

**Université Pierre et Marie Curie  
4 Place Jussieu  
75252 PARIS Cedex 05**

---

**POLITIQUE DE SÉCURITÉ  
DES SYSTÈMES D'INFORMATION**

---

*Version 3.1 (Octobre 2009)*

## Historique des modifications

Version	Date	Objet	Auteur	Statut
1.0	Oct. 2008	Création	jt	Interne pôle SSI
1.1	Oct. 2008	Restructuration	va,sd,jt	Interne pôle SSI
1.2	Nov. 2008	Restructuration	sd	Interne pôle SSI + SG et DSI
1.3	Jan. 2009	Rédaction (suite)	jt	Interne pôle SSI
2.0	Mai. 2009	Restructuration type 27002	jt	Interne pôle SSI
2.3	Juin 2009	Restructuration	sd	Interne pôle SSI
3.0	Juin 2009	1 <sup>ère</sup> version « diffusable »	sd,jt	Costrasi
3.1	Oct. 2009	Finalisation (1)	jt	CSSI, RSSI partenaires

Sources (autorisées) : PSSI CNRS

ISO 27001, 27002 (autorisation en cours)

EBIOS

## SOMMAIRE

### PARTIE 1

Avant-propos .....	7
I. Élaboration d'une PSSI.....	8
I.1. Définitions.....	8
I.2. Sécurité des systèmes d'information : enjeux.....	8
I.3. Méthodologie.....	9
I.3.1. L'expression des besoins de sécurité.....	9
I.3.2. Les critères de sécurité.....	9
I.3.3. Menaces, vulnérabilités et impacts .....	9
I.3.4. Méthodes d'analyse de risques .....	10
I.4. Le traitement des risques .....	10
II. L'UPMC.....	11
II.1. Présentation et missions .....	11
II.2. La chaîne fonctionnelle SSI .....	11
II.3. Système d'Information de l'UPMC .....	12
II.4. Système de Management de la Sécurité de l'Information, certification et PSSI à l'UPMC.....	13
II.5. PSSI d'unité .....	13
II.6. Périmètre de la PSSI d'établissement .....	14
III. Politique de sécurité .....	16
III.1. Politique de sécurité de l'information .....	16
IV. Organisation de la sécurité de l'information .....	17
IV.1. Organisation interne .....	17
IV.1.1. Attribution des responsabilités en matière de sécurité de l'information .....	17
IV.1.2. Système d'autorisation concernant les moyens de traitement de l'information .....	17
IV.1.3. Engagements de confidentialité.....	17
IV.1.4. Relations avec les autorités.....	18
IV.2. Tiers .....	18
IV.2.1. Identification des risques provenant des tiers.....	18
IV.2.2. La sécurité et les clients .....	18
IV.2.3. La sécurité dans les accords conclus avec des tiers.....	19
V. Gestion des biens .....	20
V.1. Responsabilités relatives aux biens .....	20
V.1.1. Inventaire des biens .....	20
V.1.2. Utilisation correcte des biens.....	20
V.2. Classification.....	20
V.2.1. Lignes directrices pour la classification .....	20
V.2.2. Services centraux de l'UPMC : classement « Système vital » .....	21
VI. Sécurité liée aux ressources humaines .....	22
VI.1. Fin ou modification de contrat .....	22
VI.1.1. Responsabilités en fin de contrat.....	22
VI.1.2. Restitution des biens .....	22
VI.1.3. Retrait des droits d'accès.....	23
VII. Sécurité physique et environnementale .....	24
VII.1. Zones sécurisées .....	24
VII.1.1. Contrôles physiques des accès.....	24
VII.1.2. Protection contre les menaces extérieures et environnementales.....	24
VII.2. Sécurité du matériel.....	24
VII.2.1. Protection du matériel.....	24
VII.2.2. Sécurité du matériel hors des locaux .....	25
VII.2.3. Mise au rebut ou recyclage sécurisé(e) du matériel .....	25
VIII. Gestion de l'exploitation et des télécommunications .....	26

VIII.1. Procédures et responsabilités liées à l'exploitation.....	26
VIII.1.1. Procédures d'exploitation documentées .....	28
VIII.1.2. Gestion des modifications.....	28
VIII.1.3. Séparation des tâches.....	28
VIII.1.4. Séparation des équipements de développement, de test et d'exploitation .....	29
VIII.2. Gestion de la prestation de service par un tiers.....	29
VIII.3. Protection contre les codes malveillant et mobile .....	29
VIII.4. Sauvegarde.....	30
VIII.5. Gestion de la sécurité des réseaux.....	30
VIII.5.1. Mesures sur les réseaux.....	30
VIII.5.2. Sécurité des services réseau.....	30
VIII.6. Manipulation des supports .....	31
VIII.7. Échange des informations .....	31
VIII.7.1. Accords d'échange.....	31
VIII.7.2. Supports physiques en transit.....	32
VIII.7.3. Messagerie électronique.....	32
VIII.8. Services de commerce électronique .....	32
VIII.9. Surveillance .....	32
IX. Contrôle d'accès aux ressources .....	34
IX.1. Politique de contrôle d'accès.....	34
IX.1.1. Enregistrement des utilisateurs .....	34
IX.1.2. Gestion des privilèges.....	34
IX.1.3. Gestion du mot de passe utilisateur .....	35
IX.2. Contrôle d'accès au réseau .....	35
IX.3. Contrôle d'accès au système d'exploitation .....	35
IX.4. Contrôle d'accès aux applications et à l'information .....	36
IX.4.1. Accès aux données sensibles.....	36
IX.4.2. Isolement des systèmes sensibles .....	36
IX.5. Informatique mobile et télétravail .....	36
IX.5.1. Informatique mobile et télécommunications .....	36
IX.5.2. Télétravail .....	37
X. Acquisition, développement et maintenance des systèmes d'information .....	38
X.1. Exigences de sécurité applicables aux systèmes d'information .....	38
X.2. Bon fonctionnement des applications.....	38
X.3. Mesures cryptographiques .....	38
X.3.1. Politique d'utilisation des mesures cryptographiques .....	38
X.3.2. Gestion des clés .....	39
X.4. Sécurité des fichiers système .....	39
X.5. Gestion des vulnérabilités techniques .....	39
XI. Gestion des incidents liés à la sécurité de l'information.....	40
XI.1. Signalement des événements et des failles liés à la sécurité de l'information .....	40
XI.2. Gestion des améliorations et incidents liés à la sécurité de l'information.....	40
XI.2.1. Responsabilités et procédures .....	40
XI.2.2. Collecte de preuves.....	40
XII. Gestion du plan de continuité de l'activité .....	41
XIII. Conformité .....	42
XIII.1. Conformité avec les exigences légales.....	42
XIII.1.1. Identification de la législation en vigueur .....	42
XIII.1.2. Propriété intellectuelle.....	42
XIII.1.3. Protection des données et confidentialité des informations relatives à la vie privée. 42	
XIII.1.4. Mesure préventive à l'égard du mauvais usage des moyens de traitement de l'information .....	43
XIII.1.5. Réglementation relative aux mesures cryptographiques.....	43
XIII.1.6. Conformité des équipements de surveillance.....	43
XIII.1.7. Usage privé résiduel .....	43
XIII.2. Conformité avec les politiques et normes de sécurité et conformité technique.....	44
XIII.2.1. Conformité avec les politiques et les normes de sécurité.....	44

XIII.2.2. Vérification de la conformité technique.....	44
XIII.3. Prises en compte de l'audit du système d'information.....	44
XIV. Annexe générale .....	46
XIV.1. Acronymes .....	46
XIV.2. Vocabulaire SSI .....	47
XIV.3. Contexte SSI .....	48
XIV.3.1. Aspects légaux et réglementaires .....	48
XIV.3.2. Normes et standards : bref historique.....	48
XIV.3.3. Sécurité et Défense.....	48
XIV.3.4. Plan national de prévention et de lutte « Pandémie grippale ».....	49
XIV.3.5. Incitation du ministère de tutelle .....	49
XIV.4. Contexte UPMC.....	51
XIV.4.1. Pilotage SI.....	51
XIV.4.1.1. Le COSTRASI .....	51
XIV.4.1.2. La DSI.....	51
XIV.4.1.3. Le SDSI .....	51
XIV.4.2. Les RSSI.....	52
XIV.4.3. Les CSSI.....	52
XIV.4.4. Le pôle SSI .....	53
XIV.4.4.1. Pilotage PSSI d'unité.....	53
XIV.4.4.2. Conseil et assistance.....	53
XIV.4.4.3. Formation, information, sensibilisation .....	53
XIV.4.4.4. La gestion de la sécurité au quotidien .....	53
XIV.4.4.5. Veille technique et juridique .....	54
XIV.4.4.6. Documentation.....	54
XIV.4.5. Le règlement intérieur et charte d'usage.....	54
XIV.4.6. Les référentiels .....	55
XIV.4.7. La chaîne fonctionnelle SSI : directive 901 .....	55
XIV.5. Critères de sécurité DICT.....	56
XIV.6. Avis et alertes des CERT .....	58
XIV.6.1.1. CERT-Renater .....	58
XIV.6.1.2. CERTA .....	58
XIV.7. Normes ISO/CEI 2700x et EBIOS .....	59
XIV.7.1. 27001 .....	59
XIV.7.2. 27002 .....	59
XIV.7.3. 27005 .....	59
XIV.7.4. EBIOS .....	59
XIV.8. Références .....	60
XIV.9. Référentiel SSI UPMC .....	63
XV. Annexes juridiques .....	64
XV.1. Loi n°78-17 (révisée) relative à l'informatique, aux fichiers et aux libertés dite « Informatique et Libertés ».....	64
XV.2. Légalité des contenus : crime (pédophilie) et délits (injures).....	64
XV.3. Droit d'auteur et propriété intellectuelle .....	65
XV.4. Atteintes aux systèmes de traitement automatisés de données (STAD) .....	65
XV.5. Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique dite « LCEN » .....	66
XV.6. Devoir de discrétion professionnelle.....	66
XV.7. Périmètre d'intervention des administrateurs systèmes et réseau.....	67
XV.8. Usage à titre privé des équipements informatiques mis à disposition par l'établissement ...	67
XVI. Annexes techniques.....	69

# PARTIE 1

DIFFUSION RESTREINTE

*« La Politique de sécurité des systèmes d'information constitue le principal document de référence en matière de SSI. Elle reflète la vision stratégique de l'organisme et montre l'importance qu'accorde la direction à son système d'information.*

*Elle se matérialise par un document présentant, de manière ordonnée, les règles de sécurité à appliquer et à respecter dans l'organisme. Ces règles sont généralement issues d'une étude des risques SSI. »<sup>1</sup>*

## Avant-propos

Le présent document fixe les exigences de sécurité approuvées par la direction de l'Université Pierre et Marie Curie (UPMC) et indique les mesures à mettre en œuvre pour s'y conformer. C'est la « PSSI de l'UPMC ».

Toutes les entités de l'UPMC qui contribuent à la réalisation de ses missions sont concernées : les laboratoires, les départements de formation, les facultés, les instituts, les services transversaux (administration centrale, DSI, Bibliothèques, service médical...), etc.. Les directeurs d'unité s'appuient sur la PSSI d'établissement pour établir une PSSI spécifique à leur laboratoire.

Conformément aux normes ISO 27000 en vigueur dans le domaine de la SSI, la PSSI de l'UPMC aborde les points suivants :

1. Politique de sécurité ;
2. Organisation de la sécurité de l'information ;
3. Gestion des biens ;
4. Sécurité liée aux ressources humaines ;
5. Sécurité physique et environnementale ;
6. Gestion de l'exploitation et des télécommunications ;
7. Contrôle d'accès ;
8. Acquisition, développement et maintenance des systèmes d'information ;
9. Gestion des incidents liés à la sécurité de l'information ;
10. Gestion du plan de continuité de l'activité ;
11. Conformité.

Ces points sont explicités dans la deuxième partie de ce document.

<sup>1</sup> Cf. [http://www.securite-informatique.gouv.fr/gp\\_article51.html](http://www.securite-informatique.gouv.fr/gp_article51.html).

# I. Élaboration d'une PSSI

## I.1. Définitions

Un **Système d'Information (SI)** est défini comme « *un ensemble d'entités (logiciels, matériels, réseaux, locaux, organisation, personnels) organisé pour accomplir des fonctions de traitement d'informations* »<sup>2</sup>.

Erreurs humaines, pannes matérielles, problèmes d'environnement, attaques diverses etc. mettent en évidence –généralement « après-coup »- les vulnérabilités d'un SI. « *La **sécurité des systèmes d'information (SSI)** a pour objet de contrer ces menaces par des mesures proportionnées aux risques pouvant peser sur la confidentialité de l'information, son intégrité, sa disponibilité, la possibilité d'en authentifier la source et de la signer* »<sup>3</sup>.

Une **analyse de risques** (qu'ils soient d'origine interne ou externe) consiste en l'étude fine du contexte et des menaces, des besoins et des objectifs de sécurité.

Une **Politique de Sécurité des Systèmes d'Information (PSSI)** est la conséquence naturelle d'une analyse de risque.

## I.2. Sécurité des systèmes d'information : enjeux

En raison de la dépendance croissante des organismes envers leurs systèmes d'information, la SSI est devenue un enjeu vital. Son objectif est d'assurer la protection :

- du **patrimoine matériel**, composé des biens nécessaires au bon fonctionnement de l'établissement et dont la détérioration pourrait interrompre, diminuer ou altérer son activité (serveurs, réseaux, postes de travail, téléphones...) ;
- du **patrimoine immatériel et intellectuel**, composé de toutes les informations concourant au métiers de l'organisme (processus, applications et données scientifiques, techniques, professionnelles, administratives...) ;
- des **informations relatives aux personnes** (physiques et morales) avec qui l'organisme est en relation, dont la destruction, l'altération, l'indisponibilité ou la divulgation pourrait entraîner des pertes ou porter atteinte à son image de marque voire entraîner des poursuites judiciaires.

Aujourd'hui la SSI existe sous la forme d'une juxtaposition de solutions techniques mais l'absence d'une politique globale de SSI produit un manque de cohérence dans les décisions, une application anarchique de règles purement techniques, des niveaux de protections disparates, la dilution des responsabilités et un manque de lisibilité pour les principaux acteurs qui sont les utilisateurs du système d'information.

En décrivant « *les éléments stratégiques (enjeux, référentiel, principaux besoins de sécurité et menaces) et les règles de sécurité applicables à la protection du système d'information de l'organisme* »<sup>4</sup>, la PSSI, régulièrement révisée pour tenir compte de l'évolution du contexte et des risques, constitue un outil indispensable pour la sensibilisation (prise de conscience des responsabilités, connaissance des risques courants, etc.). Elle nécessite, pour être effective, une large adhésion de l'ensemble des personnels.

<sup>2</sup> EBIOS [DCSSI / SGDN]. Voir <http://www.ssi.gouv.fr/fr/confiance/methodes.html>.

<sup>3</sup> La sécurité des systèmes d'information. Pierre Lasbordes, député. Rapport du 26/11/05.

<sup>4</sup> Cf. <http://www.ssi.gouv.fr/fr/confiance/documents/methodes/pssi-memento-2004-03-03.pdf>.



## I.3. Méthodologie

L'élaboration d'une PSSI nécessite une analyse de risque préalable consistant à établir une cartographie des composants du système d'information afin d'identifier et hiérarchiser les risques en termes de sensibilité vis-à-vis des missions de l'établissement.

### I.3.1. L'expression des besoins de sécurité

Une analyse de risques s'appuie sur les besoins de sécurité associés aux biens de l'organisme au regard des menaces recensées et de leur impact potentiel.

L'inventaire des ressources (serveurs, réseaux, postes de travail, téléphones, données, applications, etc.), leur contribution à une mission essentielle, l'identification des dépendances en relation avec les *workflows*<sup>5</sup> métiers, ont pour but d'exprimer ces besoins sous forme d'objectifs mesurables (exemple : « le serveur web institutionnel peut être indisponible pendant 4 heures maximum, doit être totalement intègre mais ne présente pas d'information confidentielle »).

La législation en vigueur implique, d'autre part, le recensement des traitements informatisés sur les données à caractère personnel et le respect du droit à la vie privée (sécurité juridique).

### I.3.2. Les critères de sécurité

Le choix des mesures de protection à mettre en œuvre est orienté par les critères de sécurité que l'on veut garantir. Ces critères, dits « DICT » d'après leurs initiales, sont :

- la **disponibilité**, qui est la faculté d'accéder, au moment voulu, aux services et données par les utilisateurs autorisés ;
- l'**intégrité**, c'est-à-dire l'état d'un SI n'ayant pas subi de modifications, accidentelles ou délibérées, non autorisées ;
- la **confidentialité**, laquelle consiste à ne divulguer l'information (données, processus, etc.) qu'aux personnes ou entités autorisées ;
- la **traçabilité**, permettant la fourniture d'indices en cas d'incident de sécurité.

Voir à ce sujet l'annexe XIV.5.

### I.3.3. Menaces, vulnérabilités et impacts

On distingue les menaces résultant d'actions volontaires (vol de support, accès illégal, diffusion d'un ver/virus, attaque par déni de service, hameçonnage<sup>6</sup>, pressions diverses, etc.) ou involontaires (erreurs humaines, perte de support, etc.) et celles résultant d'éléments menaçants naturels (incendie, inondation, etc.) ou environnementaux (pannes matérielles, coupures électriques, etc.). En général une menace existe lorsque l'on peut trouver un moyen d'exploiter une vulnérabilité du système (équipement vital non redondé, faille de sécurité, ignorance, pot-de-vin ...).

L'exécution d'une menace peut affecter temporairement ou durablement un SI. Toutes les menaces contre un système d'information peuvent être hiérarchisées selon la gravité de l'impact qui en résulterait. Il faut bien sûr en tenir compte lorsque l'on choisit la valeur des critères de sécurité (DICT) que l'on veut garantir.

<sup>5</sup> Peut se traduire par « gestion de flux d'informations ».

<sup>6</sup> « phishing » en anglais.

Les impacts les plus critiques se traduisent principalement par :

- la dégradation de l'image de marque de l'organisme (site web défiguré, etc.) ;
- la paralysie d'un système contribuant à la réalisation d'une mission essentielle (inscriptions étudiants, etc.) ;
- la perte d'un contrat (défaut d'intégrité de résultats, etc.) ;
- la fuite d'informations scientifiques (préparation d'un brevet, etc.) ;
- des préjudices divers (financiers, juridiques, etc.).

### I.3.4. Méthodes d'analyse de risques

Les normes ISO 27000 n'imposent aucune méthode d'appréciation des risques mais rend (quasi) obligatoire l'utilisation de l'une d'elles. Les principales méthodes connues en France sont :

- MEHARI<sup>7</sup> (Méthode Harmonisée d'Analyse de Risques) : proposée par le CLUSIF<sup>8</sup> depuis 1996, dérivée des méthodes MARION (Méthode d'Analyse de Risques Informatiques Optimisée par Niveau, CLUSIF) et MELISSA (Méthode d'évaluation de la vulnérabilité résiduelle des systèmes d'information, Direction Générale pour l'Armement), elle aide à gérer la sécurité de l'information et à minimiser les risques associés ;
- EBIOS<sup>9</sup> (Expression des Besoins et Identification des Objectifs de Sécurité) : proposée par la DCSSI<sup>10</sup> depuis 1995, elle permet d'apprécier et de traiter les risques relatifs à la SSI. Cette méthode permet aussi de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires afin de contribuer au processus de gestion des risques SSI.

C'est cette dernière, recommandée pour les universités, qui, adaptée à notre environnement, a été choisie à l'UPMC.

## I.4. Le traitement des risques

Un risque peut être jugé acceptable lorsqu'il y a disproportion entre la nature des biens à protéger et la mise en œuvre des moyens de prévention nécessaires pour couvrir ce risque, compte tenu de la probabilité de sinistre. En cas d'acceptation du risque, le directeur de l'entité devra justifier le rejet d'une mesure de sécurité qui lui aurait été proposée et qu'il n'aura pas retenue.

Dans notre environnement, la gestion des risques n'a généralement pas pour objectif le « risque zéro ». Elle doit cependant permettre aux responsables de connaître et d'accepter des risques résiduels en connaissance de cause (et de conséquences...).

<sup>7</sup> Cf. <http://www.clusif.asso.fr/fr/production/mehari>.

<sup>8</sup> Club de la Sécurité de l'Information Français.

<sup>9</sup> Cf. <http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html>.

<sup>10</sup> Direction Centrale de la Sécurité des Systèmes d'Information, placée sous l'autorité du Secrétaire Général de la Défense Nationale (rattaché au Premier Ministre).

## II. L'UPMC

### II.1. Présentation et missions

L'université Pierre et Marie Curie est la première université scientifique et médicale de France : 31 000 étudiants, plus de 5000 enseignants et chercheurs et plus de 2000 personnels administratifs et d'appui à la recherche, répartis sur 475000 m2 dans 7 départements et 4 régions françaises :

- Paris : Jussieu, Cordeliers, Pitié-Salpêtrière, Saint-Antoine, Voltaire, Chevaleret, Pasteur, Arago-IAP, Boucicaut, Broussais, Collège de France, Curie, Quinze-Vingts, MNHN, ENS Paris, ESPCI, Fer à Moulin, Kennedy, Raspail, Tenon, Trousseau ;
- région parisienne : St-Cyr-l'école, Vélizy Saint-Maur, Meudon, Fontenay-aux-roses, Evry, Ivry, Orsay, Gif sur Yvette, ENS Cachan, Grignon ;
- en régions : Roscoff, Banyuls sur mer, Villefranche-sur-mer, Sophia-Antipolis.

L'UPMC est dotée d'un organe de direction, le Président, ainsi que d'un organe délibérant, le Conseil d'administration (CA) et de deux organes d'études, le Conseil scientifique (CS) et le Conseil des études et de la vie universitaire (CEVU). Ces trois conseils centraux sont composés de membres élus et de personnalités extérieures.

L'UPMC se compose de sept UFR (Unité de Formation et de Recherche) en chimie, ingénierie, mathématiques, médecine, physique, sciences de la vie et de la terre, environnement et biodiversité. Elle réunit également l'École Polytechnique Universitaire, l'Institut d'Astrophysique de Paris, l'Institut Henri Poincaré et trois stations marines à Roscoff, Banyuls et Villefranche-sur-Mer. Ses 160 laboratoires sont associés à de grands organismes de recherche et à des partenaires de renom tels que le CNRS, l'INSERM, l'INRA, l'IRD, l'IFREMER, le CEA ou encore le CNES.

L'UPMC s'est fixée des missions dans les quatre domaines suivants :

- formation, orientation et insertion ;
- vie étudiante et vie du campus ;
- recherche, diffusion et valorisation ;
- relations internationales.

Le site institutionnel de l'UPMC est <http://www.upmc.fr> et son portail intranet est <http://intra.upmc.fr>.

### II.2. La chaîne fonctionnelle SSI

Le service du Haut Fonctionnaire de Défense et de Sécurité (HFDS)<sup>11</sup> anime les réseaux des fonctionnaires de sécurité de défense (FSD) et des responsables de sécurité des systèmes d'information (RSSI) relevant des services ou établissements de l'éducation nationale, de l'enseignement supérieur et de la recherche. Le HFDS s'appuie sur le Fonctionnaire de Sécurité des Systèmes d'Information (FSSI).

La « chaîne fonctionnelle SSI » de l'UPMC est mise en place afin de garantir la circulation rapide et, lorsque nécessaire, confidentielle des informations SSI de type alertes, recommandations, mesures d'urgence, incidents, etc. C'est une obligation ministérielle dans l'éventualité du déclenchement d'un plan d'urgence.

<sup>11</sup> Cf. <http://www.enseignementsup-recherche.gouv.fr/cid20302/haut-fonctionnaire-de-defense-et-de-securite-h.f.d.html>.

A l'UPMC, la chaîne fonctionnelle est composée :

- d'une Autorité Qualifiée pour la Sécurité des Systèmes d'Information (AQSSI). La responsabilité générale de la SSI de l'établissement relève du Président ;
- de deux Responsables de la Sécurité des Systèmes d'Information (RSSI titulaire et RSSI suppléant). Nommés par le Président pour l'assister dans cette fonction, leurs missions sont précisées dans un document spécifique<sup>12</sup> ;
- d'un Chargé de la Sécurité des Systèmes d'Information (CSSI) dans chaque unité (département de formation, laboratoire, service commun, service administratif...) de l'UPMC. Nommé par le responsable de l'unité, avec des missions précisées par un document spécifique<sup>13</sup>, le CSSI fait partie des chaînes d'alerte des différentes tutelles de l'unité, le cas échéant.

Voir en annexe XIV.4.5 la chaîne fonctionnelle SSI inspirée de la directive interministérielle 901.

### Le Fonctionnaire de Sécurité de Défense (FSD)

Nommé par le Président de l'établissement, le Fonctionnaire de Sécurité de Défense intervient principalement dans trois domaines : la protection du patrimoine scientifique et technique, la préparation et l'exécution des plans de défense et de sécurité et la protection du secret. Correspondant local du HFDS, il est chargé de la préparation des mesures de défense, de vigilance, de prévention de crise et de situation d'urgence (plans Vigipirate, pandémies grippales...) et d'en assurer, le cas échéant, l'exécution.

### Le correspondant informatique et libertés (CIL)

L'UPMC a désigné un Correspondant Informatique et Libertés<sup>14</sup>. Les formalités déclaratives qu'impliquent les traitements de données à caractère personnel sont allégées (hors traitements soumis à autorisation et transfert d'information hors de l'UE). Le CIL veille à la bonne application de la loi informatique et libertés dans l'établissement ; il doit établir et maintenir un registre des traitements mis en œuvre.

## II.3. Système d'Information de l'UPMC

Pour modéliser un système d'information, on distingue habituellement trois vues complémentaires : une vue métier (par exemple, le processus de paye), une vue fonctionnelle (la possibilité de disposer des éléments permettant de calculer le salaire), une vue informatique (la possibilité de déclencher effectivement le versement de sommes sur un compte associé à un personnel).

L'urbanisation repose sur la constitution de référentiels communs qui sont utilisés par les services numériques de l'établissement. Leur unicité permet de garantir l'interopérabilité des applications et l'intégrité du résultat des traitements. Ce sont, par exemple, les annuaires (des personnes, des structures, des locaux, des fournisseurs, des équipements etc.), les nomenclatures, etc.

Le rôle de la SSI consiste à formaliser l'appréciation des risques liés à l'urbanisation du système d'information de l'UPMC. Tous les dysfonctionnements susceptibles d'avoir un impact sérieux doivent pouvoir, dans la mesure du possible, être anticipés. Cela se traduit en amont par l'intégration de la méthode GISSIP<sup>15</sup> à la gestion de projet et en aval par la classification des systèmes vitaux (voir paragraphe V.2.2).

<sup>12</sup> Lettre de mission RSSI : <http://intra.upmc.fr/SSI/RSSI/MissionsRSSI-V1.pdf>.

<sup>13</sup> Lettre de mission CSSI : <http://intra.upmc.fr/SSI/RSSI/MissionsCSSI-V1.pdf>.

<sup>14</sup> Voir questions/réponses de <http://www.cnil.fr/index.php?id=1821> et <http://www.cnil.fr/?id=1689>.

<sup>15</sup> Cf. <http://www.ssi.gouv.fr/fr/confiance/documents/methodes/GISSIP-Methode-2006-12-11.pdf>.

## II.4. Système de Management de la Sécurité de l'Information, certification et PSSI à l'UPMC

Dans le domaine de la sécurité, un processus de normalisation, initié depuis plusieurs années<sup>16</sup> a récemment abouti à la publication des normes ISO 27001, 27002 et 27005. Ces normes permettent l'obtention d'une certification dite ISO 27001 valant garantie de mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI) auprès de partenaires industriels.

La mise en place d'un SMSI se déroule selon une approche méthodologique dite « Roue de Deming ». Quatre phases (PDCA)<sup>17</sup> sont appliquées itérativement : la phase « Plan » correspond à la formalisation des exigences de sécurité, la phase « Do » consiste à élaborer les mesures de sécurité et à les déployer, la phase « Check » permet de déterminer les risques résiduels c'est-à-dire non couverts par les mesures retenues et la phase « Act » consiste à adapter les mesures en fonction des écarts « Plan/Do » constatés à de la phase « Check ». Les évolutions du SI, des menaces, des technologies, des usages, de la législation, etc. justifient les tours suivants de cette « Roue ».

Concrètement, le résultat de la mise en place d'un SMSI correspond à la mise en œuvre de mesures de sécurité, généralement issues de la norme ISO 27002. La PSSI d'établissement de l'UPMC, qui définit les règles de sécurité applicables à l'ensemble des composants du système d'information : services centraux, services communs, laboratoires, départements de formation, bibliothèques etc., est issue des mesures recommandées par la norme ISO 27002.

## II.5. PSSI d'unité

Toutes les unités sont appelées à élaborer une « PSSI d'unité » qui complétera les mesures SSI préconisées par les établissements de tutelle au vu des résultats de l'analyse de risques qui aura été conduite à l'intérieur du laboratoire par le CSSI. En cas de divergence entre PSSI des différentes tutelles –sauf exceptions argumentées et approuvées par ces tutelles- les PSSI d'unité intégreront les contraintes les plus restrictives dans leur PSSI d'unité.

Le CSSI, sous l'autorité du directeur, devra assurer l'élaboration, la mise en œuvre et le suivi de la PSSI d'unité<sup>18</sup>. Le CSSI est assisté par le RSSI et le pôle SSI de la DSI qui sont chargés de lui fournir des outils méthodologiques ainsi que des documents, modèles, références et conseils (généralement issus d'une coopération avec l'équipe SSI de la Délégation Paris B du CNRS). Initiée par le responsable de l'unité et le CSSI, la PSSI d'unité est validée par le conseil de l'unité (formation, recherche).

Pédagogique par nature, la PSSI d'unité doit être élaborée dans la concertation la plus large des membres de l'unité (responsables, porteurs de projets, prestataires, administrateurs systèmes et réseau, diverses populations d'utilisateurs...) afin de dégager un consensus autour des besoins de sécurité et favoriser une appropriation (sans laquelle une PSSI est illusoire) des usages et règles qui en découlent.

La « tutelle SSI » des unités mixtes est déterminée lors de l'établissement du plan quadriennal de l'UPMC et des contrats entre les différentes tutelles. Ces documents contractuels comportent une clause précisant le partage des responsabilités entre organismes en termes de SSI. En cas d'incident de sécurité, le CSSI en réfère à la chaîne d'alerte de la tutelle ayant cette responsabilité tout en tenant informées les chaînes d'alertes des autres tutelles de l'unité. S'il y a lieu, les suites à donner

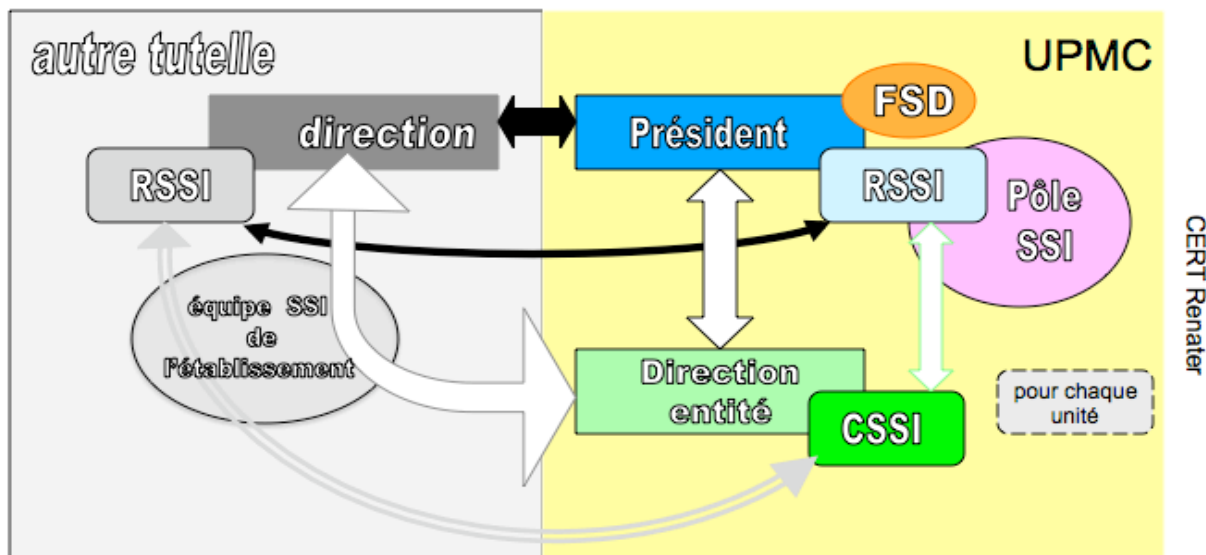
<sup>16</sup> Informations complémentaires en annexe XIV.3.2.

<sup>17</sup> « Plan – Do – Check – Act » ; traduisible par « Élaborer - Mettre en œuvre – Contrôler – Adapter ».

<sup>18</sup> Pour les services dépendant de l'administration centrale de l'UPMC, c'est le RSSI assisté du pôle SSI de la DSI qui assumeront ce rôle.

(notamment juridiques) se décident par la tutelle de référence en concertation avec les autres tutelles de l'unité.

Le schéma ci-dessous montre les chaînes fonctionnelles SSI des unités mixtes :



La mise en œuvre des plans de vigilance (Vigipirate) et/ou d'intervention (Piranet), dont la déclinaison locale doit figurer dans les annexes de la PSSI d'unité, est pilotée par la « tutelle SSI » de l'unité.

## II.6. Périmètre de la PSSI d'établissement

Le présent document décrit les orientations stratégiques en termes de sécurité des systèmes d'information de l'UPMC. Les objectifs et préconisations qui y figurent s'appliquent –sauf exceptions décrites dans les PSSI d'unités et approuvées par leur(s) tutelle(s)- à l'ensemble des unités de l'UPMC quelles que soient leur localisation géographique et leurs missions.

# PARTIE 2

DIFFUSION RESTREINTE

### III. Politique de sécurité

*« Le bon niveau de sécurité des systèmes d'information n'est pas le plus élevé mais le niveau adéquat au regard des enjeux »<sup>19</sup>.*

#### III.1. Politique de sécurité de l'information

Une PSSI énonce des principes d'ordre organisationnel et technique qu'il appartient à chaque usager (responsable, administrateurs systèmes et réseau, gérant de service numérique, utilisateur final...) de mettre en œuvre à son niveau.

Une PSSI est complétée par un ensemble de recommandations techniques et d'instructions qui en constituent les annexes techniques.

Sur proposition du CoStraSI, le Président de l'UPMC a chargé le RSSI de l'élaboration, la mise en œuvre et le suivi d'une PSSI d'établissement d'une part et d'animer la réalisation des PSSI des unités d'autre part.

La PSSI de l'UPMC a été validée par le Conseil d'Administration (?) de l'UPMC le JJ/MM/AA.

Le niveau normal des recommandations faites dans le cadre de cette PSSI correspond aux dispositions jaunes et orange du plan Vigipirate. Les dispositions internes de sécurisation doivent permettre une réactivité suffisante en cas de passage au niveau rouge de mesures propres à la SSI.

La PSSI est révisée régulièrement pour y intégrer les évolutions des usages, des ressources et de la législation d'une part, des besoins de sécurité et des menaces d'autre part.

---

<sup>19</sup> Positionnement d'un organisme en matière de maturité SSI. [SGDN/DCSSI]



## IV. Organisation de la sécurité de l'information

### IV.1. Organisation interne

La nomination des RSSI ainsi que la création du pôle SSI de la DSI permet de veiller à l'intégration systématique de la SSI aux projets de rénovation des composants du Système d'Information de l'établissement. La nomination des CSSI permet la planification et le suivi du déploiement des PSSI dans toutes les unités<sup>20</sup> ayant une tutelle UPMC.

Le comité de pilotage de la politique de sécurité de l'information est le COSTRASI.

#### IV.1.1. Attribution des responsabilités en matière de sécurité de l'information

Les responsables des unités (directeurs des laboratoires, chefs de service...) sont responsables de la sécurité des systèmes d'information de leur unité.

Les Administrateurs Systèmes et Réseau (ASR) sont chargés de la mise en œuvre et de la surveillance générale des systèmes et du réseau de leur unité et veillent au respect des règles de sécurité des systèmes d'information. Ils sont tenus de signaler au CSSI de l'unité (ou au RSSI de l'établissement le cas échéant) toute anomalie de fonctionnement ou tout incident pouvant laisser supposer une intrusion ou une tentative d'intrusion sur les systèmes ou le réseau.

Les utilisateurs s'engagent à respecter la politique de sécurité et les chartes en vigueur dans l'établissement.

#### IV.1.2. Système d'autorisation concernant les moyens de traitement de l'information

L'accès aux ressources doit être contrôlé (identification, authentification) et adapté au droit à en connaître de l'utilisateur (droits et privilèges, profil utilisateur).

#### IV.1.3. Engagements de confidentialité

Les agents de la chaîne fonctionnelle SSI<sup>21</sup>, les administrateurs systèmes et réseau, les gérants de services numériques peuvent être amenés à accéder à des informations stratégiques de l'établissement, des journaux informatiques, des courriels, des données à caractère personnel / privées / sensibles / confidentielles, etc. lors d'une recherche de dysfonctionnement ou autre investigation dans le cadre de la protection du patrimoine scientifique ou à la demande d'une autorité judiciaire. Ils sont tenus au devoir de confidentialité, voire au secret professionnel. Ils peuvent si nécessaire faire l'objet d'une habilitation au secret de défense.

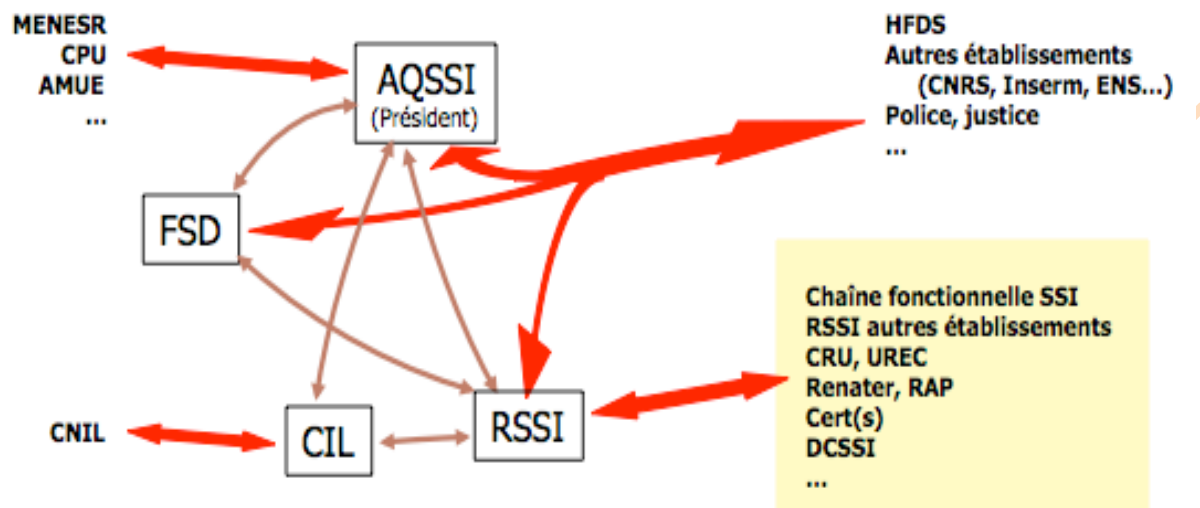
Voir annexes XV.6 (Devoir de discrétion professionnelle) et XV.7 (Périmètre d'intervention des administrateurs systèmes et réseau).

<sup>20</sup> Cf. <http://intra.upmc.fr/SSI/Documents/RapportSSI-2008.pdf>.

<sup>21</sup> Voir paragraphe II.2.

#### IV.1.4. Relations avec les autorités

Le schéma suivant montre les relations des intervenants SSI de l'UPMC avec l'environnement extérieur (ministère, autorités, autres établissements...). Elles permettent l'échange d'information, la propagation des alertes (Vigipirate, pandémie, avis/recommandations de sécurité, etc.) vers les personnes concernées, la remontée d'incidents de sécurité.



#### IV.2. Tiers

L'information dont l'accès est autorisé à des tiers (lecture, modification, administration, hébergement) ainsi que leurs moyens de traitements (applications, équipements) doivent faire l'objet d'une analyse de risque.

##### IV.2.1. Identification des risques provenant des tiers

L'infogérance correspond au fait que des sociétés ont accès au Système d'Information depuis l'extérieur ou l'intérieur de l'établissement dans le but d'en gérer un composant. Il convient de définir précisément les droits et moyens d'accès appropriés pour ces sociétés.

L'externalisation de la gestion d'exploitation d'un composant critique pour le SI est à proscrire, sauf dispositions de garantie spécifiques et validées (RSSI, FSD, AQSSI). Les informations sensibles ne doivent pas être traitées sur des systèmes informatiques non maîtrisés.

##### IV.2.2. La sécurité et les clients

À développer.  
Limite de l'usage des ressources informatiques mises à la disposition de étudiants (sont-ce des « clients » ?)  
Jeunes pousses / pépinière  
Partenaires

#### IV.2.3. La sécurité dans les accords conclus avec des tiers

Les marchés publics relatifs à des prestations informatiques (intégration de logiciels, infogérance, maintenance...) doivent comporter des clauses de confidentialité (voire d'agrément et d'habilitation de personnes) et, le cas échéant, des engagements de responsabilité.

L'accès au système d'information de la part de personnels d'entreprises extérieures doit être conforme à la politique générale d'accès aux moyens informatiques. Les obligations correspondantes, notamment la signature de la charte utilisateur et le respect de la PSSI, doivent être mentionnées dans les dispositions contractuelles.

Les procédures de gestion des changements de titulaire (notamment les phases de mise en œuvre, de renégociation et de résiliation de contrat) et de continuité de service en cas de défaillance du tiers doivent figurer dans les dispositions contractuelles. Doivent également être précisés :

- la procédure d'intervention à distance (intégration de logiciels, infogérance, maintenance) ;
- le contenu du « cahier de bord maintenance » (historique des incidents et leur résolution, installation des correctifs de dysfonctionnement et/ou de sécurité, mises à jour système ou applicatif...) ;
- la procédure de destruction des supports en fin de vie.

Le stockage chez un prestataire externe de données sensibles est interdit, sauf dispositions contractuelles de protection ou chiffrement des données.

## V. Gestion des biens

### V.1. Responsabilités relatives aux biens

#### V.1.1. Inventaire des biens

Une appréciation des risques nécessite une connaissance de l'ensemble des biens importants de l'organisme : données, logiciels, équipements, services, ressources humaines. Les informations permettant de faire face à un sinistre peuvent y être consignées (licence, sauvegarde, etc ...).

Chaque bien inventorié doit être localisé (lieu où il est hébergé) et affecté à un propriétaire. Le propriétaire est le responsable du bien même s'il en délègue la gestion ; il en détermine la criticité et veille à la mise en œuvre des protections pertinentes.

#### V.1.2. Utilisation correcte des biens

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, visant soit des recommandations d'utilisation, soit une interdiction pure et simple, (comme cela est le cas pour le logiciel Skype, par exemple).

Les informations concernant l'utilisation correcte des biens sont officiellement validées par la Direction de l'UPMC : chartes, PSSI, référentiel de règles d'usage (téléchargement, sans-fil, journaux informatiques, etc.).

### V.2. Classification

#### V.2.1. Lignes directrices pour la classification

Les données peuvent être classées en diverses catégories dans le but de hiérarchiser les niveaux de protection (liste non ordonnée) :

- **données sensibles.** Le stockage et la transmission de données « classifiées de défense » sont interdits sauf utilisation de moyens spécifiques agréés. Les données non classifiées mais présentant « un caractère sensible<sup>22</sup> » doivent être traitées en fonction des règles émises suite à l'analyse de risques (confidentialité, intégrité) les concernant<sup>23</sup>. Il sera procédé régulièrement à un réexamen de la sensibilité des données.
- **données à caractère personnel.** Les données à caractère personnel constituent des données sensibles et doivent faire l'objet de protection. Ces fichiers peuvent être de simples tableaux, des bases de données complexes, des journaux informatiques, etc...
- **données privées.** Des données privées sont tolérées sur les postes de travail personnels<sup>24</sup> mis à disposition des utilisateurs par l'établissement (voir paragraphe XIII.1.7)

<sup>22</sup> Données nominatives, brevets en préparation, contrat avec clauses de confidentialité, résultats scientifiques non publiés, données stratégiques, administratives, budgétaire, etc...

<sup>23</sup> Tenir compte du fait que l'accumulation de données a priori anodines peut conduire à une information sensible.

<sup>24</sup> À l'exclusion des postes partagés (exemple : libres-services).

- **journaux informatiques.** Une « politique de gestion des traces informatiques »<sup>25</sup> a été définie à l'UPMC. Elle précise les contenus, les durées et les accès associés à ces fichiers de données à caractère personnel. Les unités doivent d'y conformer.
- **vidéosurveillance.** La pose de caméras de surveillance dans un lieu public ou privé pour visualiser et/ou enregistrer les flux de personnes dans le but de prévenir les vols, agressions, fraudes, etc. est soumis aux dispositions de l'article 10 de la loi n°95-73 du 21 janvier 1995 sur la sécurité (modifié par la Loi n°2006-64 du 23 janvier 2006). Outre la déclaration préfectorale obligatoire, le responsable de l'installation peut être amené à effectuer une déclaration à la CNIL selon les traitements envisagés<sup>26</sup>.
- **données de recherche :** données brutes, résultats de calculs, publications à venir ou effectuées, valorisation, brevets...
- **données d'enseignement :** contenus, sujets d'examens, scolarité...
- **données administratives :** budget, RH, bilans, contrats de maintenance...

## V.2.2. Services centraux de l'UPMC : classement « Système vital »

Depuis 2008, les services du HFDS demandent aux établissements un rapport sur la cartographie de leurs « services vitaux »<sup>27</sup>. La cartographie des systèmes vitaux, tenue à jour, constitue un outil de supervision et de gouvernance de la SSI. Ce document est fondamental pour l'élaboration d'un plan de gestion de crise.

Une première identification des systèmes vitaux, administrés par la DSI, a été effectuée en 2008 :

- gestion des identités et des droits,
- gestion financière et comptable,
- gestion de la formation,
- gestion de la scolarité,
- gestion des ressources humaines,
- gestion du patrimoine,
- SI documentaire,
- environnement numérique de travail,
- données scientifiques sensibles des laboratoires,
- messagerie,
- téléphonie,
- logistique Réseau,
- stockage et archivage,
- environnement calcul scientifique,
- communication.

La deuxième phase, en cours, consiste en une analyse de risques permettant d'exprimer les besoins de sécurité de ces éléments considérés comme vitaux, et de prévoir les impacts en cas d'atteinte de ces besoins. Cette approche permet d'obtenir des éléments rationnels pour hiérarchiser les systèmes selon leur importance et anticiper les sinistres de manière proactive.

Une démarche similaire doit être effectuée par les CSSI dans les unités (services vitaux « enseignement » et « recherche »).

<sup>25</sup> cf <http://intra.upmc.fr/SSI/ReferentielUPMC/pgji-V?.pdf>.

<sup>26</sup> <http://www.cnil.fr/index.php?id=1302>.

<sup>27</sup> Un « service vital » est un service dont l'indisponibilité, l'altération, la perte de confidentialité nuit gravement à la satisfaction de l'un des objectifs ou l'une des missions essentielles de l'université.

## VI. Sécurité liée aux ressources humaines

La mise à disposition d'outils informatiques (stations de travail, postes nomades, applications, données...) doit être formalisée à l'arrivée, au changement de fonction et au départ de l'utilisateur concerné, qu'il soit personnel permanent ou non, UPMC ou non.

L'utilisateur doit prendre connaissance des droits et devoirs que lui confère la mise à disposition par son entité de ces outils. En l'absence d'autre document plus spécifique, la charte de l'UPMC peut être utilisée.

Le cas échéant, l'accès à des systèmes d'information ou à des applications spécifiques ou encore l'exercice de fonctions de gestion de ressources informatiques peut être conditionné à une habilitation de défense.

L'organisation de séances de formation et de sensibilisation des différents acteurs de la sécurité, de l'expert SSI à l'utilisateur en passant par le responsable de l'entité est cruciale pour la sécurité. Il est vivement recommandé de mettre en place des journées d'accueil destinées aux nouveaux personnels ou étudiants.

### VI.1. Fin ou modification de contrat

Cela concerne :

- fin de période scolaire,
- cessation d'activité,
- mutation d'un agent,
- échéance d'un contrat (de recherche, de maintenance...),
- accord de coopération (autre établissement...),
- etc...

#### VI.1.1. Responsabilités en fin de contrat

Diffusion d'un document formalisant les droits et devoirs (reprise des rôles après le départ ; fichiers professionnels / fichiers personnels ; tri de la messagerie selon les rôles/ messagerie personnelle, ...).

Mise à disposition (partielles ?) des ressources liées à ses rôles pendant « un certain temps » (3 mois ?). Mise à disposition de ressources au titre « d'ancien » → signature d'une charte spécifique<sup>28</sup> (ne sont plus dépendants du règlement intérieur et des chartes des personnels/étudiants)

Confidentialité sur le SI et la SSI (agent ou intervenant y ayant eu accès lors de son activité) ; pas de re-utilisation de données « recueillies » sans accord explicite

Le cas échéant, règles d'inscription à des listes « d'anciens » avec/sans automatique ou non ; mode de désabonnement explicite ; mode de désabonnement implicite (type relance annuelle)

#### VI.1.2. Restitution des biens

Équipements (poste de travail, supports électroniques, téléphone, ... badges et clé) (sauf dérogation)

Données, logiciels (licences), documents... appartenant à l'établissement (sauf dérogation)

<sup>28</sup> Cf. fiche N°5 du guide "Informatique et Libertés" pour l'enseignement supérieur et la recherche.

Les accès aux données professionnelles (mot de passe) doivent être remis au responsable hiérarchique après suppression des données personnelles. Les mots de passe « fonctionnels » (ex : administrateur système et réseau, gérant d'application) doivent être changés.

Statut des sauvegardes et archives (données privées...)

### VI.1.3. Retrait des droits d'accès

Les procédures liées aux changements de fonction (ou de missions) d'un utilisateur doivent être définies et adaptées au statut de cet utilisateur (étudiant, personnel, invité, associé, fournisseur...). Il faut notamment édicter les règles permettant l'accès à des données professionnelles par l'UPMC ainsi que le traitement des données personnelles (postes de travail, serveurs, espaces de stockage et d'archivage...) après le départ de leur propriétaire. L'utilisateur doit en être informé.

A préciser :

Accès physiques et logiques

Délais et règles (fermeture « progressive » ?)

Mise à jour du référentiel de personnes / gestion des identités ; fermeture des services numériques avec gestion locale des droits, ... ; fin des partages (ex : domaine Windows)

Gestion des mutation internes (-> changement de rôle -> retrait des droits anciens / ajouts de droits nouveaux) et des personnes n'abandonnant pas tous leurs rôles (retraits partiels)

Le processus disciplinaire pour infraction aux règles de sécurité concernant les différentes catégories d'utilisateurs doit être formalisé ou bien on se réfère à un texte qui décrit les infractions.

## VII. Sécurité physique et environnementale

### VII.1. Zones sécurisées

#### VII.1.1. Contrôles physiques des accès

Il n'y a pas de contrôle d'accès formalisé aux entrées des campus de l'UPMC (hors niveau rouge du plan Vigipirate).

Le contrôle d'accès aux locaux sécurisés de l'université est effectué :

- soit par accueil permanent avec inscription sur registre (statut cnil de ce registre ?)
- sur intervention humaine ponctuelle (sonnette et ouverture manuelle) ;
- soit par lecture d'un badge (généralement nominatif) et vérification des droits associés.

Le contrôle d'accès électronique est un système centralisé ayant donné lieu à une déclaration CNIL spécifique<sup>29</sup>.

La mise en place, par un laboratoire, de zones sécurisées dans les locaux de l'UPMC impliquant le traitement d'informations nominatives, nécessite une déclaration préalable auprès du CIL de l'UPMC.

#### VII.1.2. Protection contre les menaces extérieures et environnementales

Les menaces extérieures et environnementales doivent être prises en compte pour l'analyse de risques. Par exemple, le campus Jussieu est situé en zone inondable.

### VII.2. Sécurité du matériel

#### VII.2.1. Protection du matériel

Selon la criticité des services, il convient de mettre en œuvre les protections adéquates pour pouvoir assurer la continuité des services. Pour les services dits « vitaux » cela implique le choix de serveurs dimensionnés correctement avec prise en compte des ressources humaines, sauvegardes, accès physique, énergie, climatisation, remontées d'alarmes, maintenance, redondance physique, équilibrage de charge, serveurs virtuels etc..

En cas de mise en œuvre d'un nouveau service, si l'environnement approprié (« salle machine », redondance de serveurs...) ne peut être obtenu au sein de l'unité, on pourra recourir à l'offre d'hébergement de services numériques de la DSI.

Les câblages des locaux de l'UPMC doivent suivre les préconisations de la DSI<sup>30</sup>. En particulier, les normes portant sur les architectures, les distances et les débits en fonction des média, doivent être strictement respectées.

En fonction des besoins en termes de continuité de service, il pourra être mis en œuvre une redondance physique des réseaux (doublement des liaisons et des équipements).

<sup>29</sup> Cf. <http://intra.upmc.fr/CIL/Declarations/AccesPhysique.pdf>.

<sup>30</sup> Cf. <http://intra.upmc.fr/DSI/LogistiqueOperationnelle/Documents/PreconisationsCablage.pdf>.



### VII.2.2. Sécurité du matériel hors des locaux

Tout support contenant des données sensibles transporté à l'extérieur (clé USB, CD, DVD, disque amovible, etc... mais aussi ordinateurs portables) doit faire l'objet de mesure de protection contre le vol et/ou les informations contenues doivent être chiffrées.

La sortie et l'utilisation à l'extérieur de l'entité de tout équipement informatique professionnel doivent avoir été autorisées par la direction de l'unité.

### VII.2.3. Mise au rebut ou recyclage sécurisé(e) du matériel

Une politique de gestion des supports d'information (postes de travail fixes ou portables, serveurs, équipements réseau paramétrables, supports de données tels que disques externes, CD/DVD, clés USB...) en fin d'usage (retour vendeur, cession, don, mise au rebut ...) doit garantir la destruction sécurisée des données qu'ils contiennent.

Avant tout envoi en réparation, cession ou mise au rebut d'un matériel, il convient de s'assurer que toutes les données ont bien été effacées par un procédé efficace. En cas de panne empêchant ce nettoyage, les supports concernés devront être démontés ou détruits.

## VIII. Gestion de l'exploitation et des télécommunications

### VIII.1. Procédures et responsabilités liées à l'exploitation

Une formalisation des responsabilités et des procédures d'exploitation est obligatoire pour les systèmes vitaux (enseignement, recherche administration) et conseillée pour les services moins critiques.

#### Serveurs et administration des serveurs

Un serveur est un ordinateur offrant un ou plusieurs services (calcul scientifique, information, espace disque, ENT, application...). Il est administré par les ASR de l'unité en ayant la responsabilité. Un serveur ne doit pas être mis en service par un utilisateur n'ayant pas la qualification requise ; a fortiori s'il est visible de l'extérieur de l'unité. En cas de vacance prolongée d'administration, un serveur doit être arrêté.

Les ASR sont responsables de la mise en œuvre, des tests de bon fonctionnement, de la sécurisation et du suivi des systèmes (maintenance et licences, version de système à jour sauf contre-indications notoires, ouverture des seuls services utiles, surveillance et gestion des traces, interface avec les gérants du réseau, pose des rustines<sup>31</sup> de sécurité et/ou de fonctionnalité, sauvegarde des données, etc. ) dont ils ont la charge. Un serveur doit être arrêté s'il n'héberge plus de service utile. Les autorisations d'accès à ce serveur doivent en ce cas disparaître du système d'information.

Les accès aux serveurs (ASR, utilisateurs) doivent être journalisés (d'où nécessité de l'exactitude des dates et heures).

En cas d'administration partagée (cas des serveurs d'une unité hébergés par une autre), les limites de responsabilité doivent être bien définies dans un contrat entre les parties.

#### Services numériques et administration des applications

Une application est un logiciel s'exécutant sur un serveur, travaillant sur des données pour offrir tout ou partie d'un service (annuaire, site Web, Sifac, ENT, Sakai, Mathematica,...). Il est administré par le(s) gérant(s) de l'application (ASR ou administrateur spécifique) de l'unité en ayant la responsabilité. S'il n'est pas l'ASR du serveur hébergeant l'application, son gérant doit collaborer étroitement avec lui. Un service numérique ne doit pas être mis en œuvre par un utilisateur n'ayant pas la qualification requise ; a fortiori s'il est visible de l'extérieur de l'unité. En cas de vacance prolongée d'administration, un service doit être arrêté.

Les gérants d'applications sont responsables de la mise en œuvre des tests de bon fonctionnement, de la sécurisation et du suivi des applications (maintenance et licence, version de logiciel à jour sauf contre-indications notoires, surveillance et gestion des traces, pose des rustines de sécurité et/ou de fonctionnalité, sauvegarde des données, etc. ) dont ils ont la charge. Une application doit être arrêtée si elle n'est plus justifiée par un besoin. Les autorisations d'accès à ce service doivent alors disparaître du système d'information.

Les accès aux services (gérants, utilisateurs) doivent être journalisés (d'où nécessité de l'exactitude des dates et heures du serveur).

---

<sup>31</sup> « Patch » en anglais.

En cas d'administration partagée (cas des applications d'une unité hébergées sur des serveurs sous administration d'une autre), les limites de responsabilité doivent être bien définies dans un contrat entre les parties.

## Postes de travail

Un poste de travail<sup>32</sup> est un équipements individuel, fixe ou portable, utilisé par une seule personne, animé par un système de type Windows, MacOS ou avatar Unix, et dont l'accès aux serveurs distants et la bureautique locale sont les usages les plus courants.

L'administration des postes de travail doit, autant que faire se peut, être effectuée par les ASR de l'unité ; l'utilisateur ne possédant que les droits... d'utilisation. C'est une garantie en termes de SSI. Sauf cas de force majeure (réquisition judiciaire, demande de la chaîne fonctionnelle SSI, activité illégale, préservation de l'outil de travail,...), l'administrateurs systèmes et réseau n'intervient sur les postes (en présence ou à distance) qu'après avoir prévenu l'utilisateur, en respectant les règles de déontologie et dans un esprit de confiance mutuelle.

La sécurité d'un poste de travail administré par l'utilisateur lui-même est aléatoire et la PSSI de l'unité doit en tenir compte dans le zonage des ressources accessibles (accès direct aux SI vitaux interdit par exemple)

Quelle que soit la politique retenue par l'unité, certains règles de base doivent être respectées : mot de passe<sup>33</sup>, logiciel antivirus (si système exposé : Windows), installation de logiciels et copie de données en rapport avec l'activité professionnelle<sup>34</sup>, à partir de sources sûres et en conformité avec le droit de la propriété intellectuelle. L'installation de logiciels « non professionnels » sur le poste de travail fourni par l'établissement doit être évitée (risque de dysfonctionnement lors de son usage professionnel, risque de programme espion<sup>35</sup> installé à l'insu de l'utilisateur, etc.).

Les postes de travail mobiles (ordinateur portable, assistant personnel<sup>36</sup> ou ordinateur de poche, téléphone/smartphone...), de par leur plus grande vulnérabilité aux vols, pertes, chutes... exigent des précautions spécifiques pour garantir la confidentialité (chiffrement) et la disponibilité des données (sauvegardes distantes). En cas de données sensibles, le chiffrement de tout ou partie de l'espace de stockage est une nécessité<sup>37</sup>.

Les postes de travail en libre-service doivent être vus comme des « serveurs d'accès » et, à ce titre, administrés comme tels (cf. paragraphe « serveurs » ci-dessus).

## Réseau informatique et téléphonique

L'ingénierie et l'exploitation des dorsales filaire et sans-fil de l'UPMC sont à la charge du pôle logistique de la DSI. Sont compris dans ses missions, les interconnexions « données » avec Internet (RAP, RENATER), les interconnexions « téléphone » avec les prestataires spécialisés, les interconnexions entre les différents sites de l'UPMC, les services de bases IPv4 et IPv6 associées (réseau locaux virtuels, DNS, passerelle messagerie, antivirus et antispam, hébergement de boîtes à lettre, téléphonie, proxy web, surveillance, filtrage, métrologie...).

<sup>32</sup> Ceci ne concerne pas le poste de travail virtuel qui est un service s'exécutant sur un serveur dont le client (équipement de l'utilisateur) n'en supporte que l'affichage déporté.

<sup>33</sup> À noter que « l'ordinateur mis à la disposition du salarié peut être protégé par un mot de passe ou un login, mais cette mesure de sécurité est destinée à éviter les utilisations malveillantes ou abusives par un tiers ; elle n'a pas pour effet de transformer l'ordinateur de l'entreprise en un ordinateur privé » CNIL, février 2002.

<sup>34</sup> Voir paragraphe XIII.1.7 sur l'usage privé.

<sup>35</sup> Mouchard ou « spyware » en anglais. Il collecte et transfère des données collectées sur l'ordinateur à l'insu de l'utilisateur.

<sup>36</sup> « Personnel Digital Assistant » (PDA) en anglais.

<sup>37</sup> Le chiffrement des données (comme le mot de passe ; cf. note 33) ne doit pas empêcher l'employeur d'accéder aux données professionnelles qui y sont stockées.

Certains services de base peuvent être délégués (nommage, attribution des VLAN...) aux ASR des entités, d'autres (gestion des VLAN, téléphonie...) non. Les CSSI devront favoriser le cloisonnement des espaces d'adresses de l'unité (administration, zone publique<sup>38</sup>, zones privées, zones privées étendues (exemple : accès VPN), invités...).

Lorsque les services mis en œuvre par la DSI ne sont pas adaptés aux besoins d'une unité (test service expérimental, contraintes spécifiques...), celle-ci peut être amenée, en concertation avec la DSI, à déployer/développer un service local. En aucun cas ce dernier ne devra perturber le service général<sup>39</sup>.

### **VIII.1.1. Procédures d'exploitation documentées**

#### **Serveurs et administration des serveurs**

Un « cahier » d'exploitation (caractéristiques et paramétrages de base, description des opérations courantes, que faire en cas de panne ou incident, historique des interventions des ASR, des interventions de la maintenance, des incidents ...) doit être associé à chaque serveur.

#### **Services numériques et administration des applications**

Un « cahier » d'exploitation (caractéristiques et paramétrages de base, description des opérations courantes, que faire en cas de panne ou incident, historique des interventions des gérants du service, des interventions de la maintenance, des incidents ...) doit être associé à chaque application vitale.

### **VIII.1.2. Gestion des modifications**

La modification d'un logiciel système ou applicatif doit être justifiée, préparée, planifiée et les utilisateurs prévenus à l'avance de la cause, du périmètre et du temps d'indisponibilité du service. Une procédure de validation, fonction de l'ampleur de la modification, doit être prévue pour vérifier, a minima, la non-régression du service. Une procédure de repli doit être prévue en cas d'échec de la modification ou de dysfonctionnement du nouveau logiciel.

Les utilisateurs doivent être informés des conséquences de la modification si celle-ci ne leur est pas totalement transparente.

### **VIII.1.3. Séparation des tâches**

L'administration des serveurs est placée sous la responsabilité des ASR de l'unité ou est confiée (contrat d'hébergement) à la DSI. L'administration de serveurs par les utilisateurs eux-mêmes doit demeurer l'exception et être justifiée en termes de besoins et de compétences.

L'administration des postes de travail individuels est normalement placée sous la responsabilité des ASR de l'unité. Néanmoins, si besoin (manque d'organisation interne et/ou de ressources humaines qualifiées), elle peut être assurée par les utilisateurs eux-mêmes sous réserve de s'inscrire dans la politique de sécurité de l'unité.

La garantie d'une relation de confiance mutuelle « administrateur-utilisateur » repose sur le fait que l'utilisateur puisse conserver la maîtrise de son environnement.

<sup>38</sup> Demilitarized zone (DMZ) en anglais.

<sup>39</sup> Voir par exemple les conditions de mise en œuvre de bornes sans-fil « indépendantes » dans les unités à <http://intra.upmc.fr/ssi/ReferentielUPMC/BornesSansFil-Vi?.pdf>.

#### VIII.1.4. Séparation des équipements de développement, de test et d'exploitation

Les développements ou intégrations de logiciels ainsi que leurs tests doivent être effectués sur des équipements n'hébergeant pas de service en exploitation. La configuration de test doit être aussi proche que possible de l'environnement d'exploitation et il convient de préciser les règles de passage de la phase test à la phase exploitation.

#### VIII.2. Gestion de la prestation de service par un tiers

Il est important de mesurer les risques afin de définir précisément les droits d'accès appropriés pour les sociétés de maintenance et d'infogérance. Les prestataires de service doivent respecter les règles de sécurité énoncées dans la PSSI (répondre aux mêmes normes), auxquelles un contrôle renforcé sur les ressources mises à disposition doit être ajouté. Un contrat doit clairement préciser les responsabilités et l'imputabilité en cas d'incident.

L'externalisation de la gestion d'exploitation d'un composant critique pour le SI de l'entité est à proscrire, sauf dispositions de garantie spécifiques et validées (RSSI, FSD, AQSSI).

Le stockage chez un prestataire externe de données sensibles est interdit, sauf dispositions contractuelles de protection ou chiffrement des données.

Les analyses de sécurité doivent intégrer les situations d'hébergement sur sites extérieurs.

#### VIII.3. Protection contre les codes malveillant et mobile

Les virus<sup>40</sup>, vers<sup>41</sup>, mouchards<sup>42</sup>, et autres chevaux de Troie<sup>43</sup> constituent, avec les « spams »<sup>44</sup> qui en sont souvent les vecteurs, les principales calamités du réseau pour l'utilisateur final.

Une lutte efficace contre les codes malveillant passe par deux niveaux de protection :

- filtrage par des équipements réseau spécialisés. Situés à l'interconnexion du réseau de l'UPMC avec son fournisseur d'accès, ils sont à la charge (technologie, investissement, administration) de la DSI. Ils ne protègent bien sûr pas les flux qui ne transitent pas par ces passerelles (portables au domicile...). Idem avec les flux chiffrés (ex : VPN).
- filtrage sur le poste de travail. La mise en œuvre d'un antivirus et la mise à jour quotidienne (a minima) de sa base de signatures est obligatoire sur tout poste de travail. Le « pôle logiciels » de la DSI distribue plusieurs logiciels antivirus.

<sup>40</sup> Logiciel parasite ajouté à un logiciel « hôte » légitime pour action malveillante (contamination autres fichiers, destruction, modification système, comportement aléatoire, etc...).

<sup>41</sup> Logiciel qui se propage d'ordinateur à ordinateur, en utilisant les services réseau (ex : fichiers attachés en messagerie, pour action malveillante (destruction, espionnage, ouverture d'accès...)).

<sup>42</sup> « spyware » en anglais. Logiciel collectant des données sur les contenus et/ou les actions de l'utilisateur (à son insu) pour les transmettre ou les tenir à disposition d'un tiers.

<sup>43</sup> Intégré à un programme légitime (semblable à un virus mais sans autoreproduction), il est principalement destinée à ouvrir un accès permettant à un pirate de prendre le contrôle à distance de l'ordinateur.

<sup>44</sup> Traduction non académique : pourriel. C'est un « courriel non souhaité » envoyé massivement à des listes d'adresse volées à partir d'adresses fictives ou usurpées.

## VIII.4. Sauvegarde

Une politique de sauvegarde régulière des données avec des processus de restauration validés doit être mise en œuvre. Les sauvegardes doivent être stockées dans un local différent de celui hébergeant le support original et/ou dans une armoire plus ou moins sécurisée (blindée, ignifugée) en fonction de la criticité des données. Leur intégrité devra être régulièrement vérifiées (ex : répétition de restauration afin de vérifier l'intégrité du processus, la lisibilité du support et la pérennité du format).

Les données sauvegardées sont soumises aux mêmes règles de légalité (ex : durée de conservation des journaux informatiques) et de confidentialité (ex : sujet d'examen) que les données originales.

La DSI offre une solution de sauvegarde sécurisée dont toute unité peut-être cliente.

## VIII.5. Gestion de la sécurité des réseaux

### VIII.5.1. Mesures sur les réseaux

La sécurité des systèmes d'information implique de pouvoir surveiller le trafic sur le réseau et tracer les actions effectuées pour assurer l'imputabilité.

L'analyse des journaux des équipements réseau est une source pertinente d'informations pour la sécurité du réseau et des systèmes. Cela peut aider à anticiper des incidents en remarquant par exemple des activités anormales. Ces analyses se font sur la base d'une agrégation de trafic, non sur la surveillance du contenu de sessions utilisateurs.

### VIII.5.2. Sécurité des services réseau

Les tentatives de connexion en provenance de l'extérieur sont filtrées sur les équipements d'entrée des sites du réseau de l'UPMC sauf demande explicite d'accès entrant formulée auprès de la DSI par l'intermédiaire du CSSI de l'unité.

#### CanalIP

La connexion au réseau sans fil de l'établissement (CanalIP) nécessite une authentification basée sur l'annuaire. Les unités mettant en œuvre des équipements wifi « indépendants »<sup>45</sup> doivent assurer le même niveau d'authentification, de confidentialité et de traçabilité des échanges. Le réseau « CanalIP-UPMC » n'assurant que le chiffrement de l'échange des données lors de l'authentification (après l'authentification, toute la session de l'utilisateur circule « en clair » et peut donc être « écoutée » très facilement), on préférera le réseau « CanalIP-UPMC (TTLS) » entièrement chiffré<sup>46</sup>.

<sup>45</sup> Voir conditions à <http://intra.upmc.fr/ssi/ReferentielUPMC/BornesSansFil-Vi?.pdf>.

<sup>46</sup> L'usage du réseau « CanalIP-UPMC (TTLS) » nécessite le téléchargement d'un petit logiciel de chiffrement sur le poste utilisateur.

## Itinérance

Afin de sécuriser les accès de l'extérieur aux services numériques non publics de l'UPMC (accès ponctuels type ou télétravail), la DSI offre un service VPN<sup>47</sup> à tous les utilisateurs figurant dans l'annuaire. Cela permet de chiffrer l'intégralité des sessions lors de connexions sur des serveurs de l'UPMC.

## VIII.6. Manipulation des supports

Tout support contenant des données sensibles transporté à l'extérieur (clé USB, CD/DVD, disque externe, etc.), cela inclut aussi les ordinateurs portables) doit faire l'objet de mesure de protection contre le vol et/ou les informations contenues doivent être chiffrées.

Avant toute mise au rebut de support (postes de travail fixes ou portables, serveurs, équipements réseau paramétrables, supports de données tels que disques externes, CD/DVD, clés USB...), il convient de s'assurer que toutes les données ont bien été effacées par un procédé efficace (effacement sécurisé). En cas de panne empêchant ce nettoyage, les supports de données doivent être détruits.

## VIII.7. Échange des informations

Les échanges d'informations doivent être autorisés et en conformité avec les chartes d'usage (UPMC, Renater). Cela inclut les aspects déontologiques (ex : pas de relais de « chaînes de message ») et légaux (ex : pas d'incitation à la haine raciale, ou pas de transferts d'informations à caractère personnel non conforme à leur déclaration CNIL).

Les utilisateurs doivent être sensibilisés aux risques (confidentialité...) induits par le renvoi automatique des courriels vers une boîte à lettres extérieure puisqu'il fait passer les messages d'un niveau de sécurité supposé pertinent vers un environnement inconnu. De même l'usage de services de téléphonie non maîtrisés peut être une source de perte de confidentialité<sup>48</sup>. Par exemple, l'envoi d'un mot de passe ou d'un sujet d'examen par messagerie électronique est évidemment à proscrire...

L'usage des techniques augmentant la sécurité et le confiance des échanges (signature électronique, protocoles sécurisés, réseaux privés virtuels<sup>49</sup>, etc.) sont encouragées et peuvent être rendues obligatoires selon le risque. Les connexions dont l'authentification nécessite l'envoi d'un mot de passe « en clair » sur le réseau sont à proscrire.

### VIII.7.1. Accords d'échange

Les d'échanges avec des entités extérieures<sup>50</sup> doivent être formalisés (légalité, responsabilités, procédures, sécurité, contenus, formats d'échange normalisés, etc.) dans un accord entre les parties.

<sup>47</sup> Virtual private network. Un « réseau virtuel privé » est un tunnel chiffré entre deux équipements garantissant l'authenticité de ses extrémités d'une part et la confidentialité des informations en transit d'autre part. Cette technologie permet d'étendre le réseau local à des équipements distants. En l'occurrence il s'agit d'un serveur hébergé à la DSI autorisant la connexion sécurisée des clients que sont les ordinateurs distants situés à domicile, en déplacement, etc.

<sup>48</sup> Cf. <http://intra.upmc.fr/SSI/ReferentielUPMC/ProscriptionSkype.pdf>.

<sup>49</sup> La DSI offre un service VPN : <http://intra.upmc.fr/DSI/services/VPN>.

<sup>50</sup> Exemples : CNRS, CROUS, prestataires/hébergeurs de services externalisés, partenaires, banque...



## VIII.7.2. Supports physiques en transit

(supports physiques confiés à des tiers pour leur transport)  
Non développé dans cette version.

## VIII.7.3. Messagerie électronique

La messagerie électronique est toujours le premier moyen d'échange d'informations entre utilisateurs. À ce titre elle est un service sensible du système d'information. Extrêmement populaire, ce service est la cible de nombreux abus (virus et autres pièces jointes douteuses, spam, phishing, usurpation d'identité, etc...) rendus possibles par les failles du protocole et/ou de son implémentation, la possibilité de falsifier aisément les attributs d'un message (entête et corps) et ... la crédulité des utilisateurs. Historiquement, ce service est le premier pour lequel des règles de déontologie, toujours d'actualité, la « Netiquette »<sup>51</sup> ont été rédigées.

La sécurisation de ce service (protection du mot de passe –obligatoire- et du contenu –si nécessaire-) nécessite l'utilisation de protocoles autorisant le chiffrement des échanges (VPN SSL, https, pops, imaps, smtps). Seule la possession d'un certificat de personne<sup>52</sup> peut garantir l'identité de l'expéditeur grâce à la signature du message. Leur usage est recommandé pour l'échange d'informations sensibles.

## VIII.8. Services de commerce électronique

Pris au sens large, les échanges avec la banque lors du paiement des droits d'inscription pourrait être concerné  
A développer.

## VIII.9. Surveillance

Le SI doit comprendre des dispositifs ou procédures de journalisation dont l'objectif est de permettre de détecter les dysfonctionnements, les intrusions, les utilisations frauduleuses et de tenter d'en identifier les causes et les origines. Cela permet également d'éviter des contaminations d'autres sites par rebond et de remettre en place le système.

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 unités de formation, les unités de recherche et les services administratifs, sont tenus :

- de réserver l'accès aux postes de travail connectés (en filaire ou sans-fil) aux réseaux informatiques de l'UPMC :
  - aux personnes pouvant justifier de leur appartenance à l'une des populations de l'université (étudiants, personnels UPMC, personnels associés, invités...);
  - aux personnes ayant reçu une autorisation d'accès délivrée par un membre du personnel ;

<sup>51</sup> RFC 1855 ; traduction en français à <http://intra.upmc.fr/DSI/DocumentsDivers/Netiquette.html>.

<sup>52</sup> Service actuellement non disponible via les instances du ministère de tutelle.



- de mettre en œuvre un mécanisme d'authentification via l'annuaire de l'établissement ou par tout autre mécanisme garantissant l'imputabilité des accès et actions que ces postes de travail permettent. Dans les cas où une telle authentification ne serait pas possible, les services réseau disponibles doivent être réduits au strict minimum.

Une politique de gestion des journaux informatiques est mise en œuvre à l'UPMC<sup>53</sup>. La mise en place de dispositifs de traçabilité sur les serveurs et services d'une unité doit s'y conformer.

Deux catégories de journaux, sur lesquels les utilisateurs peuvent exercer leur droit d'accès, ont été définies :

- les journaux dits « techniques » facilitant la recherche de dysfonctionnements, les analyses et les statistiques d'utilisation, ainsi que la détection des usages abusifs. Leur accès est réservé, dans un délai de trois mois, aux personnes administrant les ressources informatiques qui ont généré ces traces ;
- les journaux dits « légaux » conservés pour une période d'un an. Leur accès est réservé aux *Responsables de la Sécurité des Systèmes d'Information* et aux personnes de la *chaîne fonctionnelle Sécurité des Systèmes d'Information* de l'UPMC, sur requête de l'autorité judiciaire.

---

<sup>53</sup> Cf. <http://intra.upmc.fr/SSI/ReferentielUPMC/pgji-V?.pdf>.

## IX. Contrôle d'accès aux ressources

### IX.1. Politique de contrôle d'accès

Toutes les ressources informatiques (autres que les ressources publiques de type web institutionnel pas exemple) de l'UPMC doivent être protégées par un mot de passe ou autre mécanisme.

Le droit d'accès d'un utilisateur aux ressources informatiques est soumis à autorisation. Ce droit est **personnel et incessible**. Il disparaît dès que son utilisateur ne remplit plus les conditions qui lui ont autorisé l'accès.

La mise à disposition de ressources propres de l'UPMC (ou pour lesquelles l'UPMC possède un droit d'usage) est subordonnée à l'information préalable du bénéficiaire quant à ses droits et devoirs en liaison avec les conditions d'usage de ces ressources. Il exprime formellement son accord par la signature de la charte de la tutelle SSI.

Le cas échéant, l'accès à des systèmes d'information ou des applications spécifiques ou encore l'exercice de fonctions de gestion de ressources informatiques peut être conditionné à une habilitation de défense.

#### IX.1.1. Enregistrement des utilisateurs

L'UPMC dispose d'un annuaire d'établissement, référentiel des personnes base de la gestion des identités et habilitations de l'ensemble des populations ayant accès aux SI de l'université. Les accès aux services et applications devront reposer sur cet annuaire directement (interrogation de l'annuaire central) ou indirectement (interrogation d'annuaires de domaines basés sur l'annuaire central) lorsque les logiciels offrent cette possibilité.

Processus d'entrée dans l'annuaire

Processus de sortie de l'annuaire

Utilisateurs hors annuaire (ex : réunion avec accès CanalIP)

#### IX.1.2. Gestion des privilèges

Il importe de bien différencier les différents rôles et de n'attribuer que les droits nécessaires. L'attribution et la modification des accès et privilèges d'un service numérique doivent être validées par le responsable du service. Il en sera régulièrement dressé un inventaire pour les services sensibles.

### IX.1.3. Gestion du mot de passe utilisateur

Le mot de passe, base de la protection des ressources informatiques est une donnée personnelle et confidentielle. Il doit être robuste<sup>54</sup>, protégé<sup>55</sup>, dédié<sup>56</sup> et ne doit jamais être communiqué<sup>57</sup> à quiconque ; a fortiori par courriel vers une adresse masquée<sup>58</sup>...

L'usage de comptes partagés et/ou anonymes doit être évité.

L'accès aux postes de travail (et aux moyens nomades) doit être protégé par mots de passe.

Les accès aux ressources n'intégrant pas la possibilité d'une authentification via un annuaire externe (ex : serveur de calcul scientifique) doivent systématiquement permettre un échange chiffré des données d'authentifications lorsqu'ils s'effectuent de/vers un réseau externe à l'unité.

### IX.2. Contrôle d'accès au réseau

L'utilisation de réseaux de télécommunication externes met en relation des utilisateurs qui n'ont, a priori, pas les mêmes exigences de sécurité. Il est donc nécessaire de définir des modalités d'utilisation sécurisée pour les accès depuis l'extérieur comme les liaisons via ADSL. Il convient de définir les différents canaux de communication utilisés et formaliser pour chacun d'entre eux les règles d'utilisation par des contrats, des engagements de la part des utilisateurs, des tiers ou des équipes délocalisées (exemple : serveur de messagerie, sauvegardes opérées par un service externe au laboratoire).

Toute liaison vers l'extérieur autre qu'à travers le réseau de l'entité (modem, ADSL, GPRS, 3G par exemple) est interdite sauf besoins particuliers et après accord du CSSI.

### IX.3. Contrôle d'accès au système d'exploitation

Les systèmes et applications ne doivent pas donner d'indication permettant une identification précise du logiciel (nom, version, etc.) avant la connexion de l'utilisateur pour ne pas alimenter les tentatives d'accès basées sur les failles connues ou non des serveurs. L'affichage d'un message sur les restrictions d'accès est souhaitable.

La limitation du nombre de tentatives infructueuses, l'affichage d'informations sur la dernière connexion (ou tentative), la fermeture des sessions inactives, etc. sont des mesures qui doivent être appliquées si l'environnement le permet. Si cette possibilité existe, on activera le mécanisme de coupure des sessions inactives.

Si un système ou une application nécessite le stockage local de mots de passe, un chiffrement robuste sera appliqué pour prévenir l'usage détourné d'un tel fichier.

Lorsqu'elles utilisent un logiciel leur permettant d'intervenir à distance sur l'ordinateur d'un utilisateur, les personnes chargées de l'administration ou du support doivent l'en avertir et respecter les principes de la loi Informatique et Libertés.

<sup>54</sup> Non simpliste ou facile à deviner (prénom à l'envers...) ou trouver (date de naissance...).

<sup>55</sup> Si possible noté nulle part (post-it, téléphone mobile, fichier de mot de passe...).

<sup>56</sup> Différents pour chaque site ou service.

<sup>57</sup> Sauf cas exceptionnel comme la continuité d'activité en cas d'absence prolongée. (voir texte...).

<sup>58</sup> Technique d'hameçonnage (« phishing » en anglais).

Voir note <http://intra.upmc.fr/SSI/ReferentielUPMC/Hameconnage.pdf>.

## IX.4. Contrôle d'accès aux applications et à l'information

Des mécanismes permettant de limiter les données auxquels à accès l'utilisateur en fonction de son profil doivent être mis en œuvre.

### IX.4.1. Accès aux données sensibles.

Les règles de base sont :

- l'accès à une donnée sensible ne doit être possible qu'après authentification et vérification de l'habilitation de l'utilisateur ;
- une donnée sensible ne doit pas faire l'objet d'un partage non contrôlé ;
- toute information sensible circulant sur un réseau externe doit être chiffrée<sup>59</sup> ;
- tout support contenant des données sensibles transporté à l'extérieur (clé USB, CD/DVD, disque externes... ordinateurs portables) doit faire l'objet de mesure de protection contre le vol ou les informations sensibles contenues doivent être chiffrées ;
- les informations sensibles ne doivent pas être stockées ou traitées sur des systèmes informatiques non maîtrisés (cybercafé, logiciel téléchargé hors sites de confiance...) ;
- le stockage chez un prestataire externe de données sensibles est interdit, sauf dispositions contractuelles de protection ou chiffrement des données (transport et stockage).

Le chiffrement constitue un moyen privilégié de protection des données. Il est d'emploi obligatoire pour le stockage et l'échange de données particulièrement sensibles.

Les produits utilisés doivent faire l'objet d'un agrément au niveau national<sup>60</sup>. Tout chiffrement implique la mise en œuvre de procédures permettant de restituer en toutes circonstances les données en clair en cas de perte du secret permettant de les déchiffrer. Cela peut se faire par séquestre de clés, procédure de recouvrement, maintien d'une copie protégée par un autre dispositif, etc.

### IX.4.2. Isolement des systèmes sensibles

Les systèmes sensibles sont hébergés dans un environnement adéquat (type salle machine) et, si nécessaire (disponibilité), sur des serveurs dédiés et redondés.

Les accès physiques aux équipements (exemple : entrée salle machine) doivent être contrôlés. Les contrats de maintenance devront comprendre des clauses de confidentialité et décrire les procédures et moyens d'intervention.

## IX.5. Informatique mobile et télétravail

### IX.5.1. Informatique mobile et télécommunications

Les utilisateurs veillent à la sécurisation des moyens nomades mis à leur disposition ou personnel. Une vérification automatique du niveau de sécurité peut être mise en œuvre à la connexion au réseau UPMC.

<sup>59</sup> Un mot de passe est une donnée sensible...

<sup>60</sup> Voir <http://www.ssi.gouv.fr>.

Une politique de sauvegardes (fréquentes et distantes) des données mobiles et la mise en œuvre de mécanismes assurant la confidentialité des informations devront être définies pour limiter les conséquences d'une indisponibilité de l'équipement (pertes, vols, pannes... plus fréquents en itinérance). La confidentialité des informations critiques devra obligatoirement être assurée par leur chiffrement.

Les informations sensibles ne doivent pas être stockées ou traitées sur des systèmes informatiques non maîtrisés (messagerie google, cybercafé... par exemple).

La connexion au système d'information d'un tiers doit respecter les règles de sécurité de ce tiers.

### IX.5.2. Télétravail

Le télétravail doit être autorisé par le responsable hiérarchique et les ASR de l'unité informés (surveillance des systèmes).

Les droits et devoirs des utilisateurs en télétravail, en termes d'accès et d'usage du système d'information, sont les mêmes que lors de leur activité dans les locaux de l'UPMC.

La connexion au système d'information de l'UPMC doit respecter les règles de sécurité de l'UPMC et l'usage de connexions sécurisées vivement encouragée<sup>61</sup>. L'usage du réseau UPMC en tant que relais vers Internet est réservée aux ayants droits (pas de prêt de mot de passe...) et doit se faire en conformité avec la législation, la déontologie et les chartes de bon usage (UPMC, Renater).

<sup>61</sup> La DSI offre un service de VPN. Cf. <http://intra.upmc.fr/DSI/Services/VPN.html>.

## X. Acquisition, développement et maintenance des systèmes d'information

### X.1. Exigences de sécurité applicables aux systèmes d'information

La sécurité doit être prise en compte à toutes les étapes d'un projet, interne ou externe, lié au système d'information de l'entité. Pour cela, un dossier de sécurité doit accompagner chaque projet et préciser les enjeux, les méthodes, les mesures préconisées, les jalonnements et les tableaux de bord éventuels<sup>62</sup>.

Les grands projets d'application de gestion doivent comporter une étude de sécurité approuvée par le RSSI, le FSD, voire le Président de l'UPMC (en tant qu'AQSSI) selon l'importance de l'application.

### X.2. Bon fonctionnement des applications

### X.3. Mesures cryptographiques

#### X.3.1. Politique d'utilisation des mesures cryptographiques

Une politique de chiffrement est souvent utile pour la protection des données. Elle est obligatoire pour le stockage et l'échange de données considérées comme sensibles. Les produits de chiffrement utilisés doivent faire l'objet d'un agrément au niveau national.

Toute politique de chiffrement implique la mise en œuvre d'une organisation permettant de restituer en toutes circonstances les données en clair en cas de perte du secret permettant de les déchiffrer. Cela peut se faire par séquestre de clés, procédure de recouvrement, voire maintien d'une copie en clair.

Le respect de ces dispositions et la mise en œuvre effective du chiffrement sont réalisés au vu de recommandations internes et avec l'appui et le conseil de la part des chaînes fonctionnelles SSI des tutelles.

Pour les serveurs.

Toute information sensible circulant sur un réseau externe doit être chiffrée.

Idem sur portable

<sup>62</sup> Le respect de normes, standards, meilleures pratiques, recommandations, etc. sera progressivement intégré dans les cahiers de charges. Exemples : ISO 2700x, GISSIP  
(<http://www.ssi.gouv.fr/fr/confiance/documents/methodes/GISSIP-Methode-2006-12-11.pdf>).

### X.3.2. Gestion des clés

#### Certification de serveurs

L'authentification de services et le chiffrement des flux entre serveur et clients peuvent être assurés par des protocoles reposant sur un mécanisme de clés numériques nécessitant une certification (dépôt de la clé publique chez un tiers de confiance).

Les RSSI de l'UPMC sont « agents d'enregistrement » de la chaîne de certification du prestataire de l'Infrastructure de Gestion de Clés (IGC<sup>63</sup>) COMODO, prestataire retenu par Renater et le Comité Réseau des Universités (CRU).

Tous les navigateurs courants contiennent par défaut l'autorité racine de COMODO.

#### Certification de personnes

Prévu avec le prestataire COMODO.

### X.4. Sécurité des fichiers système

À développer.

### X.5. Gestion des vulnérabilités techniques

Les avis des CERTs alertent sur les applications, les systèmes et les services réseaux vulnérables et donnent les informations nécessaires pour trouver les correctifs correspondants ou mettre en œuvre des moyens palliatifs. Leur application est impérative au plus tôt sur tout système accessible depuis l'extérieur.

---

<sup>63</sup> Public Key Infrastructure (PKI) en anglais.

## **XI. Gestion des incidents liés à la sécurité de l'information**

### **XI.1. Signalement des événements et des failles liés à la sécurité de l'information**

Chaque acteur du SI, utilisateur ou administrateur doit être sensibilisé à l'importance de signaler tout incident réel ou suspecté.

Une procédure de gestion des incidents, à destination des CSSI et des administrateurs systèmes et réseaux, est diffusée par le pôle SSI de la DSI.

Le signalement des incidents à la chaîne fonctionnelle SSI est systématique. Le niveau de remontée du signalement est appréciée au regard de la gravité de l'incident et/ou du caractère sensible de l'unité concernée. L'AQSSI doit être systématiquement informé si l'incident est susceptible d'implications juridiques (dépôt de plainte par exemple).

L'information des autorités hiérarchiques est impérative lorsque l'incident peut mettre en cause l'unité dans son fonctionnement, sa sécurité, sa discipline interne, son image de marque...

Dans le cas d'unités mixtes, il convient d'informer et, le cas échéant, de se concerter avec les autres tutelles.

Les données statistiques relatives à la gestion des incidents sont intégrées dans le tableau de bord de la SSI.

Les vols d'ordinateurs ou de supports de données doivent être considérés comme des incidents de SSI et traités selon le même principe.

### **XI.2. Gestion des améliorations et incidents liés à la sécurité de l'information**

#### **XI.2.1. Responsabilités et procédures**

À développer.

#### **XI.2.2. Collecte de preuves**

La durée de conservation des fichiers de traces à des fins de preuve est précisée dans le document « politique des gestion des journaux informatiques ».



## XII. Gestion du plan de continuité de l'activité

Un plan d'urgence doit permettre d'adapter la visibilité du SI par les différentes catégories d'utilisateurs (visiteurs, acteurs, administrateurs systèmes et réseau...) en fonction d'événements extérieurs : fermeture progressive en fonction du code couleur Vigipirate, grippe pandémique, demande de l'autorité judiciaire, mesure conservatoire lors d'une attaque ciblée, dysfonctionnement notoire ou atteinte avérée à la confidentialité (principe de précaution), etc. Ce plan doit préparer une réaction ordonnée et proportionnée à des événements ou requêtes dont l'urgence ne laisse pas place à l'improvisation. Le but est d'assurer, avec une dégradation programmée et contrôlée, la continuité des services vitaux en évitant à la fois un blocage de l'activité de l'Université et la propagation (dans un sens ou dans l'autre) des conséquences d'un problème grave.

Les PRA<sup>64</sup> et/ou PCA<sup>65</sup> doivent préparer la survenue d'un sinistre majeur. Tout ou partie du SI étant ou risquant d'être altéré ou indisponible. Le PRA est la description des actions à mener avant incident (sauvegardes et tests de restaurations, « spare »<sup>66</sup> ou contrat de maintenance...), pendant l'incident (disponibilité des ressources humaines, activation de procédures de changement de matériel/système et de restauration, points de reprise...) et après l'incident (vérification de l'intégrité et du bon redémarrage de l'exploitation, rapport d'incident, retour à l'état stable « avant incident »...) en fonction des moyens affectés et d'un temps maximum que l'on s'est fixé pour le remise en disponibilité du(des) service(s). Le PCA est la description des actions à mener lors d'un passage en mode « backup » (ou en mode dégradé) d'un service préventivement redondé ou tolérant aux pannes. Il consiste principalement à gérer l'accès à une ressource devenue plus rare et à prendre toutes les mesures nécessaires à un retour rapide à la normale (avant saturation et/ou nouvelle panne).

Le plan de gestion de crise de l'UPMC intègre les risques liés à l'informatique ainsi que les risques susceptibles d'une incidence sur la sécurité des systèmes d'information. Pour ces incidents, le FSD et le RSSI sont membres de la cellule de gestion de crise.

Le RSSI prévoit le dispositif organisationnel propre aux crises de nature informatique. Il doit être informé dès le déclenchement de toute crise ayant une incidence sur la sécurité des systèmes d'information.

Exercices d'alerte  
Plan de communication de crise

### Continuité de l'activité et appréciation du risque

Les unités doivent définir un plan de continuité et les procédures correspondantes afin de limiter les conséquences sur l'activité des incidents de sécurité. Ce plan doit permettre, dans un premier temps, de maintenir, fut-ce en mode dégradé, les activités critiques, puis de récupérer et de restaurer toutes les fonctionnalités du système d'information.

Figurera dans les annexes techniques

<sup>64</sup> Plan de Reprise d'Activité.

<sup>65</sup> Plan de Continuité d'Activité.

<sup>66</sup> Équipement de secours, similaire à l'équipement en activité, en réserve sur place.

## XIII. Conformité

D'un point de vue réglementaire, l'UPMC a depuis plusieurs années intégré le « bon usage des ressources informatiques » à son règlement intérieur<sup>67</sup>. Cette charte doit avoir été lue et signée par tous les utilisateurs, y compris les visiteurs, et être affichée dans les unités. Par ailleurs, le contrat liant l'UPMC à Renater en tant que réseau national d'interconnexion des sites d'enseignement supérieur et de recherche comporte une charte déontologique<sup>68</sup> dont la signature engage l'université au respect des usages de cette infrastructure en termes de type et de volume des flux.

### XIII.1. Conformité avec les exigences légales

#### XIII.1.1. Identification de la législation en vigueur

Une veille juridique est assurée par le pôle SSI de la DSI et le service juridique de la DAG.

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 jaunes et orange du plan **Vigipirate**.

#### XIII.1.2. Propriété intellectuelle

À développer.

#### XIII.1.3. Protection des données et confidentialité des informations relatives à la vie privée

Les données à caractère personnel constituent des données sensibles et comme telles doivent faire l'objet de protection.

Chaque responsable d'unité doit vérifier la conformité à la loi N°78-17 du 6 janvier 1978 modifiée des fichiers à caractère personnel et des traitements associés dont il a la responsabilité<sup>69</sup>. Toute modification dans les catégories de données collectées, leur origine, les destinataires et la finalité d'un traitement par rapport à une « déclaration CNIL » initiale doivent faire l'objet d'un complément de déclaration.

Le CSSI contribue à l'information et la sensibilisation des responsables de traitement. Il incite à la correction d'éventuelles anomalies et, en cas de difficulté, fait part des éventuels incidents à son responsable et au RSSI.

<sup>67</sup> Voir <http://intra.upmc.fr/SSI/ReferentielUPMC/CharteDeontologiqueUPMC-V2.pdf>.

<sup>68</sup> Voir [http://www.renater.fr/IMG/pdf/charte\\_fr.pdf](http://www.renater.fr/IMG/pdf/charte_fr.pdf)

<sup>69</sup> La liste des dispenses figure à <http://www.cnil.fr/index.php?id=1746>.

#### **XIII.1.4. Mesure préventive à l'égard du mauvais usage des moyens de traitement de l'information**

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.

##### **Nomination d'un CIL à l'UPMC.**

Les CSSI des entités, sous l'autorité de leur directeur d'entité, contribuent à l'information et la sensibilisation des responsables de traitement. Ils incitent à la correction d'éventuelles anomalies et en cas de difficulté font part des éventuels incidents à leur hiérarchie et à la chaîne fonctionnelle SSI.

#### **XIII.1.5. Réglementation relative aux mesures cryptographiques**

Le stockage et la transmission de données « classifiées de défense » sont interdits sauf utilisation de moyens spécifiques agréés au niveau national.

Les données non classifiées mais présentant un caractère sensible doivent être identifiées et le cas échéant repérées selon un niveau de sensibilité.

#### **XIII.1.6. Conformité des équipements de surveillance**

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).

#### **XIII.1.7. Usage privé résiduel<sup>70</sup>**

Chaque salarié et étudiant de l'UPMC a droit à « une vie privée résiduelle » sur son lieu de travail et pendant son temps de travail (messaging, consultation web, photos de famille...). Elle doit être « raisonnable » en temps passé et en volume induit sur les réseaux et supports de données. Elle ne doit pas affecter la sécurité des réseaux, serveurs et postes de travail. La charte « de bon usage » doit préciser les limites de cet usage privé, les moyens de contrôle<sup>71</sup> et les conséquences des abus.

##### **Données privées**

La règle générale est que tout ce qui n'est pas explicitement noté « privé » (fichiers, courriels, flux...) est considéré « professionnel ».

Les contenus doivent être conformes aux lois et réglementations, à l'éthique et aux chartes de bon usage UPMC et Renater.

##### **Fichiers et répertoires**

Un répertoire ou un fichier « privé » doit être identifié par un nom exprimant sans ambiguïté ce caractère<sup>72</sup>. Son contenu doit être conforme aux lois et réglementations, à l'éthique et aux chartes de bon usage UPMC et Renater.

<sup>70</sup> Voir annexe XV.8 pour plus d'information.

<sup>71</sup> Après consultation des instances représentatives du personnel (CTP dans la fonction publique). Extrait de l'article L2323-32 du code du travail : « Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés ».

<sup>72</sup> Par exemple en faisant figurer les mots « confidentiel » ou « privé » ou « personnel » dans son nom.

## Messagerie

L'usage du poste de travail pour l'échange de courriels privés est toléré et leur contenu protégé par l'obligation de respect du secret de la correspondance. Sa violation est une infraction sanctionnée par l'article 432-9 (secteur public) du code pénal. Il ne peut être levé que dans le cadre d'une instruction pénale.

Cependant, tout message envoyé ou reçu depuis un poste professionnel est présumé « professionnel » (donc accessible par l'employeur) sauf s'il est clairement identifié comme « personnel » (dans l'objet du message par exemple ou dans le nom du répertoire spécifique dans lequel il figure).

Si l'adresse électronique utilisée est l'adresse professionnelle<sup>73</sup>, l'utilisateur veillera spécialement à éviter toute dégradation de l'image de marque de l'établissement et à éviter toute éventuelle confusion sur la nature du message (professionnelle/privée) dans l'esprit de ses correspondants.

## XIII.2. Conformité avec les politiques et normes de sécurité et conformité technique

### XIII.2.1. Conformité avec les politiques et les normes de sécurité

L'ensemble des composants du Système d'Information et leur usage doit être conformes aux PSSI -tutelle(s) et unité- en vigueur.

L'ajout de nouvelles données, de nouveaux équipements -matériels et/ou logiciels-, de nouveaux usages doivent donner lieu à une analyse de risque spécifique pour vérification de conformité ou mise à jour des PSSI en vigueur. L'avis du CSSI est requis.

### XIII.2.2. Vérification de la conformité technique

Les vérifications de conformité doivent intégrer le maintien au cours du temps de l'état de sécurité des différents matériels : application des correctifs, mises à jour des anti-virus, pare-feu, etc.

Elles doivent préciser les conditions de surveillance du fonctionnement du SI de manière à s'assurer de son état de sécurité : analyse des journaux, vérification des vulnérabilités, suivi des avis de sécurité.

## XIII.3. Prises en compte de l'audit du système d'information

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 internes ou externes, en collaboration avec le CSSI de l'unité.

<sup>73</sup> Par opposition à l'usage d'une adresse privée assortie d'un système de renvoi (alias).

# ANNEXES

DIFFUSION RESTREINTE

## XIV. Annexe générale

### XIV.1. Acronymes

- **MESR** : Ministère de l'Enseignement Supérieur et de la Recherche (<http://www.enseignementsup-recherche.gouv.fr>)
- **CPU** : Conférence des Présidents d'Université (<http://www.cpu.fr>)
- **CRU** : Comité Réseau des Universités (<http://www.cru.fr>)
- **AMUE** : Agence de Mutualisation des Universités et Établissements d'enseignement supérieur et de recherche (<http://www.amue.fr>)
- **SDS-SUP** : Schéma Directeur de la Sécurité – Enseignement Supérieur
- **RENATER** : Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche (<http://www.renater.fr>)
- **RAP** : Réseau Académique Parisien (<http://www.rap.prd.fr>)
- **CNIL** : Commission Nationale Informatique et Libertés (<http://www.cnil.fr>)
- **CIL** : Correspondant Informatique et Libertés (<http://www.cnil.fr/?id=1821>)
- **SSI** : Sécurité des Systèmes d'Information
- **PSSI** : Politique de Sécurité des Systèmes d'Information
- **RSSI** : Responsable de la Sécurité des Systèmes d'Information de l'établissement
- **AQSSI** : Autorité Qualifiée en Sécurité des Systèmes d'Information (c'est le Président, personne juridiquement responsable de l'établissement)
- **CSSI** : Chargé de la Sécurité des Systèmes d'Information des unités
- **SDSI** : Schéma Directeur des Systèmes d'Information
- **SDSSI** : Schéma Directeur de la Sécurité des Systèmes d'Information
- **GISSIP** : Guide d'Intégration de la Sécurité des Systèmes d'Information dans les Projets
- **SMSI** : Système de Management de la Sécurité de l'Information
- 
- **EBIOS** : Expression des Besoins et Identification des Objectifs de Sécurité
- **HFDS** : Haut Fonctionnaire de Défense et de Sécurité
- **FSSI** : Fonctionnaire de Sécurité des Systèmes d'information (bureau du HFDS)
- **FSD** : Fonctionnaire de Sécurité de Défense de l'établissement
- **DSI** : Direction/Directeur des systèmes d'Information
- **CoStraSI** : Comité Stratégique des Systèmes d'Information
- **ASR** : Administrateurs Systèmes et Réseau
- **VLAN** : Virtual Local Area Network (Réseau local Virtuel)
- **VPN** : Virtual Private Network (Réseau privé virtuel)
- **DICT** : Disponibilité-Intégrité-Confidentialité-Traçabilité (critères d'analyse de risques)
- **SSO** (Single Sign-On) : authentification unique. L'utilisateur ne s'authentifie qu'une fois pour accéder aux diverses applications auxquelles il a droit.
- **CAS** (Central Authentication Service) : logiciel utilisé pour mettre en œuvre un système d'authentification unique (SSO).
- **ENT** : Environnement (ou Espace) Numérique de Travail. Point d'accès unique à l'ensemble des ressources auxquelles l'utilisateur a droit. Point d'accès au SI.

## XIV.2. Vocabulaire SSI

- **bien** : tout élément représentant de la valeur pour l'organisme ;
- **moyens de traitement de l'information** : tout système, service ou infrastructure de traitement de l'information, ou locaux les abritant ;
- **sécurité de l'information** : protection de la confidentialité, de l'intégrité et de la disponibilité de l'information ; en outre, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité, peuvent également être concernées ;
- **incident lié à la sécurité de l'information** : un incident lié à la sécurité de l'information est indiqué par un ou plusieurs événement(s) de sécurité de l'information indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information ;
- **mesure de sécurité** : moyen de gérer un risque, comprenant la politique, les procédures, les lignes directrices, et les pratiques ou structures organisationnelles, et pouvant être de nature administrative, technique, gestionnaire ou juridique ;
- **menace** : cause potentielle d'un incident indésirable, pouvant entraîner des dommages au sein d'un système ou d'un organisme ;
- **vulnérabilité** : faiblesse d'un bien ou d'un groupe de biens pouvant faire l'objet d'une menace ;
- **risque** : combinaison de la probabilité d'un événement et de ses conséquences ;
- **évaluation du risque** : processus de comparaison du risque estimé avec des critères de risque donnés pour déterminer l'importance d'un risque ;
- **traitement du risque** : processus de sélection et de mise en œuvre des mesures visant à modifier le risque ;
- **management du risque** : activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque.

## XIV.3. Contexte SSI

### XIV.3.1. Aspects légaux et réglementaires

La réduction du risque juridique passe par la conformité des SI et de la SSI avec les lois et règlements en vigueur.

Les textes les plus importants concernent :

- le traitement des données à caractère personnel ;
- l'intrusion et l'usage abusif ;
- la légalité des contenus ;
- la propriété intellectuelle ;
- la communication électronique et Internet ;
- la traçabilité.

Enfin, la jurisprudence commence à cerner avec précision le périmètre d'intervention des Administrateurs Systèmes et Réseau (ASR)<sup>74</sup>.

Voir annexe XV pour en savoir plus.

### XIV.3.2. Normes et standards : bref historique

En mai 1990 (puis 1992), la France, l'Allemagne, les Pays-Bas et le Royaume Uni ont publié les *Critères d'Évaluation de la Sécurité des Systèmes Informatiques* [ITSEC] fondés sur les travaux à l'échelle nationale existant dans ces différents pays. Résultat de la convergence (1996) entre les normes de l'*Orange Book* de la NSA (USA) et celles de l'ITSEC, la norme ISO 15408<sup>75</sup> (rebaptisée « Critères Communs ») a été la première norme internationale d'évaluation du niveau de sécurité des composants d'un système d'informations.

Parallèlement un document énumérant les mesures qui doivent être prises en matière de SSI a été rédigé par la British Standards Institution (équivalent britannique de l'AFNOR) en 1995 : c'est la norme BS 7799. Il a été repris par l'ISO en 2000 (norme ISO 17799) puis enrichi en 2005 (norme ISO 27001<sup>76</sup>), en 2007 (norme ISO 27002<sup>77</sup>) et en 2008 (norme ISO 27005<sup>78</sup>).

### XIV.3.3. Sécurité et Défense

Le plan gouvernemental de vigilance, de prévention et de protection face aux menaces d'actions terroristes [VIGIPIRATE] participe à la lutte contre le terrorisme en demandant aux ministères de mettre en place et d'appliquer une série de mesures. Elle est répartie en 17 domaines d'activités dont la sécurité des systèmes d'information (SSI) fait partie. Le plan gouvernemental d'intervention contre une attaque terroriste sur les systèmes d'information [PIRANET] constitue le cœur de la réaction SSI. Il s'appuie notamment sur les mesures du plan de vigilance afin de réagir de manière efficace à la crise.

<sup>74</sup> Généralement informaticien, il met en service, assure le bon fonctionnement, maintient à jour, surveille l'exploitation et veille à l'adéquation des équipements, systèmes et applications nécessaires aux missions de l'unité.

<sup>75</sup> Technologies de l'information - Techniques de sécurité - Critères d'évaluation pour la sécurité des technologies de l'information.

<sup>76</sup> Technologies de l'information – Techniques de sécurité - Systèmes de gestion de la sécurité de l'information - Exigences.

<sup>77</sup> Technologies de l'information – Techniques de sécurité - Code de bonne pratique pour la gestion de la sécurité de l'information.

<sup>78</sup> Technologies de l'information – Techniques de sécurité - Gestion du risque en sécurité de l'information.



Voir aussi <http://www.education.gouv.fr/bo/2008/8/MENN0800143C.htm>.

#### XIV.3.4. Plan national de prévention et de lutte « Pandémie grippale »

Un plan gouvernemental de lutte contre les pandémies et ses annexes techniques<sup>79</sup> ont été élaborés en 2004 (suite à l'alerte dite « grippe aviaire ») et sont tenus à jour depuis cette date. Il a pour objectifs :

- de protéger la population contre la menace pandémique ;
- de préserver un fonctionnement aussi normal que possible du service public, de la vie sociale et économique.

Cela se traduit, pour un établissement d'enseignement supérieur et de recherche, en un certain nombre de mesures d'urgences organisationnelles, techniques et sanitaires, adaptées à chaque phase d'alerte<sup>80</sup>, telles que : stockage d'équipements destinés à freiner la contagion, activation d'une cellule de crise, communication de crise, organisation des réquisitions sur le lieu de travail et du télétravail, formation à distance, etc... La faculté de médecine de l'UPMC a son propre plan de crise.

Le plan de continuité d'activité, conçu en période hors crise, comporte un important volet SSI afin d'assurer la continuité informatique nécessaire à la continuité administrative et pédagogique (paye, messagerie, téléphonie, VPN, intranet, ENT, visioconf, vidéo à la demande, etc...).

#### XIV.3.5. Incitation du ministère de tutelle

S'appuyant sur une méthodologie élaborée par le bureau conseil de la DCSSI, le « rapport annuel SSI » des établissements d'enseignement supérieur et de recherche porte sur les systèmes standards et sensibles des périmètres gestion, pédagogie et recherche. Il propose une méthodologie en trois étapes pour chaque système de chaque périmètre : déterminer le niveau de maturité SSI adéquat (besoin), déterminer le niveau de maturité SSI effectif (état courant) et élaborer un plan d'action (de la maturité effective à la maturité adéquate).

Depuis 2008, les services du HFDS demandent aux établissements un rapport sur la cartographie de leurs « services vitaux »<sup>81</sup>. Amorce d'une étude de risque de l'ensemble des systèmes d'information de l'établissement, la « méthode SYVIT » permet d'identifier les ressources informatiques vitales, d'en apprécier les risques et les conséquences d'une atteinte à leur besoins de sécurité. Ce document ne vise pas l'exhaustivité dès sa première itération mais s'inscrit dans une démarche d'amélioration continue. Il est fondamental dans l'élaboration d'un plan de gestion de crise.

Les plan quadriennaux comportent désormais un volet SSI (à développer)

Les contrats entre les tutelles comportent un volet SSI. (à développer)

<sup>79</sup> Cf. plan [http://www.pandemie-grippale.gouv.fr/IMG/pdf/PLAN\\_PG\\_2009.pdf](http://www.pandemie-grippale.gouv.fr/IMG/pdf/PLAN_PG_2009.pdf) ; les fiches techniques : [http://www.grippeaviaire.gouv.fr/article.php3?id\\_article=574](http://www.grippeaviaire.gouv.fr/article.php3?id_article=574) ; sa déclinaison Éducation Nationale <http://www.education.gouv.fr/cid23214/menn0800945c.html>

<sup>80</sup> Voir site <http://www.pandemie-grippale.gouv.fr/sommaire2.php3>.

<sup>81</sup> Un « service vital » est un service dont l'indisponibilité, l'altération, la perte de confidentialité nuit gravement à la satisfaction de l'un des objectifs ou l'une des missions essentielles de l'université.

Le groupe de travail SDS-SUP, mandaté par la Conférence des Présidents d'Université (CPU), la direction générale de l'enseignement supérieur (DGES), la direction générale de la recherche et l'innovation (DGRI), et le Haut fonctionnaire de défense et de Sécurité (HFDS) du ministère en charge de l'enseignement supérieur et la recherche, a été créé pour adapter et accompagner la mise en œuvre du plan d'actions du SDSSI au sein des établissements d'enseignement supérieur et de recherche. L'aide à la mise en place des PSSI d'établissement fait partie de son programme de travail.

Co-piloté par la Direction de la Recherche (Ministère en charge de l'enseignement supérieur et de la recherche) et la Conférence des présidents de l'Université (CPU), le Comité Réseau des Universités (CRU) fournit conseils et recommandations pour la mise en œuvre de la sécurité dans les SI. Il est notamment l'animateur du réseau des RSSI des établissements d'enseignement supérieur et, à ce titre, élément moteur de l'élaboration de PSSI.

## XIV.4. Contexte UPMC

### XIV.4.1. Pilotage SI

L'UPMC s'est engagée en 2006 dans la rénovation complète de son système d'information en se dotant de 3 outils indissociables :

- un comité stratégique des systèmes d'information (COSTRASI) qui constitue l'organe de gouvernance du système d'information ;
- une direction des systèmes d'information (DSI) qui regroupe les principaux services de développement, auparavant dissociés ;
- un schéma directeur des systèmes d'information (SDSI) qui dresse un tableau général des outils et trace les lignes de force de leurs évolutions à venir.

#### XIV.4.1.1. Le COSTRASI

Le rôle de ce comité stratégique est permettre la concertation entre tous les acteurs, de recommander des solutions et d'arbitrer les priorités. Il facilite les prises de décisions des actions de la DSI avant d'engager la maîtrise d'œuvre. C'est l'instance de validation de l'ensemble des projets dont le cahier des charges est finalisé. Il s'assure que l'ensemble MOA et MOE fonctionne correctement et il valide les écarts au cahier des charges lorsque cela s'impose.

Comité de pilotage de la sécurité des systèmes d'information, le COSTRASI en définit les orientations stratégiques sur propositions du RSSI et les soumet au Président pour validation.

#### XIV.4.1.2. La DSI

La réflexion sur l'évolution des SI de l'UPMC doit être menée au sein de ses différentes directions (finance et comptabilité, offre pédagogique, scolarité, recherche et valorisation, bibliothèques, ressources humaines, patrimoine). La direction de l'université, sur propositions du COSTRASI, définit les priorités à partir des besoins exprimés et en fonction des ressources humaines et financières disponibles.

La DSI est chargée de proposer les réponses adaptées. En d'autres termes, la DSI a un rôle d'assistance à maîtrise d'ouvrage, de maîtrise d'œuvre, de suivi des projets et du contrôle qualité de la recette.

#### XIV.4.1.3. Le SDSI

Le schéma directeur des systèmes d'information est un document stratégique sur les orientations en termes d'adaptation des systèmes d'information au projet d'établissement. À partir de l'état des lieux de l'informatique à l'UPMC, des évolutions structurelles (LRU), pédagogiques (LMD) et de la recherche (contractualisation des liens avec les EPST (CNRS, INSERM...), il propose des objectifs en termes d'organisation SI et de fonctionnalités (référentiels, besoins métiers, interopérabilité, SSI, intégration SI MENESR...).

#### XIV.4.2. Les RSSI

La rénovation des SI s'est accompagnée d'une volonté forte d'intégrer la dimension « sécurité des systèmes d'information ». La première conséquence a été l'affectation de ressources humaines propres SSI : nomination des responsables de la sécurité des systèmes d'information et création d'un « pôle SSI » au sein de la DSI.

Les « missions RSSI »<sup>82</sup> consistent à :

- élaborer une politique de sécurité informatique suite à une étude de risques et la tenir à jour en fonction des évolutions des besoins, des usages et des technologies ;
- s'assurer que les mesures de sécurité qui en découlent sont bien mises en œuvre et que « les chartes de bon usage des ressources informatiques » de l'UPMC sont bien respectées ;
- contrôler et auditer le système d'information afin de prévenir toute dérive de son niveau de sécurité ;
- agir face à une menace ou à un incident de sécurité ;
- assurer la communication interne et externe relative à la sécurité ;
- organiser l'information et la formation SSI des utilisateurs ;
- créer et animer un réseau de « chargés de sécurité » dans les laboratoires et services.

Afin de couvrir l'ensemble de ces missions sur le périmètre défini -avec continuité du service-, cette charge est assurée par un « RSSI titulaire » et un « RSSI suppléant »

Le RSSI titulaire est responsable du pôle SSI de la DSI.

#### XIV.4.3. Les CSSI

Nommé par les directeurs d'unités en accord avec le (les) établissement(s) tutelle(s), les Chargés de Sécurité du Système d'Information des unités ont pour principales missions :

- la sensibilisation des utilisateurs du SI à leurs devoirs et l'information de leurs droits notamment par la rédaction d'une charte de bon usage des ressources informatiques et sa large diffusion (règlement intérieur, signature, affichage...) ;
- l'élaboration de la PSSI locale, sa mise en œuvre et la sensibilisation à son respect de l'ensemble des membres de l'unité. Le suivi et l'évolution de cette PSSI, l'adaptation des règles de sécurité seront ensuite une tâche récurrente ;
- la diffusion de l'information SSI et, notamment, des avis du CERT-Renater et du CERTA, les instructions et recommandations SSI des tutelles ; veiller à leur bonne application ;
- les remontées d'incidents et en assurer le suivi auprès des RSSI des tutelles en tant que maillon local de la chaîne d'alerte SSI ; participer, selon son degré d'expertise, à la résolution de l'incident jusqu'au retour à l'exploitation normale ; prendre les mesures nécessaires (ou s'assurer qu'elles sont prises) tant sur les aspects techniques qu'organisationnels.

Dans toutes ces actions, le CSSI sera assisté si besoin par le pôle SSI.

<sup>82</sup> Ces missions sont détaillées dans le document <http://intra.upmc.fr/SSI/RSSI/MissionsRSSI-V1.pdf>.

#### XIV.4.4. Le pôle SSI

Intégré à la DSI, le pôle SSI est chargé d'assister le RSSI dans ses missions.

##### XIV.4.4.1. Pilotage PSSI d'unité

Le pôle SSI a pour mission, en collaboration avec les chaînes fonctionnelles SSI des autres tutelles, d'assister les CSSI lors de l'élaboration, la mise en œuvre et l'évolution des PSSI des unités de l'UPMC. Il propose aux CSSI une méthodologie et des outils pour l'inventaire, l'analyse de risque et l'élaboration des mesures de sécurité qui en découlent.

La cartographie, l'analyse de risque, la mise en œuvre et le suivi de la politique de sécurité des systèmes d'information sous la responsabilité de la DSI (référentiels, administration de l'enseignement, administration de la recherche, gestion financière et comptable, gestion des ressources humaines, gestion du patrimoine) entrent dans le périmètre d'action du pôle SSI.

##### XIV.4.4.2. Conseil et assistance

Le pôle SSI est chargé de l'animation du réseau des CSSI des unités en coordination avec les responsables SSI des autres tutelles. Il apporte son « expertise SSI » tout au long des projets de création ou rénovation des SI et des « système vitaux » auxquels il est systématiquement associé. Il est également une force de proposition pour l'amélioration de la sécurité de l'existant.

##### XIV.4.4.3. Formation, information, sensibilisation

Il n'y a pas de SSI sans participation active de tous les acteurs. La formation, l'information, la sensibilisation de tous (responsables, chaîne fonctionnelle SSI, administrateurs systèmes et réseau, gérant de service numérique, utilisateurs finaux) sont fondamentales pour la sécurité des SI.

En coordination avec les équipes chargées de la SSI des autres tutelles, le pôle SSI organise et/ou intervient lors de séances de sensibilisation ou de formation spécifiques (exemple : formation des CSSI à l'élaboration d'une PSSI) ou génériques (exemple : « *que faire sur son poste de travail en cas d'incident* »). Il utilise principalement l'intranet (listes de distribution, ENT, canal annonce de mon.upmc...) pour l'information des utilisateurs.

Une information SSI préalable à l'usage des ressources informatiques de l'établissement de tout étudiant primo-entrant (via l'ENT ou en présentiel) et de tout nouveau membre du personnel (via l'ENT ou lors des journées d'accueil) doit être faite.

##### XIV.4.4.4. La gestion de la sécurité au quotidien

L'exploitation SSI « au jour le jour » consiste en :

- écoute d'indicateurs (analyse de logues, remontées d'alarmes, etc.) ;
- veille technologique (nouveau virus, nouvelle technologie d'attaque et de défense, etc.) ;
- actions préventives (rédaction de recommandations UPMC, conseil, diffusion des avis des CERT, etc.) ;
- actions curatives (assistance, gestion technique des incidents de sécurité, etc.).

Le pôle SSI, en coordination avec les CSSI concernés et les pôles impliqués de la DSI, est amené à tester, mettre en œuvre et exploiter des solutions (matérielles et logicielles) de surveillance de réseau, d'exécution des règles SSI, d'audit de conformité à la PSSI.

#### XIV.4.4.5. Veille technique et juridique

Une veille technique et juridique est assurée par le pôle SSI de la DSI. Il se fera assister par le Service Juridique de l'UPMC pour les aspects juridiques. Il pourra créer des groupes d'experts (généralement des administrateurs systèmes et réseau) pour la veille sur des thèmes précis (Windows, analyse post-intrusion, etc...).

Les avis et alertes du CERT Renater et du CERTA<sup>83</sup> seront relayés vers les CSSI dont le rôle consiste à prendre les mesures adéquates (information des utilisateurs, intervention ou demande d'intervention sur les objets de l'avis/alerte) en fonction de leur pertinence et de l'urgence (cf. la cartographie des systèmes de l'unité effectuée lors de l'élaboration de la PSSI d'unité).

#### XIV.4.4.6. Documentation

La documentation SSI est constituée de documents :

- politique générale (document SSI HFDS/FSSI, SDS-SUP, CRU/RSSI...) ;
- politique UPMC (chartes de bon usage, PSSI, indicateurs, rapports SSI...) ;
- alertes et avis de sécurité (recommandation des tutelles, CERT...) ;
- « recommandations » UPMC (skype, téléchargements, wifi, « pair-à-pair », gestion des journaux informatiques...) ;
- techniques (failles de sécurité, technologies SSI, action en cas d'incident...) ;
- juridiques (dispositions législatives et réglementaires) ;
- etc.

Les documents publics sont publiés dans l'espace SSI de l'intranet s'ils ne sont pas aisément disponibles par ailleurs.

### XIV.4.5. Le règlement intérieur et charte d'usage

Afin de préciser leurs conditions d'usage, l'UPMC a intégré le « bon usage des ressources informatiques » à son règlement intérieur<sup>84</sup>. Les chartes « étudiants » et « personnels » de l'UPMC destinées à la signature des intéressés en reprennent les termes.

La charte de « bon usage des ressources informatiques » de l'unité doit avoir été lue et signée par tous les utilisateurs, y compris les visiteurs, et être affichée dans les unités.

Le contrat liant l'UPMC à Renater en tant que réseau national d'interconnexion des sites d'enseignement supérieur et de recherche comporte une charte déontologique<sup>85</sup> dont la signature engage l'université au respect des usages de cette infrastructure en termes de type et de volume des flux.

<sup>83</sup> Les CERT (Computer Emergency Response Team) établissent et maintiennent une base de vulnérabilités. Ils diffusent les informations sur les précautions à prendre pour minimiser les risques d'incident ou leurs conséquences. Le CERT-RENATER est dédié à la communauté RENATER ; le CERTA est dédié au secteur de l'administration française.

<sup>84</sup> Voir <http://intra.upmc.fr/SSI/ReferentielUPMC/CharteDeontologiqueUPMC-V2.pdf>.

<sup>85</sup> Voir [http://www.renater.fr/IMG/pdf/charte\\_fr.pdf](http://www.renater.fr/IMG/pdf/charte_fr.pdf)

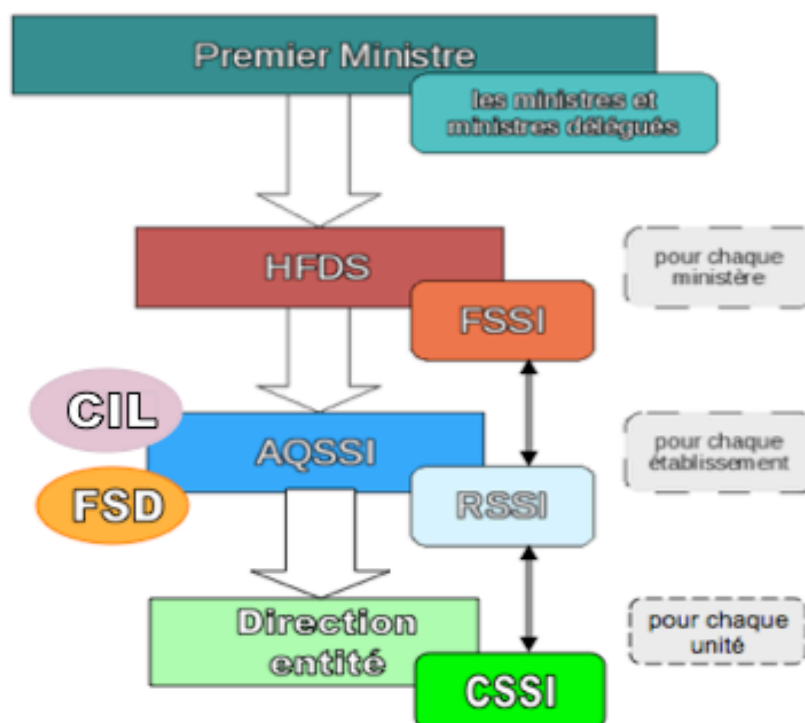
#### XIV.4.6. Les référentiels

Un référentiel est un ensemble de données (avec leurs accès) constituant les "références" d'un SI d'établissement. Les services numériques ont besoin de ces « données de référence » (si possible uniques) pour fonctionner ; c'est fondamental pour l'interopérabilité des applications et l'intégrité de leurs résultats. Ce sont, par exemple, les annuaires (des personnes, des structures, des locaux, des fournisseurs, des équipements etc.), les nomenclatures, etc.

Le référentiel de l'UPMC est en cours de constitution.

#### XIV.4.7. La chaîne fonctionnelle SSI : directive 901

La chaîne fonctionnelle SSI, inspirée de la directive interministérielle 901 :



Voir annexe XIV.1 la signification des acronymes.

## XIV.5. Critères de sécurité DICT

Les critères de sécurité sont la disponibilité, l'intégrité, la confidentialité et la traçabilité

La **Disponibilité** est la faculté d'accéder, au moment voulu, aux services et données par les utilisateurs autorisés. Les pannes diverses, les vols de matériels, les coupures d'énergie, les ruptures de fibres optiques, les attaques de types « déni de service » ou virales, etc. peuvent paralyser partiellement ou totalement le fonctionnement de l'Université.

Échelle extraite du document « cartographie des systèmes vitaux » :

Niveaux de l'échelle	Niveau	Description détaillée de l'échelle
Plus de 72 heures	0	Le système et les informations qu'il traite peuvent être indisponibles plus de 72 heures.
Entre 24 et 72 heures	1	Le système et les informations qu'il traite doivent être disponibles dans les 72 heures.
Entre 4 et 24 heures	2	Le système et les informations qu'il traite doivent être disponibles dans les 24 heures.
Moins de 4 heures	3	Le système et les informations qu'il traite doivent être disponibles dans les 4 heures.

L'**intégrité** est l'état d'un SI n'ayant pas subi de modifications, accidentelles ou délibérées, non autorisées. Les erreurs des systèmes et applications (« bugs »), l'introduction de codes malicieux, l'altération (volontaire ou non) de données, la défiguration de pages web, le détournement de serveurs, etc. peuvent être fatals à l'intégrité voire la pérennité du SI.

Échelle extraite du document « cartographie des systèmes vitaux » :

Niveaux de l'échelle	Niveau	Description détaillée de l'échelle
Altérable	0	Le système peut ne pas réaliser sa fonction conformément aux enjeux. Les informations qu'il traite peuvent ne pas être intégrées.
DéTECTABLE	1	Le système peut ne pas réaliser sa fonction conformément à ses enjeux, dans la mesure où la non conformité est identifiée. Les informations qu'il traite peuvent ne pas être intégrées, dans la mesure où l'altération est identifiée.
Maîtrisé	2	Le système vital peut ne pas réaliser sa fonction conformément à ses enjeux, dans la mesure où la non conformité est identifiée et un retour à la normale est possible. Les informations qu'il traite peuvent ne pas être intégrées, dans la mesure où l'altération est identifiée et les informations récupérables.
Intègre	3	Le système vital doit toujours réaliser sa fonction conformément à ses enjeux Les informations qu'il traite doivent être rigoureusement intégrées.

La **Confidentialité** consiste à ne divulguer l'information (données, processus, ...) qu'aux personnes ou entités ayant à en connaître. L'intrusion dans un système, le prêt ou l'attribution non contrôlée de comptes informatiques, l'envoi en maintenance de supports informatiques non « nettoyés », l'utilisation de codes d'écoute de réseaux (« sniffers ») permettent aisément à des tiers d'avoir communication de contenus plus ou moins confidentiels. La présence sur le Campus de laboratoires « sensibles » en augmente l'attractivité.



Échelle extraite du document « cartographie des systèmes vitaux » :

Niveaux de l'échelle	Niveau	Description détaillée de l'échelle
Public	0	Les informations traitées par le système vital sont publiques.
Limité	1	Les informations traitées par le système vital ne doivent être accessibles qu'au personnel de l'organisme et de ses partenaires.
Réservé	2	Les informations traitées par le système vital ne doivent être accessibles qu'aux personnes impliquées.
Privé	3	Les informations traitées par le système vital ne doivent être accessibles qu'à des personnes identifiées et ayant le besoin d'en connaître le contenu.

La **Traçabilité** est la propriété d'un système journalisant les événements en vue de l'imputabilité des actions. Les journaux d'événements (« logs ») peuvent être plus ou moins précis sur l'activité des acteurs d'un SI (de la simple note d'accès à la trace complète de toutes les actions).

Échelle :

Niveaux de l'échelle	Niveau	Description détaillée de l'échelle
Sans	0	Les accès au système et les actions ne sont pas journalisées (pas de logs).
Accès	1	Les accès au système sont journalisés mais non les différentes actions effectuée par l'utilisateur (logs partiels).
Complet	2	Les accès au système et toutes les actions des utilisateurs sont journalisés (logs complets).

## XIV.6. Avis et alertes des CERT

### XIV.6.1.1. CERT-Renater

La diffusion d'information par le CERT Renater se fait

- sous la forme de notes envoyées aux RSSI des sites.
- via le site <http://www.cert.uhp-nancy.fr/services/Securite-informatique/Avis-de-securite>

Ces informations sont réparties en quatre catégories :

- VULN : elles informent les correspondants Sécurité des vulnérabilités découvertes sur les systèmes d'exploitation et les applications ;
- STAT : elles résument, tous les vendredis, l'ensemble des incidents traités au cours de la semaine écoulée et rappellent quelques recommandations appropriées. Le CERT-RENATER utilise également les statistiques concernant les incidents traités comme indicateur pour mieux prévoir les évolutions dans les menaces et les failles utilisées ;
- INFO : elles décrivent de la manière la plus détaillée et pédagogique possible, un phénomène lié à un problème de sécurité, mais sans caractère d'urgence ;
- ALER : elles donnent l'alerte sur un problème de sécurité qui touche l'ensemble du réseau ou qui menace de s'étendre rapidement à un grand nombre de sites.

### XIV.6.1.2. CERTA

La diffusion d'information par le CERTA se fait

- sous la forme de notes envoyées aux responsables sécurité des sites.
- via le site <http://www.certa.ssi.gouv.fr>

Ces informations sont réparties en quatre catégories :

- ALE : les alertes sont des documents destinés à prévenir d'un danger immédiat ;
- AVI : les avis sont des documents faisant état de vulnérabilités et des moyens de s'en prémunir ;
- ACT : les bulletins d'actualités fournissent une illustration par l'actualité récente de certaines mesures pragmatiques à appliquer ;
- INF : Les notes d'information font état de phénomènes à portée générale.

## **XIV.7. Normes ISO/CEI 2700x et EBIOS**

Présentation succincte des normes 27000 et d'EBIOS.

### **XIV.7.1. 27001**

### **XIV.7.2. 27002**

Les objectifs de sécurité et les mesures de sécurité mentionnés doivent être sélectionnés comme partie intégrante du processus d'application du SMSI spécifié **N.N.N.**

### **XIV.7.3. 27005**

### **XIV.7.4. EBIOS**

## XIV.8. Références

- Articles 323-1 à 323-7 du Code pénal relatifs à la fraude informatique
  - Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés
  - Loi n° 88-19 du 5 janvier 1988. relative à la fraude informatique (« STAD »)
  - Loi no 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications
  - Loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information (DADVSI)
  - Loi no 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne (« LSQ »)
  - Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure (« LSI » )
  - Loi no 2003-706 du 1er août 2003 relative à la sécurité financière (« LSF »)
  - Loi n° 2004-575 du 21 juin 2004 pour la confiance en l'économie numérique
  - Loi N° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme
  - Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques
  - Loi n° 2006-911 du 24 juillet 2006 relative à l'immigration et à l'intégration (dite Sarkozy I)
  - Schéma directeur de la SSI. Organisation et orientation de la SSI pour les communautés éducatives [MENESR, mars 2005] :  
[http://www.cru.fr/\\_media/activites/securite/sdssi-livret1-organisationetorientation.pdf](http://www.cru.fr/_media/activites/securite/sdssi-livret1-organisationetorientation.pdf)
  - Cadre de cohérence technique du système d'information de l'enseignement supérieur et de la recherche [MENESR /AMUE/CPU, septembre 2008]
  - PSSI – Guide d'élaboration de politiques de sécurité des systèmes d'information [SGDN/DCSSI]
  - ISO 27001 et suivantes
  - Recommandation interministérielle n°901/DCSSI/SCSSI du 2 mars 1994 : Description de l'organisation de la SSI
  - SDSI de l'UPMC. Version 3.02.
  - Bulletin « Sécurité Informatique » ; CNRS.
  - PSSI CNRS (V1.0, 15/11/2006).
  - PSSI INSERM
  - DEC 99 8407 DCAJ ; charte utilisateur pour l'usage des ressources informatiques et de services Internet (CNRS 1999).
  - DEC 04 P014 DSI ; gestion des traces (CNRS, 11/11/04
  - EBIOS / DCSSI / SGDN
  - La sécurité des systèmes d'information. Pierre Lasbordes, député. Rapport du 26/11/05.
  - Défense et Sécurité nationale. Le livre blanc (juin 2008)
  - Lettre de mission RSSI
  - Lettre de mission CSSI
  - les plan gouvernementaux VIGIPIRATE volet SSI et PIRANET ;
  - les recommandations et documents de référence de la Direction Centrale de la Sécurité des Systèmes d'Information (SGDN/DCSSI) ;
  - le schéma directeur de la sécurité des systèmes d'information (SDSSI) du Ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche ;
  - le règlement intérieur de l'UPMC ;
  - le schéma directeur des systèmes d'information de l'UPMC ;
  - la politique de sécurité des systèmes d'information (PSSI) de l'UPMC;
  - les PSSI des établissements avec lesquels l'UPMC partage la tutelle des unités mixtes de recherche (CNRS, INSERM...) :
- [www.sg.cnrs.fr/FSD/securite-systemes/documentations\\_pdf/securite\\_systemes/PSSI-V1.pdf](http://www.sg.cnrs.fr/FSD/securite-systemes/documentations_pdf/securite_systemes/PSSI-V1.pdf)  
<https://mssi.inserm.fr/Mssi/Spip/IMG/pdf/politique-securite-Inserm.pdf>

- la charte des personnels de l'éducation nationale liée à l'usage des technologies de l'information et de la communication<sup>86</sup> ;
- la charte des organisations syndicales<sup>87</sup> ;
- la charte utilisateurs UPMC en cours de validité ;
- la charte des étudiants UPMC en cours de validité ;
- la charte administrateurs des ressources informatiques<sup>88</sup> ;
- la charte déontologique RENATER en cours de validité ;
- la charte déontologique RAP en cours de validité ;
- la charte déontologique UPMC en cours de validité.
- La « Charte pour l'usage de ressources informatiques et des services Internet » du CNRS (janvier 2007) : <http://www.dsi.cnrs.fr/BO/2007/03-07/415-bo0307-dec070007dAj.htm>.
- [http://www.upmc.fr/fr/recherche/transfert\\_technologique/gestion\\_de\\_la\\_recherche.html](http://www.upmc.fr/fr/recherche/transfert_technologique/gestion_de_la_recherche.html)
- Politique type de gestion des journaux informatiques (CRU/SDS-SUP, CPU, DR, DES, HFDS) en cours de validation par la CNIL : <http://www.cru.fr/media/activites/securite/gestiondesjournaux.pdf>.
- Politique de gestion des traces d'utilisation des moyens informatiques et des services réseau au CNRS. [http://www.apc.univ-paris7.fr/APC\\_CS/Services/Informatique/Docu/Po\\_gest\\_traces.pdf](http://www.apc.univ-paris7.fr/APC_CS/Services/Informatique/Docu/Po_gest_traces.pdf).
- Recommandations pour l'utilisation des services gratuits sur Internet : [http://www.sg.cnrs.fr/FSD/securite-systemes/documentations\\_pdf/securite\\_systemes/Recommandations%20sur%20les%20services%20gratuits.pdf](http://www.sg.cnrs.fr/FSD/securite-systemes/documentations_pdf/securite_systemes/Recommandations%20sur%20les%20services%20gratuits.pdf)
- [http://www.cnil.fr/fileadmin/documents/La\\_CNIL/publications/CNIL\\_GuideTravail.pdf](http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_GuideTravail.pdf)
- DCSSI, Guide d'élaboration de politiques de sécurité des systèmes d'information
- DCSSI, Guide d'élaboration de tableaux de bord de sécurité des systèmes d'information
- DCSSI, Présentation d'EBIOS
- <http://www.ssi.gouv.fr/fr/confiance/documents/methodes/GISSIP-Methode-2006-12-11.pdf>
- Organisation et orientations de la sécurité des systèmes d'information et de télécommunication du MJENR
- Cadre commun de la sécurité des systèmes d'information et de télécommunication
- Charte des administrateurs réseaux et systèmes. En cours de validation
- Charte liée à l'utilisation des ressources informatiques. En cours de validation
- Annexe juridique
- Guide technique type de l'utilisateur
- Exemple de charte. La charte élève (secondaire)
- fiche d'enquête CAPSEC
- ISO13335-1 : Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management
- ISO13335-3 : – Part 3: Techniques for the management of IT Security
- ISO13335-4 : – Part 4: Selection of safeguards
- ISO13335-5 : – Part 5: Management guidance on network security
- ISO17799 : Information technology – Security techniques – Code of practice for information security management
- ISO27001
- ISO27002
- ISO27005
- présentation de la norme 17799 par le CLUSIF
- Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : "vers une culture de la sécurité" , 2002
- ISO15408-1 : Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model
- ISO15408-2 : – Part 2: Security functional requirements ISO15408-3 : – Part 3: Security assurance requirements

<sup>86</sup> À paraître.

<sup>87</sup> À paraître.

<sup>88</sup> À paraître.

- Articles 226-1 à 226-8 du Code pénal
- Articles R 226-1 à R 226-8 du Code pénal
- Article 9 du Code civil
- Articles 226-13, 226-14 du Code pénal
- Loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires
- Articles 226-15, 432-9 du Code pénal
- Loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication
- Circulaire du 17 février 1988 prise en application de l'article 43 de la loi 86-1067 du 30 septembre 1986 relative à la liberté de communication, concernant le régime déclaratif applicable à certains services de communication audiovisuelle
- Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par voie de télécommunications
- DCSSI : réglementation française (décrets, directives, instructions interministérielles...) relative à la sécurité des systèmes d'information, à l'évaluation et certification et à la cryptologie.
- DCSSI : réglementation concernant la cryptologie
- DCSSI : contexte juridique européen
- <http://www.secinfo.gouv.fr/>
- Le Guide "Informatique et Libertés" pour l'enseignement supérieur et la recherche
- RGI : Référentiel Général d'Interopérabilité ([http://www.referencessmodernisation.gouv.fr/sites/default/files/RGI\\_Version1%200.pdf](http://www.referencessmodernisation.gouv.fr/sites/default/files/RGI_Version1%200.pdf)).
- RGS : Référentiel Général de Sécurité) : <http://www.ssi.gouv.fr/fr/RGS/rgs0.98.pdf>.

Pour mémoire ; à ne pas mettre dans la version finale :

- Informatique, Télécoms, Internet (Bensoussan ; Éditions Francis Lefebvre)
- Informatique et Libertés (Bensoussan ; Éditions Francis Lefebvre)
- Sécurité informatique (Bloch, Wolfhugel ; Éditions Eyrolles)
- Management de la sécurité de l'information (Fernandez-Toro ; Éditions Eyrolles)
- ITIL pour un service informatique optimal (Dumont ; Éditions Eyrolles)
- Processus métiers et SI (Morley, Hugues, Leblanc, Hugues ; Editions Dunod)

## **XIV.9. Référentiel SSI UPMC**

Mission RSSI  
Mission CSSI  
Chartes  
Journaux informatiques  
Antispam /Phishing  
Skype  
Wifi  
P2P  
Recommandations diverses

DIFFUSION RESTREINTE

## XV. Annexes juridiques

### XV.1. Loi n°78-17 (révisée) relative à l'informatique, aux fichiers et aux libertés dite « Informatique et Libertés »

*« l'informatique doit être au service de chaque citoyen »*

Cette loi concerne bien sûr les fichiers nominatifs classiques (annuaires, liste d'étudiants...) mais aussi les journaux informatiques<sup>89</sup> des composantes des SI.

Les articles pertinents vis-à-vis d'une PSSI :

- **L'article 6** (conditions de licéité des traitements de données à caractère personnel) précise que les traitements ne peuvent porter que sur des données
  - collectées et traitées de manière loyale et licite ;
  - collectées pour des finalités déterminées, explicites et légitimes ;
  - adéquates, pertinentes et non excessives au regard de leur finalité ;
  - exactes, complètes et tenues à jour ;
  - non conservées plus que la durée nécessaire aux finalités pour lesquelles elles ont été collectées.
- **L'article 7** met l'accent sur le consentement des personnes concernées et **l'article 8** sur les conditions de collecte et de traitements de « certaines catégories de données »<sup>90</sup>
- **Les articles 38 à 43** portent sur les « droits des personnes à l'égard des traitements de données à caractère personnel » (droit d'opposition au traitement, droits d'accès et de rectification des données).
- **L'article 34** ajoute l'obligation de protection de ces données : « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».
- **Les articles 50 à 52** de la loi « info et libertés » ainsi que les **articles 226-16 à 226-24 du Code Pénal**<sup>91</sup> donnent les peines encourues pour les « atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques ».

Tous les fichiers de données à caractère personnels et les traitements associés<sup>92</sup> doivent donc faire l'objet d'une déclaration simplifiée ou d'une déclaration normale ou d'une demande d'autorisation selon le niveau de sensibilité des

### XV.2. Légalité des contenus : crime (pédophilie) et délits (injures)...

<sup>89</sup> « traces », « logs » en anglais, « logues » en français, qui doivent être conformes à la politique de gestion des journaux informatiques de l'UPMC (<http://intra.upmc.fr/SSI/ReferentielUPMC/pgji-Vi?.pdf>) ou à leur déclaration CNIL spécifique.

<sup>90</sup> Par exemple, les « traitements automatisés d'informations nominatives ayant pour fin la recherche dans le domaine de la santé » nécessite une demande d'autorisation spécifique à la CNIL.

Voir également <http://www.cnil.fr/index.php?id=1536> sur l'anonymisation.

<sup>91</sup> Cf. <http://www.cnil.fr/index.php?id=303>.

<sup>92</sup> Liste des dispenses à <http://www.cnil.fr/index.php?id=1746>.



### XV.3. Droit d'auteur et propriété intellectuelle

Les articles L. 112-1 à L. 112-4 du Code de la Propriété Intellectuelle définissent les « œuvres protégées », les articles L. 122-5 à L. 122-6-2 les « droits patrimoniaux » et les articles L. 335-2 à L. 335-10 les sanctions de leur non-respect.

La loi « Droit d'Auteur et Droits Voisins dans la Société de l'Information » (DADVSI)<sup>93</sup> a principalement pour objectif la pénalisation du contournement des « mesures techniques de protection »<sup>94</sup>.

La loi « Création et Internet »<sup>95</sup> propose la création d'une autorité administrative indépendante qui aura pour rôle la mise en œuvre d'une « réponse graduée » contre le téléchargement numérique illégal.

Licence d'utilisation de logiciel

### XV.4. Atteintes aux systèmes de traitement automatisés de données (STAD)

Elles sont sanctionnées par les articles 323-1 à 323-7 du code pénal (version consolidée au 6 août 2008)<sup>96</sup>. L'article 323-3-1, introduit plus tardivement, concerne –entre autres- la conception et propagation volontaire des virus.

Sont concernés les faits suivants :

- 323-1 : *...d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système... et ...soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système... ;*
- 323-2 : *...d'entraver ou de fausser le fonctionnement d'un système... ;*
- 323-3 : *...d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données... ;*
- 323-3-1 : *...sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3... ;*

sachant que :

- 323-4 : *La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1... ;*
- 323-7 : *La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines ;*

c'est-à-dire 2 à 5 ans d'emprisonnement et 30 000 à 75 000 € d'amende.

<sup>93</sup> <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000266350&dateTexte=vig>.

<sup>94</sup> Aussi appelés « Dispositifs de Contrôle d'Usage » (DCU) ou « Digital Rights Management System (DRMS) en anglais.

<sup>95</sup> Également appelée « loi Hodapi » (pour Haute Autorité....) ou « loi Olivennes » (nom du rapporteur)

<sup>96</sup> <http://legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000006149839&cidTexte=LEGITEXT000006070719&dateTexte=vig>.

S'il n'y a pas encore -à notre connaissance- de condamnation pour « administration négligée de service numérique », le fait de ne pas sécuriser suffisamment un serveur a déjà fait son entrée dans la jurisprudence avec la relaxe d'un internaute curieux : c'est l'« affaire Tati ». Suite à la publication du mode d'accès au répertoire « clients » de la société Tati "accessible à tout internaute averti, non ingénieur, non technicien, non spécialisé, mais qui sait lire un mode d'emploi" et après information -restée sans suite- des administrateurs du serveur sur cette faille de sécurité, l'animateur du site kitetoo.com a été condamné en première instance pour accès frauduleux dans un traitement automatisé de données<sup>97</sup> puis relaxé en appel<sup>98</sup>. "Lorsqu'une base de données est, par la faute de celui qui l'exploite, en accès libre par le biais de l'utilisation d'un logiciel de navigation grand public (...), le seul fait d'en prendre connaissance (...), d'en réaliser une copie (par simple copie d'écran, ce qui a été le cas) sans intention malveillante, sans révélations permettant d'éventuelles identifications (de codes, de chiffres comptables, de clients d'une société par exemple, ...) ne saurait constituer une infraction".

## XV.5. Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique<sup>99</sup> dite « LCEN »

## XV.6. Devoir de discrétion professionnelle

Nombreuses sont les professions régies par un code de déontologie (plus ou moins reconnu devant les tribunaux) poussant leurs membres au respect d'une éthique professionnelle. Depuis le RFC 1855<sup>100</sup> introduisant en 1995 la « netiquette » c'est-à-dire les règles de base du savoir-vivre dans les rapports électroniques de l'époque (principalement courriel, listes de distribution, et news), un certain nombre de textes ont été rédigés (chartes déontologiques par exemple) pour les utilisateurs et métiers de l'informatique<sup>101</sup>.

Si le « devoir de réserve » n'existe pas en tant que tel dans le droit administratif de la fonction publique<sup>102</sup>, le « devoir de confidentialité » (ou « devoir de discrétion professionnelle ») voire le « secret professionnel » (selon leur rôle) concerne les acteurs du SI amenés, accidentellement (tout utilisateur) ou de par leur activité (intervenant « informaticiens » ou « métiers »), à accéder à des informations non publiques.

<sup>97</sup> [http://www.legalis.net/jurisprudence-decision.php3?id\\_article=152](http://www.legalis.net/jurisprudence-decision.php3?id_article=152).

<sup>98</sup> [http://www.legalis.net/jurisprudence-decision.php3?id\\_article=136](http://www.legalis.net/jurisprudence-decision.php3?id_article=136).

<sup>99</sup> <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005789847&dateTexte=vig>.

<sup>100</sup> Les « Request For Comments » sont les textes fondateurs de l'Internet (le n°1 date d'avril 1969 ; le n° 5390 d'octobre 2008) : définitions des protocoles et autres standards. Voir liste à <http://www.rfc-editor.org/rfc-index.html> et la netiquette -toujours d'actualité dans son esprit- à <http://www.sri.ucl.ac.be/SRI/rfc1855.fr.html>.

<sup>101</sup> Voir par exemple [http://fr.wikipedia.org/wiki/Éthique\\_de\\_l'informatique](http://fr.wikipedia.org/wiki/Éthique_de_l'informatique) pour l'informatique.

<sup>102</sup> Texte de référence : loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires dite « loi Le Pors » confirmé en 2001 (<http://questions.assemblee-nationale.fr/q11/11-63846QE.htm>).

## XV.7. Périmètre d'intervention des administrateurs systèmes et réseau

Entre l'obligation de protection du patrimoine de l'entité et le respect de la vie privée de ses utilisateurs, l'action de l'administrateur systèmes et réseau doit être légitimée et encadrée. L'UPMC reprendra dès que disponible la « Charte administrateurs des ressources informatiques » en cours d'élaboration par le groupe SDS-SUP du MENESR.

Extraits de « La cybersurveillance sur les lieux de travail » (CNIL, 11 février 2002)<sup>103</sup>

*« Les administrateurs qui doivent veiller à assurer le fonctionnement normal et la sécurité des réseaux et systèmes sont conduits par leurs fonctions même à avoir accès à l'ensemble des informations relatives aux utilisateurs (messagerie, connexions au internet, fichiers "logs" ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail. »*

*« Aucune exploitation à des fins autres que celles liées au bon fonctionnement et à la sécurité des applications des informations dont les administrateurs de réseaux et systèmes peuvent avoir connaissance dans l'exercice de leurs fonctions ne saurait être opérée, d'initiative ou sur ordre hiérarchique. »*

*« Tenus au secret professionnel, les administrateurs de réseaux et systèmes ne doivent pas divulguer des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de l'entreprise. Ils ne sauraient non plus être contraints de le faire, sauf disposition législative particulière en ce sens. »*

Les abus ont créé une jurisprudence (par exemple cette célèbre condamnation<sup>104</sup> adoucie en appel<sup>105</sup>).

## XV.8. Usage à titre privé des équipements informatiques mis à disposition par l'établissement

Textes de base :

- Pose du principe : extrait d'un arrêt de la cour de cassation en date du 2 octobre 2001<sup>106</sup> : *« [...] le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée; celle-ci implique en particulier le secret des correspondances; que l'employeur ne peut dès lors, sans violation de cette liberté fondamentale, prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur »*
- Idem avec restrictions : extrait d'un arrêt de la Cour de cassation en date du 17 mai 2005<sup>107</sup> : *« [...] sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé »*

<sup>103</sup> [http://www.cnil.fr/fileadmin/documents/approfondir/dossier/travail/cyber\\_fiches.pdf](http://www.cnil.fr/fileadmin/documents/approfondir/dossier/travail/cyber_fiches.pdf).

<sup>104</sup> [http://www.legalis.net/jurisprudence-decision.php3?id\\_article=167](http://www.legalis.net/jurisprudence-decision.php3?id_article=167).

<sup>105</sup> [http://www.legalis.net/jurisprudence-decision.php3?id\\_article=1182](http://www.legalis.net/jurisprudence-decision.php3?id_article=1182).

<sup>106</sup> [http://www.courdecassation.fr/jurisprudence\\_2/chambre\\_sociale\\_576/arrets\\_577/br\\_arret\\_1159.html](http://www.courdecassation.fr/jurisprudence_2/chambre_sociale_576/arrets_577/br_arret_1159.html).

<sup>107</sup> [http://www.courdecassation.fr/jurisprudence\\_2/chambre\\_sociale\\_576/arrets\\_577/br\\_arret\\_998.html](http://www.courdecassation.fr/jurisprudence_2/chambre_sociale_576/arrets_577/br_arret_998.html).

- Affirmation de la présomption du caractère professionnel : extrait d'un arrêt de la Cour de cassation en date du 18 octobre 2006<sup>108</sup> : « [...] les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors sa présence »
- Un exemple de « risque ou événement particulier » (usage déloyal) permettant à l'employeur d'accéder aux fichiers privés : extrait d'un arrêt de la Cour de cassation en date du 23 mai 2007<sup>109</sup> : Casse l'arrêt de la cour d'appel de Douai qui avait jugé que : « [...] la mesure d'instruction sollicitée et ordonnée a pour effet de donner à l'employeur connaissance de messages personnels émis et reçus par le salarié et en déduit qu'elle porte atteinte à une liberté fondamentale et n'est pas légalement admissible » parce que « [...] l'employeur avait des motifs légitimes de suspecter des actes de concurrence déloyale »
- La présomption de caractère professionnel des connexions<sup>110</sup> permet un contrôle hors la présence du salarié : extrait d'un arrêt de la Cour de cassation en date du 9 juillet 2008<sup>111</sup> : « [...] les connexions établies par un salarié sur des sites Internet pendant son temps de travail grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumées avoir un caractère professionnel de sorte que l'employeur peut les rechercher aux fins de les identifier, hors de sa présence »
- Enfin, dans un arrêt du 23 février 2009, la cour d'appel de Limoges a considéré que l'utilisation de ma messagerie professionnelle aux fins de dénigrement de son employeur est une violation de l'obligation de loyauté<sup>112</sup>.

proportionnalité de la surveillance : article L.120-2 du Code du travail.

<sup>108</sup> <http://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000007054915&dateTexte=vig>.

<sup>109</sup> [http://www.courdecassation.fr/jurisprudence\\_2/chambre\\_sociale\\_576/arrets\\_577/br\\_arret\\_10429.html](http://www.courdecassation.fr/jurisprudence_2/chambre_sociale_576/arrets_577/br_arret_10429.html).

<sup>110</sup> Dans le but de limiter les risques juridiques inhérents, L'UPMC se réserve le droit de mettre en place un système de filtrage qui empêchera techniquement l'accès à certains sites Internet à partir de tout ou partie du réseau, dans le respect du principe de transparence (consulter préalablement les représentants du personnel et/ou des étudiants, information des utilisateurs).

<sup>111</sup> <http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/cour-de-cassation-chambre-sociale-9-juillet-2008-2760.html>.

<sup>112</sup> [http://www.legalis.net/jurisprudence-decision.php3?id\\_article=2649](http://www.legalis.net/jurisprudence-decision.php3?id_article=2649).

## **XVI. Annexes techniques**

A venir.

DIFFUSION RESTREINTE