formaliser le plan d'action qui permettra de planifier la mise en œuvre des règles qui ne sont pas appliquées à 100%.

NOTA : Pour la formalisation du plan d'action, se reporter à la fiche ORG-2

Organisation :

ORG-1 implémentation de la règle (23/01/2017)
Sensibilité : *

Organisation : ***Le DU est responsable de la sécurité des systèmes d'information (SSI) dans son unité et nomme une personne chargée de la SSI (CSSI) pour l'assister en la matière.***

Pour certaines unités, le rôle du CSSI est porté par un RSSI.

Pour toutes les autres unités, la nomination du CSSI de l'unité est du seul ressort du Directeur de l'unité qui la notifie au RSSI de sa DR de rattachement.

Selon l'importance et la structure de l'unité, le CSSI peut être secondé dans ces missions par d'autres personnes de l'unité. La ventilation des tâches doit être alors précisée.

Cette fonction peut aussi être mutualisée entre plusieurs unités. Il est important que les fonctions de CSSI soient officialisées et reconnues tant en interne qu'en externe. À ce titre, il fera partie d'un réseau de compétence régional et sera identifié auprès de l'instance régionale de coordination comme le référent unique du laboratoire.

Le CSSI d'une unité CNRS doit obligatoirement faire partie d'une structure sous contrat avec le CNRS et faire partie du personnel déclaré dans l'annuaire du CNRS.

Le CSSI d'une unité peut ne pas faire partie du personnel de l'unité si cela est justifié, par exemple :
- CSSI mutualisé entre plusieurs unités de très faible taille ;
- compétences SSI non disponibles dans l'unité ;
- opportunité organisationnelle dans le cas d'unités jointes sur le même site ;
- etc.

NOTA : dans le cas où un même CSSI est nommé par plusieurs DU pour plusieurs unités, il convient cependant de s'assurer de conserver un plan d'action SSI spécifique et identifié pour chacune de ces unités.

Le CSSI assiste le Directeur d'Unité dans l'exercice de ses responsabilités en matière de SSI. En particulier :
- il assiste son DU pour la mise en œuvre de la PSSI du CNRS dans son unité et l'adapte en fonction des risques locaux ;
- il sensibilise les personnels à la SSI ;
- il met en œuvre ou s'assure de la mise en œuvre des recommandations SSI transmises par le RSSI du CNRS via le RSSI de DR ;
- il gère les alertes et incidents en lien avec le RSSI de DR à qui il signale tout incident de sécurité ;
- il planifie, applique ou coordonne la mise en place des mesures de sécurité (mises à jour des OS, etc.) sur les infrastructures et dans les projets de SI (analyse de risque, etc.) de l'unité ;
- il assiste son DU pour répondre aux enquêtes nationales SSI et rapport annuel SSI.

ORG-2 implémentation de la règle (23/01/2017)
Sensibilité : *

Organisation : ***Le DU est responsable de la formalisation et du suivi du plan d'action de mise en œuvre des règles de la PSSI dans l'unité.***

Le plan d'action doit reprendre l'ensemble des règles de la PSSI opérationnelle applicables pour le niveau de couverture des risques défini pour l'unité. Ce plan d'action est pluriannuel, idéalement avec une projection à 5 ans, au minimum à 3 ans, afin de rapprocher son cadencement de celui de la construction budgétaire de l'unité.

Pour chaque règle le plan d'action indique au minimum :

- Dans le cas où la règle fait l'objet d'une dérogation :
  - o la référence du document qui expose les motifs de la dérogation et qui a été validé par le DU,
  - o la date de la signature de cette dérogation par le DU.
- Dans le cas où la règle ne fait pas l'objet d'une dérogation :
  - o l'état de mise en œuvre
    - ♣ évaluation / spécifications du chantier de mise en œuvre en cours
      - date prévue pour la mise en œuvre du chantier,
      - évaluation de la charge interne en jours-hommes pour l'évaluation du chantier,
      - évaluation de la charge financière en € pour l'évaluation du chantier.
    - ♣ chantier de mise en œuvre lancé
      - date prévue pour le début de la mise en œuvre de la règle,
      - évaluation de la charge interne en jours-homme pour le chantier,
      - évaluation de la charge financière en € pour le chantier.
    - ♣ mise en œuvre en cours
      - date prévue pour la mise en œuvre complète de la règle,
      - pourcentage de mise en œuvre par pas de 25%,
      - évaluation de la charge interne en jours-homme pour la mise en œuvre annuelle,
      - évaluation de la charge financière en € pour la mise en œuvre annuelle.
    - ♣ mise en œuvre effective
      - date du début de la mise en œuvre complète,
      - évaluation de la charge interne en jours-homme pour la mise en œuvre annuelle,
      - évaluation de la charge financière en € pour la mise en œuvre annuelle.
  - o Budget demandé au dialogue budgétaire annuel, budget alloué pour la mise en œuvre de la mesure ou de l'ensemble de mesures
  - o Ressources humaines nécessaires (en fraction d'équivalent temps plein) Le CSSI au niveau local, le RSI-DR régional et le RSSI au niveau national ont la charge, selon les consignes nationales, de produire et tenir à jour un tableau de bord permettant de contrôler la réalisation d'objectifs opérationnels, d'améliorer la qualité de service et de détecter au plus tôt les retards dans la réalisation de certains objectifs de sécurité.

ORG-4[2] implémentation de la règle (23/01/2017)

Sensibilité : *

Organisation : ***La sensibilisation à la SSI de l'ensemble des personnels de l'unité doit être réalisée.***

Toute personne affectée à l'unité doit être sensibilisée à la SSI lors de son arrivée. Toute personne affectée à l'unité doit être régulièrement sensibilisée à la SSI, ce qui permet de lui faire prendre connaissance des nouvelles menaces et nouvelles recommandations.

[2] Il semble que ORG-3 n'existe pas, sans doute par erreur de numérotation.

ORG-5 implémentation de la règle (23/01/2017)
Sensibilité : *

Organisation : ***La SSI et notamment les conditions d'hébergement des données sensibles doivent être prises en compte dans les contrats avec les tiers et les prestations contrôlées.***

Avant de contractualiser avec un tiers, il convient de mesurer les risques de confier une activité à celui-ci. À ce titre, il est recommandé d'effectuer une analyse des risques ad hoc.

Le CSSI doit être associé à la rédaction de tout contrat avec un tiers dans la mesure où ce contrat est susceptible de donner lieu à la mise en place de traitements d'informations.

Les menaces de haut niveau les plus courantes liées aux tiers extérieurs sont en général :
- la fuite d'information,
- la perte de disponibilité,
- le défaut de performance,
- la perte de contrôle d'une activité,
- la perte de connaissances et d'expertise et l'irréversibilité,
- les erreurs,
- la malveillance.

Ces différentes menaces viennent en plus, ou du moins de façon plus stigmatisée, des menaces qui existaient déjà sur les systèmes d'information.

Ces menaces sont également à considérer en fonction du type de prestation contractualisée. Les implications ne sont pas les mêmes entre un tiers local ayant pour tâche l'entretien des bâtiments (et donc ayant un accès physique aux téléphones et aux postes de travail) et un tiers à qui l'on confierait l'exploitation de sa messagerie.

Il existe autant de clauses possibles que de type de prestation ou de partenariat. À ce sujet, L'ANSSI a publié un guide de l'externalisation de certaines prestations informatiques. Ce guide recommande notamment :
- d'évaluer les risques ;
- de prévoir des clauses de sécurité adaptées dans les contrats ;
- de suivre la mise en place de la sécurité lors de la prise en charge, du cycle de vie et de la fin de prestation ou de partenariat ;
- de mettre en place un plan d'assurance sécurité et des comités sécurité.

Dans tous les cas, il est nécessaire de :
- S'assurer que les besoins de confidentialité sont matérialisés par une clause adaptée dans les documents contractuels (par exemple : le cahier des clauses particulières d'un marché public). Lorsque ces besoins sont importants, il est indispensable de demander conseil au service compétant de la délégation régionale.
- Se donner les moyens de vérifier ce qui va être exigé. C'est pour cela qu'il convient de vérifier qu'une clause d'audit est bien présente dans le contrat et qu'elle permet de le faire réaliser par un autre tiers en encadrant les délais, la durée, la situation géographique et les droits des auditeurs.

Ensuite, dans les éléments qu'il convient de cadrer au minimum dans le cas d'une externalisation de tout ou d'une partie du système d'information, il est recommandé de prendre en compte :
- la localisation géographique des informations,

- la localisation géographique du personnel,
- le niveau de conformité vis-à-vis de la réglementation sur les données à caractère personnel, et pour cela, se rapprocher du service du CoSIL CNRS local, ou du service du CIL compétent,
- les niveaux de mutualisation,
- l'analyse juridique dans le cas des contrats d'adhésion ou de licence (type Google),
- la territorialité des tribunaux compétents en cas de recours,
- les niveaux de performance,
- les responsabilités financières des parties,
- la réversibilité,
- la restitution et, le cas échéant, la destruction des biens de l'unité en fin de collaboration.

Il est indispensable, en cas de doute ou de besoin d'assistance, de se mettre en relation avec les services compétents du CNRS (RSSI-DR ou RSSI-C, Direction des affaires juridiques, service du Correspondant informatique et libertés, services achats régionaux ou national…). Selon les termes de la PSSIE, l'hébergement des données sensibles de l'administration sur le territoire national est obligatoire, sauf dérogation dûment motivée et précisée dans la décision d'homologation.

ORG-6 implémentation de la règle (23/01/2017)
Sensibilité : *

Organisation : ***Toute dérogation aux règles de la PSSI doit être validée par le DU avec avis motivé.***

Le directeur d'unité ayant défini le niveau de risque qu'il souhaite couvrir (* à ***) obtient donc la liste des règles qu'il doit mettre en œuvre pour cela, conformément à la règle POL-1.

Il va ensuite définir un plan d'action visant la mise en œuvre progressive des règles applicables conformément à la règle ORG-2.

Dans le cas où le directeur considère :

- que le rapport coût / bénéfice d'une règle est trop important au regard des possibilités de mise en œuvre dans l'unité
- et s'il ne pense pas pouvoir dégager, à court ou moyen terme, les moyens nécessaires à la mise en œuvre de cette règle,

il pourra établir une dérogation à la règle. À cette dérogation doit être joint un argumentaire détaillé qui sera soumis au CSSI de l'unité pour avis. L'avis du CSSI sera consigné et la dérogation signée du directeur sera jointe au plan d'action SSI de l'unité. La dérogation est limitée dans le temps (3 ans maximum).

Les accès spécifiques à Internet nécessitant des droits particuliers pour un usage métier ne peuvent être mis en place que sur dérogation dûment justifiée, et sur des machines isolées physiquement et séparées du réseau de l'entité, après validation préalable de l'autorité d'homologation (le directeur en l'occurrence).

Les dérogations pourront être examinées lors des audits menés dans le cadre du contrôle de l'application de la PSSI du CNRS.

Protection des documents et des informations :

PDI-1 Implémentation de la règle (21/08/2018)
Sensibilité : *

Protection des documents et des informations : ***Les documents électroniques produits dans l'unité doivent être marqués par leur producteur suivant leur niveau de confidentialité.***

La confidentialité des documents électroniques

Afin de garantir un niveau de protection approprié aux informations, il convient de définir le niveau de sensibilité des informations (action de *classification*) pour indiquer le besoin, les priorités et le degré souhaité de protection lors de leur manipulation.

La sensibilité en confidentialité d'un document peut s'évaluer en se posant la question de l'impact que pourrait avoir la diffusion du document à une audience large. Quel impact peut avoir la diffusion non contrôlée du document sur l'image de l'établissement, de l'unité ou de ses agents, sur la sécurité des agents, des partenaires, sur le bon fonctionnement des institutions, sur la protection du potentiel scientifique et technique, sur le respect des personnes ?

Il faut évaluer l'impact (faible, modéré, important, catastrophique) lié à la divulgation d'une information selon ses conséquences :
- pour l'organisme, en termes juridiques, financiers, d'image, de patrimoine scientifique et technologique
- pour les personnes physiques concernées
- pour la Nation

L'évaluation de cet impact va conditionner le niveau de classification à attribuer à l'information.

Exemples :
Impact catastrophique pour l'établissement :
- Peut entrainer des condamnations pénales au titre de la règlementation sur la protection du secret de la défense nationale (IGI 1300).
- Peut remettre en cause le fonctionnement de l'organisme ou des partenaires

Impact catastrophique sur les personnes : Les personnes concernées pourraient connaitre des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter (péril financier tel que des dettes importantes ou une impossibilité de travailler, affection psychologique ou physique de longue durée, décès...)
Impact catastrophique pour la Nation : Peut porter atteinte à la souveraineté, la sécurité ou aux intérêts économiques essentiels de la France au titre de la loi n°68-678.

Impact important pour l'établissement :
- Contentieux ou peut entrainer des condamnations civiles ou pénales (règlementation I&L)
- Peut nuire à l'image ou induire le discrédit de l'organisme ou des partenaires
- Peut favoriser l'émergence de la concurrence ou lui donner un avantage décisif

Impact important sur les personnes : Les personnes concernées pourraient connaitre des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés (frais supplémentaires, refus d'accès à des prestations commerciales, peur, incompréhension, stress, affection physique mineure...) ou de sérieuses difficultés (détournements d'argent, interdiction bancaire, dégradation de biens, perte d'emploi, assignation en justice, aggravation de l'état de santé...)

Impact modéré sur l'établissement : Pénalités contractuelles.
Impact modéré sur les personnes : Les personnes concernées ne seront pas impactées ou pourraient connaitre quelques désagréments, qu'elles surmonteront sans difficulté (perte de temps pour réitérer des démarches ou pour attendre de les réaliser, agacement, énervement...).

Les données sensibles au sens de la Loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés sont celles qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou sont relatives à la santé ou à la vie sexuelle de celles-ci. Sont aussi concernées les données dites à risque (génétiques, relatives aux infractions pénales, aux condamnations, comportant des appréciations sur les difficultés sociales des personnes, données biométriques, comprenant le numéro NIR).

Niveaux de confidentialité des documents électroniques au CNRS

Le niveau de classification est lié aux impacts d'une éventuelle divulgation non autorisée des informations tels que définis précédemment et à la cible de la diffusion. Il détermine les précautions à prendre pour leur manipulation.

C'est l'impact potentiel le plus élevé du fait d'une divulgation non autorisée qui détermine le niveau de classification.

Le niveau de classification s'applique quelle que soit la forme que prend l'information ; ce sont les règles de gestion associées qui peuvent varier en fonction du support de l'information.

Les différents niveaux de classification ainsi définis sont les suivants :
- PUBLIC pour une information dont la cible de diffusion n'est pas contrôlée. Cette publication de l'information présente un impact nul pour l'organisme ;
- DIFFUSION LIMITÉE + Mention pour une information dont la cible n'est pas nominative mais dont la mention précise les structures ou entités destinataires de l'information ou des personnes es-qualité. La mention spécifique associée au niveau de classification peut être suffisante pour définir la liste de diffusion. Une divulgation non autorisée de l'information aurait un impact modéré ;
- CONFIDENTIEL pour une information dont la cible n'est pas nominative mais précise les structures ou entités destinataires de l'information, des personnes es-qualité et qui doit être diffusée via un canal dont l'accès est strictement contrôlé. Une divulgation non autorisée de l'information aurait un impact important.
- DIFFUSION RESTREINTE conformément à l'II 901 pour une information dont la cible est nominative ou précise les structures ou entités destinataires de l'information, des personnes es-qualité ayant besoin d'en connaître et qui doit être diffusée via un canal dont l'accès est strictement contrôlé. Une divulgation non autorisée de l'information aurait un impact catastrophique.

Ainsi :
Pour un impact nul : PUBLIC
Pour un impact modéré : DIFFUSION LIMITÉE + Mention
Pour un impact important : CONFIDENTIEL + Mention
Pour un impact catastrophique : DIFFUSION RESTREINTE + Mention

À partir du niveau DIFFUSION LIMITÉE, le niveau de classification doit être assorti d'une mention qui définit la cible de diffusion.
- <ORGANISME> si l'information n'est applicable qu'à l'organisme et ne doit pas être diffusée en dehors ;

- <STRUCTURE> si l'information ne doit être échangée qu'au sein de la structure (laboratoire, institut, délégation régionale, …) ;
- <GROUPE> si l'information ne doit être échangée qu'au sein d'une communauté définie ;
- <PROJET> si l'information est liée à un projet donné et qu'elle ne doit être échangée qu'avec les partenaires du projet ; une convention commune à l'ensemble des partenaires du projet pourra être établie au démarrage pour s'assurer que les informations bénéficient des mêmes protections quel que soit le partenaire qui les manipule.

La mention caractérise le périmètre de diffusion *en réservant l'accès à l'information aux seules personnes ayant besoin de les connaître pour l'accomplissement de leur fonction ou de leur mission*. Il n'est pas défini de mention par défaut.

Dans tous les cas, c'est le niveau de classification qui détermine les règles à respecter pour protéger une information. La mention accolée au niveau de classification précise ou renforce le cas échéant les règles applicables.

Les données en Open Data, par définition, ne peuvent concerner que des données publiques.

NOTA : Les niveaux de classification n'interfèrent pas avec le droit de la propriété intellectuelle ou le droit d'auteur.

Mise en place d'un référentiel d'établissement

Il est de la responsabilité du chef d'établissement de mettre en place un référentiel partagé, indiquant pour chaque type de document le niveau de classification initiale adéquat.

Ce référentiel est tenu à jour par le FSD de l'établissement, qui s'assure qu'il connaît une publicité adéquate afin d'être porté à la connaissance de tous. Le FSD de l'établissement se coordonne avec les FSD des établissements partenaires afin d'harmoniser autant que possible les niveaux de classification de documents identiques par nature.
Il n'y a pas de FSD à l'ESE.

Le référentiel est mis à jour au fil du temps avec les informations remontées des différents services et unités, par exemple lorsqu'un document d'un nouveau type, ne figurant pas dans le référentiel est inventorié.

Le référentiel alimente les propriétés de sensibilité des objets métiers dans les cadres nationaux de cohérences recherche et enseignement pour une applicabilité globale.

Le FSD est responsable de la mise en place d'un processus opérationnel de mise à jour du référentiel. Ce processus est publié avec le référentiel afin d'être connu de tous.

Responsabilité du Directeur d'Unité

Le directeur de l'unité de recherche est responsable de la bonne mise en œuvre de ces dispositions dans son unité. Il est également responsable de l'application du référentiel d'établissement par les personnes travaillant au sein de son unité. Il est le garant du choix du niveau de classification proposé par le producteur.

Il doit mettre en place un processus de classification permettant de valider le choix d'un niveau de classification et de déroger au référentiel d'établissement.

Lorsqu'une information produite ne figure pas dans le référentiel, le processus mis en place prévoit une classification par défaut et d'en informer le FSD de l'établissement afin qu'il détermine le bon niveau final de classification.

Rôle du producteur de l'information

Le producteur d'une information s'appuie sur le référentiel en place pour proposer le niveau de classification de cette information. Dans le cas où il estime que le niveau indiqué dans le référentiel ne s'applique pas à l'information qu'il vient de produire, il peut y déroger suivant le processus existant dans l'unité.

Si le producteur rencontre une difficulté pour identifier le niveau de classification d'une information, il peut faire appel à sa ligne managériale ou se faire conseiller par son correspondant de sécurité du SI.

Le producteur d'une information est le responsable du suivi de la classification de cette information. Si l'information est produite dans le cadre d'un projet, les producteurs de l'information et le responsable du projet sont co-responsables du suivi de la classification de l'information. Dans la mesure du possible, la durée de classification de l'information doit être indiquée.

Le processus de classification de l'information s'applique sur toutes les versions d'un document y compris les versions de travail.
Le responsable du suivi de la classification d'une information est en charge de suivre et faire évoluer la classification de cette information tout au long de son cycle de vie.

Dans le cas où le responsable du suivi de la classification d'une information change de fonction, quitte son service ou l'établissement il appartient à sa hiérarchie de désigner un nouveau responsable pour cette information.

Si le service venait à disparaître, c'est le responsable de l'unité ou de la direction à laquelle il appartenait qui devient le nouveau responsable de l'information.

Rôle du destinataire de l'information

Le destinataire d'une information doit être informé des règles qu'il doit respecter pour garantir la protection de l'information qui lui a été confiée. En particulier, les échanges d'information avec des tiers dans le cadre d'une relation contractuelle ou partenariale doivent faire l'objet de clauses de sécurité pour définir les exigences qu'il doit respecter en fonction du niveau de classification des informations reçues ; ces clauses sont garantes d'une protection adéquate des informations par son destinataire.

Le destinataire d'une information peut décider, si le besoin est motivé et justifié, de retransmettre une information reçue, dans le respect des engagements auxquels il est soumis, en appliquant le principe du « besoin d'en connaître » et à condition qu'il respecte les mesures de protection applicables du fait de la classification de cette information et de la mention spécifique éventuellement associée.

Pour une information de niveau DIFFUSION LIMITÉE, destinée à une population nominativement identifiée le destinataire doit informer l'émetteur de l'information en cas de diffusion au-delà du périmètre indiqué par la mention.

Pour une information de niveau CONFIDENTIEL, destinée à une population nominativement identifiée le destinataire doit préalablement obtenir l'accord de l'émetteur de l'information en cas de diffusion au-delà du périmètre indiqué par la mention.

Le fait que l'émetteur d'une information n'ait pas fait mention de son caractère sensible ne signifie pas que le destinataire, qui est soumis à l'obligation de discrétion et qui doit respecter le principe du « besoin d'en connaître », puisse la diffuser largement. Il peut par ailleurs interroger l'émetteur de l'information pour connaître les éventuelles précautions qu'il doit respecter concernant l'information que ce dernier lui a transmise. En particulier, la diffusion publique d'une information doit être le résultat d'une démarche volontaire et maîtrisée.

Durée de classification

La sensibilité d'un document évolue au cours du temps, très généralement dans le sens de la diminution des besoins en confidentialité. Par exemple une fois brevetée, une invention n'a plus à être confidentielle. Tout document est destiné à terme à être une archive publique ou disparaitre. Lorsque c'est possible, la date ou l'événement à partir duquel le niveau de classification peut être revu doit être indiqué dans le document.

La législation, la réglementation ou les dispositions contractuelles peuvent imposer une durée de classification. Elle s'impose alors à toute autre disposition du présent document.

Procédure de déclassification

Le niveau de classification d'une information ou la mention de diffusion peuvent être revus à tout moment par le responsable de cette information.

Le marquage initial de la classification doit indiquer explicitement la durée de classification. À l'issue de cette durée, le responsable de l'information doit décider s'il prolonge la durée de classification au même niveau ou s'il modifie le niveau de classification en conformité avec le processus de son unité.

À défaut d'indication de la durée de classification, le niveau de classification est modifié à la baisse d'un niveau tous les 5 ans.

Marquage

Pour faciliter la gestion de l'information, le niveau de classification, la mention spécifique et la durée de classification doivent être apposés ou doivent accompagner sa diffusion :

- Le niveau de classification doit être mentionné dans le nom du fichier – Le nommage peut respecter la nomenclature suivante : NiveauClassification-NomFichier-Version.extension.
- Pour un document, le marquage doit être apposé en haut de chaque page en caractères gras et en capitales ;
- Pour une information transmise oralement ou visuellement, l'interlocuteur doit être averti le cas échéant du niveau de classification et de la mention spécifique de l'information qui lui est transmise.

Tout au long de sa vie, une information doit changer de niveau de classification, l'émetteur prendra soin d'apposer un marquage en cohérence avec le nouveau niveau de classification.

Il est obligatoire de faire apparaître sur les supports de stockage informatiques amovibles (DVD, clé USB, disque externe, …) le niveau maximum de classification des informations contenues dans ce support et le cas échéant, la mention spécifique correspondante. L'usage de supports de stockage informatiques amovibles différentiés (e.g. clé USB dont le format est prévu pour permettre un tel marquage) peut faciliter la mise en œuvre de cette obligation.

Gestion de l'information en fonction de sa confidentialité au CNRS

Cf. Règle PDI-2

PDI-2 implémentation de la règle (23/01/2017)
Sensibilité : *

Protection des documents et des informations : ***Les documents électroniques doivent être stockés, manipulés, transmis via les procédures et avec les outils propres à assurer leur confidentialité au niveau adéquat.***

Dans tous les cas, le fichier se retrouve dans le système de fichiers du poste de travail de la personne qui l'a extrait, produit, reçu. Le poste de travail peut être un ordinateur fixe ou portable comme un smartphone ou une tablette. Il peut s'agir aussi d'un périphérique de stockage amovible (clé USB, disque externe, carte mémoire…).

Niveau de confidentialité des documents électroniques

La classification d'un document est déterminée en appliquant la règle PDI-1-implémentation

Mesures de protection des documents en fonction de leur sensibilité

Les informations doivent être créées, stockées et sauvegardées sur des systèmes d'information dont le niveau de sensibilité est cohérent avec le niveau de classification. Des outils de sécurisation spécifiques (e.g. moyen de chiffrement) peuvent être mis à disposition des utilisateurs pour répondre à des besoins en confidentialité qui vont au-delà du niveau de sécurité offert par ces systèmes d'information.

Les informations professionnelles ne doivent pas être traitées (ni créées, ni stockées, ni sauvegardées) sur des moyens informatiques qui sont hors du périmètre de confiance de l'organisme (les moyens personnels, les moyens accessibles au public, les moyens mis à disposition par un tiers hors des clauses de sécurité établies entre l'organisme et ce tiers). Le stockage sur cloud externe (Google Drive, Dropbox, …) est interdit. En particulier, l'usage à des fins professionnelles d'une messagerie électronique personnelle est interdit. Gmail et autre est interdit et donc les redirections vers ces comptes.

Tout support de stockage informatique amovible (DVD, clé USB, disque externe, …) ou document papier marqué au niveau CONFIDENTIEL ou supérieur :
- doit être stocké dans une armoire fermant à clé ou dans un local protégé (bureau fermé à clé en l'absence de surveillance, zone à accès contrôlé, …).
- doit assurer que les informations sur stockage numérique sont chiffrées. En effet, lors des déplacements (transports, hôtels, …), un utilisateur s'expose au risque de vol de son poste de travail ou des supports de stockage qu'il détient.

Par ailleurs, lorsqu'un utilisateur prévoit de se déplacer à l'étranger, il doit :
- préalablement vérifier que les démarches ont bien été réalisées pour lui permettre d'exporter et d'utiliser les outils mis à sa disposition par l'organisme (notamment les outils de chiffrement),
- préalablement vérifier que le pays de destination ne prohibe pas l'usage de tel équipement ou dispositif de sécurité (par exemple : usage de VPN),
- limiter le transport d'informations sensibles, y compris chiffrées, notamment à destination des pays qui imposent aux visiteurs, avant d'entrer sur le territoire ou d'en sortir, de mettre à disposition en

clair et à des fins de contrôle le contenu de leur poste de travail ou de leurs supports de stockage informatiques amovibles (DVD, clé USB, disque externe, …).

Le correspondant à la sécurité du système d'information de l'unité, le RSSI ou le FSD de l'organisme est à sa disposition pour l'assister dans ses démarches.

Impression, reproduction

Les moyens d'impression et de reproduction constituent un système d'information particulier du domaine de fonctionnement de l'organisme et chaque moyen est différent (photocopieurs en réseau, imprimantes individuelles, …).

Les imprimantes utilisées pour l'impression des documents CONFIDENTIELS ou plus doivent être sécurisées conformément aux préconisations de la Politique de Sécurité du SI de l'État (notamment les règles PDT-MUL-DURCISS, PDT-MUL-AUTH et PDT-MUL-SECNUM).

Acheminement

Il peut être nécessaire de transmettre des informations sous forme physique (document papier, support de stockage informatique amovible, …). Dans ce cas, les règles suivantes doivent être respectées :

- Les informations de niveau DIFFUSION LIMITÉE peuvent être transmises sous simple enveloppe, par le courrier interne de l'organisme ou par voie postale et adressées à une personne physique ;
- Les informations de niveau CONFIDENTIEL doivent être transmises sous simple enveloppe portant la mention « Personnel à l'attention de… » ;
- Les informations de niveau DIFFUSION RESTREINTE doivent être transmises sous double enveloppe (l'enveloppe extérieure ne faisant pas apparaître de mention de confidentialité et l'enveloppe intérieure portant la mention « DIFFUSION RESTREINTE » et les références du document).

Echanges numériques et périmètre de confiance

Les échanges numériques regroupent notamment les usages suivants, sans que cette liste soit exhaustive :
- La messagerie électronique
- La messagerie instantanée
- La visioconférence ou l'audioconférence avec utilisation d'un pont de visioconférence
- La visioconférence ou l'audioconférence sur le poste de travail
- Le partage d'écran sur le poste de travail
- Les plateformes de synchronisation de fichiers entre postes de travail
- Les plateformes collaboratives
- Les plateformes d'édition en ligne

Ces applications permettent donc de façon générale l'échange d'information de façon synchrone ou asynchrone entre plusieurs personnes ou équipements.

Confiance dans l'opérateur de l'infrastructure

La confiance dans l'entité qui opère ces services est un facteur important permettant d'évaluer leur adaptation à la transmission d'information classifiées selon l'échelle de sensibilité, que ce soit au sein de l'organisme ou entre organismes.

L'ESE a des informations sur la façon dont l'infrastructure est opérée et sur le niveau de confidentialité des échanges ou la gestion et l'exploitation des métadonnées. Aucun État étranger n'a la possibilité de disposer d'un accès aux informations. La réglementation européenne est applicable. Il y a des relations contractuelles entre l'ESE et l'opérateur de l'infrastructure (RENATER).

Confiance dans une solution d'échange numérique

La confiance accordée à une solution d'échange numérique ne se résume pas seulement au niveau de confiance qu'on accorde à l'opérateur de cette solution.

Elle dépend d'autres facteurs, tels que :

- L'exposition de la solution à Internet : une solution exposée à Internet subit plus d'attaques et expose les données hébergées de façon plus importante qu'une solution qui n'est accessible qu'en interne.
- L'utilisation du chiffrement de bout en bout :
    - o Si le service d'échange numérique propose un chiffrement de bout en bout (possibilité pour plusieurs personnes d'échanger des informations de façon chiffrée sans que les administrateurs du service chez l'opérateur n'aient la possibilité de déchiffrer les données), ceci augmente considérablement le niveau de confiance qu'on peut accorder à la solution.
    - o S'il est possible d'utiliser une solution de chiffrement tierce permettant d'utiliser le service d'échange numérique comme infrastructure d'échange sans que l'opérateur n'ait le moyen de déchiffrer les données.

Les solutions de chiffrement utilisées doivent être validées par le RSSI du CNRS.

Usages autorisés d'une solution d'échange numérique en fonction du niveau de classification

Le tableau suivant indique pour un niveau de classification d'une information quelles sont les solutions d'échange numérique autorisées en fonction du niveau de confiance accordé à ces solutions.

Si plusieurs solutions d'échanges numériques sont simultanément disponibles et si le choix est possible, alors la solution offrant le niveau de confiance le plus élevé doit systématiquement être choisie. *Le choix d'une solution offrant un niveau de confiance minimum ne doit pas être un choix par défaut mais le résultat d'une impossibilité technique, de l'absence de la possibilité de choisir ou d'une solution imposée par un partenaire.*

Toute utilisation d'une solution inadéquate vis-à-vis du niveau de classification doit faire l'objet d'un signalement au directeur de l'unité et d'une déclaration d'incident de sécurité.

Niveau de classification	Niveau autorisé de confiance dans la solution d'échanges numériques	Chiffrement de bout en bout obligatoire (sauf si le niveau de confiance ne peut être atteint qu'avec le chiffrement)	Mention
PUBLIC	Faible	Non	Non
DIFFUSION LIMITÉE	Moyen	Non	Dans le corps d'un message, 1ère ligne. Marquage d'un document ou d'une
CONFIDENTIEL	Important	Non	
RESTREINT	Très important	Chiffré avec un logiciel qualifié par l'ANSSI.	

			présentation en pied de page (chaque page). Mention orale au début d'une audio ou visioconférence. Destinataires ou participants cohérents avec la cible de diffusion

Affichage et consultation « en local »

On traite ici de l'utilisation de l'information (écran ordinateur, écran projeté, tablette, smartphone, etc.), ou encore dans le cas d'un support papier, de la consultation du document.

Niveau de classification	Environnement public	Environnement interne ou contrôlé (partenaire)
PUBLIC	Aucune recommandation particulière	Aucune recommandation particulière
DIFFUSION LIMITÉE	L'utilisateur doit s'assurer avant d'afficher le document que son environnement permet l'affichage en toute discrétion	Pas de contraintes ou de restriction pour la consultation
CONFIDENTIEL	Utilisation d'un filtre polarisant écran recommandée mais non obligatoire Consultation déconseillée du document papier L'utilisateur doit s'assurer avant d'afficher le document que son environnement permet l'affichage en toute discrétion	L'utilisateur doit s'assurer avant de consulter le document que son environnement permet la consultation en toute discrétion quel que soit le support En cas de projection locale, s'assurer que l'ensemble des participants a besoin d'en connaître
RESTREINT	Utilisation d'un filtre de confidentialité obligatoire L'utilisateur doit s'assurer avant d'afficher le document que son environnement permet l'affichage en toute discrétion Pas de consultation du document papier dans un lieu public	L'utilisateur doit s'assurer avant de consulter le document que son environnement permet la consultation en toute discrétion quel que soit le support En cas de projection locale, s'assurer que l'ensemble des participants a besoin d'en connaître

Réaffectation interne de matériel

Si le support est chiffré, il doit être reformaté et chiffré de nouveau avant d'être mis à la disposition d'un nouvel utilisateur.

Si le support n'est pas chiffré et qu'il contient des informations classifiées DIFFUSION LIMITÉE ou plus, il doit être effacé avec une procédure d'effacement sécurisée validée par le RSSI avant d'être mis à la disposition d'un nouvel utilisateur.

Fin de vie du support au sein de l'organisme

Si la surface est chiffrée, effacement sécurisé selon une procédure validée par le RSSI de l'établissement, puis traitement habituel de fin de vie sans autre précautions

Si la surface n'est pas chiffrée et le niveau de classification DIFFUSION LIMITÉE, CONFIDENTIEL ou RESTREINT, destruction physique selon une procédure validée par le RSSI de l'établissement.

PDI-3 implémentation de la règle (23/01/2017)
Sensibilité : *

Protection des documents et des informations : ***Les systèmes d'information utilisés dans l'unité doivent être référencés et leur niveau de sensibilité évalué.***

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

La norme ISO 27005:2011 définit la notion d'actif ainsi : « Un actif désigne tout élément ayant de la valeur pour l'organisme et nécessitant, par conséquent, une protection ».

Cette même norme fait la distinction entre deux types d'actifs : les actif primordiaux (ou biens essentiels) et les actifs de support.

L'actif primordial est un actif impalpable, comme un processus métier, une activité ou une information. L'actif primordial repose sur un ou plusieurs actifs de support.

L'actif de support est un actif physique ou palpable. Ces actifs sont plus nombreux et peuvent être classés par type (communément : matériel, logiciel, réseau, personnel, site, structure de l'organisation).

Tout actif doit avoir un propriétaire.

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).

La détermination des actifs a été faite à l'ESE. Le résultat est donné dans le document PGSI_PSSI.pdf. Après une première passe, les niveaux des actifs sont « Très sensibles » ou « Critique », c'est-à-dire de niveau ** et ***. Peut-être que ces sensibilités ont été surévaluées.
Un niveau de sensibilité englobe les niveaux inférieurs, c'est-à-dire que pour les actifs de niveaux **, il faut prendre en compte aussi le niveau *, et pour les actifs de niveau ***, il faut prendre en compte aussi * et **.
Dans ce document de premier jet, seules les règles de niveau * sont décrites. Les règles ** et *** seront décrites plus tard.

Le référencement et l'analyse de la sensibilité des SI principaux utilisés par l'unité, permettent de déterminer rapidement le niveau de couverture de risque à appliquer à cette unité dans le cadre de la PSSI CNRS.

Ressources humaines :

GRH-1 implémentation de la règle (23/01/2017)
Sensibilité : *

Ressources humaines : ***Le personnel entrant dans l'unité doit être accueilli suivant une procédure d'accueil formalisée qui inclut la prise de connaissance de la charte SSI et des règles élémentaires de sécurité informatique avant l'ouverture des accès sur le SI.***

Le personnel entrant dans l'unité doit avoir pris connaissance de la charte SSI et approuver les dispositions mises en place avant ouverture de ses accès et mise à disposition de matériels avant d'avoir accès au système d'information (la signature d'un document démontrant cet engagement peut être un moyen mis en place pour formaliser cette procédure). Comme indiqué dans la décision d'approbation de la charte, celle-ci doit être portée à la connaissance du personnel par tous moyens et notamment :

- par envoi sur messagerie lorsqu'un compte est ouvert pour un utilisateur, celui-ci devant déclarer avoir pris connaissance de la présente charte,
- par voie d'affichage dans les locaux de l'entité, par voie d'annexe au règlement intérieur de l'entité ou par remise d'un exemplaire papier de la charte.

Concernant les personnels intervenant dans l'unité mais qui ne lui sont pas rattachés (exemple : prestataires de services), les dispositions de la charte doivent être rendues opposables à l'employeur de ces personnels lors de la contractualisation avec cette personne morale.

Les personnels disposant de privilèges élevés sur le système d'information (notamment les ASR) sont identifiés et autorisés par la direction de l'unité à effectuer des actions d'administration.

Il est essentiel aussi que le personnel entrant ait pris connaissance des règles élémentaires de sécurité qui reposent principalement sur :

• La protection technique du poste de travail :
  o sauvegarde systématique et quotidienne des données,
  o configuration maîtrisée et mise à jour régulièrement,
  o Chiffrement des supports de stockage (postes de travail, clés USB, disques externes, etc.).
• Un comportement avisé de l'utilisateur :
  o protection de son poste de travail et tous les périphériques qui lui sont confiés, notamment lorsque ceux-ci sont des supports de données, contre le vol et les accès illégitimes,
  o mots de passe robustes et personnels (cela concerne aussi les codes d'accès du téléphone et de la messagerie vocale),
  o attitude prudente vis-à-vis des supports de données amovibles qui lui sont remis par des tiers (clés USB, etc.),
  o utilisation prudente d'Internet (téléchargements, utilisation de services en ligne),
  o attitude prudente vis à vis des messages reçus.
• Le devoir d'alerte des responsables techniques et sécurité en cas d'évènement anormal.

GRH-1-1 implémentation de la règle (23/01/2017)
Sensibilité : *

Ressources humaines : ***Les personnes qui ne font pas partie du personnel doivent prendre connaissance des règles SSI de l'unité avant toute connexion au SI de l'unité.***

Les personnes qui ne font pas partie du personnel sont les visiteurs occasionnels, les personnels hébergés, les personnels invités et les prestataires de service.

Lorsqu'ils sont autorisés à se connecter au SI de l'unité, ils doivent être formellement avertis – par une fiche remise à l'accueil par exemple – des limites afférentes à cette connexion. Ils prennent connaissance des chartes et règlements en vigueur dans l'unité.

S'agissant des prestataires de services, les dispositions de ces documents doivent avoir été contractualisées avec leur employeur pour leur être opposables : ces documents doivent leur être mis à disposition pour prise de connaissance si nécessaire.

Les visiteurs peuvent être mis sur le réseau filaire des visiteurs 172.23.32.0. Pour avoir accès à Internet à partir de ce réseau, ils doivent activer le proxy :
http://cache.universite-paris-saclay.fr sur le port 8080

GRH-2 implémentation de la règle (23/01/2017)
Sensibilité : *

Ressources humaines : ***Le personnel quittant l'unité doit être connu de l'équipe informatique qui applique une procédure de départ formalisée incluant la fermeture des droits sur le SI et la restitution des matériels appartenant à l'unité.***

La procédure de départ du personnel formalise notamment :
- les responsabilités pour garantir la bonne gestion du départ,
- la procédure de réintégration de tout le matériel mis à la disposition de l'agent (équipements informatiques, badges, clés…),
- la procédure de suppression de tous les droits d'accès sur le SI (Il est conseillé de réexaminer également à cette occasion les droits d'accès des autres utilisateurs), en particulier lorsque cet agent disposait de privilèges élevés (administrateur),
- la réintégration des données professionnelles,
- le devenir et l'accès aux données à caractère personnel (fichiers, mails,…).

Un document attestant du bon déroulement de la procédure est signé par le CSSI et l'agent sortant (quitus).

Ce document n'existe pas à l'ESE. Les départs se font sans être signalés au CSSI.

Si l'agent sortant avait la connaissance de certains identifiants partagés entre plusieurs agents (mots de passe administrateur par exemple), il est important de changer ces identifiants.

Le départ doit être signalé à l'ensemble des partenaires avec qui l'agent sortant collaborait.

Le cas du décès d'un agent sera également traité comme un cas d'agent sortant de l'unité. Les données ayant été identifiées comme « privées » par le personnel décédé seront archivées en vue d'une éventuelle remise aux héritiers.

NOTA : parfois, certains comptes doivent rester ouverts pour du personnel ayant quitté officiellement l'unité mais qui continue de travailler pour cette unité (par exemple terminer une thèse), cette dérogation nécessite un avis écrit et motivé du DU. Elle doit être limitée dans le temps.

A l'ESE, il est fréquent de prolonger les comptes e-mails. La prolongation est limitée dans le temps. Mais il n'existe pas de dérogation écrite par le DU.

Au 29/03/24, liste des comptes e-mail actifs des agents qui ne font plus parti de l'effectif, et sans limite de date :
Zoran Cerovic, Gabriel Cornic, Éric Dufrêne, Emmanuelle Jestin, Caroline Mauve, Jean-Yves Pontailler, François Ramade, Christian Raquin, Hélène Roche, Bernard Saugier, Dara Sihachakr, Ameline Vallet

GRH-3 implémentation de la règle (23/01/2017)
Sensibilité : *

Ressources humaines : ***Le personnel en mission doit avoir suivi, avant son départ, une sensibilisation spécifique aux risques SSI relatifs à ces déplacements.***

Avant le départ en mission, l'agent est informé par son CSSI des risques spécifiques inhérents au nomadisme, et à sa destination. Le CSSI s'assure notamment que l'agent respecte les dispositions réglementaires locales en matière d'usage de produits de chiffrement, d'accès VPN… Il s'assure enfin que l'agent dispose des matériels et logiciels nécessaire à la protection de ses données (exemple : filtre de confidentialité écran, coffre-fort de mots de passe…).

Le CSSI prendra attache avec le service du RSSI-C ou du FSD en cas de difficulté ou de doute sur les conditions particulières pour une destination.

Dans la mesure du possible, lorsque les contraintes réglementaires locales à destination ne permettent pas une protection adéquate des données du CNRS par les moyens techniques décrits ci-dessus, l'agent utilise des moyens d'informations vierges de données sensibles et dédiés aux missions disponibles dans l'unité, configurés et remis par le CSSI ou l'équipe informatique locale.
Avant de partir à l'étranger, le personnel consultera et appliquera les recommandations disponibles sur les sites suivants :
- FSD du CNRS ;
- Ministère des affaires étrangères ;
- ANSSI avec notamment le passeport de conseils aux voyageurs.

Sécurité physique :

PHY-1 implémentation de la règle (23/01/2017)
Sensibilité : *

Sécurité physique : ***Un plan détaillé des locaux doit permettre d'identifier les locaux et/ou des zones sensibles (locaux ou zones qui contiennent des matériels, informations ou SI sensibles) qui seront marqués suivant leur niveau de sensibilité.***

La demande du fond de plan peut être faite auprès du service du patrimoine de la Délégation pour des bâtiments dont le CNRS est propriétaire.
Le CNRS n'est pas propriétaire des bâtiments de l'Ideev.

Les zones peuvent être classées en 5 catégories :
• Zone 0 : zone publique (éventuellement terrain environnant le bâtiment).
• Zone 1 : zone destinée à l'accueil du public.
• Zone 2 : zones réservées aux personnels administratifs et personnels chercheurs (y compris stagiaires de longue durée),
• Zone 3 : zone sensible donnant accès aux bureaux de personnes à responsabilité ou titulaires de postes de confiance, etc.
• Zone 4 : zones dédiées aux matériels et informations critiques.

Les zones de livraison et de chargement sont situées dans des zones de niveau 0 ou 1. **Le plan ne doit pas faire apparaître explicitement les zones définies comme à régime restrictif (ZRR), ce zonage étant soumis à une classification Confidentiel Défense.**

Le niveau de sensibilité des locaux peut être déterminé suivant l'échelle suivante :
• Peu sensible (Z0 et Z1) :
- zone publique (éventuellement terrain environnant le bâtiment) ;
- locaux destinés à l'accueil du public (hall, salles de cours, etc.).
• Sensible (Z2) :
- locaux réservés aux personnels (administratifs, techniciens, ingénieurs, chercheurs, y compris stagiaires longue durée).
• Très sensible (Z3) :
- bureaux de personnes menant des travaux qui doivent être protégés vis-à-vis de tiers externes au laboratoire ;
- bureaux des personnels ayant des droits élevés sur les SI d'informations ou contenant les machines utilisées pour l'administration, la gestion du réseau, des serveurs, des applications, etc. ;
- locaux techniques abritant des dispositifs permettant un accès au réseau du laboratoire ;
- locaux techniques abritant des SI permettant de piloter des expériences (« informatique industrielle ») ou des SI traitant de travaux qui doivent être protégés vis-à-vis de tiers externes au laboratoire (serveurs de fichiers, bases de données, etc.).
• Critique (Z4) :
- bureaux de personnes menant des travaux qui doivent être protégés au titre de la Protection du Potentiel Scientifique et Technique ou bureaux des personnes ayant accès à ces travaux ;
- locaux techniques abritant des SI permettant de piloter des expériences (« informatique industrielle ») ou des SI traitant de travaux qui doivent être protégés au titre de la Protection du Potentiel Scientifique et Technique ou dont le délai maximum de remise en service est inférieur à 24h (serveurs de fichiers, bases de données, etc.)
A l'ESE, les zones sont Z0, Z1 et Z2.

PHY-2 implémentation de la règle (23/01/2017)
Sensibilité : *

Sécurité physique : ***Les locaux et/ou zones doivent être protégés par les moyens recommandés suivant leur niveau de sensibilité (peu sensible, sensible, très sensible, critique).***

La classification des zones est définie dans la règle PHY-1.

- Peu sensible (niveau Z0 ou Z1) :
  - o Pas de recommandation pour une couverture des risques * et **.
- Sensible (niveau Z2) :
  - o Pas de recommandation pour une couverture des risques * et **.
- Très sensible (niveau Z3) :
  - o Pas de recommandation pour une couverture des risques *.
  - o Pour le niveau **
    - ♣ Une procédure décrit les modalités permettant d'autoriser l'accès dans les zones sécurisées (zone 3 et zone 4) aux intervenants de prestataires et sociétés externes ainsi qu'aux visiteurs présentant un besoin.
- Critique (niveau Z4) :
  - o Tout local hébergeant des systèmes informatiques de niveau "critique" dispose d'une protection contre les accès non autorisés : système de fermeture par clé et/ou serrure magnétique et badge d'accès individuel.

A l'Ideev, badge et code pour les salles de brassage et pour la salle serveur.

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.

NOTA : Tout local hébergeant des systèmes informatiques dispose des équipements d'infrastructure nécessaires au bon fonctionnement de ces moyens informatiques : climatisation, équipements de protection incendie, alimentation électrique régulée et secourue, protection contre les dégâts des eaux.

L'alimentation secteur des équipements devra 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.

Un dispositif de climatisation dimensionné en fonction des besoins énergétiques du système informatique doit être installé. Des procédures de réaction en cas de panne, connues du personnel, doivent être élaborées et vérifiées annuellement. Ces dispositions visent à prévenir toute surchauffe des équipements, pouvant engendrer une perte du service voire une détérioration du matériel.

L'installation de matériel de protection contre le feu est obligatoire. Des procédures de réaction à un incendie sont définies et régulièrement testées. Les salles techniques doivent être propres. Aucun carton, papier, ou autre source potentielle de départ de feu ne doit être entreposé dans ces locaux.

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.

Il convient de protéger le câblage réseau contre les dommages et les interceptions des communications qu'ils transmettent. En complément, les panneaux de raccordements et les salles des câbles doivent être placés en dehors des zones d'accueil du public et leur accès doit être contrôlé.

Exploitation des SI :

EXP-3 implémentation de la règle (23/01/2017)
Sensibilité : *

Exploitation des SI : ***Lorsque tout ou partie de l'exploitation des SI est confiée à un tiers, il doit être assuré que les mesures de sécurité définies par cette politique sont reportées dans le contrat.***

Lorsque tout ou partie de l'exploitation d'un SI est confiée à un tiers il y a infogérance (externalisation dans le domaine des systèmes d'information).

D'après l'ANSSI, l'infogérance peut être classée en trois grandes catégories :
- la gestion d'infrastructures : maintenance, hébergement, administration, supervision, etc. ;
- la gestion des applications : support fonctionnel, maintenance préventive ou corrective, gestion des évolutions ;
- l'hébergement de services : le prestataire héberge pour le compte de son client une application utilisée comme un service.

Ces prestations d'infogérance peuvent induire, en fonction du contexte dans lequel elles sont réalisées, des risques pour le système d'information comme pour les données (intégrité, disponibilité, confidentialité), venant s'ajouter aux risques qui seraient déjà présents sur le SI s'il était géré en interne. L'ANSSI identifie trois grands domaines de risques :
- la perte de maîtrise du système d'information ;
- les interventions à distance ;
- l'hébergement mutualisé.

Les mesures spécifiques aux risques de l'infogérance doivent être pris en compte : on se référera au guide de l'externalisation de l'ANSSI.

Il convient de noter que la télémaintenance est une forme d'infogérance et que :
- les services de télémaintenance doivent être systématiquement encadrés par des accords contractuels qui précisent les conditions dans lesquelles sont effectuées les opérations de télémaintenance ;
- cela concerne aussi bien les matériels que les logiciels. En particulier les photocopieurs, équipements réseau, matériels téléphoniques, etc. doivent être pris en compte ;
- les accès de télémaintenance (comptes dédiés, accès réseau) doivent être fermés en dehors des périodes de télémaintenance. Ils sont ouverts à la demande des télé-mainteneurs et à l'initiative des exploitants du système télé-maintenu et sont fermés à la fin de toute opération de télémaintenance ;
- il convient de s'assurer, via les conditions d'emploi, que les télé-mainteneurs informent systématiquement les exploitants de la fin de chaque opération de maintenance afin de leur permettre de fermer les accès ;
- les opérations de télémaintenance sont tracées et journalisées et elles font l'objet d'un contrôle a posteriori systématique ;
- les outils utilisés pour la télémaintenance doivent être validés, **en particulier il ne peut être fait usage d'un service dans le cloud/qui dépend d'un ou plusieurs serveurs tiers non maîtrisés (exemple Teamviewer).**
L'utilisation de TeamViewer sur le PC de la Serre constitue un écart par rapport à la PSSI.

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 l'entité ou le ministère.

EXP-4 implémentation de la règle (23/01/2017)
Sensibilité : *

Exploitation des SI : ***L'usage d'outils permettant d'administrer à distance un système ou permettant d'effectuer des diagnostics techniques est réservé aux seuls administrateurs techniques autorisés.***

Il convient de répertorier ces outils. Il est conseillé de les regrouper en catégories.

Une liste identifiant les administrateurs techniques autorisés à utiliser chaque catégorie d'outils doit être maintenue. Toute modification de cette liste doit être validée par le CSSI.

La traçabilité de l'utilisation de ces outils doit être garantie : il doit être possible de répondre à la question « Qui a eu accès à tel outil ou telle interface d'administration et quand ? ».

Des audits réguliers sont effectués sur ces outils pour vérifier que les comptes des administrateurs et les comptes de service créés, ainsi que les privilèges qui leur sont associés, correspondent bien à la politique qui est définie dans l'unité.

NOTA : Beaucoup d'équipements s'administrent via une connexion SSH ou HTTP. Les outils susvisés sont, dans ce cas des outils généraux : client SSH, navigateur web. Il n'est pas envisageable de restreindre l'accès à ces logiciels mais il faut poser les restrictions d'accès au niveau des équipements (identification, droits, restriction sur la base de l'origine des connexions). Il est également nécessaire d'afficher clairement sur la page d'accueil et avant connexion que l'accès est réservé aux administrateurs au moyen d'une bannière.

Certains outils de diagnostic sont susceptibles d'exposer des informations confidentielles ou de nature à permettre une escalade de privilèges. Les outils permettant d'écouter le réseau appartiennent à cette catégorie et ne doivent pas pouvoir être utilisés par des personnes non habilitées. Leur accès doit être attribué suivant le principe du moindre privilège.

On vérifiera qu'aucun équipement du réseau ne comporte d'interface d'administration accessible directement depuis l'Internet.

IPM (IP Management du réseau filaire de l'Ideev) n'est pas accessible de l'extérieur de l'Université, sauf par VPN GlobalProtect.

Il convient de mettre en œuvre des moyens pour sécuriser la connexion (filtrage, VPN, authentification forte, etc.).

EXP-4 outils (23/01/2017)
Sensibilité : *

Exploitation des SI : ***L'usage d'outils permettant d'administrer à distance un système ou permettant d'effectuer des diagnostics techniques est réservé aux seuls administrateurs techniques autorisés.***

Le cas des outils permettant la prise de contrôle à distance mérite d'être étudié et encadré (VNC, TSE/RDP Teamviewer, etc.).

L'outil choisi doit répondre aux spécifications minimales suivantes :
- Authentification de l'utilisateur, si possible plus forte qu'un simple mot de passe
- Traçabilité des actions
- Possibilité de désactivation en cas de non utilisation

- Indépendance de services Cloud ou de briques techniques hébergées en dehors du contrôle de l'unité
- Usage uniquement de protocoles chiffrés

La plus grande attention sera portée à la sécurisation des serveurs sur lesquels ces outils sont installés. Il est recommandé d'héberger les serveurs dans des locaux sécurisés non accessibles au public (par exemple en salle machine). **Quand les outils nécessitent le passage des flux par un serveur intermédiaire, nécessairement hébergé sur Internet et qui n'est pas sous le contrôle de l'unité, leur usage est alors prohibé.**

Des passerelles sécurisées peuvent être utilisées pour permettre aux administrateurs techniques d'utiliser ces outils à distance.

Une bonne pratique consiste à créer un compte de service différent pour chaque outil et de configurer une authentification en deux étapes selon le principe suivant :
- L'administrateur s'authentifie sur le serveur où l'outil est accessible (ou sur la passerelle).
- L'administrateur s'authentifie pour utiliser le compte de service associé à l'outil (par exemple, sous UNIX, avec la commande : sudo, su compte_de_service).

EXP-5 implémentation de la règle (23/01/2017)
Sensibilité : *

Exploitation des SI : ***La gestion des traces de l'activité des systèmes informatiques doit respecter les directives nationales.***

La maîtrise de la sécurité de fonctionnement des systèmes passe par un contrôle s'appuyant nécessairement sur l'enregistrement systématique et temporaire d'un certain nombre d'informations caractérisant les transactions effectuées sur ces systèmes, appelées traces.

Ces traces ont plusieurs objectifs :
- la métrologie du réseau : contrôler le volume d'utilisation de la ressource, détecter des anomalies, mettre en place de la qualité de service, faire évoluer les équipements en fonction des besoins ;
- vérifier que les règles en matière de SSI sont correctement appliquées et que la sécurité des SI et du réseau telle qu'elle a été définie par la politique de sécurité de l'unité est assurée ;
- détecter toute défaillance ou anomalie de sécurité, volontaire ou accidentelle, passive ou active, d'origine matérielle ou humaine ;
- détecter toute violation de la loi ou tout abus d'utilisation des moyens informatiques pouvant engager la responsabilité du CNRS ;
- être à même de fournir des preuves nécessaires pour mener les enquêtes en cas d'incident de sécurité et de répondre à toute réquisition officielle présentée dans les formes légales.

Les traces à enregistrer de manière systématique portent sur l'utilisation des moyens suivants :
- les serveurs et postes de travail ;
- les équipements d'extrémité de réseau et la surveillance des services réseau (routeurs, pare-feux, etc …) ;
- les équipements de surveillance du trafic réseau (IDS, antivirus, antispam, ...) ;
- tout équipement informatique fourni à l'utilisateur par le CNRS ou ses partenaires à des fins professionnelles ;
- les applications spécifiques.

La durée maximum de conservation des traces est de 12 mois glissants sauf disposition contraire imposée par une réglementation spécifique.

Il est préconisé de mettre en œuvre un système de centralisation des traces collectées sur les différents systèmes, ceci afin de faciliter la gestion et la consultation, et de garantir une meilleure intégrité de ces traces en cas de compromission du système générateur. Si un tel système est mis en œuvre, la durée de conservation des traces sur le système générateur ne dépassent pas un mois. Le système centralisateur conserve les traces 12 mois glissants.

Les objectifs précités imposent d'aller au-delà d'un enregistrement et d'une exploitation de données statistiques. Ils impliquent nécessairement l'enregistrement, la conservation temporaire et l'éventuelle exploitation de données à caractère personnel, dans la mesure où des éléments contenus dans les traces permettent de remonter directement ou indirectement à l'identité de l'utilisateur.

Ces traces et leur traitement doivent respecter les droits de chacun et notamment être conformes à la réglementation de protection des données personnelles en vigueur, qui fixe les principes suivants :
- finalité : usage déterminé et légitime ;
- proportionnalité : informations pertinentes et nécessaires ;
- durée limitée de conservation des données ;
- sécurité et confidentialité : le responsable du traitement doit prendre les mesures nécessaires pour garantir la confidentialité des données et éviter leur divulgation ;
- respect du droit des personnes.

Chaque utilisateur des SI doit être informé de l'existence de ces traces et de leur traitement via notamment la lecture de la Charte SSI du CNRS.

Les informations enregistrées :

Informations journalisées par les serveurs (hors messagerie et Web) et postes de travail

Pour chaque tentative de connexion ou d'ouverture de session de travail les informations suivantes - ou une partie de ces informations - peuvent être enregistrées automatiquement par les mécanismes de journalisation du service :
- l'identité de l'émetteur de la requête qui peut être :
    - o dans le cas d'une authentification à l'aide d'un certificat, les différents éléments de celui-ci : l'émetteur, le nom de l'utilisateur, son adresse électronique, le numéro de l'unité ;
    - o sinon on enregistre l'identifiant ou/et l'adresse IP (adresse proprement dite ou nom de machine et dans un certain nombre de cas le serveur DHCP, PXE) ;
    - o On peut enregistrer aussi l'adresse Ethernet ou des informations identifiant la machine comme le nom que lui a donné son propriétaire ou même des identifiants internes ;
    - o Etc.
- la date et l'heure de la tentative ;
- le résultat de la tentative (succès ou échec) ;
- le nombre de connexions ;
- Les commandes passées.

Serveurs de messagerie

Les serveurs de messagerie enregistrent pour chaque message émis ou reçu les informations suivantes (ou une partie seulement de ces informations) :
- l'adresse de l'expéditeur et éventuellement des éléments identifiant celui qui s'est connecté au serveur lorsque est utilisée une authentification par identifiant/mot de passe ou par certificat. Par exemple pour éviter de laisser un relais ouvert à tout le monde mais faciliter la connexion des

utilisateurs distants, il arrive de n'autoriser le relais qu'aux utilisateurs dûment authentifiés par certificat ;
- l'adresse du destinataire ;
- la date et l'heure de la tentative ;
- les différentes machines (relais de messagerie) dont il est reçu des messages ou auxquelles il en est envoyé ;
- le traitement « accepté ou rejeté » du message (on peut rejeter des messages ne respectant pas les standards) ;
- le sujet du message dans le cas où il ne contiendrait pas que des caractères standards ;
- parfois la taille du message ainsi que l'en-tête "message-id" qui peut contenir, en fonction des outils utilisés, des éléments formés à partir d'adresse électronique ;
- le cas échéant le résultat du traitement antispam ou antivirus sur ce message.

Le serveur de messagerie utilisé à l'ESE est principalement celui de l'Université Paris Saclay. Le personnel CNRS peut utiliser le serveur de messagerie du CNRS. Le personnel d'AgroParisTech peut utiliser le serveur de messagerie d'AgroParisTech.

Serveurs Web

Pour chaque connexion les serveurs Web enregistrent les informations suivantes (ou une partie seulement de ces informations) :
- l'adresse IP source et destination et les différentes données d'authentification (identifiant/authentifiant ou certificat) dans le cas où il est effectué une authentification de l'utilisateur ;
- la page consultée et les informations fournies par le client (navigateur, robot, ...) comme le type de navigateur et le système d'exploitation du client ;
- les numéros des ports source et destination ainsi que le protocole ;
- le type de la requête ;
- la date et l'heure de la tentative ;
- le volume de données transférées ;
- les différents paramètres passés au « cgi-bin ».

Les serveurs web utilisés sont ceux de l'Université Paris Saclay (UPS) ou ceux du CNRS. Je ne sais pas si les serveurs web de l'UPS respectent l'intégralité de cette règle, mais les serveurs du CNRS devraient la respecter.

Les équipements d'extrémité de réseau et la surveillance des services réseau (routeurs, pare-feux, commutateur, borne d'accès, …)

Pour chaque paquet qui traverse l'équipement les informations suivantes (ou une partie seulement de ces informations) sont collectées :
- l'adresse IP source et destination ;
- les numéros de port source et destination ainsi que le protocole. Ces informations permettent de déterminer le service demandé ;
- la date et l'heure de la tentative ;
- la façon dont le paquet a été traité par l'équipement : transmis ou filtré ;
- le nombre de paquets et le nombre d'octet transférés pour chaque connexion (une connexion étant identifiée par la même adresse IP source, la même adresse IP destination, le même port source et le même port destination.).

S'ajoutent, éventuellement, à ces informations pour certains types de matériel (pare-feu, sans fil utilisant les protocoles 802.1X dont l'authentification est indispensable.) les données d'authentification (identifiant ou certificat) et parfois l'historique des commandes passées.

Système de détection d'intrusion (IDS) et de l'enregistrement des paramètres d'utilisations des services réseau.

Les IDS à détection par scénario ont pour rôle la remontée d'alerte en temps réel par la détection de signatures connues d'attaque. Les informations collectées par ces systèmes, qui peuvent être l'ensemble des trames qui circulent sur le réseau, ne sont stockées que le temps nécessaire à la remontée de l'alerte, sauf pour certaines unités de services utilisant des réseaux haut-débits sur lesquels il n'est pas possible, pour des raisons de performance, de faire fonctionner un IDS en temps réel. Dans ces cas exceptionnels, les traces peuvent être conservées le temps de les faire vérifier par un IDS hors connexion.

NOTA : Les IDS à détection par comportement ne rentrent pas dans le cadre de ce document et doivent, quant à eux, faire l'objet d'une demande spécifique à la CNIL.

Les applications spécifiques.

On entend par "applications spécifiques", toute application autre que celles mentionnées ci-dessus qui nécessite pour des raisons de comptabilité, de gestion, de sécurité ou de développement, l'enregistrement de certains paramètres de connexion et d'utilisation. Il en est ainsi, par exemple, pour les SGBD (dont la sécurité sera renforcée quand ils traitent de données nominatives), les logiciels commerciaux partagés, les autres services réseau (FTP, SSH, …), l'instrumentation scientifique (pilotage d'appareillages ou de machines.), ou encore les applications à accès restreints comme celles relatives aux activités de gestion et de direction des laboratoires, des délégations régionales ou de l'organisme.

Les informations suivantes (ou une partie seulement de ces informations) peuvent être collectées :
- le n° IP source et l'identité de l'émetteur de la requête qui peut être :
    - o dans le cas d'une authentification à l'aide d'un certificat les différents éléments de celui-ci.
    - o sinon l'identifiant/authentifiant ou/et l'adresse IP (adresse proprement dite ou nom de machine et dans un certain nombre de cas le serveur DHCP, PXE).
    - o on peut enregistrer aussi l'adresse Ethernet ou des informations identifiant la machine comme le nom que lui a donné son propriétaire ou même des identifiants internes ;
- la date et l'heure de la tentative ;
- le résultat de la tentative (succès ou échec) ;
- le volume de données transférées ;
- le nombre de connexions.

De plus, pour certaines applications, les traces peuvent comporter une fraction, ou un échantillon des données échangées :
- dans le cas où ces traces sont produites et traitées de façon systématique pour répondre à une fonction spécifiée par la maîtrise d'ouvrage (MOA) – par exemple dans le cas d'applications financières pour respecter la règlementation en la matière -, **la MOA doit s'assurer de la conformité de son SI et de la gestion des traces avec les dispositions de protection des données personnelles en vigueur.**
- dans la mise au point de logiciel ou de réglage de paramètres, il est très souvent nécessaire d'activer un « mode bavard » pour retrouver les sources de dysfonctionnements éventuels. Un maximum d'informations est alors temporairement enregistré, ces traces de mise au point qui ne doivent être conservées que le temps nécessaire à rendre l'application stable. **Les utilisateurs doivent être avertis quand ce mode d'exploitation est activé.**

Dans certains cas, la règlementation impose un archivage des traces sur une durée supérieure à 1 an. Les SI concernés font l'objet de déclarations spécifiques auprès de la CNIL.

Les traitements effectués

Les traitements réalisés ont pour objectif :
- de surveiller le bon fonctionnement des SI et en particulier leurs fonctions de sécurité ;
- de réaliser un diagnostic en cas d'incident technique ou de sécurité ;
- d'apporter des éléments de preuve en cas de dépôt de plainte.

Pour tout traitement répondant à d'autres objectifs que ceux-là, une demande d'autorisation spécifique devra être faite à la CNIL.

Les fichiers de traces contiennent un ensemble d'informations, relatives aux actions ou aux transactions accomplies, qui peuvent avoir un caractère nominatif par l'enregistrement du « login » ou de l'adresse IP d'une machine à partir desquels, par association, on peut identifier un utilisateur. Les traitements effectués sur ces informations doivent permettre d'obtenir des journaux qui répondent aux principes de base énoncés précédemment, tout en restant conformes aux obligations légales sur la protection des informations personnelles, en particulier celles concernant le respect de la vie privée et le principe d'information préalable et de transparence.

Les traitements permettent d'obtenir :
- des résultats statistiques systématiques ;
- des résultats d'analyse ;
- des résultats ciblés et nominatifs ;
- des journaux bruts.

Les administrateurs systèmes et réseau des unités du CNRS sont chargés de ces traitements sous le contrôle de la chaîne fonctionnelle SSI. Ils sont, pour cette activité, soumis au secret professionnel.

Des résultats statistiques systématiques

Ceux-ci, effectués automatiquement, permettent de contrôler les volumes d'utilisation des moyens mis à la disposition des utilisateurs en tant qu'outil de travail. Parmi ces traitements on trouvera : des traitements statistiques en anonymes en volume transféré et en nombre de connexions, des calculs de « top ten » des services les plus utilisés en volume de données et en nombre de connexion, des « top ten » des machines ayant consommé le plus de réseau en volume transféré et en nombre de connexions.

Des résultats d'analyse

La vérification visuelle des traces ou le contrôle effectué manuellement d'événements atypiques permettent de veiller à l'application des règles de sécurité.

Des résultats ciblés et nominatifs

Ceux-ci, ne peuvent être effectués qu'à la demande :
- de l'utilisateur concerné lorsqu'il a cru déceler des actions anormales sur sa machine, ses fichiers ou ses applications ;
- de la chaîne fonctionnelle SSI notamment en cas de suspicion d'incident de sécurité ;

- de l’autorité judiciaire.

La production de journaux bruts

Ceux-ci permettent de replacer une action particulière dans son contexte, à des fins d'enquête.

La production de journaux bruts sera requise dès l'apparition d'un incident. On considère comme incident tout événement ou comportement individuel non conforme aux politiques de sécurité ou aux règles d'exploitation en vigueur sur le système concerné.

Destinataires des traitements effectués :

Destinataires des traitements statistiques

Des traitements systématiques sont effectués pour la métrologie générale des systèmes sur l'ensemble des données que constituent toutes les traces. Il s'agit de traitements statistiques en volume et en nombre de connexions qui sont anonymes.

Ces traitements sont effectués de façon automatique et peuvent être diffusés sur des sites Internet accessibles à tous. Les traitements statistiques de type « top ten » par service réseau ou par machine pouvant faire apparaître des adresses IP de machine personnelle permettant de remonter au nom de la personne en possession de cette machine, sont à la seule disposition des administrateurs système et réseau.

Destinataires des analyses effectuées manuellement par les administrateurs système et réseau

La politique de sécurité, applicable à chaque moyen ou système qui génère des traces, définit des règles d'analyse systématique de ces traces afin de pouvoir détecter, dans les meilleurs délais, les incidents relatifs à la sécurité des systèmes d'information.

En cas d’incident ou de suspicion d’incident des analyses peuvent être faites sur les traces disponibles.

Ces analyses, effectuées à la demande de la chaîne fonctionnelle SSI, sont faites par les administrateurs et les résultats sont transmis en cas de suspicions légitimes au directeur de l’unité, au CERT-Renater, ainsi qu’à la chaîne fonctionnelle SSI.

Dans ce cas, l'accès aux trafics et aux traces est limité aux exploitants des systèmes en charge d'analyser l'incident ainsi qu’à la chaîne fonctionnelle SSI.

L'extraction de l'information et son utilisation sont strictement limitées à la résolution. Si l’incident n’est pas avéré, les résultats d’analyse sont immédiatement détruits.

A ce stade les informations ayant un caractère nominatif et susceptibles notamment de mettre en cause des personnes identifiées demeurent confidentielles au niveau de l’administrateur système et réseau et ne peuvent être transmises qu’à la chaine fonctionnelle SSI.

Destinataires des journaux bruts

Les journaux bruts sont remis, sur requête, à la chaîne SSI ou à l’autorité judiciaire afin de lui permettre de poursuivre une enquête.

Les accès individuels

Chaque agent peut demander à consulter les traces télématiques ou informatiques qui le concernent. Les demandes doivent être faites par écrit auprès du directeur de l'unité concernée.

La recherche est faite par l'administrateur, sur demande de sa hiérarchie, et les résultats sont transmis directement à l'utilisateur demandeur, sous la forme d'un « courrier personnel ».

Les intervenants :

Les utilisateurs

L'activité des utilisateurs génère des traces qui ne doivent pas subir des détournements de finalité. Ils ont des devoirs, dont l'essentiel est qu'ils sont responsables de l'utilisation des moyens mis à leur disposition, en temps qu'outils de travail, par le CNRS et qu'ils doivent respecter les règles d'utilisation et de sécurité définies dans la « Charte SSI ».

Les administrateurs système et réseau

Ils sont chargés de la mise en œuvre et de la surveillance générale des systèmes et du réseau et responsables du respect des règles de sécurité.

À ce titre, ils gèrent les traces et rapportent à la chaîne fonctionnelle SSI toute anomalie de fonctionnement (les utilisateurs aussi !) ou tout incident pouvant laisser supposer une intrusion ou une tentative d'intrusion sur le système ou les réseaux.

À ce titre, ils ont des droits et devoirs particuliers définis dans la « Charte SSI ».

Le responsable de l'unité et son chargé de SSI (CSSI)

Il représente l'unité du CNRS qu'il dirige. Sa responsabilité peut être engagée, dans la limite de ce qu'il peut connaître et de ce qu'il peut exiger, en cas d'incident ou d'accident impliquant l'unité dont il a la charge. Il s'assure de la diffusion de la charte d'utilisation des moyens informatiques auprès de chaque utilisateur et veille à son respect ainsi qu'à celui du règlement intérieur. **Il n'a pas à avoir accès aux traces permettant de mettre en cause une personne.**

Le RSSI de la Délégation Régionale concernée et les experts de la Coordination Régionale SSI

Ils sont les interlocuteurs au quotidien des administrateurs pour la gestion et le contrôle des systèmes et des réseaux dans le respect des règles SSI.

Ils ont accès aux rapports d'analyse des traces des moyens et des systèmes mis en œuvre sur l'établissement.

Ils ont en particulier accès aux informations nominatives et sont par conséquent soumis au secret professionnel.

En cas d'incident de sécurité nécessitant une investigation, ainsi qu'en cas d'enquêtes internes ou diligentées par les autorités compétentes ils rapportent au RSSI du CNRS tout incident pouvant laisser supposer une intrusion ou une tentative d'intrusion sur le système ou les réseaux.

L'ESE s'adresse au RSSI de la DR04 du CNRS dans le cadre de la PSSI du CNRS.

Le RSSI du CNRS

Il anime la chaîne fonctionnelle SSI du CNRS et assure le suivi des incidents de sécurité des SI au plan national.

Il assure l'interface avec le Fonctionnaire de Sécurité et de Défense (FSD) en ce qui concerne la réglementation relative à la Protection du Potentiel Scientifique et Technique (PPST) et avec la Direction des Affaires Juridiques (DAJ) pour ce qui concerne le respect de la réglementation et les procédures judiciaires.

Il a accès aux rapports d'analyse des traces des moyens et des systèmes mis en œuvre sur l'établissement. Il a en particulier accès aux informations nominatives et il est par conséquent soumis au secret professionnel.

Son adjoint, ainsi que les membres de son équipe ont accès aux informations issues des traces en tant que de besoin et sont soumis au secret professionnel.

Le Fonctionnaire Sécurité Défense du CNRS

Le FSD est destinataire des informations en tant que de besoin dans le cadre de ses fonctions.

Le Délégué à la Protection des Données Personnelles du CNRS

Le DPD est destinataire des informations en tant que de besoin dans le cadre de ses fonctions, notamment en ce qui concerne la gestion des incidents impactant des données à caractère personnel.

EXP-8 implémentation de la règle (23/01/2017)
Sensibilité : *

Exploitation des SI : ***Tout appareil ou système incluant de l'informatique doit être traité comme un SI à part entière en fonction de sa sensibilité.***

Il convient de prendre en compte tout appareil ou système incluant de l'informatique :
- systèmes d'acquisition et de contrôle des données ;
- systèmes industriels ou de pilotage d'expériences ;
- téléphonie sur IP ;
- gestion technique des bâtiments ;
- Internet des objets (IoT) ;
- SI de sûreté (contrôle des accès, vidéoprotection, détection incendie…) au sens de la PSSIE ;
- Etc.

Évaluez la sensibilité des systèmes qui sont sous votre responsabilité suivant PDI-3.
Les actifs ont été évalués et sont déclarés de sensibilité ** et ***. Peut-être ont-ils été surévalués.

Traitez les systèmes suivants les règles de la PSSI en fonction de leur sensibilité.

Prenez en compte les recommandations de l'ANSSI sur les systèmes industriels. Le CNRS a émis des recommandations nationales concernant le déploiement des SI de sûreté (disponibles auprès des RSI).

Pour les sites physiques considérés comme importants, des mesures de protection doivent être définies et appliquées en se basant sur les conclusions d'une analyse de risques. L'analyse de risques conduit à

la désignation des briques essentielles dont il faut assurer la protection contre des actes malveillants. Un système de gestion de la sécurité du SI de sûreté (s'inspirant de la norme ISO 27001) assure le maintien en condition de sécurité. L'emploi de produits labellisés, quand ils existent, est fortement recommandé.

EXP-9 implémentation de la règle (23/01/2017)
Sensibilité : *

Exploitation des SI : ***Les systèmes doivent être maintenus à jour et les correctifs de sécurité appliqués.***

Lorsqu'il n'est pas possible de maintenir à jour un système, il convient de l'isoler des autres systèmes de l'unité.
Les ordinateurs de laboratoires de Peter Streb et Gwendal Latouche, qui gardent leurs anciens systèmes d'exploitation, ne sont pas connectés au réseau filaire.

EXP-10 implémentation de la règle (23/01/2017)
Sensibilité : *

Exploitation des SI : ***Le parc logiciel de l'unité est géré et permet notamment un suivi de l'attribution des logiciels au personnel.***

Les logiciels utilisés au sein de l'unité doivent être gérés et faire l'objet d'un suivi de l'attribution lors de l'installation sur un matériel.

En règle générale, l'attribution d'un logiciel se fait au poste de travail qui fait lui-même l'objet d'une procédure de gestion de parc au sein de l'unité (cf. EXP-MAT1).

Dans le cas où le poste de travail est nominatif, affecté et n'est utilisé que par une seule personne, le lien poste de travail/utilisateur permet de retrouver le personnel utilisant le logiciel.

Cas particuliers :
- Certaines licences logicielles sont attribuées nominativement à un utilisateur par le fournisseur (ex : les licences étudiantes ESRI). Dans ce cas le suivi est directement logiciel/utilisateur.
- Les licences flottantes pour lesquels il faut d'une part gérer le nombre licences disponibles sur le serveur de licences et d'autre part avoir un suivi des installations du logiciel client sur les postes.

Selon la taille et la structure de l'unité, cette gestion peut se limiter à l'utilisation d'un simple tableur, ou bien utiliser un outil dédié lié, ou pas, à l'outil de gestion du parc matériel.

L'inventaire est tenu à disposition du RSSI. Il comprend la liste des « briques » logicielles utilisées, ainsi que leurs versions exactes. Il est constitué d'une base de données de configuration, maintenue à jour et tenue à disposition du RSSI. L'historique des attributions des biens inventoriés doit être conservé, dans le respect de la législation.
A l'ESE, actuellement seul le système IPM permet d'avoir une vue sur le parc à travers les adresses IP. Un système de Gestion de parc machines et de logiciels portés sur ces machines (GLPI) a existé mais a été abandonné. D'autre part l'inventaire des logiciels par postes ne peut pas être fait parce que le personnel refuse de se voir installer des logiciels « espions » sur leurs postes.
Se renseigner pour savoir si un outil est mis à la disposition par le DI de l'Université Paris Saclay.

EXP-CNF-3 implémentation de la règle (23/01/2017)
Sensibilité : *

Exploitation des SI : ***La configuration des matériels utilisés par le personnel doit être sécurisée suivant les recommandations nationales spécifiques à chaque type de matériel, OS, et usage.***

Les ressources informatiques concernées sont :
- les postes de travail (fixes ou mobiles) ;
- les smartphones ;
- les tablettes ;
- les serveurs gérés localement ;
- les équipements réseau et de télécommunication (dont autocommutateurs PABX/IPBX) ;
- les autres périphériques : imprimantes, fax, scanners, etc. ;
- les dispositifs de pilotage d'expériences, les appareils de mesure contenant de l'informatique (SCADA, etc.) ;
- objets communicants, internet des objets.

Les mesures à implémenter sont les suivantes :
- utilisation de versions maintenues par le constructeur ou un service tiers ;
- activation des mesures de protection offertes par le système d'exploitation ou par des outils tiers, suivant les directives nationales ;
- changement des mots de passe, codes secrets et certificats par défaut ;
- désactivation ou suppression des services inutiles ;
- désactivation ou suppression des comptes inutiles (compte invité, comptes de support éditeur par défaut...) ;
- gestion des droits d'accès selon la règle du « moindre privilège » ;
- sécurisation du processus de démarrage ;
- désactivation de l'exécution automatique lors de l'insertion d'un périphérique amovible ;
- verrouillage du poste par un écran de veille protégé par mot de passe et se déclenchant au bout d'un délai d'inactivité ;
- activer et configurer le pare-feu local des postes de travail et des serveurs ;
- interdire tout accès à Internet depuis les compte d'administration ;
- mise en place d'outils centralisés pour la gestion, la maintenance et la surveillance du parc ;
- 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.

Pour l'explicitation de cette règle, il convient de mettre en œuvre les bonnes pratiques reconnues et en particulier celles spécifiées dans la PSSIE ou dans les guides de le l'ANSSI.
- Windows et Active Directory
    - o Une politique explicite de gestion des comptes du domaine doit être documentée.
    - o 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.
    - o 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.
    - o L'appartenance aux groupes du domaine ADMINISTRATEURS DE L'ORGANISME 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.

- 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, il est nécessaire de maîtriser leur utilisation.
- Les comptes de service doivent faire l'objet d'une restriction des droits, en suivant le principe du moindre privilège.
- Il est nécessaire 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.
- Afin d'empêcher la réutilisation des empreintes d'un compte utilisateur local d'une machine à une autre, il faut soit utiliser des mots de passe différents pour les comptes locaux d'administration, soit interdire la connexion à distance via ces comptes.

• Lutte contre les codes malfaisants

- 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.
- Les événements de sécurité de l'antivirus doivent être remontés sur un serveur national pour analyse statistique et gestion des problèmes a posteriori (exemples : serveur constamment infecté, virus détecté et non éradiqué par l'antivirus, etc.).
- 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 les services centraux.

• Poste de travail

- 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.
- Les privilèges d'accès « administrateur » doivent être utilisés uniquement pour les actions d'administration le nécessitant.
- 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.
- Sauf pour des besoins spécifiques, le partage de répertoires ou de données hébergées localement sur les postes de travail n'est pas autorisé.
- 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.
- Une procédure formalisée de configuration des postes de travail est établie par chaque entité, conformément aux directives nationales existantes.

• Postes nomades

- Les accès à distance aux SI de l'entité (accès dits « nomades ») doivent être réalisés via des réseaux privés virtuels (VPN) de confiance.
- Un pare-feu local conforme aux directives nationales doit être installé sur les postes nomades.
- 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.
- 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 de l'entité.
- Des règles de configuration des interfaces de connexion sans fil (Wifi, Bluetooth, 3G…), permettant d'interdire les usages non maîtrisés et d'éviter les intrusions via ces interfaces, doivent être définies et appliquées. Les interfaces sans fil ne doivent être activées qu'en cas de besoin.

- La configuration des interfaces de connexion sans fil doit interdire les usages dangereux de ces interfaces.

- Téléphonie
  - 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.
  - 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.
- Imprimantes
  - Les imprimantes et copieurs multifonctions hébergés localement dans une entité 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.
  - Lorsqu'elle est activée, la fonction de numérisation sur les copieurs multifonctions hébergés dans une entité doit être sécurisée. Les mesures de sécurité suivantes doivent notamment être appliquées : envoi de documents uniquement à destination d'une adresse de messagerie interne à l'entité, envoi uniquement à une seule adresse de messagerie.
  - 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.
- Navigateur
  - 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.).
- Systèmes d'exploitation
  - 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.
- Logiciels
  - La mise en œuvre d'une configuration renforcée est obligatoire sur les logiciels déployés pour le tiers présentation (ex : serveur Web, Reverse Proxy).
  - 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).
  - Les échanges de fichiers entre applications doivent privilégier les protocoles sécurisés (SSL/TLS, FTPS...).
- Correctifs de sécurité
  - Le maintien dans le temps du niveau de sécurité d'un système d'information 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.
  - 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.

- 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.

- Général
  - Une solution de chiffrement labellisée doit être mise à disposition des utilisateurs et des administrateurs afin de chiffrer les données sensibles pour les stocker sur les postes de travail, les serveurs, les espaces de travail, ou les supports amovibles.
  - 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.

Cette règle va être déclinée pour les 3 types de systèmes : Linux, Mac et Windows.

EXP-CNF-3 poste de travail Linux (23/01/2017)
Sensibilité : *

Exploitation des SI : ***La configuration logicielle des matériels utilisés par le personnel doit être sécurisée suivant les recommandations nationales spécifiques à chaque type de matériel, OS, et usage.***

Utilisation de versions maintenues par le constructeur ou un service tiers

Ne pas utiliser d'anciennes versions de Linux qui ne sont plus maintenues. Attention pour certaines distribution (Fedora, Ubuntu non LTS, etc.) les versions ont une durée de support courte, ce qui exige de régulièrement effectuer des mises à niveau (quasiment une réinstallation).

Activation des mesures de protection offertes par le système d'exploitation ou par des outils tiers, suivant les directives nationales

Installer et configurer de manière restrictive un pare-feu local (iptables par exemple). La plupart des distributions ont un outil qui permet de le faire simplement lors de l'installation du système.

Les échanges de fichiers entre applications doivent privilégier les protocoles sécurisés (SSL/TLS, FTPS...).

Changement des mots de passe / codes secrets par défaut

En principe aujourd'hui plus aucune distribution ne contient des mots de passe par défaut. Penser à modifier les mots de passe et secrets (notamment les clés SSH) lorsque l'on clone des machines (physiques ou virtuelles).

Désactivation ou suppression des services inutiles

Lors de l'installation d'une distribution, ne sélectionner que les outils nécessaires. En particulier ne pas installer ceux qui sont spécifiques aux serveurs (pour ce qui concerne les postes de travail, objets de cette règle).

Désactivation ou suppression des comptes inutiles (compte invité, comptes de support éditeur par défaut...)

Les distributions récentes n'installent pas, en principe, de compte permettant de se connecter avec un mot de passe. Les différents comptes sont désactivés (pas de shell ou mot de passe verrouillé dans /etc/shadow). Il faut s'assurer dans les fichiers /etc/passwd et /etc/shadow que les comptes ne correspondant pas à des utilisateurs (personnes physiques) ne permettent pas d'ouvrir une session.

Gestion des droits d'accès selon la règle du « moindre privilège »

Ne jamais se connecter sur le compte « root ». Utiliser « sudo » pour élever les privilèges lorsque cela est nécessaire.

Sécurisation du processus de démarrage

Utiliser un mécanisme de boot sécurisé qui vérifie la chaîne de démarrage et interdise l'utilisation d'un autre système (TPM).

Mettre un mot de passe pour protéger la configuration du BIOS. Même si elle peut être contournée, cette mesure reste utile.

Chiffrer l'intégralité du disque (DM-CRYPT + LUKS)
Remarque personnelle : Je me demande si cette mesure, dans un contexte de confidentialité moyen, ne met pas au contraire le danger dans l'exploitation (perte de temps pour l'application du chiffrage suivant une technique à apprendre, perte totale des données dans le cas d'une perte de mot de passe, …)

Désactivation de l'exécution automatique lors de l'insertion d'un périphérique amovible

Monter les périphériques amovibles avec l'option « noexec » ce qui interdira l'exécution de tout programme à partir du périphérique monté.

Verrouillage du poste par un écran de veille protégé par mot de passe et se déclenchant au bout d'un délai d'inactivité

Lorsque le disque est chiffré (ce qui devrait être le cas de tous les portables), configurer la veille de telle sorte qu'après un certain délai d'inactivité, le système bascule dans un mode qui impose la saisie du mot de passe du disque au réveil.

EXP-CNF-3 poste de travail MacIntosh (23/01/2017)
Sensibilité : *

Exploitation des SI : ***La configuration logicielle des matériels utilisés par le personnel doit être sécurisée suivant les recommandations nationales spécifiques à chaque type de matériel, OS, et usage.***

Utilisation de versions maintenues par le constructeur ou un service tiers

Toujours faire les mises à jour vers la dernière version mineure de Mac OS X disponible (ex. Si on a installé la 10.6, faire la mise à jour vers la dernière 10.6.x). Pour cela, il suffit de cliquer sur le menu Pomme > Mise à jour de logiciels.

Dans Préférences Système > Mise à jour de logiciels, cocher « Rechercher automatiquement les mises à jour » et « Télécharger automatiquement les mises à jour ».

Activation des mesures de protection offertes par le système d'exploitation ou par des outils tiers, suivant les directives nationales

Mac OS X est livré par défaut avec un pare-feu intégré depuis la version 10.5, mais sur certaines versions de Mac OS X il est désactivé par défaut. Pour l'activer, aller dans Préférences Système > Coupe-feu > et cliquer sur le bouton « Démarrer ».

Recommandations du constructeur ou de l'éditeur du logiciel en matière de sécurité

Consulter les Mac OS X Security Configuration Guides qui correspondent à votre version de Mac OS X.

Changement des mots de passe / codes secrets par défaut

Mac OS X ne semble pas en utiliser.

Attention aux accessoires Bluetooth (souris, trackpad, clavier), qui ont souvent « 0000 » comme code par défaut, mais je ne sais pas si on peut changer les codes des accessoires Bluetooth ?

Désactivation ou suppression des services inutiles

N'activez que les services de partage dont vous avez réellement besoin (Préférences Système > Partage).

Si vous n'en avez pas l'utilité, désactivez le Bluetooth, ou au moins rendez-le non détectable (Préférences Système > Bluetooth).

Même chose pour la télécommande infrarouge (Préférences Système > Sécurité > Général).

Dans Préférences Système > Economiseur d'énergie, décocher « Réactiver l'ordinateur lors d'un accès réseau Ethernet » (sauf si vous en avez l'utilité, c.a.d. uniquement sur un serveur en principe).

Dans Préférences Système > Imprimantes et Fax, décocher « Partager cette imprimante sur le réseau » pour toutes les imprimantes installées sur la machine.

Désactivation ou suppression des comptes inutiles (compte invité, comptes de support éditeur par défaut...)

Désactiver le compte d'invité dans Préférences Système > Comptes (ou Utilisateurs et Groupe, suivant la version de Mac OS X). Dans cette même boîte de dialogue, désactiver également l'ouverture de session automatique au démarrage en cliquant sur « Options ». On peut également la désactiver définitivement (c.a.d. empêcher les utilisateurs de la machine de la réactiver ultérieurement) en allant dans Préférences Système > Sécurité > Général > Désactiver l'ouverture de session automatique.

Par défaut le compte root est désactivé sous Mac OS X. Pour vérifier que c'est bien le cas :

- sous Mac OS X 10.6 ou ultérieur, lancez l'utilitaire d'annuaire. Il se trouve dans /Système/Bibliothèque/CoreServices/ mais on peut également l'ouvrir en allant dans Préférences Système > Comptes (ou Utilisateurs et Groupe, suivant la version de Mac OS X) > bouton « Joindre » ou « Modifier » (en bas à droite) puis « Ouvrir l'utilitaire d'annuaire ». Dans l'utilitaire d'annuaire, cliquer sur le petit cadenas pour le déverrouiller, puis aller dans le menu Edition > Désactiver l'utilisateur root. Ne pas oublier de re-verrouiller le cadenas avant de refermer l'utilitaire d'annuaire.

Le 05/04/24, la version est 14.4.1, bien au-delà de la 10.6.

Gestion des droits d'accès selon la règle du « moindre privilège »

Préférences Système > Sécurité > Général : cocher « Mot de passe requis pour déverrouiller chaque sous-fenêtre des Préférences Système ».

Préférences Système > Comptes (ou Utilisateurs et Groupe, suivant la version de Mac OS X) : pour chaque utilisateur standard de la machine, ne pas donner les droits d'administration sur la machine (c.a.d décocher la case « Autorisation à administrer cet ordinateur » pour chacun des comptes de la machine, sauf pour le compte « administrateur » utilisé par le service informatique)

Sécurisation du processus de démarrage

[portable] Chiffrer l'intégralité du disque => depuis Mac OS X 10.7, il est possible de chiffrer l'intégralité du disque dur via une fonctionnalité standard de Mac OS X (FileVault).

Penser également à crypter le fichier de swap (Préférences Système > Sécurité > Général > Utiliser la mémoire virtuelle sécurisée).

Désactivation de l'exécution automatique lors de l'insertion d'un périphérique amovible

L'exécution automatique lors de l'insertion d'un périphérique amovible n'est plus disponible dans Mac OS X (cette fonctionnalité existait à l'époque de Mac OS 9 mais elle a été retirée dans Mac OS X, pour des raisons de sécurité justement), il n'y a donc rien à faire à ce niveau-là.

Verrouillage du poste par un écran de veille protégé par mot de passe et se déclenchant au bout d'un délai d'inactivité

Aller dans Préférences Système > Sécurité > Général :
- Exiger le mot de passe […] (délai à paramétrer) après la suspension d'activité ou le lancement de l'économiseur d'écran.
- Pour plus de sécurité, on peut également cocher Déconnexion automatique après […] minutes d'inactivité.

Dans Préférences Système > Economiseur d'énergie, mettre l'écran en veille après un délai raisonnable.

EXP-CNF-3 poste de travail Windows (23/01/2017)
Sensibilité : *

Exploitation des SI : ***La configuration logicielle des matériels utilisés par le personnel doit être sécurisée suivant les recommandations nationales spécifiques à chaque type de matériel, OS, et usage.***

Utilisation de versions maintenues par le constructeur ou un service tiers

Ne pas utiliser d'anciennes versions de Windows qui ne sont plus maintenues (plus aucun correctif de sécurité n'est diffusé).

Activer « Windows Update » afin que les mises à jour s'effectuent automatiquement à partir d'un serveur de Microsoft ou bien d'un serveur local WSUS. La fréquence des mises à jour doit être quotidienne. Dans la mesure du possible, utiliser des GPO (Group Policy Object) pour diffuser la configuration et les mises à jour.

Pour les produits tiers (Adobe, Java, Firefox, etc.), configurer les applications afin qu'elles se mettent à jour automatiquement sur le site du fournisseur. Dans la mesure du possible utiliser des GPO ou un outil de gestion de parc pour s'assurer que les mises à jour sont bien effectuées ou appliquer directement les mises à jour.

Activation des mesures de protection offertes par le système d'exploitation ou par des outils tiers, suivant les directives nationales

Installer l'antivirus et le configurer pour que les signatures soient maintenues à jour régulièrement (au moins une fois par jour).

*** Gérer l'antivirus à partir d'une console d'administration pour la distribution des mises à jour et la remontée des alertes. Analyser et traiter tous les incidents

A l'ESE, il n'y a pas d'Antivirus géré de façon centralisée. Sur Windows, seul l'Antivirus Windows Defender est utilisé depuis 2 ans. Ceci oblige à surveiller les mises à jour.
Sinon, l'UPS propose TREND MICRO (pour Mac et pour Windows), et une version Serveur. C'est le seul Antivirus proposé par l'UPS aujourd'hui (il y en avait d'autres autrefois, Kasperski et Symantec). J'ai demandé la version Serveur le 05/04/24. Peut-être par ce moyen, pourra-t-on surveiller l'état des AV sur le parc …

Changement des mots de passe / codes secrets par défaut

Windows ne semble pas en utiliser.

Désactivation ou suppression des services inutiles

Ne pas installer ou activer de nouveaux services en plus de ceux qui viennent avec l'installation standard du système à moins d'en avoir un réel besoin.

En particulier, on s'attachera à empêcher l'exécution de OneDrive.
Il faut désinstaller Microsoft OneDrive des applications.

*** Établir une politique de sécurité qui spécifie les services à activer, construire un modèle de système à installer et l'utiliser sur toutes les machines. Diffuser la politique sur toutes les machines (GPO).

Désactivation ou suppression des comptes inutiles (compte invité, comptes de support éditeur par défaut...)

Désactiver (Windows Vista et ultérieurs) ou supprimer (Windows XP et antérieurs), s'il existe, le compte invité (sauf pour les machines spécifiquement dédiées à cet usage).

Mais les machines Windows autres que Windows 10 et Windows 11 ne doivent pas être sur le réseau.

Gestion des droits d'accès selon la règle du « moindre privilège »

Les comptes des utilisateurs ne doivent pas avoir le privilège « administrateur ». Réserver l'usage d'un compte « administrateur » uniquement aux opérations qui l'exigent.

Pour les opérations d'administration, ouvrir une session utilisateur normale et utiliser le mécanisme de l'UAC pour élever les privilèges uniquement pour les opérations le nécessitant.

Sécurisation du processus de démarrage

*** Utiliser un mécanisme de boot sécurisé qui vérifie la chaîne de démarrage et interdise l'utilisation d'un autre système (TPM).

*** Mettre un mot de passe pour protéger la configuration du BIOS. Même si elle peut être contournée, cette mesure reste utile.

Chiffrer l'intégralité du disque.

Désactivation de l'exécution automatique lors de l'insertion d'un périphérique amovible

Ne pas activer l'exécution automatique (autorun, autoplay).

Verrouillage du poste par un écran de veille protégé par mot de passe et se déclenchant au bout d'un délai d'inactivité

Paramétrer le système afin qu'après un temps d'inactivité de la machine, un écran de veille s'affiche et qu'il soit nécessaire de fournir le mot de passe pour sortir de cet état.

*** Diffuser cette politique (GPO).

Sur les portables, activer la mise en veille automatique après une période d'inactivité. En fonction de l'outil de chiffrement utilisé (tous les portables doivent être chiffrés), il peut être nécessaire de désactiver le mode veille normale pour n'autoriser que veille prolongée (hibernation) afin que le mot de passe protégeant le disque soit bien demandé à la sortie de la veille.

Paramétrage de confidentialité de Windows 10

Voir à ce sujet : https://www.ssi.gouv.fr/guide/restreindre-la-collecte-de-donnees-sous-windows-10

A l'installation d'un ordinateur Windows, je ne choisis que le minimum d'informations à transmettre (carré bleu inférieur).

EXP-CNF-3 serveur Linux (23/01/2017)
Sensibilité : *

Exploitation des SI : ***La configuration logicielle des matériels utilisés par le personnel doit être sécurisée suivant les recommandations nationales spécifiques à chaque type de matériel, OS, et usage.***

Aujourd'hui à l'ESE, les serveurs (Linux) ne peuvent être installés que dans la DMZ (Demilitarized Zone) de la salle serveur dans le local technique du Rez-de-Chaussée. Ils ne peuvent pas être installés, ni dans les bureaux ni dans les laboratoires.

Utilisation de versions maintenues par le constructeur ou un service tiers

Ne pas utiliser d'anciennes versions de Linux qui ne sont plus maintenues. Attention pour certaines distributions (Fedora, Ubuntu non LTS, etc.) les versions ont une durée de support courte, ce qui exige de régulièrement effectuer des mises à niveau (quasiment une réinstallation).

Activation des mesures de protection offertes par le système d'exploitation ou par des outils tiers, suivant les directives nationales

Installer et configurer de manière restrictive un pare-feu. La plupart des distributions ont un outil qui permet de le faire simplement lors de l'installation du système.

Changement des mots de passe / codes secrets par défaut

En principe aujourd'hui plus aucune distribution ne contient des mots de passe par défaut.

Penser à modifier les mots de passe et secrets (notamment les clés SSH) lorsque l'on clone des machines (physiques ou virtuelles).

Désactivation ou suppression des services inutiles

Désactivation ou suppression des comptes inutiles (compte invité, comptes de support éditeur par défaut...)

Gestion des droits d'accès selon la règle du « moindre privilège »

Ne jamais se connecter sur le compte « root ».

Utiliser « sudo » pour élever les privilèges lorsque cela est nécessaire.

Sécurisation du processus de démarrage

Désactivation de l'exécution automatique lors de l'insertion d'un périphérique amovible

Ne pas monter de périphérique amovible sur un serveur. Si toutefois il était nécessaire de monter un périphérique amovible, le faire avec l'option « noexec », ce qui interdira l'exécution de tout programme à partir du périphérique monté.

Verrouillage du poste par un écran de veille protégé par mot de passe et se déclenchant au bout d'un délai d'inactivité

Ne s'applique que dans le cas où une interface graphique est ouverte sur le serveur.

EXP-CNF-3 serveur windows (23/01/2017)
Sensibilité : *

Exploitation des SI : ***La configuration logicielle des matériels utilisés par le personnel doit être sécurisée suivant les recommandations nationales spécifiques à chaque type de matériel, OS, et usage.***

Sauf erreur de ma part, il n'y a pas des serveurs Windows à l'ESE.

Utilisation de versions maintenues par le constructeur ou un service tiers

Ne pas utiliser d'anciennes versions de Windows qui ne sont plus maintenues (plus aucun correctif de sécurité n'est diffusé).

Activer « Windows Update » afin que les mises à jour s'effectuent automatiquement à partir d'un serveur de Microsoft ou bien d'un serveur local WSUS. La fréquence des mises à jour doit être quotidienne. Dans la mesure du possible utiliser des GPO pour diffuser la configuration et les mises à jour.

Pour les produits tiers (Adobe, Java, Firefox, etc.) configurer les applications afin qu'elles se mettent à jour automatiquement sur le site du fournisseur (cela peut exiger de fournir à l'utilisateur un mot de passe d'un autre compte ayant les privilèges de l'administrateur pour permettre l'installation). Dans la mesure du possible utiliser des GPO pour s'assurer que les mises à jour sont bien effectuées ou diffuser directement les mises à jour.

Activation des mesures de protection offertes par le système d'exploitation ou par des outils tiers, suivant les directives nationales

Installer l'antivirus et le configurer pour que les signatures soient maintenues à jour régulièrement (au moins une fois par jour).

Analyser et traiter tous les incidents.

Changement des mots de passe / codes secrets par défaut

Désactivation ou suppression des services inutiles

Lors de la procédure d'installation n'installer et activer que les services réellement nécessaires.

Désactivation ou suppression des comptes inutiles (compte invité, comptes de support éditeur par défaut...)

Gestion des droits d'accès selon la règle du « moindre privilège »

Pour les opérations d'administration ouvrir une session utilisateur normale et utiliser le mécanisme de l'UAC pour élever les privilèges uniquement pour les opérations le nécessitant.

Sécurisation du processus de démarrage

Désactivation de l'exécution automatique lors de l'insertion d'un périphérique amovible

Verrouillage du poste par un écran de veille protégé par mot de passe et se déclenchant au bout d'un certain délai d'inactivité.

EXP-CNF-3 smartphone (23/01/2017)
Sensibilité : *

Exploitation des SI : ***La configuration logicielle des matériels utilisés par le personnel doit être sécurisée suivant les recommandations nationales spécifiques à chaque type de matériel, OS, et usage.***

Utilisation de versions maintenues par le constructeur ou un service tiers

L'utilisation de versions non maintenues des systèmes mobiles (iOS, Android) est à proscrire. On s'assure que les mises à jour fournies par les éditeurs, les constructeurs sont correctement et régulièrement appliquées.

Activation des mesures de protection offertes par le système d'exploitation ou par des outils tiers, suivant les directives nationales

- Chiffrement : Il est activé sur le stockage interne du smartphone et sur tout périphérique de stockage (carte SD…) qui y est inséré. Il s'agit du chiffrement intégré au système d'exploitation, on n'utilisera pas de solution de chiffrement applicative non validée par le RSSI.

- Protection contre les logiciels malveillants : l'utilisation d'une solution antivirale gratuite d'un éditeur reconnu (Symantec, Avast, Eset) est une excellente pratique. Ce logiciel vérifie en tâche de fond et de manière planifiée la présence de logiciels malveillants sur le smartphone.
La solution russe Kaspersky doit être rejetée.

- Configuration durcie : le smartphone est configuré selon le principe de la moindre surface d'attaque. Tout élément logiciel qui n'est pas strictement utile est désactivé par l'utilisateur.

- Vigilance sur les systèmes de synchronisation embarqués : la majorité des systèmes d'exploitation mobiles proposent des solutions embarquées de synchronisation de données vers le Cloud (iCloud, OneDrive, Samsung Cloud etc…). Conformément aux règles PDI-1 et PDI-2, ces systèmes présente des niveaux de confiance insuffisants pour les besoins du CNRS et ne doivent pas être activés. La synchronisation de données est préférentiellement réalisée par des solutions validées par le CNRS (exemple : MyCore/OwnCloud du CNRS).

- Utilisation d'authentifiants robustes

Les smartphones proposent souvent plusieurs moyens pour restreindre l'accès au terminal. On utilisera a minima dans tous les cas et quelles que soient les solutions techniques supplémentaires proposées :
- Un code PIN non trivial pour verrouiller l'accès à la carte SIM
- Un code personnel numérique suffisamment robuste (minimum 6 chiffres) pour restreindre l'accès au système

L'usage d'une empreinte digitale est toléré en complément des moyens décrits supra. Elle ne doit pas être utilisée seule.

Tout autre moyen d'authentification biométrique (reconnaissance faciale, reconnaissance de l'iris, de la voix…) ou comportemental (schémas à tracer…) est à proscrire car non fiable.

Désactivation ou suppression des services inutiles

Ne conserver les interfaces de communication actives que si elles sont nécessaires et utilisées (WLAN mode point d'accès ou client, Bluetooth, NFC, GSM 3G/4G/5G…).

EXP-4 implémentation de la règle (23/01/2017)
Sensibilité : *

Exploitation des SI : ***La prise de main à distance sur le poste de travail d'un utilisateur ne doit se faire que suivant une procédure sécurisée en suivant les directives nationales.***

La prise de main à distance sur le poste de travail d'un utilisateur ne peut être réalisée que dans les conditions suivantes :
1) L'intervenant doit être clairement identifié et habilité par l'unité à administrer les postes de travail

2) La présence de l'utilisateur habituel ou du propriétaire du poste de travail est obligatoire
3) L'outil de prise de main à distance utilisé doit lui-même répondre à plusieurs critères :
    a. Outil sûr et référencé par l'ANSSI et/ou le CNRS en connexion point à point sans utilisation de solution type "cloud", sauf si celle-ci est interne à l'unité ou au CNRS et complétement maitrisée.
    NOTA : les outils non maitrisés (en particulier les outils tiers utilisant des services hébergés sur Internet en mode SaaS) sont proscrits pour la prise de main à distance.
    b. Avoir un mécanisme qui oblige une acceptation préalable, par l'utilisateur du poste, à la prise de main par l'intervenant.
    c. Visibilité totale par l'utilisateur des actions réalisées par l'intervenant
    d. Possibilité pour l'utilisateur de forcer la déconnexion de l'intervenant à tout moment

Cas particulier d'intervention sur des postes situées en ZRR

Dans le cas où un poste de travail situé en ZRR nécessite une intervention avec prise de main à distance, il faut s'assurer que le personnel intervenant réponde aux critères de conditions d'accès à la ZRR concernée.

A l'ESE, il n'y a pas de ZRR.

Authentification et contrôle d'accès :

AUT-1 implémentation de la règle (23/01/2017)

Sensibilité : *

Authentification et contrôle d'accès : ***Seuls les comptes individuels (non partagés) sont autorisés pour l'identification préalable à l'accès aux ressources informatiques (postes de travail, systèmes d'information, etc.).***

Les utilisateurs disposent de comptes individuels, liés à leur identité et non partagés. Les secrets d'authentification (mots de passes ou clés) ne doivent jamais être transmis à des tiers.

Cette disposition est nécessaire notamment pour permettre :
- une bonne gestion des droits d'accès aux informations (le bon utilisateur a accès aux informations auxquelles il a droit) ;
- une traçabilité correcte des accès aux informations (ces traces sont utilisées en cas d'audit ou d'incident de sécurité).

Cette disposition s'applique aussi aux administrateurs. Chaque administrateur doit disposer d'un mot de passe propre et destiné à l'administration.

Les utilisateurs disposent de comptes individuels, liés à leur identité et non partagés. Les secrets d'authentification (mots de passes ou clés) ne doivent jamais être transmis à des tiers.

AUT-2 implémentation de la règle (23/01/2017)

Sensibilité : *

Authentification et contrôle d'accès : ***Toute action d'autorisation d'accès d'un utilisateur à une ressource des 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'entrée et de sortie du personnel.***

Le processus traite les entrées et sorties des personnels : attribution des droits lors de l'affectation sur le poste, fermeture des droits lors du départ.

Un processus de demande est défini et adapté à chaque profil de poste pour la validation d'accès aux ressources :
- le processus de demande doit être formalisé sous la responsabilité du DU avec les acteurs concernés ;
- un processus de retrait des droits d'accès est défini selon les profils ;
- le processus doit permettre de tracer les ouvertures et fermetures des droits d'accès.

Le DU dispose de la liste des utilisateurs ayants des droits très étendus sur les SI :
- des utilisateurs qui disposent d'un compte administrateur (doit être exceptionnel et dûment motivé);
- des utilisateurs qui disposent des droits suffisants pour accéder aux espaces de travail (répertoires partagés, espaces collaboratifs partagés, etc.) ;
- des principaux chercheurs et/ou de l'encadrement de l'unité ;
- de l'ensemble des utilisateurs.

Pour les accès de visiteurs ou les accès à distance de collaborateurs externes, qui n'effectuent pas le processus d'entrée/sortie classique, il est également nécessaire de définir un processus d'autorisation formalisé permettant de tracer les ouvertures et fermetures des droits d'accès.

NOTA : lors d'un changement de fonction d'un utilisateur, ses autorisations d'accès doivent être modifiées conformément à ses nouvelles fonctions, il y a fermeture des droits liés à l'ancien poste et ouverture des droits liés au nouveau poste.

Les applications manipulant des données sensibles doivent permettre une gestion fine par profils d'accès. Les principes du besoin d'en connaître et du moindre privilège s'appliquent.

AUT-4 implémentation de la règle (23/01/2017)
Sensibilité : *

Authentification et contrôle d'accès : ***La gestion des moyens d'authentification des utilisateurs sur les SI doit se faire suivant les recommandations nationales.***

Les connexions aux différentes ressources du système d'information nécessitent une authentification. Celle-ci peut prendre différentes formes. On peut citer les mots de passe « classiques » mais également un ensemble de clefs privées liées aux clefs publiques utilisées (clef privée d'un certificat, clef privé SSH, …). Il existe aussi d'autres méthodes d'identification, telles des éléments biométriques (empreintes digitales p.ex.) ou physiques (cartes à puce p.ex.).

Ces éléments d'authentification sont extrêmement sensibles car ils fournissent un accès authentifié à certaines ressources protégées (sinon, celles-ci seraient publiques et ne nécessiteraient aucune authentification).

On peut différencier les mots de passe « classiques », choisis en général par l'utilisateur et les « clefs » qui sont des fichiers générés par le système.

Les mots de passe classiques sont une suite plus ou moins longue (la longueur est essentielle pour empêcher le craquage par une méthode de force brute, essayant toutes les combinaisons possibles) de caractères (au sens large, incluant les minuscules, majuscules, les chiffres et des caractères spéciaux).

On peut ajouter à cette liste des secrets du système d'exploitation, par exemple le mot de passe de chiffrement des disques des ordinateurs portables, ainsi que les mots de passe techniques qui servent à l'administration des machines (les mots de passe root ou administrateur), éventuellement utilisés par plusieurs personnes. Le séquestre de ces mots de passe est essentiel pour assurer une continuité de service.

Les clefs sont des fichiers générés par le système, fichiers qu'il convient de protéger et de rendre non publics. On peut distinguer plusieurs types de clefs :
1. Les clefs privées d'authentification (clefs SSH ou de certificat) sont conservées par l'utilisateur. L'administrateur n'en a nul besoin et le séquestre n'est pas nécessaire. En cas de compromission, l'utilisateur change ses clefs (révocation du certificat).
2. Les clefs de signature sont également à charge de l'utilisateur. Vu qu'elles sont destinées à signer un document, le séquestre par l'administrateur est interdit.
3. Les clefs de chiffrement sont par contre à conserver par l'administrateur, puisqu'elles seules permettraient de récupérer les données qui sont stockées dans le conteneur (disque) chiffré.

Dans les deux cas, la non-divulgation et le non-accès à ces secrets sont essentiels. Il est donc indispensable que chaque utilisateur qui les possède en soit pleinement conscient. Il est également indispensable que le séquestre éventuel soit protégé.

Quelques règles à appliquer :
1. Le mot de passe initial ou les fichiers « clefs » initiaux doivent être transmis de manière sûre, en évitant par exemple une transmission en texte clair dans un message électronique.
2. Lorsque les utilisateurs doivent changer leur mot de passe, il convient que le mot de passe initial soit temporaire et suffisamment sécurisé (difficile à deviner) et que les utilisateurs soient forcés de le changer à la première connexion.
3. Les utilisateurs sont responsables de leurs secrets. Ils ne doivent en aucun cas le communiquer ou le mettre à disposition de qui que ce soit. Ils ne doivent pas les écrire en clair sur quelque support que ce soit (papier, disque d'ordinateur, message électronique...). Les mots de passe ne doivent pas transiter en clair sur les réseaux. Ils peuvent éventuellement être stockés dans un « coffre-fort » électronique comme par exemple une zone chiffrée. Les séquestres qui sont conservés sous format papier doivent être stockés dans un coffre-fort. Sous format électronique, il faut les stocker de manière sûre, par exemple dans une zone chiffrée. On conseille l'utilisation de KeePass.
4. Il convient de mettre en œuvre les recommandations de l'ANSSI.
5. Il convient de vérifier la robustesse des mots de passe lors de leur changement ou par contrôle périodique.
6. Lorsqu'un mot de passe sert à protéger une ressource chiffrée et qu'il n'existe aucun autre moyen de recouvrement, il est nécessaire de séquestrer ce mot de passe.
7. Les authentifiants permettant l'administration des ressources des SI doivent être placés sous séquestre et tenus à jour, dans un coffre ou une armoire fermée à clé. L'authentifié doit être informé de l'existence de ces opérations de gestion, de leurs finalités et limites. Tout accès d'administration à une ressource informatique doit pouvoir être tracé et permettre de remonter à la personne exerçant 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.
8. L'accès à toute ressource non publique doit nécessiter une identification et une authentification 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.
9. Les informations d'authentification (mots de passe d'accès aux SI, clés privées liées aux certificats électroniques, etc.) doivent être considérées comme des données sensibles.

Lorsque la réglementation l'exige, on utilise des certificats conformes au RGS et au règlement européen eIDAS.

AUT-5 implémentation de la règle (23/01/2017)

Sensibilité : *

Authentification et contrôle d'accès : ***Si exceptionnellement un administrateur est amené à s'authentifier au nom d'un utilisateur, celui-ci doit en être informé et y consentir, la procédure utilisée doit être sécurisée.***

Bien que cela soit proscrit, il est des situations exceptionnelles où pour résoudre des problèmes on ne peut éviter qu'un administrateur soit amené à effectuer des actions au nom d'un utilisateur et en empruntant son authentification. Dans ce cas l'utilisateur doit en être informé et donner son consentement.

La procédure utilisée pour échanger les secrets d'authentification doit être sécurisée. Une bonne méthode consiste pour l'utilisateur à changer son mot de passe avant de le fournir à l'administrateur. Une fois les actions effectuées, l'utilisateur établira un nouveau mot de passe.

Les systèmes, les applications doivent être conçues pour éviter de se retrouver avec une telle nécessité.

Développement des SI :

Une seule règle de sensibilité **.

Gestion des incidents :

INC-1 implémentation de la règle (23/01/2017)
Sensibilité : *

Gestion des incidents : ***Tout incident de sécurité doit être géré suivant la procédure formalisée par le RSSI du CNRS (qualification, protection, alerte, etc.).***

Il y a incident lié à la sécurité de l'information lorsque : surviennent un ou plusieurs événements indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information.

L'occurrence d'un événement lié à la sécurité de l'information ne signifie pas nécessairement que la tentative a réussi et qu'il y a eu atteinte à la confidentialité, l'intégrité ou la disponibilité. Tous les évènements ne sont donc pas classifiés comme incidents.

L'unité doit être organisée de façon à être prête à répondre aux événements et incidents :
- au minimum, identification des personnels habilités à gérer les incidents ;
- jusqu'à la formalisation des procédures liées à l'activation d'une cellule de crise (pour les sites particulièrement sensibles).

Lorsqu'un évènement anormal survient, l'utilisateur ou l'ASR qui le détecte doit le signaler au CSSI qui pourra qualifier cet évènement, éventuellement en faisant appel à un membre de la CRSSI de la DR dont dépend l'unité.

L'attention des utilisateurs doit être attirée sur l'importance de signaler tout événement et a fortiori incident de sécurité.

La perte ou le vol d'une ressource d'un système d'information est un incident et doit être déclaré en tant que tel.

Lorsque le CSSI a qualifié un évènement anormal en incident de sécurité, il le déclare au RSSI de la DR dont dépend l'unité. Lorsque le RSSI de DR a connaissance d'un incident il l'enregistre et, en fonction de sa gravité, le signale au RSSI du CNRS et autres entités concernées.

L'incident doit être traité de façon à stopper et contenir le problème.

Le RSSI du CNRS rapporte les incidents significatifs aux instances nationales : HFDS, FSSI, ANSSI, CERT.

NOTA : Ne jamais traiter une compromission de machine sans tenter de savoir quel a été le scénario d'incident et sans vérifier qu'il n'y a pas eu propagation à d'autres machines.

Incident impactant des données à caractère personnel

La procédure de traitement des incidents impactant des données à caractère personnel n'est pas fondamentalement différente de celle décrite ci-dessus.

Il faut cependant noter que :
- il est fondamental d'évaluer :
    - La portée de l'incident : quel est le nombre de personnes physiques concernées par la violation de données ? quelle est la « quantité » de données qui ont été exfiltrées, modifiées ou supprimées ?

- L'impact sur la vie privée des personnes concernées : la divulgation de certaines données, en fonction de leur sensibilité, fait varier cet impact. Par exemple, la divulgation conjointe d'un nom, prénom, date et ville de naissance augmente la facilité d'une usurpation d'identité.

- selon la portée et l'impact sur la vie privée des personnes concernées, il peut être imposé au CNRS d'informer l'autorité de contrôle et/ou ces personnes de la violation de données dans un délai contraint (72 heures). Il est donc nécessaire que le traitement de l'incident soit réalisé dans un délai court (idéalement 48 heures) afin de laisser le temps nécessaire à la formalisation de cette communication par les services compétents (DPD, DAJ).

Lorsqu'un incident concerne une divulgation, une compromission de données à caractère personnel, il est notifié au Délégué à la Protection des Données désigné comme compétent pour l'unité.

Continuité d'activité :

CNT-1 implémentation de la règle (23/01/2017)
Sensibilité : *

Continuité d'activité : ***Un plan de sauvegarde informatique de l'unité doit être formalisé et mis en œuvre de façon à garantir la récupération des données en cas de sinistre ou de panne matérielle et/ou logicielle sur les matériels gérés par l'unité.***

Les sauvegardes sont nécessaires pour récupérer l'information suite à un sinistre de nature accidentelle, mais aussi à une action délibérée d'un attaquant (effacement de fichiers, chiffrement par un rançongiciel).

Le plan de sauvegarde intègre les types de données suivants :
- Données utilisateur : données utilisateur stockées sur un serveur de fichier. Ces données ne sont pas les données stockées sur le poste de travail de l'utilisateur.
- Données applicatives : données utilisées par les applications métiers. Ces données sont généralement modifiées en permanence par les utilisateurs ou des processus applicatifs automatisés.
- Bases de données : les bases de données contiennent une grande quantité d'informations nécessaires aux applications. Ces données métiers sont constamment modifiées par les utilisateurs ou les applicatifs. Les bases de données nécessitent généralement des procédures de sauvegarde spécifiques.
- Courrier électronique : Courriers électroniques, agendas, contacts, et autres fonctionnalités de messagerie offerte aux utilisateurs.
- Applications et systèmes : données opérationnelles et environnementales avec leurs configurations respectives. Pour chaque donnée ou ensemble de données, les besoins de sauvegarde sont établis en considérant :
    - les obligations légales, réglementaires ou contractuelles en matière de sauvegarde ou d'archivage ;
    - le temps maximal d'indisponibilité admissible, qui détermine la durée maximale pour la restauration des données et du service à partir d'une sauvegarde ;
    - le temps maximal d'indisponibilité admissible, qui détermine la durée maximale pour la restauration des données et du service à partir d'une sauvegarde.

Il est essentiel de fournir un document formalisant ce qui est sauvegardé et ce qui ne l'est pas (quelle qu'en soit la raison, financière par exemple). Ainsi chacun peut savoir où stocker des données qui doivent être sauvegardées et quels espaces sont des zones "scratch".

Il faut également sensibiliser les utilisateurs sur les risques, par exemple pour leurs « bookmarks » ou leur liste de contacts. Ces documents peuvent être stockés sur un espace centralisé ou non, dépendant souvent de la volonté de chaque utilisateur (soit dans leur HOME, soit dans un profil itinérant sous Windows). S'ils sont situés dans les espaces « système », ils sont rarement sauvegardés.

Il reste le problème de portables. Souvent les utilisateurs stockent leurs documents sur les disques locaux, ce qui leur permet de travailler lorsqu'ils n'ont pas accès aux ressources informatiques de leur laboratoire via le réseau. Mais, en cas de perte ou de vol de leur portable, ou de panne du disque local, ces précieuses données seront perdues.

Plusieurs solutions sont possibles. Une sauvegarde sur un disque externe peut pallier à ces inconvénients, mais pas s'il est perdu ou volé en même temps que l'ordinateur (souvent dans la même sacoche...). Ces disques sont souvent non chiffrés, incluant donc une faille de sécurité.

D'autres solutions de sauvegardes à distance sont également possibles, allant du simple logiciel rsync à des logiciels payant, transférant, de manière sécurisée (chiffrée), les données locales vers des serveurs hébergés dans leur laboratoire ou dans un espace de confiance.

Les sauvegardes de données ne doivent pas être soumises aux mêmes risques de sinistres que les données sauvegardées.

Les sauvegardes doivent être traitées de manière à garantir leur confidentialité et leur intégrité. Leur chiffrement est une option à considérer.

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.

Conformité :

CNF-1 implémentation de la règle (23/01/2017)
Sensibilité : *

Conformité : ***Le DU s'assure que l'utilisation du SI se fait dans le respect des exigences légales, réglementaires et contractuelles.***

Au minimum, le DU s'assure de :
• la sensibilisation des agents au respect de la propriété intellectuelle et de la création artistique, en particulier sur l'usage responsable des logiciels de partage de fichiers, notamment les logiciels peer-to-peer ;
• la prise en compte de la SSI dans les systèmes que l'unité exploite localement, pour éviter qu'ils ne soient détournés de leur usage professionnel.

Le DU s'assure :
• que l'unité ne réalise ses acquisitions de logiciels qu'à partir de sources connues et réputées ;
• que les licences originales et preuves d'achats des matériels et logiciels utilisés sont conservées par l'unité.

Le DU s'assure que le personnel est sensibilisé au respect du droit de la propriété intellectuelle et en particulier que le personnel est informé du fait qu'il est totalement proscrit de télécharger, utiliser ou diffuser via le réseau de l'unité des fichiers dont les droits de propriété intellectuelle n'ont pas été respectés.

Cas particulier de la réglementation informatique et libertés

L'unité est responsable des traitements de données à caractère personnel mis en œuvre au sens de la réglementation. Le DU est responsable des traitements de données à caractère personnel mis en œuvre dans son unité. A ce titre, il veille à l'application des procédures liées à la mise en œuvre de la réglementation relative au traitement automatisé des données à caractère personnel réalisés sur des systèmes qui sont sous la responsabilité de l'unité.

Pour cela il s'adressera au Délégué à la Protection des Données (DPD) compétent pour son unité.

NOTA : Pour les traitements réalisés par des systèmes d'informations mis à disposition de l'unité par une entité tierce (d'autres entités du CNRS, des partenaires universitaires, etc.), c'est le responsable du système d'information de l'entité tierce qui porte la responsabilité du respect de ces règles. Lorsque des données à caractère personnel sont extraites de ces systèmes et subissent des traitements spécifiques non prévus et/ou validés de façon explicite par l'entité tierce, il convient de vérifier que la réglementation concernant le traitement des données à caractère personnel est bien respectée.

CNF-6 implémentation de la règle (23/01/2017)
Sensibilité : *

Conformité : ***Le DU doit mettre à disposition de l'audit interne du CNRS, du RSSI du CNRS, du RSSI de la DR dont il dépend tout document permettant de juger du niveau d'application des règles de sécurité des SI dans l'unité.***

En particulier, le DU doit au minimum disposer :
• de la liste des règles applicables à son unité,

- du plan d'action SSI de son unité,
- des rapports SSI transmis au RSSI de DR.

Les autres documents qui pourront être consultés sont notamment, en fonction du type d'unité :
- le catalogue des services SI gérés par l'équipe informatique,
- le référentiel des configurations gérées,
- les enregistrements,
- etc.

Le RSSI pilote des audits réguliers du système d'information relevant de sa responsabilité.

CNF-7 implémentation de la règle (23/01/2017)
Sensibilité : *

Conformité : ***Le DU s'assure de la prise en compte de la sécurité au niveau adéquat par tout projet de SI conçu sous sa responsabilité et valide les risques résiduels avant mise en œuvre. Pour les SI les plus sensibles, cela se traduit par une homologation.***

Pour chaque Système d'Information conçu sous sa responsabilité, le DU doit s'assurer que les procédures décrites par la règle DEV-1 sont respectées et il doit prendre ses décisions en matière de gestion des risques SSI. Pour cela il doit notamment :

1. Prendre connaissance du document qui formalise l'évaluation initiale de la sensibilité SSI du SI et viser ce document qui doit au minimum décrire :
    a. Une synthèse SSI
        i. Niveau de sensibilité du SI suivant l'échelle définie dans cette PSSI (niveau de sensibilité global de « aucun » à « critique »)
        ii. Niveau du besoin global de sécurité du SI suivant les échelles définies dans cette PSSI (besoin en Disponibilité, Intégrité, Confidentialité, Auditabilité du niveau « aucun » à « critique »)
        iii. Niveau de prise en compte de la SSI adéquat et actions SSI préconisées (études, audits, tests, etc.)
        iv. Niveau de validation des risques résiduels (ad hoc, approbation officielle, homologation)
    b. Une présentation détaillée du projet de SI
        i. PRESENTATION DU PROJET
            1. Contexte et objectifs du projet
            2. Grandes fonctionnalités
            3. Organisation du projet
            4. Planning du projet
        ii. CONTEXTE DE LA SECURITE DE L'INFORMATION
            1. Informations et processus principaux gérées par le système cible
            2. Utilisateurs du système d'information et destinataires des traitements
            3. Exigences réglementaires et notamment RGS / DR / PPST / CNIL
            4. Eléments techniques et notamment architecture
            5. Contexte d'hébergement et de maintenance du SI
        iii. EVALUATION DE LA SECURITE DE L'INFORMATION
            1. Complexité du SI
            2. Conséquences / Impacts redoutés en cas d'incident sécurité
            3. Réalité de la menace en fonction de l'intérêt et des moyens des attaquants
            4. Besoins de sécurité (en DICA)

iv. RECOMMANDATIONS SSI

1. Niveau de prise en compte de la SSI adéquat et actions préconisées
2. Niveau de validation des risques résiduels recommandé

2. S'assurer que les modalités de prise en compte de la SSI respectent tout le long du projet les procédures détaillées dans la règle DEV-1 et qu'un dossier sécurité soit constitué des pièces suivantes

a. l'évaluation initiale de la sensibilité SSI du SI visée par le DU ;
b. la trace des décisions prises suite aux recommandations établies lors de l'évaluation initiale de la sensibilité SSI du SI ;
c. (**) l'étude détaillée des risques SSI menée selon une méthode éprouvée conforme aux normes existantes en matière de gestion des risques SSI et le plan de réduction des risques associé ;
d. (***) la politique de sécurité du système ;
e. (**) les procédures d'exploitation de la sécurité ;
f. (***) la gestion des risques résiduels ;
g. (**) les résultats des tests et des audits menés pour vérifier la conformité du système au plan de réduction des risques et/ou à la politique de sécurité et aux procédures d'exploitation, ainsi que les plans d'actions associés validés par les entités responsables de leur mise en œuvre ;
h. (***) la cartographie technique du réseau.

3. Valider les risques résiduels avant mise en service du SI (ou lors de toute modification substantielle des types d'informations manipulés, des types de traitements effectués, des destinataires des informations gérées, de l'environnement technique ou organisationnel du SI considéré) :

a. Par une Homologation officielle du SI lorsque cela est nécessaire au plan réglementaire

i. Une homologation officielle est nécessaire lorsqu'un des critères déterminants est identifié

1. Le système d'information gère des informations dont le niveau de sensibilité est « Diffusion Restreinte »
2. Le système d'information rentre dans le cadre du RGS : échanges d'informations entre plusieurs autorités administratives ou entre une autorité administrative et des usagers de l'administration

ii. modalités de la décision d'homologation SSI du SI

1. L'instruction du dossier d'homologation est réalisée sous la responsabilité de l'autorité d'homologation (DU) responsable du SI, le dossier contient

a. Une note synthétique qui présente le SI et les aspects SSI
b. Le dossier sécurité du SI
c. Une synthèse des risques résiduels après les audits et tests réalisés
d. Une proposition d'homologation portée par l'autorité d'homologation (DU)

2. La réunion du comité d'homologation permet à l'autorité d'homologation de présenter le dossier d'homologation au représentant de l'autorité administrative en présence des experts requis
3. La décision d'homologation est prise par le représentant de l'autorité administrative et elle est officialisée suivant une procédure définie par la DAJ

b. ou par une Approbation officielle des risques si l'évaluation initiale de la sensibilité SSI du SI identifie des besoins SSI de niveau « très sensible » ou « critique »

i. L'instruction du dossier d'approbation des risques est réalisée sous la responsabilité du DU responsable du SI, le dossier contient

1. Une note synthétique qui présente le SI et les aspects SSI

2. Le dossier sécurité du SI
3. Une synthèse des risques résiduels après les audits et tests réalisés

ii. L'approbation officielle des risques résiduels est prise par le DU et elle est officialisée suivant une procédure définie par la DAJ

c. ou par toute méthode permettant de tracer la prise de connaissance par le DU des risques résiduels formalisés sous la forme d'un document par le CSSI.

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.