Politique de Sécurité du Système d'Information

(PSSI)

Auteurs : RSSI(-S) / DIO

Validé par le Conseil d'Administration le 17 mai 2024

Version 1, Mai 2024

Historique des modifications

Version	Objet de la modification	date
Version 1	Version initiale de la PSSI	Mai 2024

Document rédigé avec la participation des informaticiens de proximité, du service juridique, des fonctionnaires de sécurité et de défense, de l'ensemble de la DIO, La Commission du Numérique de l'Observatoire de Paris, des Directeurs de départements et de la Présidence.

Sommaire

1 Contexte et objectifs

1.1 Contexte

L'Observatoire de Paris regroupe 5 départements scientifiques, 1 institut, 2 services scientifiques et les services communs, soit respectivement :

- GEPI
- LERMA
- LESIA
- LUTH
- SYRTE
- IMCCE
- ORN
- UFE
- UAR

L'Observatoire de Paris est implanté sur 3 sites principaux :

- Paris
- Meudon
- Nançay

Les sites sont numériquement interconnectés via le Groupement d'Interêt Public (GIP) "RÉseau NAtional de Télécommunications pour la technologie, l'Enseignement et la Recherche" (RENATER). L'Observatoire de Paris dont le rayonnement est international héberge des services numériques stratégiques. A ce titre, le système d'information fait l'objet d'un traitement particulier.

1.2 Périmètre de la Sécurité du Système d'Information (SSI)

La sécurité du système d'information de l'Observatoire de Paris couvre l'ensemble des systèmes d'information de l'établissement avec toute la diversité que cela implique dans les usages scientifiques, d'enseignement et administratifs, les équipements, les lieux, les méthodes d'accès, les personnes impliquées...

- le système informatique de gestion ;
  - les applications institutionnelles (messagerie, moyens scientifiques de calcul, stockage...) ;
  - les moyens de communication, visioconférence, contrôle d'accès, téléphonie, etc. ;
  - les interconnexions avec les différentes tutelles et organismes (CNRS, INSU, ANSSI...).

1.3 Besoins de sécurité

La SSI repose sur les critères suivants :

- Confidentialité : « Propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés » norme ISO 7498-2.
  - Disponibilité : « Propriété d'être accessible et utilisable sur demande par une entité autorisée » norme ISO 7498-2.
  - Intégrité : « Propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée » norme ISO 7498-2.

  Les besoins de sécurité s'appliquent aussi bien aux ressources du système d'information (postes informatiques, réseaux, applications...) qu'aux données traitées par ces ressources. Il est nécessaire d'inventorier et de classifier ces données (défense, scientifique, gestion, nominative, stratégique...) afin d'en identifier le degré de sensibilité et donc le niveau de protection nécessaire.

1.4 Menaces

Afin de mettre en place les moyens de sécurité adéquates, la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité – ANSSI) préconise de connaître les typologies de menaces et leurs impacts. On distingue ainsi :

- les attaques visant directement le système d'information : vol de données et éventuellement les ressources supportant ces données, modification des données, déni de service...
- les attaques visant les ressources informatiques : vol de ressources, détournement des ressources, altération des données, émission de logiciels malveillants...
- les accidents : sinistres naturels, altérations accidentelles des données ou ressources...

Pour chaque menace, il est alors nécessaire d'en évaluer le risque, considérer la probabilité que celle-ci devienne réalité et détecter les éventuels facteurs aggravants (négligence constatée, insuffisance d'information, de consignes...).

1.5 Analyse de risque

L'analyse des risques vise à identifier, évaluer, hiérarchiser et cartographier les risques susceptibles de porter atteinte au SI. Ce rapport d'analyse est signé par la présidence. Ce document évoluera, pour chaque modification la présidence en sera informée par courriel. Il revient à chaque département et institut d'informer les RSSI lors de la mise en service de nouveaux moyens afin que cette analyse de risque soit réalisée en conformité avec les décrets en vigeur. L'architecture du SI doit être en conformité avec le Décret 2022-634 du 22 avril 2022. «L'État se dote d'une politique de contrôle et d'audit internes, fondée sur une analyse des risques. A ce titre, chaque département ministériel met en place une analyse des risques ainsi que des dispositifs de contrôle et d'audit internes, adaptés aux

missions et à l'organisation de ses services et visant à assurer la maîtrise des risques liés à la gestion des politiques publiques dont ces services ont la charge.»

1.6 Pilotage

La responsabilité générale de la sécurité du système d'information relève de la personne à la tête de la Présidence de l'Observatoire de Paris en tant qu'Autorité Qualifiée pour la Sécurité du Systèmes d'Information (AQSSI). Elle est assistée dans ses fonctions par le Responsable de la Sécurité du Système d'Information (RSSI) de l'établissement, du Fonctionnaire de Sécurité et de Défense (FSD) ainsi que le Fonctionnaire de Sécurité et de Défense Adjoint (FSDA). L'Observatoire de Paris a un RSSI et plusieurs RSSI-Suppléant (RSSI-S) qui ont par convention tout droit décisionnel. La dénomination RSSI(-S) englobe le RSSI et les RSSI-Suppléant. Le rôle de conseiller à la sécurité numérique (CSN) est assuré par les RSSI(-S)

La Politique de Sécurité du Système d'Information (PSSI) de l'Observatoire de Paris s'inscrit dans le cadre de la politique et des directives émanant de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), en charge de la sécurité des systèmes d'information au niveau national. Cette politique et ces directives sont relayées par le Haut Fonctionnaire de la Défense et de Sécurité (HFDS) du Ministère de l'Education Nationale, de l'Enseignement Supérieur et de la Recherche et par le Fonctionnaire de Sécurité des Systèmes d'Information (FSSI). Le CNRS étant une tutelle importante des unités de l'Observatoire de Paris, la PSSI intègre également les consignes de sécurité de celui-ci.

Le pilotage courant est de la responsabilité des RSSI(-S) qui ont toute légitimité pour œuvrer. Les Directeurs des départements et institut sont responsables de la sécurité du système d'information de leur périmètre respectif. Pour assurer cette fonction, ils nomment une personne Chargée de la SSI (CSSI) qui est le relais privilégié des RSSI(-S) de l'établissement au sein de leur département et institut tant pour appliquer et faire respecter la PSSI de l'établissement que pour lui remonter les éventuels incidents.

1.7 Rôle et responsabilités des acteurs de la SSI

1.7.1 La Présidence de l'Observatoire de Paris

La Présidence de l'Observatoire assure la responsabilité globale de la sécurité du système d'information de l'établissement. Elle peut être juridiquement responsable en cas d'incident de sécurité. La Présidence :

- s'appuie sur le RSSI, chargé de l'assister dans le pilotage et la gestion de la SSI ;
- veille à la mise en œuvre des dispositions contractuelles et réglementaires sur la sécurité du SI, s'assure que les contrôles internes de sécurité sont régulièrement effectués et fait organiser la sensibilisation et la formation du personnel aux questions de sécurité ;

- propose au conseil d'administration la Politique de Sécurité du Système d'Information et les mesures de sécurité retenues par celle-ci ;
- accorde les moyens budgétaires, humains, techniques pour mettre en application les directives de celle-ci ;
- s'implique dans les décisions de management, et soutient la démarche engagée.

1.7.2 Les Directeurs de départements et institut

Les directeurs de département et institut sont les garants de la protection des données scientifiques et industrielles sensibles de leur périmètre. Ils veillent à faire appliquer les règles de sécurité de la PSSI, et s'assurent que les personnels de leur département et institut respectent les bonnes pratiques et la charte de bon usage du système d'information. En tant que responsable de la SSI de son département et institut, le directeur :

- s'assure que les documents de PSSI de son unité (charte, gestion des traces...) sont en accord avec ceux de toutes ses tutelles (CNRS, EPST...) ;
- désigne le CSSI de son unité, celui-ci étant le « chargé sécurité » pour les autres tutelles. Ce CSSI fait partie des chaînes fonctionnelles de chaque tutelle et assure les liens d'information correspondants. Il conviendra d'inscrire sur la fiche de poste de l'agent un temps dédié à la fonction qu'il pourra ainsi utiliser pour mettre en place des outils de sécurité ou suivre des formations ;
- s'assure que les personnels de leur direction respectent les bonnes pratiques et la charte de bon usage du système d'information ;
- veille à ce que tout nouveau projet fasse l'objet d'une étude formalisant les besoins, risques et objectifs de sécurité ;
- valide les demandes de droit d'accès à une application de leur périmètre. Ils s'assurent de leur mise à jour en cas de mouvement du personnel ;
- remonte au RSSI les procédures déjà en place, les besoins de sécurité et les incidents et vulnérabilités décelés pouvant porter atteinte à la sécurité des informations. L'analyse des incidents de sécurité menée par les RSSI(-S) sera, selon le degré de gravité de l'incident, transmise au Délégué à la Protection des Données (DPD).

Dans le cas particulier des départements et instituts en Zone à Régime Restrictif (ZRR), des mesures de sécurité plus spécifiques doivent être mises en œuvre et font l'objet d'une politique spécifique.

En cas d'incident, celui-ci est traité par la voie fonctionnelle de la tutelle responsable, en assurant l'information des autres partenaires et notamment les RSSI(-S) de l'établissement.

1.7.3 Le Chargé de la Sécurité du Système d'Information

Le CSSI d'un département ou institut est nommé par le directeur de l'unité. Il est acteur de la SSI et à ce titre, contact privilégié des RSSI(-S). Il est fondamental dans la chaîne SSI de l'établissement, il a notamment pour rôles :

- conseiller le directeur d'unité en matière de SSI ;
- d'assurer la gestion des incidents de sécurité de son périmètre ;
- de s'assurer que les personnels de leur direction respectent les bonnes pratiques et la charte de bon usage du système d'information ;
- d'être acteur de la PSSI de l'établissement et faire évoluer celle-ci en fonction des besoins de son département et ou institut en osmose avec l'ensemble des CSSI ;
- veiller à ce que tout nouveau projet fasse l'objet d'une homologation de sécurité formalisant les besoins, risques et objectifs de sécurité avant la mise en production. En cas de litige le directeur de l'unité et ou les RSSI(-S) peuvent être saisis ;
- s'assurer de la mise en pratique de la PSSI de l'établissement ainsi que les PSSI des autres tutelles ;
- s'assurer du respect des consignes de sécurité notamment de l'ANSSI ;
- limiter autant que possible la surface d'attaque ;
- remonter au RSSI(-S) tout litige, incident ou suspicion d'incident ;
- garantir le niveau de sécurité des équipements de son périmètre ;
- assurer la veille technologique et participer à toutes formations de sécurité ;
- s'assurer du respect des règles RGPD et saisir le DPD si nécessaire.

Les CSSI exercent leur fonction dans le respect des règles de confidentialité.

1.7.4 Les Administrateurs du SI

Les administrateurs du SI assurent des missions de conception, d'exploitation et de maintien en condition opérationnelle des ressources informatiques. Ils possèdent à ce titre des accès étendus aux ressources informatiques. Ces accès doivent être utilisés dans un cadre légal et respectueux des utilisateurs et de la déontologie. Ils :

- participent activement à la protection du système d'information ;
- veillent à sécuriser les ressources qu'ils administrent ;
- suivent les règles de sécurité de la PSSI ;
- informent le RSSI des incidents de sécurité dont ils seraient témoins ;
- participent à la sensibilisation des utilisateurs à la sécurité du SI.

1.7.5 Le Directeur de la Direction Informatique de l'Observatoire (DIO)

Le directeur de la DIO a pour mission :

- la mise en œuvre de la PSSI et de faire appliquer les règles de sécurité dans son périmètre ;

- le maintien et la garantie de la disponibilité et le bon fonctionnement des moyens et ressources informatiques ;
- la participation active à la veille sécuritaire et technologique ;
- la vérification régulière de la vulnérabilité des infrastructures techniques en collaboration avec les RSSI(-S) en l'informant systématiquement des travaux susceptibles d'impacter les dispositifs de sécurité en place ou d'influencer la cartographie des risques.

1.7.6 Le Fonctionnaire de Sécurité et de Défense

Nommé par le Haut Fonctionnaire de Défense et Sécurité (HFDS) du ministère, il est son relais fonctionnel au sein de l'établissement. Les FSD ont pour rôle :

- la coordination, le conseil, l'information et la mise en œuvre dans le cadre de la Protection du Potentiel Scientifique et Technique de la nation (PPST), de la protection du secret et de la préparation / exécution des plans de défense et de sécurité ;
- la participation à l'identification, à l'évaluation et au traitement des risques.

1.7.7 Le Responsable de la Sécurité du Système d'Information et Suppléants

Désigné par la Présidence dont il dépend fonctionnellement en matière de SSI, il veille à la sécurité des données et informations de l'établissement en termes de confidentialité, intégrité, disponibilité et traçabilité. Les RSSI(-S) doivent être formés à la SSI. Cette fonction ne peut être externalisée. Les RSSI(-S) :

- s'assurent de l'identification, de l'évaluation et du traitement des risques relatifs au système d'information ;
- pilotent les actions de sensibilisation et de formation du personnel de l'établissement ;
- participent à la veille technique et juridique ;
- assurent la coordination avec les organismes concernés par la SSI ;
- coordonnent et vérifient, en appui avec le service Juridique, l'intégration et le respect des clauses de sécurité dans tout contrat ou convention impliquant un accès au SI par des tiers ;
- assurent la gestion des incidents SSI et maintiennent à jour les indicateurs et le suivi des incidents ;
- pilotent en collaboration avec le Directeur de la DIO, la mise en œuvre opérationnelle de la sécurité et organisent régulièrement des audits de sécurité ;
- sont responsables de l'élaboration de la PSSI, de sa mise à jour, du contrôle et du suivi de l'application des mesures de celle-ci ;
- élaborent et assurent le suivi des plans d'action nécessaires à la mise en œuvre de la PSSI ;
- élaborent l'analyse des risques du système d'information de l'établissement, adaptent cette analyse dans le temps, émettent des préconisations pour

diminuer les risques encourus. L'analyse des risques doit être signée par la Présidence ;
- administrent les outils de détection d'intrusion et s'assurent de la robustesse du système d'information ;
- assistent tous les projets de l'établissement utilisant des ressources informatiques afin de veiller à la mise en œuvre au sein de ces derniers des éléments technologiques nécessaires à l'application de la PSSI ;
- diffusent à l'ensemble de la communauté de l'Observatoire les documents relatifs à la PSSI et son application ;
- sont l'intermédiaire direct en cas de problème entre la Présidence de l'université et les autorités compétentes ;
- définissent et maintiennent les indicateurs et tableaux de bord SSI à destination des comités de pilotage.

1.7.8 Le Délégué à la Protection des Données (DPD)

Conformément au règlement européen sur la protection des données (RGPD), il est nommé par la Présidence.

Le DPD a pour mission :

- d'informer et conseiller le responsable de traitement (la présidence de l'établissement), ainsi que les personnels qui procèdent au traitement, sur les obligations qui leur incombent en matière de protection des données à caractère personnel ;
- d'auditer et de contrôler le respect du RGPD et du droit national en matière de protection des données ;
- de veiller à l'application du principe de protection des données dès la conception et par défaut dans tous les projets comportant un traitement de données personnelles ;
- d'être l'interlocuteur privilégié de l'autorité de contrôle (CNIL) et coopérer avec elle ;
- de dispenser des conseils en ce qui concerne les analyses d'impact relatives à la protection des données et d'en vérifier l'exécution ;
- de tenir l'inventaire et documenter les traitements de données à caractère personnel en tenant compte du risque associé à chacun d'entre eux compte tenu de sa nature, sa portée, du contexte et de sa finalité ;
- de rendre compte de ses activités au responsable de traitement.

Le DPD de l'Observatoire de Paris a toute légitimité pour œuvrer sur le périmètre de l'établissement.

Dans le cas ou un département, un institut, une unité, un projet, serait rattaché à un DPD externe à l'établissement, le recours à celui-ci est à privilégier. Par ex un projet scientifique à dimension régional voire international peut avoir inscrit comme DPD de référence celui d'une autre tutelle, le recours à celui-ci est alors à privilégier.

1.7.9 La Direction des Ressources Humaines

La direction des ressources humaines effectue l'ensemble des démarches nécessaires à l'accompagnement de nouvelles mesures de sécurité. Elle veille notamment à l'intégration de sessions de formation à la sécurité du système d'information dans le plan de formation du personnel dont le cahier des charges aura été préalablement défini par les RSSI(-S). Elle informe le service informatique de toute arrivée / départ / modification contractuelle (ex prolongement d'un contrat) des agents, permettant ainsi au responsable informatique de modifier les modalités d'accès aux ressources numériques (ex prolongation du compte informatique). Pour les personnels extérieurs à l'Observatoire de Paris (ex agents CNRS), ce rôle incombe aux administrateurs des départements.

1.7.10 Le Service Juridique

Le service juridique s'assure que les mesures de la politique de sécurité sont conformes aux exigences réglementaires et doit être particulièrement vigilant afin d'inclure les clauses de sécurité dans les documents, contrats, conventions, etc., impliquant un accès au SI par des tiers.

1.7.11 Les Utilisateurs du SI

Toute personne ayant un accès au système d'information de l'établissement est responsable du respect des règles de sécurité des outils mis à sa disposition et des données qu'elle manipule. Elle se doit de se conformer à la charte informatique annexée au règlement intérieur de l'établissement et d'informer les RSSI(-S) des incidents de sécurité dont elle serait témoin (vol de document, vol de poste de travail, divulgation de données à caractère personnel, usurpation d'identité, etc.).

2 Mise en œuvre de la PSSI

La PSSI de l'établissement affiche un ensemble de principes d'ordre organisationnel et technique à caractère prioritaire. Ces principes sont explicités, voire complétés, dans le cadre d'instructions ou dispositions techniques dont la responsabilité d'élaboration, de diffusion et d'information relève de la chaîne fonctionnelle SSI.

2.1 Organisation - Responsabilités

2.1.1 Responsabilité des différents acteurs

Les acteurs intervenant en matière de sécurité des systèmes d'information doivent être informés de leurs responsabilités en matière de SSI. Dans l'exercice de leur activité, ils sont liés à leur devoir de réserve voire à des obligations de secret professionnel. La Présidence de l'Observatoire, la Direction Générale des Services, le RSSI ainsi que les suppléants relèvent du droit d'en connaitre.

2.1.2 Évolution de la PSSI

La PSSI est revue annuellement, ou chaque fois qu'un changement majeur dans le contexte de l'établissement l'imposerait (évolution du système d'information, des besoins de sécurité et des risques identifiés). La version modifiée est soumise pour approbation :

- aux CSSI
- aux RSSI(-S)
- au service juridique
- au DPD
- au FSD
- à la Commission du Numérique de l'Observatoire de Paris
- à la présidence.

En l'absence de retour dans un délai d'un mois les modifications seront supposées acceptées. Tous les 3 ans la PSSI sera proposée au Conseil d'Administration.

Pour demander une modification de celle-ci vous pouvez vous rapprocher de votre service informatique de proximité ou de la DIO.

2.1.3 Plan d'actions

Les RSSI(-S) élaborent les plans d'actions nécessaires à la mise en œuvre de la PSSI. Ceux-ci seront fournis au FSD pour vérifier que les moyens mis en œuvre sont en adéquation avec les besoins de la PPST. Après validation, les moyens financiers seront assurés par la présidence de l'Observatoire de Paris. Les RSSI(-S) assurent la coordination de la mise en œuvre des plans d'actions et rendent compte régulièrement.

2.1.4 Poste clé de la SSI

Les personnes occupant les postes clés de la SSI (RSSI, administrateurs des SI, chargés SSI, etc.) ainsi que les postes dits de confiance (manipulant des informations sensibles) doivent être régulièrement sensibilisés aux devoirs liés à leur fonction. L'aptitude à respecter les règles de sécurité doit être prise en considération lors du recrutement du personnel. La fiche de poste doit également préciser la sensibilité SSI, les risques SSI et la protection du patrimoine et potentiel scientifique et technique liés à ces postes :

- biens sensibles concernés et mesures spécifiques ;
- activités sensibles et règles à suivre ;
- engagement de confidentialité sur les informations accédées.

2.1.5 Accès aux ressources informatiques

La mise à disposition d'un utilisateur (personnel universitaire titulaire ou contractuel, CNRS, étudiant, émérite, VLD, ...) de moyens informatiques doit être formalisée à l'arrivée, au changement de fonction et au départ de l'intéressé.

L'accès aux ressources doit être contrôlé (identification, authentification) et adapté au droit à en connaître de l'utilisateur (droits et privilèges, profil utilisateur). Il conviendra de fermer les accès dès lors que ceux-ci n'ont plus de raison contractuelle.

2.1.6 Charte informatique

Préalablement à son accès aux outils informatiques, l'utilisateur doit prendre connaissance des droits et devoirs que lui confère la mise à disposition par sa composante de ces outils. Cette information se fait au travers de la « charte informatique » intégrée dans le règlement intérieur de l'Observatoire. L'acceptation du contrat de travail implique l'acceptation du règlement intérieur et de la charte informatique intégrée à celui-ci. En l'absence de contrat de travail la charte doit être signée par l'utilisateur par exemple dans le cadre d'une collaboration.

2.1.7 Cyber surveillance

La sécurité des systèmes d'information exige de pouvoir surveiller le trafic sur le réseau et tracer les actions effectuées. Les dispositifs mis en œuvre doivent être conformes à la réglementation en vigueur et respecter les principes de proportionnalité (adaptation du niveau des moyens à l'enjeu effectif de la sécurité) et de transparence (information des partenaires sociaux et utilisateurs).

2.1.8 Mouvement de personnel

Des procédures relatives aux arrivées, mutations et départs des personnes sont élaborées en collaboration par les directions concernées.

Ces procédures définissent a minima les principes de la gestion du cycle de vie des comptes numériques, des droits d'accès aux ressources du système d'information, du contrôle d'accès aux locaux, des équipements mobiles. Tout mouvement doit être signalé au service informatique afférant. Il revient au service des ressources humaines de s'assurer de l'harmonisation des ces procédures.

En cas de mouvement d'un personnel d'un poste à un autre, celui-ci perd automatiquement, à la date de sa nouvelle affectation, les droits d'accès aux applications métier conférés par le poste qu'il occupait, sauf demande formelle du directeur de la structure de départ, sur un temps limité et sous réserve d'accord du CSSI ou des RSSI(-S).

Les comptes informatiques doivent avoir une durée limitée et à plus forte raison pour les comptes ayant des privilèges. L'ANSSI recommande une durée de 1 à 3 ans. En l'absence de relation contractuelle entre l'utilisateur et l'Observatoire de Paris, tout compte informatique doit être clos. Toute dérogation doit être validée par le CSSI ou le directeur d'unité.

2.2 Gestion des biens

2.2.1 Inventaire des ressources

L'ensemble des ressources informatiques (applications, serveurs, équipements réseau, postes de travail, smartphones, imprimantes, téléphones IP et de façon générale tout équipement sous la responsabilité de l'établissement) fait l'objet d'un inventaire, accessible aux RSSI(-S), à la DIO et aux responsables de structure pour le parc qui les concerne. Chaque nouveau projet ou acquisition entraîne l'inventaire des ressources associées. Il conviendra de contrôler périodiquement cet inventaire afin d'en garantir la cohérence. La réalisation de l'inventaire et son maintien à jour incombent aux services informatiques de proximité. Pour l'UAR, ce rôle revient à la dio.

2.2.2 Appartenance du matériel

Le matériel informatique appartient à la tutelle l'ayant financé. Il doit donc :

- être comptablement référencé par l'acquéreur
- être restitué au départ de l'agent.

Dans le cas d'un mouvement de personnel celui-ci peut "bouger" avec son matériel sous réserve que :

- le directeur de la structure de départ accepte
- que le service comptable de la structure de départ l'accepte, retire le poste informatique et traçe la structure bénéficiaire
- que le directeur de la structure d'accueil l'accepte
- que le comptable de la structure d'accueil intègre le matériel dans son inventaire.

2.2.3 Envoi en maintenance et mise au rebut

Avant tout envoi en maintenance d'un matériel, les données sensibles doivent être effacées. Il appartient aux propriétaires des données de prévenir en cas de risques sur la sensibilité de celles-ci.

Les supports de données sont effacés avant la mise au rebut de tout matériel.

Les opérations de chiffrement et d'effacement doivent faire appel à des produits qualifiés ou respecter les procédures établies. Dans l'hypothèse de données sensibles, l'effacement consiste en la suppression des données de telle façon qu'elles ne puissent être récupérées par aucun moyen d'aucune sorte.

Dans le cas où le matériel n'est plus utilisable comme une carte mère hors service, et que le support contenant les données n'est pas amovible, il n'est dès lors plus possible d'effacer les données. Si le média était chiffré, celui-ci peut être envoyé en maintenance ou mis au rebut dans l'état. Si celui-ci contient des données non chiffrées. Il faut alors confier la réparation à un centre agréé « données sensibles », ou procéder à la destruction mécanique avant la mise au rebut.

2.2.4 Lutte contre les codes malveillants

Un anti-virus doit être déployé sur l'ensemble des serveurs (si possible) et postes de travail de l'établissement par les équipes techniques de la DIO ou des services informatiques des départements et instituts. L'accès à l'antivirus pour les postes de travail est fourni par l'établissement. Les mises à jour des bases antivirales et des moteurs anti-virus sont déployées automatiquement. Les évènements de sécurité de l'anti-virus sont envoyés à un serveur central pour analyse statistique et détection des problèmes a posteriori. Les équipes techniques analysent régulièrement les journaux du serveur central pour détecter au plus tôt un éventuel problème.

2.2.5 Périmètre des postes de travail et périphérique personnel

Est considéré comme poste de travail personnel tous les équipements non financés par l'Observatoire de Paris, ou une de ses tutelles, et n'étant pas affectés à un personnel de l'établissement. Seul le réseau sans fil EDUROAM est accessible si le titulaire possède un compte sur ce réseau. Un compte «invité» à accès restreint est possible pour une durée limitée, il conviendra de se rapprocher du service informatique de proximité afin de pouvoir en bénéficier. Les postes personnels sont interdits dans les ZRR. Il est à noter également que les équipes informatique n'interviendront pas sur ces équipements.

2.2.6 Support amovible

Les supports amovibles type clé USB ou SSD/disques durs externes, représentent un risque non négligeable (code malveillant, vol de données, destruction de matériel, etc.), leur utilisation requiert la plus grande vigilance et nécessite quelques précautions :

- ne jamais brancher un support amovible non connu sur un poste de travail ;
- avoir un anti-virus à jour permettant l'analyse des fichiers contenus et/ou exécutés ;
- dans la mesure du possible dédier un poste de travail pour la récupération des documents sur clés USB (reprographie, bibliothèque, salles pédagogiques, etc.) ;
- tout périphérique amovible doit être chiffré.

2.3 Protection des données

2.3.1 Disponibilité, confidentialité et intégrité des données

Le traitement et le stockage des données numériques, l'accès aux applications et services et les échanges de données entre systèmes d'information doivent être réalisés selon des méthodes visant :

- à prévenir la perte ;
- à s'assurer de l'intégrité des données ;

- à s'assurer de la bonne utilisation des données ;
- à se prémunir de toute divulgation possible des données principalement celles à caractère sensible.

Une sauvegarde régulière des données avec des processus de restauration régulièrement validés doit être mise en place. On distinguera les sauvegardes de production (par exemple, restauration d'une donnée) des sauvegardes de secours (par exemple, reprise des services sur des moyens externes suite à incident majeur). Une étude fine des données (criticité, volatilité, fluctuation...) permettra de définir la périodicité et le type de sauvegarde ainsi que la durée de rétention dans le respect des législations en vigueur.

2.3.2 Protection des données sensibles

Le stockage et la transmission de données « classifiées de défense » sont interdits sauf utilisation de moyens spécifiques agréés au niveau national. L'habilitation est nécessaire pour accéder à un document classifié. Les données non classifiées mais présentant un caractère sensible doivent être identifiées et le cas échéant repérées selon un niveau de sensibilité ; il sera procédé régulièrement à un réexamen de la sensibilité des données. Ces données devront faire l'objet d'une protection au niveau du contrôle d'accès (authentification et contrôle d'autorisation), du traitement, du stockage ou de l'échange (chiffrement) pour en assurer la confidentialité. Avant toute cession ou mise au rebut d'un matériel ayant contenu des données sensibles, il est nécessaire de s'assurer que toutes les données ont bien été effacées par un procédé efficace et selon les recommandations techniques nationales. Si cela s'avère impossible les supports concernés devront être détruits.

2.3.3 Protection des informations

Les données professionnelles sont de préférence stockées sur les espaces centralisés dédiés à cet usage (serveur de fichiers) proposé par l'établissement ou les tutelles. Les données scientifiques étant d'un volume de stockage conséquent ne sont pas sauvegardées automatiquement, il conviendra de s'assurer, si besoin est, qu'elles sont bien sauvegardée en prenant contact avec la DIO. Dans le cas où des données sont stockées sur le poste de travail, l'utilisation de la solution de sauvegarde de l'établissement est obligatoire.

Dans le cas particulier d'un poste de prêt, les données doivent être supprimées avant sa restitution. Le poste sera réinstallé entre deux prêts et toutes les données seront détruites à l'exception des postes prêtés dans le cadre des visios ou des présentations. La réaffectation d'un poste de travail entraine obligatoirement sa réinitialisation.

Toute utilisation d'outils ou services externes tels que Google docs, Google Forms, Google Agenda, Gmail, etc. qui conduisent à faire transiter ou à déposer des informations professionnelles et/ou pédagogiques hors des supports et des services offerts par l'université, engage la responsabilité de celui qui les utilise. Leur utilisation est proscrite dans l'enseignement et la recherche. En effet,

ces pratiques présentent un risque de vulnérabilité particulier du point de vue, d'une part, de la confidentialité des données, et d'autre part, de la PPST, mais également des libertés individuelles. Tous les outils ou supports de stockage relevant du Cloud Act sont interdits car la confidentialité des données n'est pas assurée.

2.3.4 Courriel

La redirection automatique des courriels vers une messagerie externe est à proscrire. Une tolérance existe pour une redirection vers un organisme de l'enseignement et la recherche tel qu'une université partenaire ou le CNRS. Toute redirection vers un organisme dépendant du Cloud Act (ex gmail) est formellement interdite. La perte de courriel liée à la redirection ne peut être imputée à l'établissement. Certains fournisseurs détectent le rebond et pénalisent le courriel, il peut alors être considéré comme spam voire même être détruit.

2.3.5 Stockage type Cloud

La DIO et le CNRS mettent à disposition des utilisateurs un espace de stockage dématérialisé, respectivement Share et MyCore. Il est interdit d'utiliser des services équivalents relevant de droit non souverain (Dropbox,...). Dans le cas ou ce type de produit est imposé par un accord de recherche, les CSSI ou les RSSI(-S) doivent en être informés. Les données doivent alors être placées dans un conteneur chiffré afin d'en garantir la confidentialité.

2.3.6 Données à caractère personnel

Dans le cadre de la loi, le DPD représente la Commission Nationale Informatique et Libertés (CNIL) dans l'établissement. Toute personne mettant en œuvre un traitement de données au sein de l'établissement doit prendre contact avec celui-ci impérativement dès la phase de conception du projet et avant sa mise en œuvre. Constitue un traitement de données à caractère personnel, toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. Les traitements de données susceptibles de contenir des informations à caractère personnel (au sens de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés) doivent faire l'objet des formalités requises de déclaration ou de demande d'autorisation auprès de la CNIL. Les données à caractère personnel constituent des données sensibles et comme telles doivent faire l'objet de protection. Il conviendra de limiter au strict nécessaire toute collecte et rétention de données personnelles, d'en informer l'utilisateur et notamment sur l'utilisation faite de celles-ci.

2.3.7 Accès aux données utilisateur

L'accès aux données d'un utilisateur que ce soit sur le poste de travail, sa messagerie, share, etc., par une tierce personne telle que son responsable hiérarchique n'est possible qu'après avoir recueilli le consentement par écrit de l'utilisateur. Pour des raisons de service et si l'utilisateur n'est pas ou plus joignable, une dérogation peut être accordée. Il conviendra alors de fournir, dans la mesure du possible, uniquement l'information nécessaire au supérieur hiérarchique après accord du DPD et du CSSI ou des RSSI-(S). À titre d'exemple, l'accès complet à la boite mail d'un utilisateur sauf accord de celui-ci est à proscrire, la boite mail pouvant contenir des informations professionnelles à caractère strictement personnel telles que les données médicales (médecine du travail). Plutôt que fournir un accès complet à la boite courriel, il est préférable d'expliquer de quel élément le service a besoin. Cet élément sera alors recherché et fourni au supérieur hiérarchique dans la mesure des moyens humain et technique. L'utilisateur doit être notifié de cet accès, il pourra alors prendre contact avec le DPD, le CSSI ou les RSSI(-S) dès son retour.

2.3.8 Chiffrement

Le chiffrement, en tant que moyen de protection, est obligatoire pour le stockage et l'échange de données sensibles. Les postes de travail fixes et à plus forte raison nomades, doivent obligatoirement être chiffrés. Le télétravail sur un poste non chiffré n'est pas autorisé. Les produits matériels et logiciels utilisés pour le chiffrage doivent faire l'objet d'un agrément par l'ANSSI. Une copie des clés permettant de restituer les données en clair doit être stockée dans un lieu sécurisé (ex coffre fort numérique du service informatique).

2.3.9 VPN

L'établissement fournira un service VPN qu'il conviendra d'utiliser en priorité pour les accès distants. Le serveur VPN sera maintenu à jour par la DIO conformément aux recommandations de l'ANSSI. Le client VPN sera maintenu à jour par l'équipe en charge du maintien en condition opérationnelle du poste de travail. Pour que le VPN fonctionne correctement et dans des conditions de sécurité optimale, le client devra obligatoirement être à jour, à défaut le service pourra être suspendu. Dans le cadre du télétravail, le client VPN doit être obligatoirement installé et le poste de travail doit être chiffré.

2.4 Sécurisation du Système d'information

2.4.1 Administration des serveurs

L'administration des serveurs de l'établissement est placée sous la responsabilité des administrateurs systèmes et réseaux de la Direction Informatique de l'Observatoire de Paris (DIO). L'administration des serveurs des départements

et instituts est placée sous la responsabilité de leur administrateurs systèmes et réseaux.

Chaque administrateur est responsable de la sécurité du poste de travail à partir duquel il administre les ressources du SI dont il a la charge. Il évitera toute pratique à risque qui pourrait le compromettre.

L'accès aux outils et interfaces d'administration doit être strictement limité aux personnes habilitées.

Selon le principe du « moindre privilège », une session de travail doit s'effectuer avec un compte sans privilège. Les privilèges d'accès administrateur ne doivent être utilisés que pour réaliser des tâches d'administration le nécessitant.

L'ANSSI recommande de séparer le poste utilisateur, du poste permettant l'administration des serveurs. Il est également recommandé de mettre en place une authentification forte de type double facteur pour les accès aux SI critique ou SI à régime restrictif.

2.4.2 Chiffrement des serveurs

Dans la mesure du possible, les serveurs doivent être chiffrés, une tolérance existe pour les équipements se trouvant dans des salles sécurisées à accès authentifié et contrôlé.

2.4.3 Administration des postes de travail

L'administration des postes de travail de l'UAR2201 est placé sous la responsabilité de la DIO. L'administration des postes de travail individuels des départements et instituts est placée sous la responsabilité des administrateurs systèmes et réseaux internes.

L'administration des postes par les utilisateurs eux-mêmes doit demeurer l'exception et être justifiée en termes de besoins et de compétences. Dans cette hypothèse, les services informatiques sont déchargés de la responsabilité de la gestion du poste de travail et l'utilisateur s'engage à respecter les directives de configuration en termes de sécurité demandées par les RSSI(-S) les CSSI et les PSSI des tutelles concernées.

Les administrateurs systèmes et réseaux de l'établissement peuvent intervenir à distance pour des opérations de maintenance sur le poste de travail d'un utilisateur de leur périmètre sous réserve de l'en avoir averti en amont et en respectant les principes de la loi Informatique et Libertés.

Selon le principe du « moindre privilège », une session de travail doit s'effectuer avec un compte sans privilège. Les privilèges d'accès administrateur ne doivent être utilisés que pour réaliser des tâches d'administration le nécessitant.

Le compte administrateur local est strictement réservé aux services informatiques en charge de la gestion du poste de travail.

2.4.4 Sécurisation des postes de travail et des moyens nomades

La sécurisation des postes de travail et des moyens nomades est placée sous la responsabilité des administrateurs systèmes et réseaux respectifs. L'accès aux postes de travail et moyens nomades doit être protégé par un mot de passe suffisamment robuste ; chaque mot de passe est personnel et confidentiel et, à ce titre, il ne doit pas être divulgué à un tiers, quel qu'il soit, ni laissé sans protection (post-it, carnet de mot de passe, etc.). Les utilisateurs veillent au bon déroulement des applicatifs de sécurisation installés sur les moyens informatiques mis à leur disposition : mises à jour effectives de l'anti-virus, du système d'exploitation et des applications présentes, remontée des dysfonctionnements et incidents auprès du chargé de sécurité de leur département et institut. En particulier, les utilisateurs prendront des mesures spécifiques adaptées en cas d'utilisation des moyens nomades en dehors de leur zone de sécurité (protection contre le vol, chiffrement...).

Il conviendra d'utiliser les connexions sécurisées de l'établissement ou à défaut de son département ou institut (type VPN) lors d'utilisation des moyens nomades.

2.4.5 mise à jour des systèmes et des logiciels

Une procédure de suivi et d'application des correctifs de sécurité pour le périmètre des serveurs, et celui des postes de travail doit être définie et mise en œuvre. Une bonne pratique consiste à mettre en place un système de mises à jour automatique. Dans le cas où cette recommandation n'est pas possible, il revient à l'administrateur du service ou du serveur de définir la procédure. Le processus de gestion des correctifs est adapté suivant les contraintes et le niveau d'exposition des systèmes. Les systèmes obsolètes doivent être migrés vers une version pour laquelle l'éditeur assure le support et la diffusion des correctifs. A défaut, les systèmes devront être répertoriés par les équipes techniques de la DIO ou des services informatiques des départements et instituts et isolés du reste du SI.

L'ANSSI et Renater ont délégation pour analyser l'état face au risque cyber de tout périphérique de l'établissement visible sur l'extérieur. Pour les services non visibles de l'extérieur la DIO et les RSSI(-S) utilisent des outils de détection similaires.

2.4.6 Contrôle d'accès numérique

Tout accès au système d'information est soumis à l'identification et authentification du demandeur et au contrôle de ses autorisations/habilitations. L'authentification doit se faire, dans la mesure du possible, au travers de l'annuaire LDAP de l'établissement. Il importe de bien définir les autorisations et de n'attribuer que les privilèges nécessaires. Les accès doivent être journalisés. L'utilisation de comptes partagés ou anonymes doit demeurer l'exception et être justifiée en termes de besoins. L'attribution et la modification des accès et privilèges d'un service doivent être validées par le propriétaire du service. Pour les services sensibles, un inventaire régulièrement mis à jour sera dressé.

Les applications manipulant des données particulièrement sensibles doivent permettre une gestion fine des accès des utilisateurs et privilégier une authentification forte.

Le processus d'autorisation d'accès à une ressource informatique est formalisé et s'appuie sur les procédures relatives aux arrivées, mutations et départs des personnes.

2.4.7 Contrôle d'accès physique

Des procédures relatives à l'attribution, révocation des habilitations d'accès aux locaux et à la délivrance, restitution des cartes, badges, clés, etc. sont élaborées par le PSIS. La validation du PSIS et du FSD ou du FSDA est obligatoire pour tout accès d'une personne extérieure. Les habilitations d'accès aux locaux sont revues a minima une fois par an. Les badges d'accès aux salles serveurs doivent être validées par le directeur de la DIO ou le responsable des salles serveurs.

2.4.8 Gestion des authentifications

Les informations d'authentification, comme les mots de passe, sont considérées comme des données sensibles. Elles doivent être conservées de manière sécurisée, et ne doivent être ni stockées, ni transitées en clair sur les réseaux.

Sauf contrainte technique particulière, l'accès aux différentes ressources informatiques de l'établissement doit être basé sur une authentification centralisée utilisant les comptes numériques délivrés par la DIO, et automatiquement désactivés, selon le cycle de vie défini par l'établissement.

Le cycle de vie des comptes locaux doit être formalisé et suivi. En particulier, chaque compte local accédant à une ressource doit être créé avec un mot de passe initial fort respectant les règles de gestion de mots de passe de l'établissement et doit être supprimé au départ de l'utilisateur.

Il est recommandé d'utiliser une application de gestion des mots de passe labellisé par l'ANSSI telle que Keepass. Il est de plus recommandé de changer les mots de passe annuellement.

Ex de bonne pratique en matière de gestion des mots de passe :

- utiliser des mots de passe robustes (3 casses, 10 caractères voire plus pour les comptes sensibles)
- les changer régulièrement
- ne pas les partager
- ne pas les laisser trainer, ne pas les inscrire sur un post-it ou dans un carnet qui pourrait être accessible ou visible
- utiliser un coffre fort type Keepass
- utiliser un mot de passe différent pour chaque service et surtout pour les sites web externes
- éviter les informations personnelles

- toujours modifier les mots de passe par défaut.

Pour un mot de passe sans droit particulier, il n'est pas nécessaire d'imposer une durée maximale, même si celle-ci est recommandée. En revanche pour un accès ouvrant des droits une durée limite de 1 a 3 ans est une bonne pratique préconisée par l'ANSSI dans son guide « Recommandations relatives à l'authentification multifacteur et aux mots de passe » version 2021.

2.4.9 Gestion des authentifiants d'administration

L'administration des postes de travail et serveurs doit se faire en utilisant des comptes d'administration nominatifs et non les comptes d'administrateur locaux.

Les identifiants d'administration génériques non nominatifs font l'objet d'un séquestre auprès des RSSI(-S). Cette démarche a pour but d'assurer la continuité d'activité, en cas de décès ou d'absence prolongée de la personne les détenant. Les CSSI assurent les séquestres de leur périmètre respectif. Le séquestre doit s'effectuer dans un coffre fort numérique recommandé par l'ANSSI ou un conteneur chiffré. Le séquestre ne peut être hébergé à l'extérieur.

Les comptes de services créés pour des besoins applicatifs, sont cartographiés afin de maitriser leur utilisation et font l'objet d'une restriction des droits selon le principe du moindre privilège.

Les comptes de services et d'administration sont désactivés et supprimés dès lors que leur existence n'est plus utile et font l'objet d'une revue annuelle, a minima.

Le cycle de vie des comptes d'administration ne suit pas celui des comptes utilisateurs. En effet, la fermeture d'un compte d'administration est immédiate et intervient le jour même du départ de l'administrateur. Les mots de passe génériques auxquels il avait accès sont également immédiatement changés.

Cas particulier pour les domaines windows :

une politique de gestion des comptes du domaine est documentée et appliquée. Les groupes « Administrateurs de l'entreprise » et « Administrateurs du domaine » sont restreints au maximum et ne sont accessibles qu'aux seuls personnels administrant le domaine.

2.4.10 Sécurité des salles serveurs

Dans le cas où les locaux seraient mutualisés entre plusieurs entités, un découpage en zone est à réaliser.

Dans le cadre d'hébergement de tiers, une convention de service définissant les responsabilités des différentes parties doit être établie.

Les locaux bénéficient d'une procédure de surveillance adaptée ainsi que d'un contrôle d'accès permettant une traçabilité. Les locaux les plus sensibles doivent disposer d'un système d'alarme et de vidéoprotection. Les accès physiques de

ces locaux sont sécurisés notamment en minimisant les ouvertures sur l'extérieur, en les équipant de barreaux, grilles, volets, etc.

Les locaux disposent des équipements d'infrastructure (climatisation, équipement de protection incendie, alimentation électrique ...) correctement dimensionnés, adaptés à la spécificité de l'usage qu'il en est fait (notamment datacenter) et présentant dans la mesure du possible une redondance suffisante. Ces équipements sont couverts par des contrats de maintenance et si nécessaire par des contrats de service pour en assurer l'exploitation. Des procédures de réaction en cas de panne ou d'incident sont formalisées, connues du personnel et vérifiées annuellement.

2.4.11 SI de sureté

Le SI de sûreté regroupe :

- les services support des activités de contrôle d'accès et de détection d'intrusion ;
- les services support des activités de vidéoprotection ;
- les services support de la gestion technique des bâtiments ;
- les services support de la sécurité incendie.

Tous les éléments composant le SI de sûreté doivent faire l'objet de mesures de sécurité spécifiques.

Dans le cas particulier de la vidéoprotection, un système de gestion centralisée est préférable à plusieurs systèmes autonomes. Les procédures de gestion de celui-ci définissant les rôles de chacun sont établies et suivies. La rétention des données est effectuée sur une fenêtre glissante d'un mois et les vidéos sont conservées sur un système isolé dont l'exploitation est restreinte aux seules personnes habilitées.

2.4.12 Sécurité des applications

La sécurité doit être prise en compte à toutes les étapes d'un projet, interne ou externe, lié au système d'information de l'établissement. Pour cela, un dossier de sécurité doit accompagner chaque projet et préciser les objectifs, les méthodes et les mesures préconisées. En particulier, les applications informatiques de gestion et les applications internet doivent être sécurisées, en cohérence avec la sensibilité des informations traitées et échangées. Chaque dossier de d'homologation de sécurité doit être rédigé et ou approuvée par les RSSI(-S) conformement au décret 2022-513 du 8 avril 2022 et signé par l'autorité compétente qui en accepte le risque (AQSSI). Pour chaque application nouvellement installée, une attention particulière sera portée :

- aux données utilisateurs relevant du RGPD. En cas de doute le DPD doit être consulté ;
- à la documentation ;
- à son référencement dans la cartographie du SI ;
- à la conformité avec le plan de continuité et/ou de reprise d'activité ;

- aux suivi des mises à jour et de préférences automatiques dans le cadre d'un service exposé à l'extérieur ;
- aux flux entrants et sortants nouvellement créés ;
- aux risques cyber ;
- au chiffrement des protocoles de communication.

2.4.13 Développement spécifique via une prestation

Si le développement est confié à un prestataire, des clauses SSI doivent être intégrées dans le contrat le liant à l'établissement. Le prestataire s'engage, notamment, à respecter les règles de développement qui s'imposent aux développeurs internes. Règles de développement préconisées :

- avoir suivi une formation (au minimum être sensibilisé) au développement sécurisé afin d'éviter les vulnérabilités classiques ;
- s'engager à suivre les règles de bonnes pratiques publiées par l'OWASP et l'ANSSI ;
- utiliser des outils de développement permettant de minimiser les erreurs introduites durant le développement (utilisation de bibliothèques, contrôle des données en entrée, analyse de code, chiffrement des mots de passe stockés) ;
- rédiger une documentation technique permettant la reprise du développement par un autre développeur ;
- mettre à disposition de la DIO ou du service informatique de proximité les sources de l'application ;
- réduire l'adhérence de l'application vis-à-vis de l'environnement sur lequel elle repose, il est nécessaire de pouvoir faire évoluer l'environnement en cas de découverte de vulnérabilités sur celui-ci (version du langage, version du système d'exploitation, version de la base de données, etc.) ;
- mettre en œuvre une gestion fine des rôles concernant l'accès aux données à caractère personnel (DCP) ;
- journaliser les accès et les actions à auditer permettant l'analyse d'une attaque ou d'un dysfonctionnement. Les délais de rétention sont définis selon la sensibilité de l'application et conformément à la législation en vigueur ;
- se conformer au cadre légal et règlementaire relatif à la protection des données personnelles (RGPD, loi Informatique et Libertés modifiée, etc.) ;
- s'engager à maintenir, faire évoluer l'application et corriger les vulnérabilités qui seraient découvertes.

Une homologation de sécurité doit être réalisé avant la mise en production du service.

2.4.14 Développement spécifique en interne

Pour tout développement réalisé en interne, il conviendra également de respecter autant que possible les bonnes pratiques publiées par l'OWASP et l'ANSSI

et de concevoir la sécurité nécessaire au plus tôt. Le maintien en condition opérationnelle et la correction des vulnérabilités de l'application et des éventuelles dépendances doivent être réalisés tout au long du cycle de vie de l'application. Ce rôle revient par défaut au producteur du code. Il est également recommandé de maintenir une documentation à jour.

Une attention particulière sera portée pour toute application :

- visible de l'extérieur ;
- hébergeant des données personnelles ;
- hébergeant des données sensibles.

Il est alors fortement recommandé d'appliquer les mises à jour de sécurité de manière automatisée et de corriger les vulnérabilités dès que possible. Une journalisation et une gestion fine des droits d'accès sont souvent nécessaires pour ces applications.

Dans le cas où le niveau de sécurité minimum ne peut être atteint, une étude sera réalisée afin de réduire le risque, par ex :

- cloisonnement réseau de l'application pour éviter toute latéralisation ;
- mise en place de reverse-proxy ;
- réduction de la surface d'attaque.

Pour toutes questions, vous pouvez vous rapprocher des RSSI(-S) via une demande auprès de la DIO afin d'étudier le risque cyber.

Une homologation de sécurité doit être réalisée avant la mise en production du service. Les développements spécifiques seront prioritaires.

2.4.15 Produit et service labellisés

Lorsqu'ils sont disponibles, les produits ou services labellisés par l'ANSSI doivent être utilisés.

2.4.16 Infogérance et télémaintenance externe

L'infogérance correspond au fait que des sociétés extérieures, chargées de gérer une partie de l'informatique de l'établissement ou d'un département et institut, puissent avoir accès au système d'information depuis l'extérieur ou l'intérieur.

Tout recours à des prestataires extérieurs doit être porté à la connaissance de la DIO ou de son représentant. Des clauses de sécurité issues d'une rapide analyse de risque, doivent être intégrées au cahier des charges de tout projet relatif au SI. Dans le cadre d'un hébergement externalisé, le contrat détaille les mesures prises pour assurer la sécurité des données, et la réversibilité de celles-ci. Dès lors qu'il s'agit de données personnelles, l'hébergement est limité à des entreprises de droit européen, sauf dérogation des RSSI(-S). Une clause de confidentialité est annexée dans les contrats signés avec les tiers, dès lors que la prestation nécessite un accès au SI et/ou à des informations sensibles. Lorsqu'il s'avère qu'un

prestataire sous-traite les données de l'université (hébergement ou maintenance d'un service informatique, intégrateur de logiciel et plus généralement, tout organisme offrant une prestation impliquant un traitement de données pour le compte de l'université...), le prestataire doit présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées. Un contrat ou autre acte juridique est alors signé entre l'université et le sous-traitant (prestataire) et contient les dispositions de l'article 28 du RGPD. Le DPD et le service Juridique sont préalablement consultés pour l'élaboration du contrat. Les intervenants signent la charte informatique de l'établissement et s'engagent à ne pas divulguer les informations dont ils auraient pu prendre connaissance.

L'externalisation de la gestion d'exploitation d'un composant critique pour le système d'information est à proscrire, sauf dispositions de garantie spécifiques et validées au niveau des RSSI(-S), voire la Présidence de l'Observatoire de Paris selon l'importance de l'application.

2.4.17 Réseau

L'administration du réseau de l'établissement est sous la responsabilité exclusive de la composante « Pool of Awesome Network Devices Administrators » (PANDA) rattachée à la DIO. Les systèmes d'information doivent être protégés vis-à-vis de l'extérieur à l'aide de filtres d'accès appliqués sur les équipements en tête de son réseau. Ces filtres s'appliquent tant sur les flux réseau entrants que sur les flux sortants. L'accès direct aux postes de travail depuis l'extérieur est interdit. Il doit obligatoirement passer par des frontales et sas de sécurité.

La politique de définition des filtres d'accès décrivant les flux réseau entrants est systématiquement du type « tout ce qui n'est pas explicitement autorisé est interdit ».

Les serveurs doivent être protégés spécifiquement vis-à-vis des postes de travail et des autres serveurs. On distinguera les serveurs accessibles uniquement à partir du réseau interne (Serveur Interne SI) et ceux accessibles aussi de l'extérieur (Serveur Externe SE). Pour chaque réseau de serveurs, les filtres d'accès, tant sur les flux réseau entrants que sur les flux sortants, sont systématiquement du type « tout ce qui n'est pas explicitement autorisé est interdit ». Les serveurs potentiellement accessibles de l'extérieur feront l'objet d'une surveillance accrue (outils d'analyse des trace, de métrologie...). L'accès depuis l'extérieur aux serveurs par les moyens nomades doivent s'effectuer au travers de connexion sécurisée de type VPN.

Une attention particulière doit être portée aux moyens nomades lors de leur réintégration sur le réseau d'établissement afin d'éviter l'introduction de logiciel malveillant.

Les flux informatique font l'objet d'analyse tant au niveau de l'établissement que de l'ANSSI et du GIP RENATER afin de détecter toute trace d'intrusion. En

cas d'incident, les RSSI(-S) et l'équipe PANDA se réservent le droit de mettre en place toute action qu'ils jugeront nécessaire afin de protéger le SI.

Le déploiement d'équipements réseau (commutateur, borne, vpn, hub, etc.) sur l'ensemble du campus relève exclusivement de la responsabilité de l'équipe PANDA. Ainsi, aucun équipement ne peut être mis sur le réseau de l'établissement sans accord préalable.

Les nouveaux besoins de connexion au réseau nécessitant par exemple l'activation de prise, l'ajout de prise, etc. font l'objet d'une demande formelle à l'adresse admin.dio@obspm.fr Une réponse est apportée dans les meilleurs délais par l'équipe réseau. Les switchs dans les bureaux doivent être manageables, gérés par l'équipe réseau exclusivement et achetés uniquement après demande formelle auprès de la DIO. Ils sont supervisés et ne doivent pas être éteints.

Les équipements réseau sont identifiés et répertoriés et font l'objet d'un document de cartographie.

Les documents de cartographie sont classés comme sensibles et font l'objet d'une protection adaptée. Leur accès est limité aux personnes habilitées.

Les journaux d'audit sont classés comme sensibles, ils sont sauvegardés, protégés et conservés pendant une période satisfaisant les exigences légales.

2.4.18 Réseau sans fil (WiFi)

Le déploiement de bornes et réseaux sans fil (WiFi) sur l'ensemble du campus relève exclusivement de la responsabilité de l'équipe PANDA de la DIO.

L'accès au réseau sans-fil doit faire l'objet d'un contrôle spécifique et n'être accessible qu'après authentification de l'utilisateur.

L'ajout d'un hotspot sans accord préalable de l'équipe réseau est interdit.

2.4.19 Réseau WiFi public

L'utilisation des réseaux sans fil (WiFi) public n'est pas sans risque, il est obligatoire d'avoir un anti-virus à jour, un pare-feu logiciel actif (firewall), il est recommandé de désactiver tout partage de fichier et de consulter uniquement des sites sécurisés (https) ou non sensibles. De plus, afin de sécuriser les échanges sur ce type de réseau, la passerelle d'accès sécurisé (VPN) de l'établissement doit être utilisée.

2.4.20 Accès réseau spécifique

Les accès spécifiques nécessitant des droits particuliers ne sont possibles que sur dérogation dûment justifiée et font l'objet d'une demande formelle étudiée par les équipes techniques de la DIO pour une réponse adaptée.

2.4.21 Locaux techniques réseau

Toutes les prises réseau sont identifiées et localisées et font l'objet d'une cartographie. Une politique concernant le brassage et l'activation des prises réseau est établie et mise en œuvre, conciliant sécurisation de l'accès au réseau et qualité de service aux usagers.

Les accès aux locaux de brassage sont protégés.

Les équipements critiques sont configurés voire redondés pour en assurer la disponibilité. Les activités réseau font l'objet d'une surveillance afin de s'assurer de la disponibilité et de la qualité de service du réseau.

2.4.22 Maintien du niveau de sécurité

Le maintien du niveau de sécurité doit faire l'objet de dispositions techniques sous la responsabilité des RSSI(-S). Ces dispositions doivent intégrer le maintien au cours du temps de l'état de sécurité des différents équipement :

- application des correctifs
- mise à jour des systèmes d'exploitation et des applications
- retrait/remplacement de tout équipement ne bénéficiant plus de correctif de sécurité

Une vigilance particulière sera portée sur tout équipement visible de l'extérieur.

Une surveillance du fonctionnement du système d'information permet de s'assurer de son état de sécurité :

- analyse des journaux ;
- supervision matérielle et applicative ;
- console d'administration anti-virus ;
- vérification des vulnérabilités ;
- analyse de la robustesse des comptes ;
- suivi des avis de sécurité ;
- surveillance des intrusions ;
- surveillance des flux ;
- analyse de compromission ;
- résistance du système d'information ;
- etc.

2.4.23 Modification du SI

Tous changement opérationnel du SI de l'établissement est sous la responsabilité du directeur de la DIO. Celui-ci doit s'assurer :

- du respect des règles de sécurité et de développement préconisées ;
- de la validation du bon fonctionnement de l'application ou du matériel par une phase de recette ;

- de la correction des vulnérabilités découvertes par les éventuels tests réalisés (analyse de code, test d'intrusion, recherche de vulnérabilités, etc.) ;
- de l'ajout de l'application ou du matériel à la cartographie du SI ;
- de la déclaration du traitement auprès du DPD et de la réalisation d'une analyse d'impact sur la protection des données si besoin ;
- de l'estimation du niveau de sécurité requis en termes de disponibilité, intégrité et confidentialité ;
- d'une analyse du risque de type EBIOS-RM ;
- de la sécurisation de l'environnement de l'application ou du matériel (plan de mise à jour, supervision, sauvegarde, documentation d'exploitation, etc.).

Il incombe au responsable du déploiement de l'application ou du matériel au sein du SI, de constituer et de transmettre à la DIO, le dossier permettant cette analyse.

2.4.24 Opération de maintenance

Les opérations de maintenance sont documentées, planifiées et annoncées aux usagers.

2.5 Mesure du niveau effectif de sécurité

2.5.1 Contrôle de gestion

Le contrôle de gestion de la sécurité des systèmes d'information s'opère sous la responsabilité des RSSI(-S).

2.5.2 Audit

Le niveau de sécurité des systèmes d'information et la conformité de mise en œuvre des recommandations sur le terrain peuvent donner lieu à des audits sous la responsabilité des RSSI(-S).

Ces audits portent sur les aspects techniques (architecture, systèmes, applications, réseaux, sécurité physique...) et organisationnels (procédures liées à la sécurité, suivi de la sécurité dans les contrats...) mis en œuvre.

Les résultats de ces audits font l'objet d'une analyse et de plans d'actions permettant de réviser, améliorer les procédures et mesures de sécurité mises en œuvre. Le suivi de la mise en œuvre des plans d'action est de la responsabilité de la DIO et/ou des RSSI(-S).

Sous l'autorité des RSSI(-S), de l'ANSSI et du GIP RENATER, des tests de vulnérabilités logiques sont effectués périodiquement sur les services (applications/serveurs) accessibles via internet. Les vulnérabilités identifiées font l'objet de corrections immédiates par les équipes en charge de ceux-ci, aidées si besoin, par des experts du domaine. Le retrait d'un service numérique jugé trop vulnérable peut être envisagé selon les risques encourus par l'établissement.

Les outils d'audit (logiciels ou fichiers de données) ne doivent pas impacter les activités de l'établissement et ne sont accessibles que pour les personnes habilitées. Les outils et résultats des audits sont considérés comme sensibles.

2.5.3 Journalisation

Le système d'information doit comprendre des dispositifs de journalisation centralisés de l'utilisation des services. L'objectif est de permettre de détecter des intrusions ou des utilisations frauduleuses, de tenter d'identifier les causes et les origines, d'éviter des contaminations d'autres sites par rebond. Conformément à la législation française, ces informations peuvent faire l'objet d'une transmission aux autorités compétentes après avis de la Présidence. La durée de conservation des fichiers de traces à des fins de preuve doit être conforme aux lois et règlements en vigueur. Il importe de définir, et de faire connaître aux utilisateurs, les règles d'exploitation des fichiers de traces (contenu, durée de conservation, utilisation) dans le respect du « principe de proportionnalité » et des contraintes législatives et réglementaires concernant notamment le traitement des informations à caractère personnel. Les logs des serveurs sont à conserver 1 an. Il est possible de les conserver plus longtemps dans le cadre d'analyse faisant suite à un incident ou en cas de suspicion d'intrusion. Il conviendra alors de les isoler, d'en restreindre l'accès qui devra être tracé et conserver pendant toute la durée de rétention.

2.5.4 Fichiers de traces

Les fichiers de traces seront systématiquement analysés afin de repérer d'éventuels problèmes et de produire des statistiques et tableaux de bord. Aucune donnée personnelle ne doit apparaitre dans les statistiques ou tableaux de bord.

2.5.5 Posture de sécurité

En matière de sécurité des systèmes d'information, le niveau normal des recommandations faites dans le cadre de la politique interne de SSI correspond aux dispositions du plan Vigipirate. Ces recommandations sont rappelées régulièrement par le FSSI. Les dispositions internes de sécurisation doivent permettre une réactivité suffisante en cas de passage au niveau rouge de mesures propres à la SSI. Le plan d'intervention gouvernemental PIRANET fait l'objet d'exercices destinés à tester la réactivité de la chaîne d'intervention et la faisabilité des mesures préconisées.

2.5.6 Mise en garde

L'utilisation de certains matériels ou logiciels peut s'avérer préjudiciable à la sécurité des systèmes d'information. Ces produits font l'objet de « mises en garde » de la part de la chaîne fonctionnelle SSI (HFDS, FSD, RSSI...), visant soit des recommandations d'utilisation, soit une interdiction pure et simple.

2.5.7 Respect des droits de propriété intellectuelle

Des contrôles sont régulièrement effectués afin de vérifier le respect de la réglementation concernant le téléchargement d'œuvres protégées et l'usage des logiciels. Il est de la responsabilité de l'utilisateur de conserver les preuves d'achat des matériels et logiciels utilisés n'ayant pas été fournis par la DIO, l'établissement ou son service informatique. En cas de manquement caractérisé, des poursuites ou sanctions peuvent être engagées à l'encontre des contrevenants.

2.5.8 Gestion d'incidents

Chaque acteur du système d'information, utilisateur ou administrateur, doit être sensibilisé à l'importance de signaler tout incident réel ou suspecté. Ceci inclut par exemple :

- le vol et pertes de moyens informatiques ou de supports de données ;
- la présence d'un site d'hameçonnage ayant pour finalité l'extorsion de données de l'Observatoire de Paris tel que les comptes utilisateur ;
- une attaque ciblée de filoutage ;
- la divulgation de données ;
- la modification frauduleuse de site web ;
- l'infection d'un équipement par code malveillant ;
- les attaques informatiques;
- tout soupçon de compromission ;
- etc.

Le signalement des incidents à la chaîne fonctionnelle SSI et aux autorités hiérarchiques doit être systématique.

Lorsqu'un incident peut mettre en cause l'ensemble d'un département ou institut, et à plus forte raison si celui-ci est ZRR, ou l'ensemble de l'établissement, les RSSI(-S) informeront les autorités compétentes (HFDS, CERT-RENATER, ANSSI. . .).

Toute infraction susceptible d'implications juridiques fera l'objet d'un dépôt de plainte par le service juridique de l'Observatoire de Paris sous la supervision des RSSI(-S) auprès des autorités compétentes.

Dans le cas d'unités mixtes, il convient d'informer et le cas échéant de se concerter avec les autres tutelles. En cas d'alerte de sécurité identifiée au niveau national, les RSSI(-S) s'assurent de la bonne application des exigences formulées par les instances nationales au niveau de l'établissement dans les meilleurs délais.

En cas d'incident de sécurité suffisamment avéré et constitutif d'une violation de donnée à caractère personnel, les RSSI(-S) documentent l'incident : ils consignent les faits concernant la violation, ses effets et les mesures prises pour y remédier. Ils adressent ensuite cette documentation au DPD concerné afin que celui-ci notifie la violation de données à la CNIL. Dans le cas ou l'incident surviendrait uniquement au niveau d'un département, institut, unité, projet,

sans débordement sur l'établissement et que celui-ci est rattaché à un DPD externe à l'établissement, le recours à ce dernier est à privilégier.

Tout incident de sécurité ayant ou pouvant avoir un impact hors établissement, doit être signalé à la chaine SSI ministérielle.

2.5.9 Processus de gestion des incidents

La gestion des incidents suit le processus suivant : détection / signalement, analyse, diagnostic, résolution, rétablissement du service affecté, validation des mesures correctives, bilan et communication. Selon l'importance de l'incident une fiche de traitement est établie lors de la phase de bilan, afin d'analyser, d'identifier les faiblesses et définir les mesures préventives et correctives permettant d'en limiter la répétition ou les impacts. Les fiches de traitement permettent également d'établir des fiches réflexes mises à disposition des usagers. Les traces et éléments susceptibles de servir de preuve sont conservés et éventuellement transmis au CERT-RENATER pour analyses complémentaires.

2.5.10 Gestion de crise

En cas de crise de nature informatique, le FSD, les RSSI(-S), le directeur de la DIO et la Présidence de l'Observatoire doivent être informés dès le déclenchement. Suivant la gravité et en cas d'atteinte à la sécurité du système d'information, le HFDS et l'ANSSI seront saisis.

2.5.11 Plan de reprise ou continuité d'activité (PCA/PRA)

L'observatoire de Paris doit définir un plan de continuité d'activité et les procédures correspondantes. Chaque département doit annexer à ce plan les spécificités propres à leurs activités. Ce plan doit permettre dans un premier temps de maintenir les activités critiques éventuellement en mode dégradé. Le plan sera complété par un plan de reprise d'activité permettant de récupérer et restaurer toutes les fonctionnalités du système d'information dans un délai raisonnable. L'infrastructure de stockage et de sauvegarde doit reposer sur une architecture dédiée. Il conviendra de tester le bon fonctionnement de la sauvegarde périodiquement pour s'assurer que les données soient effectivement récupérables à partir de celle-ci.

Les équipes techniques définissent l'architecture et les mesures techniques et organisationnelles à mettre en œuvre. Elles rédigent les procédures opérationnelles nécessaires à la mise en œuvre du PCA/PRA

La pertinence et l'efficacité du PCA/PRA/Sauvegarde doivent être testées et validées au minimum une fois par an dans le cadre d'exercices.

Il revient à la DIO de rédiger, adapter, tester les plans de reprise ou continuité d'activité.

3 Glossaire

- ANSSI Agence Nationale de la Sécurité des Systèmes d'Information
- AQSSI Autorité Qualifiée pour la SSI (président de l'établissement)
- CERT-RENATER Centre d'alerte et de réaction aux attaques informatiques des membres du groupement d'intérêt public RENATER
- CA Conseil d'administration
- CISCO Commission informatique des services communs de l'Observatoire
- CIL Correspondant Informatique et Liberté (fonction remplacée par le DPD)
- CNIL Commission nationale de l'informatique et des libertés
- CNO Commission numérique de l'Observatoire
- CSSI Chargé de la Sécurité du Système d'Information
- DCP Données à caractère Personnel
- DGS Directeur Général des Services
- DIO Direction informatique de l'observatoire
- DIL Direction immobilière et logistique
- DPD Délégué à la Protection des données (anciennement CIL)
- DRH Direction des Ressources Humaines
- FSD Fonctionnaire de Sécurité et de Défense
- FSDA Fonctionnaire de Sécurité et de Défense Adjoint
- FSSI Fonctionnaire de la Sécurité des Systèmes d'Information
- GIP Groupement d'Interet Public
- HFDS Haut Fonctionnaire de Défense et de Sécurité
- OWASP Open Web Application Security Project
- PCA Plan de Continuité d'Activité
- PPST Protection du Potentiel Scientifique et Technique de la nation
- PRA Plan de Reprise d'Activité
- PSIS Prôle Sécurité incendie sureté
- PSSI Politique de Sécurité du Système d'Information
- PSSIE Politique de Sécurité des Systèmes d'Information de l'Etat
- RENATER Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche
- RGPD Règlement Européen sur la protection des données
- RSSI Responsable de la Sécurité du Système d'Information
- RSSI-S Responsable de la Sécurité du Système d'Information Suppléant
- RSSI(-S) Ensemble des RSSI et RSSI-S
- SI Système d'Information
- SSI Sécurité du Système d'Information
- VPN Virtual Private Network (tunnel chiffré permettant un accès sécurisé)
- ZRR Zone à Régime Restrictif

3.1 Référence extérieure

`Cloud-Act / Patriot Act / FISA`

- « Le Clarifying Lawful Overseas Use of Data Act ou CLOUD Act (H.R. 4943) est une loi fédérale des États-Unis adoptée en 2018 sur l'accès aux données de communication (données personnelles), notamment opérées dans le Cloud. Elle modifie principalement le Stored Communications Act (en) (SCA) de 1986 en permettant aux instances de justice (fédérales ou locales, y compris municipales 1) de contraindre les fournisseurs de services établis sur le territoire des États-Unis, par mandat ou assignation, à fournir les données relatives aux communications électroniques des "US Persons" c'est-à-dire des citoyens US ou des résidents US, stockées sur des serveurs, qu'ils soient situés aux États-Unis ou dans des pays étrangers »
- « Le Foreign Intelligence Surveillance Act (FISA) est une loi du Congrès des États-Unis de 1978 décrivant les procédures des surveillances physiques et électronique, ainsi que la collecte d'information sur des puissances étrangères soit directement, soit par l'échange d'informations avec d'autres puissances étrangères. »
- Seul le Cloud-Act est cité dans la PSSI, mais chaque grande puissance possède des textes équivalent notamment la Chine.

`Decret 2022-513`

> « L'homologation de sécurité est une décision formelle prise par l'autorité qualifiée en sécurité des systèmes d'information ou par toute personne à qui elle délègue cette fonction. Elle atteste que les risques pesant sur la sécurité ont été identifiés et que les mesures nécessaires pour maîtriser ces risques sont mises en œuvre. Elle atteste également que les éventuels risques résiduels ont été identifiés et acceptés par l'autorité qualifiée en sécurité des systèmes d'information. »

`decret 2022-634`

> « L'État se dote d'une politique de contrôle et d'audit internes, fondée sur une analyse des risques. »

`Nis2`

> « La directive NIS 2 a été publiée le 27 décembre 2022 au Journal Officiel de l'Union européenne et elle prévoit un délai de 21 mois pour que chaque Etat membre transpose en droit national les différentes exigences réglementaires. »
>
> « L'ANSSI aura la capacité de réaliser des contrôles pouvant amener à des injonctions en cas de non-conformité identifiée »

`IGI 1337`

> « instruction générale interministérielle no 1337/sgdsn/anssi sur l'organisation de la sécurité numérique du système d'information

et de communication de l'état et de ses établissements publics »

`Charte informatique de l'Observatoire de Paris :`

- version française visible en première page du site dio.obspm.fr
- version anglaise. Seule la version française a valeur légale. Version anglaise accessible via dio.obspm.fr/Fichiers/charte/.