Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR, DE LA RECHERCHE ET DE L'INNOVATION

Guide méthodologique sur la protection des informations numériques sensibles liées aux activités des ZRR

Contexte règlementaire

1. Décret N°2011-1425 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation [2 novembre 2011]
2. Instruction générale interministérielle (IGI) 1300 portant sur la protection du secret de la défense nationale [30 novembre 2011]
3. Arrêté du Premier Ministre relatif à la protection du potentiel scientifique et technique de la nation [3 juillet 2012]
4. Circulaire interministérielle de mise en œuvre du dispositif de la protection du potentiel scientifique et technique de la nation N°3415/SGDSN/AIST/PPST [7 novembre 2012]
5. Lettre N°356 du directeur de cabinet et sa pièce jointe [22 février 2013]
6. Politique de sécurité des systèmes d'information de l'Etat (PSSIE) – circulaire du Premier Ministre N°5725 [17 juillet 2014]
7. Instruction interministérielle N°901 relative à la protection des systèmes d'information sensibles [11 février 2015]
8. Note thématique HFDS N°0404 - Création des ZRR [03 avril 2013]
9. Note thématique HFDS N°0408 - Accès à une ZRR [04 avril 2013]
10. Note thématique HFDS N°0499 - Gestion des coopérations [24 juin 2013]
11. Note thématique HFDS N°500 - Gestion des incidents et rapports [24 juin 2013]

Préambule

La mise en place d'une politique de sécurité des systèmes d'information (PSSI) vise à répondre aux besoins en sécurité inhérents aux enjeux des métiers et à ceux précisés dans les règlementations s'appliquant aux SI concernés (ex : CNIL, données médicales, SI confidentiel défense, …). Parmi ces règlementations, la PPST a pour but d'empêcher la captation indue, au sein des établissements publics et privés, des savoirs et savoir-faire stratégiques ainsi que des technologies sensibles. Le dispositif offre une protection juridique et administrative fondée sur le contrôle des accès à certaines zones et aux informations stratégiques ou sensibles détenues. L'objet de ce guide est d'accompagner la prise en compte des besoins spécifiques formalisés par la PPST au sein d'une PSSI locale. Cette dernière devant aussi couvrir l'ensemble des risques identifiés tels que la destruction ou l'altération des données, éventuellement précisés dans d'autres textes règlementaires tel que la PSSI de l'Etat. Plusieurs guides sont disponibles sur le site de l'Agence nationale de la sécurité des systèmes d'information (ANSSI - www.ssi.gouv.fr) pour accompagner cette démarche de sécurisation globale des systèmes d'information.

Enjeux

Le dispositif de la PPST permet de contrôler et de règlementer l'accès physique à une zone géographique spécifique, la ZRR, et de pénaliser l'infraction constatée d'une personne présente dans cette zone sans autorisation. Il permet également de protéger les savoirs et savoir-faire issus des recherches menées par les personnels rattachés administrativement à cette zone. L'argument juridique lié à une zone a cependant une portée très réduite dans le domaine de la SSI car les infractions peuvent être commises à distance ou être d'origine inconnue. De plus, la répartition géographique des chercheurs au sein des équipes, la dilution des systèmes d'information (SI) sensibles dans les autres SI et la présence de documents sensibles dans les équipements informatiques mobiles des personnels de laboratoire, rendent extrêmement difficile le « zonage » des SI.

Le principe des autorisations d'accès aux ZRR permet de contrôler les personnes devant y accéder, et le cas échéant, de faire sortir et/ou de poursuivre les contrevenants. Pour les systèmes d'information, il s'agit d'empêcher l'accès illicite aux données numériques sensibles et d'en empêcher non seulement la captation, mais aussi l'altération et la destruction.

En complément des sujets couverts par la politique de sécurité des systèmes d'information de l'État -PSSIE- (cf. réf. 6), la mise en place d'une politique SSI efficace couvrant les ZRR doit tenir compte d'un certain nombre d'aspects qui sont l'objet de ce guide.

Gouvernance et rôles

La PSSI doit être conforme à la PSSIE (PSSI de l'Etat) qui propose notamment un modèle organisationnel ; elle s'intègre dans une politique de sécurité interne (PSI) traitant des risques dans leur globalité et elle est cohérente avec le dispositif PPST.

Le **chef d'établissement**, en tant que responsable de la PPST, nomme un **responsable de la ZRR** pour sa mise en œuvre. Le chef d'établissement autorise des accès aux ZRR et aux informations associées, après avis favorable du Ministre, sollicité par le **Fonctionnaire de Sécurité de Défense (FSD)**.

Le responsable de la politique de sécurisation des SI, nommé « autorité qualifiée en sécurité des systèmes d'information » (AQSSI), est le chef d'établissement ; dans ce cadre, ce dernier s'appuie, avec le responsable de la ZRR, sur une chaîne opérationnelle SSI pour définir et mettre en œuvre une PSSI adaptée à l'établissement et aux éléments constitutifs du potentiel scientifique et technique des ZRR concernées. L'AQSSI désigne un responsable de la SSI **(RSSI).**

Le pilotage de la SSI au sein de l'établissement, en particulier pour la protection des informations sensibles, s'effectue **en concertation entre tous les acteurs de la SSI et de la PPST**.

Les mesures de sécurité et leur respect par les utilisateurs et les administrateurs sont régulièrement contrôlés, notamment sur demande de l'AQSSI ou du Haut Fonctionnaire de Défense et de Sécurité (HFDS).

Définitions et applications

a) Définitions

La notion de sensibilité étant abordée dans plusieurs règlementations et différents contextes, il est nécessaire, dans le cadre de ce guide, d'en préciser le sens et de définir la notion d'information sensible.

Cadre général

Une information est dite « sensible » lorsque sa divulgation, sa perte ou sa modification entraîne des conséquences néfastes pour l'activité d'une organisation, pour les usagers ou pour la sécurité publique. Cette notion de « sensibilité » est encadrée par plusieurs textes règlementaires tels que la CNIL, la protection des données médicales, l'instruction interministérielle N°901 (cf. réf. 7) ou la PPST.

Ces textes imposent la mise en place de mesures de protection des informations sensibles ; lorsque les mesures sont effectives, alors ces informations sensibles sont dites « sécurisées ».

Cadre spécifique PPST/ZRR

Un ensemble d'informations, quel que soit son support, est qualifié de « sensible » au sens de la PPST lorsque sa divulgation à des tiers non autorisés aurait un impact significatif au regard des risques ayant justifié la création de la ZRR. Il est appelé dans la suite du document **: « Information à Régime Restrictif » (IRR)**.

Un système d'information donnant accès directement à des IRR est nommé dans la suite du document « **Système d'Information à Régime Restrictif » (SIRR)**. Il intègre *de facto* tous supports et équipements électroniques stockant ou véhiculant un ensemble d'IRR non sécurisé.

b) Applications

Echelle de sensibilité

Selon l'II 901 (cf. réf. 7), chaque entité manipulant des données sensibles doit adopter localement une **échelle de sensibilité** de ses informations en tenant compte des contraintes règlementaires (PPST, CNIL, accord de non-divulgation..), de la typologie des données et de l'organisation spécifique à cette entité. Ce principe s'applique aux travaux de recherche des ZRR qui portent par définition sur certaines informations sensibles.

Si le processus d'identification des IRR n'est pas réalisé, alors la totalité des informations et systèmes qui hébergent les données de la ZRR sont considérés comme IRR et SIRR et doivent respecter les mesures de sécurité correspondantes.

Les données les plus sensibles qui ont justifié un classement ZRR de l'unité de recherche et qui relèvent des « spécialités sensibles » (R3, R4) au sens de la PPST, sont des IRR de niveau DR « diffusion restreinte », conformément à l'II N°901 relative à la protection des SI sensibles.

Marquage des IRR

Les IRR étant par définition sensibles, elles sont soumises à l'II N°901 et doivent à ce titre être marquées en fonction de l'échelle de sensibilité adoptée localement.

L'objet du marquage est d'apporter la connaissance du niveau de sensibilité des informations à une personne les manipulant. Il peut être fait classiquement sur les documents, par exemple à l'aide d'encadrés rouges. Dans le cas des fichiers informatiques, le marquage peut être fait sur le nom du fichier, le nom du répertoire voire sur le support physique, par exemple à l'aide d'une étiquette sur une clé USB. Cela permet notamment au détenteur d'avoir connaissance du niveau de sensibilité avant toutes manipulations telle que l'ouverture ou la copie.

Le marquage des IRR doit donc être explicite afin qu'une personne, en les manipulant, ne puisse en ignorer la sensibilité et qu'elle puisse se référer à une échelle précisant les précautions associées.

En cas d'échange avec d'autres entités, l'échelle de sensibilité doit aussi être transmise afin que le receveur ait connaissance des précautions de manipulation associées à un marquage et qu'il sache par exemple s'il peut la diffuser ou la retransmettre.

Accès aux informations

Conformément à la terminologie employée dans la PPST, un accès à une IRR ou à un SIRR, quelle que soit la localisation de l'accédant, est considéré comme un **accès virtuel** à la ZRR. Cet accès nécessite un avis ministériel, comme s'il s'agissait d'un accès physique.

La possibilité de donner l'accès ou de transmettre une information provenant d'un SIRR à un tiers non autorisé doit être évaluée en tenant compte des critères suivants :

- **si l'information est une IRR, un avis ministériel est nécessaire comme pour un accès physique** (un élément d'information isolé provenant d'un SIRR n'est pas forcément une IRR) ;
- si l'information n'est pas une IRR, un accord de confidentialité peut toutefois être nécessaire (ex : accord commercial ou échanges internationaux) ;
- si l'information n'est pas confidentielle, ou ne l'est plus suite à une réévaluation, elle peut être dans certains cas rendue publique, par exemple lors de la publication d'une thèse ou dans des revues spécialisées.

Mesures de protection des IRR et SIRR et évaluation

a) Mesures de protection des IRR et SIRR

Il appartient au responsable de la ZRR ou son coordonnateur pour la PPST, de s'assurer que des analyses de risques sont conduites régulièrement sur les SIRR, que les mesures de protection adéquates sont mises en œuvre et que les risques résiduels sont acceptés par le chef d'établissement.

Conformément à la circulaire (cf. réf. 4), le responsable ou le coordonnateur de la PPST est chargé de la préparation et de l'exécution des mesures de protection. Dans le domaine de la SSI, le RSSI doit être consulté sur l'évaluation des mesures en rapport avec les éléments constitutifs du potentiel scientifique et technique concernés. En fonction des organisations des unités, des correspondants SSI peuvent être localement désignés en relation avec le RSSI.

Les mesures d'ordre technique et organisationnel doivent être conformes avec la PSSIE et l'II N°901 et doivent prendre en compte la formation et la sensibilisation des utilisateurs concernés, notamment au travers de chartes adaptées. Ces mesures peuvent être logiques (chiffrement, droits d'accès…) ou physiques (ex : système strictement interne à un laboratoire).

Le choix et le déploiement des outils de sécurisation doit être fait en lien avec l'établissement ou la structure en charge des systèmes d'information mis à disposition des ZRR.

b) Précisions sur les mesures de protection des IRR et SIRR

Définition d'une IRR : un fichier sensible au sens de la PPST est une IRR. Il peut s'agir de travaux de recherche dans un format bureautique, de données techniques provenant d'équipements, d'images ou autres.

Définition d'un SIRR : un système contenant des IRR est un SIRR. Il peut s'agir d'un ordinateur portable, d'une clé USB, d'un serveur de fichier etc. Certains SIRR, comme les serveurs, sont fixes mais la liste des personnes pouvant y accéder physiquement n'est pas forcément maîtrisée (ex : data centre partagé). D'autres sont mobiles et en cas de perte ou de vol, les personnes pouvant y accéder sont donc inconnues. Pour cela, Les mesures de protection doivent limiter l'accès à l'information sensible, soit en protégeant les IRR, donc les fichiers, soit en protégeant le SIRR dans sa globalité.

Les mesures de protection peuvent être logicielles ; à titre d'exemple il peut s'agir :

- du chiffrement des IRR à l'aide de solution qualifiées telles ACID ou Zed! ;
- du chiffrement du disque dur complet d'un ordinateur portable contenant des IRR ;
- d'un contrôle d'accès avec chiffrement des répertoires partagés sur un serveur mutualisé à l'aide d'outils tels que ZoneCentral.

Ces mesures peuvent aussi être physiques, par exemple :

- une machine ou un réseau local à la ZRR, accessible uniquement depuis les locaux soumis au contrôle d'accès.

Les mesures peuvent aussi être mixtes :

- Une baie sécurisée dans un data centre partagé, dont la clé est détenue par le responsable de la ZRR, et dont les échanges avec la ZRR sont chiffrés.

L'ensemble des mesures de sécurisation, physiques et logiques, doivent permettre de garantir que les IRR ne peuvent être manipulées que par des personnes autorisées à accéder à la ZRR qui protège ces informations et cela, à chaque instant et quel que soit le lieu où elles se trouvent (serveur, portables, méls, …).

Des IRR chiffrées, donc sécurisées, peuvent être manipulées comme tout autre fichier. En effet, accéder à de tels fichiers sans pouvoir les ouvrir ne permet pas la divulgation des IRR.

Un SI contenant ou véhiculant des IRR sécurisées n'est pas pour autant un SIRR. Echanger par courriel des IRR chiffrées n'implique pas que les serveurs de messagerie soient des SIRR.

Un SIRR peut contenir des informations sensibles au titre d'une autre règlementation et qui ne sont donc pas des IRR.

Les systèmes d'information sensible au sens de l'II N°901 tel que les systèmes d'information concourant à la sécurité physique (caméra, contrôle d'accès et d'intrusion, détection d'incendie…) ne sont pas des SIRR.

c) Analyse et maîtrise de risques des IRR et SIRR

Tous les équipements mobiles (clés USB, ordinateurs portables, smartphones, etc…) ou pouvant être amenés à manipuler des IRR (ex. équipements de recherche, imprimantes, photocopieurs, scanners, etc...), font partie du SIRR et doivent être considérés dans l'analyse des risques.

La maîtrise des SIRR implique nécessairement de disposer d'une cartographie technique et fonctionnelle à jour, d'intégrer les problématiques de SSI dans l'ensemble des phases du cycle de vie des projets et de contrôler les accès aux IRR.

d) Gestion des incidents SSI impliquant des IRR ou des SIRR

L'établissement définit et met en œuvre une politique de gestion des traces d'accès et de fonctionnement des SIRR permettant la détection et la résolution des incidents.

Les incidents SSI impliquant des IRR ou des SIRR sont remontés sans délai au RSSI et au Fonctionnaire de Sécurité de Défense (FSD) selon une organisation locale prédéfinie et régulièrement testée, conformément à la Note thématique HFDS (cf. réf.11).

En fonction de sa gravité, l'incident est remonté sans délai au service du HFDS qui pourra le faire suivre à l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

e) Évaluation des mesures de protection des IRR et SIRR

L'efficacité des mesures de protection des IRR est régulièrement contrôlée, notamment au moyen d'audits planifiés (techniques et organisationnels), d'analyses des incidents et d'une vigilance accrue sur les sources ouvertes quant à la diffusion illégitime d'IRR.

Mise en place de la protection des informations numériques sensibles

- 10 étapes concrètes -

Ce chapitre présente une démarche structurée pour la mise en place de la protection des données sensibles.

1. **Définir les responsabilités, l'organisation et le processus** permettant de planifier et de suivre les étapes suivantes.
2. **Identifier les typologies d'informations sensibles**, notamment les IRR, et les règlementations associées. Il peut s'agir par exemple de données de recherche, médicales, personnelles ou contractuelles.
3. **Analyser les risques** portant sur les informations sensibles et les conséquences en cas d'incident : conséquences pour les intérêts fondamentaux de la nation, perte d'exclusivité de découvertes, conséquences pour les partenaires industriels, non-respect du secret médical, fuite de données personnelles, rupture de contrat…
4. **Décider d'une échelle de sensibilité** avec la nomenclature associée et définir les processus de marquage (dans les fichiers, dans les noms de fichiers ou de répertoires, sur les supports …). Le marquage doit permettre à une personne accédant à une IRR d'avoir conscience du niveau de sensibilité de l'information. En cas d'échange avec d'autres entités, l'échelle de sensibilité doit aussi être transmise afin que le receveur ait connaissance des précautions de manipulation associées à un marquage et qu'il sache par exemple s'il peut la diffuser ou la retransmettre.
5. **Localiser les IRR.** L'objectif est d'identifier les entités qui produisent ou manipulent des informations sensibles. Il s'agit classiquement des laboratoires mais il peut y en avoir d'autres. Par exemple, les services juridiques peuvent être concernés s'ils manipulent des contrats, des structures externes en charge de donner de la visibilité aux travaux de recherche et les sous-traitants.
6. **Cartographier les SI supports actuels.** Il s'agit, à cette étape, d'identifier les moyens utilisés pour exploiter, véhiculer ou échanger les informations sensibles. Ordinateurs portables, serveurs, clefs USB, stockage en ligne, messagerie (…). Aujourd'hui, ces moyens sont nombreux et peuvent évoluer dans le temps.
7. **Identifier et mettre en place des mesures de sécurité** limitant les accès des IRR aux personnes autorisées. Une fois les SI supports identifiés, il faut les renforcer ou proposer des alternatives sécurisées pour traiter les IRR et être qualifiés de SIRR. Ces mesures peuvent être logiques (chiffrement, droits d'accès…) ou physiques (ex : système strictement interne à un laboratoire).
8. **Formaliser une politique SSI**, ou ajouter un volet spécifique dans celle existante, reprenant les points précédents et précisant les procédures de remontée des incidents aux autorités et au RSSI. En fonction de la sensibilité, ce dernier informera le fonctionnaire de sécurité des systèmes d'information (FSSI) et le service du HFDS.
9. **Contrôler** le processus de marquage des informations sensibles et leur bonne protection.
10. **Réévaluer la politique de sécurité des SI** périodiquement ou en cas de changements majeurs des activités ou de l'organisation.