Politique de Management de la Sécurité de l'Information

Classification	Restreint : Personnel Université François Rabelais		
Référence	Politique de Management de l'Information		
Version	1.0		
	Nom Prénom	**Entité**	**Date**
Propriétaire	COPIL PSSI	Université Tours	31/10/2013
Rédigé par	MESR et Fidens SA		02 Mars 2011
Validé par	COPIL PSSI	Université Tours	
Historique des mises à jour			
Date	**Modifié par**	**Description du changement**	
31/10/2013	Christophe Pedoux	Remise en forme depuis le document originel.	

Table des matières

1. Introduction

1.1 Objet du document

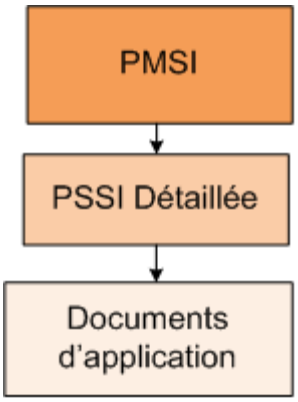
Le présent document constitue la politique de management de la sécurité de l'établissement. Il est établi conformément aux exigences exprimées par la norme ISO 27001. A ce titre,

- Il précise le domaine d'application du système de management de la sécurité ;
- Il définit les orientations générales et les grands principes en matière de sécurité de l'information ;
- Il rappelle les principales exigences légales, règlementaires, de l'établissement ;
- Il définit la stratégie de gestion du risque ;
- Il présente l'organisation dévolue au management de la sécurité ;
- Il liste les principaux documents applicables.

Cette politique de Management de la Sécurité de l'Information a pour objectif de définir un encadrement précis en matière de gestion de la sécurité des systèmes d'information de l'établissement, afin de permettre l'amélioration continue et de garantir la disponibilité, l'intégrité, la confidentialité et la traçabilité des données contre les principaux risques pouvant impacter le système, tels que l'intrusion, l'altération des données, la divulgation ou les pertes des données et l'utilisation abusive des ressources informatiques.

1.2 Référentiel documentaire du Système de Management de Sécurité de l'Information

Le Système de Management de la Sécurité de l'Information s'appuie sur un référentiel documentaire (politiques, procédures), constitué des documents suivants :



- Politique de Management de la sécurité

(Ce document)

- Politique de Sécurité du Système d'Information détaillée

Document décrivant les règles et les mesures de sécurité domaine par domaine

- Document d'application / Plan d'action de traitement des risques

Document basé sur l'analyse de risques, décrivant les actions correctives et préventives décidées et leur plan de déploiement.

- Inventaire des biens du système d'information
- Procédure de mise au rebut des biens sensibles
- Chartes d'usage et de sécurité des systèmes d'information (utilisateur, administrateur, wifi, nomades, voix sur IP, étudiants…)
- Plan d'infrastructure des bâtiments et mesures de sécurité physiques
- Politique de gestion des habilitations, des profils et des droits d'accès (physiques et logiques)

- Procédure de gestion des habilitations, des profils et des droits d'accès (physiques et logiques)
- Politique de gestion des authentifiants
- Politique de sauvegarde
- Plan de sauvegarde
- Document d'application relatif à la mobilité
- Guide de bonnes pratiques de développement
- Documents d'architecture réseau
- Procédures d'administration et d'exploitation du réseau
- Politique de contrôle et filtrage des flux réseaux
- Procédures d'exploitation des systèmes informatiques
- Procédures de configuration de sécurité des serveurs et postes de travail
- Plan de gestion des mises à jour et correctifs
- Procédure de gestion des changements
- Procédure de gestion des incidents
- Inventaire des traitements de données personnelles
- Plan de formation et sensibilisation en matière de sécurité
- Politique d'utilisation des outils de cryptographie
- Programme d'audit de sécurité du système d'information
- Inventaire des équipements réseau et de sécurité non maitrisés
- Procédure de gestion et de suivi des matériels sensibles
- Politique de journalisation
- Corpus documentaire règlementaire

2. Contexte

2.1 Domaine d'application

Le système de management de la sécurité de l'Information s'applique à l'ensemble des processus opérés par l'établissement, et à l'ensemble des moyens mis en œuvre pour réaliser ses missions au sein des activités de Gestion, Enseignement et Recherche.

2.2 Enjeux et objectifs

L'établissement se doit de protéger son patrimoine informationnel face aux risques pouvant impacter ses orientations stratégiques, ou pouvant affecter la réalisation de ses missions. Parmi les missions génériques les plus critiques de l'Établissement, on distingue :

- Formation : Une offre de formation plus lisible, cohérente et innovante, mieux adaptée à l'insertion professionnelle et aux besoins à venir
- Recherche : Une politique de recherche ambitieuse et structurante à l'échelle de l'établissement, la valorisation des travaux de recherche
- Coopération internationale : Une intégration des laboratoires dans des réseaux internationaux renforcée, avec des liens plus structurés au niveau de la formation et des échanges d'étudiants
- Support : Une meilleure définition de la gouvernance et du pilotage pour promouvoir l'efficacité par la responsabilité, un service rendu amélioré répondant aux besoins de qualité et compétitivité.

Au-delà de ces missions critiques, l'ensemble de l'activité de l'établissement s'appuie sur des informations, qui doivent être protégées tout comme les moyens informatiques (matériels et logiciels) nécessaires à leur traitement.

Pour ce faire, l'établissement s'est fixé l'objectif de mettre en place une politique de management permettant :

- D'adopter une approche globale de la sécurité ;
- De développer la culture de la sécurité au sein de l'établissement ;
- De gérer et anticiper les incidents liés à la Sécurité des Systèmes d'Information, de manière continue ;
- D'adapter les mesures de sécurité aux besoins identifiés ;
- D'impliquer la Direction dans l'arbitrage des risques.
- D'impliquer les différents services dans la mise en œuvre de la sécurité

Conformément à l'approche normative, l'établissement est chargé d'analyser les besoins de sécurité, de les décliner en mesures opérationnelles et de s'assurer de la mise en œuvre et du suivi des mesures retenues par les intervenants concernés afin :

- D'assurer la confidentialité des données sensibles qui lui sont confiées ;
- De garantir l'intégrité des données et des applications ;
- D'offrir une disponibilité appropriée de manière à assurer la continuité des services selon des conditions prédéfinies d'horaires, de délais et de performance ;

- D'assurer la traçabilité des opérations réalisées.

2.3 Contexte légal et règlementaire

Chaque établissement est responsable de ses données et doit appliquer les lois et règlements en vigueur, notamment dans les domaines suivants :

- Informatique et liberté
- Sécurité intérieure
- Propriété intellectuelle
- E-administration
- Cybercriminalité – Internet
- Éducation – Recherche

Le détail des lois sont donnés dans le document « Corpus documentaire règlementaire »

3. Grands principes

3.1 Principes de gouvernance

Le SMSI mis en œuvre tire ses bases de la norme ISO 27001 dont il décline les exigences en matière :

- d'élaboration
- de mise en œuvre
- de fonctionnement
- de surveillance et de réexamen
- de mise à jour
- d'amélioration

} d'un système de management de la sécurité

Ce SMSI s'appuie sur l'organisation décrite au paragraphe 5 de la présente politique, dans un souci de performance et d'amélioration continue.

3.2 Principes de sécurité

La Politique de Management de la Sécurité définit des principes généraux, qui seront adaptés sous forme de mesures opérationnelles propres à chacune des différentes activités fonctionnelles et techniques de l'établissement, en prenant en considération le niveau de risque de chacune d'entre elle : la PSSI est le document qui décline les règles concrètes retenues pour implémenter ces principes. Elle est complétée par des modes opératoires particuliers chaque fois que nécessaire, qui font l'objet de documents d'applications.

1. Tout utilisateur du système d'information (fonctionnaire, vacataire, contractuel, intervenant extérieur, étudiant) doit participer activement, en fonction de son niveau de responsabilité et des tâches qu'il exerce, à la mise en œuvre et au respect de la politique de management.

2. Chaque ressource matérielle ou immatérielle du système d'information est placée sous la responsabilité d'un dépositaire.

3. Chaque dépositaire définit le degré de sensibilité des composantes du Système d'Information sous sa responsabilité.

4. Les privilèges ou droits d'accès sont limités dans leur domaine d'application et leur durée et doivent être justifiés par le besoin d'en connaître. Ces droits sont à usage strictement personnel.

5. Toute opération sur une composante sensible du système d'information (traitement, accès, modification des droits d'accès) doit être formalisée et auditable. Tout ce qui n'est pas explicitement autorisé est interdit.

6. Ces principes généraux sont adaptés sous forme de mesures opérationnelles propres à chacune des différentes activités fonctionnelles et techniques de l'Établissement d'Enseignement Supérieur et au niveau de risque de chacune d'entre elle.

7. Toute dérogation aux principes de sécurité fait, au préalable, l'objet d'une justification documentée

8. Les évolutions des présents principes généraux, ainsi que leurs déclinaisons adaptées aux différentes activités sont de la responsabilité du pilote du management de la Sécurité, en accord avec le comité de pilotage.

4. Gestion des risques

4.1 Stratégie

Une analyse de risques a été réalisée sur trois périmètres (Gestion Recherche, Pédagogie), conformément à la norme ISO-27005 de Gestion des Risques. Elle est revue par le comité de sécurité opérationnelle (voir § 5.2) de façon annuelle, ainsi que lors de tout changement important du contexte.

Sur proposition du comité de sécurité opérationnelle, le comité de pilotage stratégique (voir § 5.1) décide du traitement à appliquer à chaque risque, en fonction du niveau de risque calculé et des possibilités de mettre en œuvre les mesures afférentes au traitement. Un plan de Traitement des Risques est ainsi rédigé, pour décrire les actions décidées afin de ramener les risques jugés trop importants jusqu'à un niveau acceptable. La revue annuelle de l'analyse de risques a pour objet de vérifier la réduction effective de ces risques, et d'évaluer le nouveau niveau de risque résiduel, afin d'ajuster le plan de traitement.

Pour permettre l'évaluation des risques et le choix de traitement, une échelle de 5 niveaux de risques a été retenue.

- Les risques liés à une infraction envers la loi ne peuvent pas être acceptés.
- Les risques de niveau 4 ne peuvent pas être acceptés.
- Les risques identifiés aux niveaux 4 et 3 doivent bénéficier de mesures de sécurité et être réduit au moins au niveau 2.
- Les risques de niveau 2 ; 1 et 0 sont par principe acceptés s'il existe des risques de niveau supérieur. Des mesures peuvent être mises en œuvre selon les cas.

Les délais de traitement des risques s'accordent avec les principes du Schéma Directeur de l'établissement. Cependant les risques les plus critiques de niveau 4 doivent être réduits dans un délai maximum de 12 mois.

4.2 Critères

Les critères d'appréciation des risques et l'identification des niveaux de risques acceptables sont définis dans le document d'analyse de risques élaboré à partir de la méthode EBIOS. Cette méthode permet de considérer les différentes menaces pesant sur les systèmes d'information, et l'impact qu'elles auraient sur les biens et les services de l'organisme. Ces impacts s'expriment en termes de perte de disponibilité, d'intégrité, ou de confidentialité, et sont mesurés selon des échelles également définies dans le rapport d'analyse de risques. Des objectifs et mesures de sécurité sont retenus en réponse aux risques à traiter, et sont consignés dans le plan d'action. Les nouvelles mesures de sécurité ou leurs modifications sont mentionnées dans une mise à jour de la Politique de Sécurité (PSSI).

4.3 Audit et contrôle

La mise en œuvre d'un SMSI implique le déploiement d'un certain nombre de moyens de contrôles, permettant d'examiner l'efficacité des mesures de sécurité mises en place, ainsi que le respect des règles de sécurité dans le temps. Ces contrôles sont effectués au travers de la saisie d'indicateurs, de tableaux de bords, et d'audits internes annuels. Les résultats de ces contrôles sont analysés une fois par an par le Comité de Pilotage Stratégique de la Sécurité, afin d'identifier les ajustements nécessaires dans la politique et les procédures de sécurité de l'établissement.

5. Organisation de la sécurité

5.1 Le Comité de Pilotage Stratégique

Un **Comité de Pilotage Stratégique** est mis en place, qui gère la mise en œuvre de la SSI dans l'établissement. Il donne une orientation claire, et fournit un soutien visible de la Présidence aux principes de sécurité. Il arbitre et traite les risques relatifs à la sécurité du système d'information qui lui sont remontés et réalise les arbitrages budgétaires et organisationnels inhérents à la mise en place de la politique de sécurité.

Ce comité de pilotage est composé des membres suivants :

- Le Chef de l'établissement ou son représentant direct ;
- Le Vice-Président des Technologies de l'Information et de la Communication (VP TIC) ;
- Le Vice-Président du conseil scientifique chargé de la recherche, des études doctorales et de la valorisation ;
- Le directeur de la Direction des Technologies de l'Information et de la Communication (DTIC);
- Le directeur adjoint de la DTIC ;
- Le Directeur Général des Services (DGS) ;
- Le Fonctionnaire de Sécurité de Défense (FSD) de l'établissement ;

- Le Responsable Sécurité des Systèmes d'Information (RSSI) ;
- Le RSSI adjoint ;
- Le Correspondant Informatique et Liberté (CIL);
- L'Ingénieur Hygiène et Sécurité ;

En fonction des sujets traités, des personnes qualifiées peuvent être invitées à se joindre à ce comité.

Ce comité de pilotage a pour rôle de manager le processus sécurité des systèmes informations et de réaliser le suivi, l'animation et la supervision des chantiers afférents. Pour ce faire, il s'appuie sur des états périodiques de la sécurité des systèmes d'information (incidents relevés, avancement des plans d'action, nouveaux services…) et des tableaux de bord. Il se réunit au **minimum une fois par an**.

Sous le contrôle du Chef de l'Établissement ou de son représentant, il a la charge de :

- Concevoir, proposer et promouvoir la politique de sécurité et les plans d'actions afférents ;
- Approuver le plan de traitement des risques
- Valider les actions de sensibilisation à la sécurité des systèmes d'information ;
- Proposer et mettre en œuvre les processus de suivi et de contrôle des mesures techniques et procédurales ;
- S'assurer de la pérennité de la politique et de l'adéquation des mesures de sécurité aux besoins et proposer les correctifs nécessaires.

5.2 Le Comité de Sécurité Opérationnelle

Un **Comité de Sécurité Opérationnelle** est mis en place au sein de l'établissement, afin de coordonner les activités quotidiennes liées à la sécurité, de relayer les décisions du Comité de Pilotage Stratégique et de lui fournir la visibilité nécessaire sur l'état des lieux de la sécurité du système d'information. Ce Comité de Sécurité Opérationnelle se réunit au **minimum 3 fois par an**.

Ce comité opérationnel est composé des membres suivants :

- le RSSI de l'établissement ;
- le RSSI adjoint de l'établissement ;
- les Représentants de la DTIC ;
- les Correspondants de sécurité : intégration des spécificités métiers, coordination avec les moyens existants au sein des différentes composantes ;

Le Comité de Sécurité Opérationnelle a pour mission :

- d'apprécier les risques ;
- de proposer un plan de traitement des risques en cohérence avec la procédure de gestion du changement ;
- de piloter les plans d'action sécurité nécessaires à la mise en œuvre des mesures retenues dans la politique ;

- de suivre les plans d'action à partir d'indicateurs définis (tableaux de bord) ;
- d'assurer un suivi des incidents de sécurité ;
- de prendre en compte les évolutions et les nouveaux besoins.

5.3 Fonctions présentes aux comités

Les fonctions présentes lors des différents comités sont indiquées dans ce tableau :

Fréquence :	**1 par an**	**3 par an**
Comité : Fonctions	Comité de Pilotage Stratégique	Comité de Sécurité Opérationnelle
Présidence de l'Etablissement	Président ou représentant	
Fonctionnaire de Sécurité de Défense (FSD)	FSD	
VP	Vice-Président	
CIL	CIL	
Hygiène et Sécurité	IHS	
Direction des Technologies de l'Information et de la Communication (DTIC)	Responsables DTIC	Représentants de la DTIC
Responsable du Comité de Sécurité Opérationnelle (RSSI)	RSSI	RSSI
Responsable de la Sécurité des Systèmes d'Information (RSSI)	RSSI	RSSI
Correspondant Sécurité des Systèmes d'Information (CSSI)		Les CSSI composantes ou campus
Directions métier et représentants / correspondants sécurité tutelles recherches		Responsables métier/CSSI Tutelles

5.4 Rôles et responsabilités

Un des principes fondamentaux de la gestion continue de la sécurité repose sur le besoin d'impliquer les responsables de haut niveau dans le processus : la définition et la validation de l'orientation à suivre en matière de sécurité de l'information au sein de l'établissement ne peuvent être optimisées sans la participation active de ces responsables.

Ainsi, l'organisation de la sécurité repose sur un travail de coopération entre les différents responsables et intervenants, en particulier au travers d'instances de décision dédiées.

5.4.1 Le Chef de l'Établissement ou son représentant direct

Le représentant de la **Présidence** a pour mission principale de valider la politique de sécurité et les mesures proposées afin de pallier les risques pouvant impacter le système d'information de l'Etablissement d'Enseignement Supérieur. Il participe au comité de pilotage stratégique et décide d'approuver ou non les actions proposées.

5.4.2 Le Fonctionnaire de Sécurité de Défense (FSD)

Relais fonctionnel du **Haut Fonctionnaire de Défense** et Sécurité du MESR au sein de l'Etablissement d'Enseignement Supérieur, le Fonctionnaire de Sécurité de Défense a une fonction de protection concernant le patrimoine scientifique et technique, la sécurité de l'information, la défense et la sécurité publique. Le FSD a donc pour mission de participer à l'identification et l'évaluation et au traitement des risques. Il définit, anime, coordonne les règles à appliquer et en contrôle les applications en termes de Sécurité Générale et Sécurité des Systèmes d'Information. Il s'assure de la mise en œuvre de la politique de sécurité.

5.4.3 La Direction des Technologies de l'Information et de la Communication (DTIC)

Le responsable de la Direction des Technologies de l'Information et de la Communication a pour rôle le management de la mise en œuvre de la sécurité dans sa composante :

- Valider les plans d'actions
- Faire appliquer dans son périmètre les règles de sécurité
- Informer systématiquement le responsable du Comité de Sécurité Opérationnelle (ou le RSSI) des travaux susceptibles d'impacter les dispositifs de sécurité en place ou d'influencer la cartographie de risques ;

La Direction des Technologies de l'Information et de la Communication est responsable de la déclinaison opérationnelle des règles pour la composante DTIC :

- Appliquer les mesures de sécurité;
- Participer activement à la veille sécuritaire et technologique, en collaboration avec le RSSI ;
- Vérifier régulièrement la vulnérabilité des infrastructures techniques et de remonter les résultats au RSSI ;

5.4.4 Les Responsables de la Sécurité des Systèmes d'Information (RSSI[1])

Le Responsable de la Sécurité des Systèmes d'Information a pour mission de veiller au respect de la confidentialité, l'intégrité, la disponibilité et la traçabilité des données ou informations de l'Etablissement. Il s'assure de l'identification, de l'évaluation et du traitement des risques relatifs au système d'information. Il propose, fait valider et vérifie la mise en œuvre de la politique de sécurité du SI. Il met en œuvre l'ensemble des procédures requises à cet effet et en assure le suivi et la gestion.

Le RSSI doit également veiller à la communication interne et à la sensibilisation des personnes en matière de sécurité, afin de fournir à chaque acteur le niveau d'information et de connaissances nécessaire à l'exercice de ses missions.

Le RSSI a également pour mission de :

- gérer les incidents de sécurité ;

[1] Les missions du RSSI sont précisées dans la lettre de mission qui accompagne sa désignation. A ce titre, il convient de s'y référer pour une description exhaustive.

- assurer la coordination avec les organismes concernés (tutelles, universités partenaires,
- participer à la veille technique et juridique.]

5.4.5 Le rôle de « Correspondant de Sécurité »

Le périmètre d'activité du correspondant de sécurité est celui d'une composante ou d'un campus selon organisation.

- Les correspondants de sécurité assurent le relais des décisions de sécurité vers l'ensemble des composantes qui mettent en œuvre ces mesures (unités d'enseignement, laboratoires, services techniques, domaines de gestion).
- Ils sont en charge du suivi de mise en œuvre opérationnelle de la sécurité sur les sites, du pilotage de la sécurité, et de la remontée d'information en Comité de Sécurité Opérationnelle.
- Ils répercutent les actions de sensibilisation en termes de sécurité.
- Ils collectent et remontent les besoins de sécurité des sites et contribuent à la revue de l'analyse de risque, de la PSSI, et aident à l'amélioration globale de la sécurité.
- Ils participent au traitement des incidents de sécurité et à la diffusion des avis de sécurité.
- Ils animent un réseau local de correspondants au niveau des laboratoires de recherche et autres entités hébergées (startup, associations, …)

5.4.6 Les Directions métier

Chaque **Direction métier** doit être le garant dans son domaine d'activité de l'application des règles de sécurité. Les représentants des directeurs métiers remontent les besoins de sécurité lors des analyses de risque, ou lors de tout changement important dans leur contexte de travail. Ils remontent également au RSSI, selon les procédures mises en place, tous les incidents et vulnérabilités décelés pouvant porter atteinte à la sécurité des informations (indicateurs d'alerte, tentatives d'accès non autorisées, intrusions,…)

5.4.7 Le Correspondant Informatique et Libertés (CIL)

Le Correspondant Informatique et Libertés s'assure de l'application de la loi informatique et libertés.

Il a l'obligation légale de faire un rapport d'activités annuel au responsable des traitements (le chef d'établissement).

Il remonte un bilan de ses activités au représentant de la DTIC si le chef d'établissement donne son accord.

Le CIL a également pour mission de sensibiliser le personnel à la loi informatique et libertés.

6. Mesure et amélioration de la sécurité

6.1 Amélioration du niveau de sécurité

6.1.1 Indicateurs et tableaux de bord sécurité

Le déploiement de mesures de sécurité sera suivi au travers d'indicateurs d'avancement, permettant de mesurer l'état des plans d'action.

Chaque mesure de sécurité déployée fait ensuite l'objet d'au moins un indicateur d'efficacité (un indicateur pouvant parfois regrouper plusieurs mesures). La documentation de mise en œuvre des mesures doit indiquer systématiquement les indicateurs associés.

Ces indicateurs sont suivis individuellement par le Comité de Sécurité Opérationnelle lors de chacune de ses réunions périodiques. Ils sont ensuite agrégés en Tableaux de Bords fournis au Comité de Pilotage Stratégique.

6.1.2 Audits internes techniques

Des tests et audits techniques sont menés régulièrement, sous la direction du pilote du comité sécurité opérationnelle (ou le RSSI), afin de contrôler le bon fonctionnement des mesures de sécurité déployées. Les rapports de ces audits sont étudiés par le Comité de Sécurité Opérationnelle et les conclusions remontées au Comité de Pilotage Stratégique.

6.1.3 Gestion d'incidents

La Procédure de Gestion d'incidents donne lieu à des actions correctives et préventives, permettant d'améliorer le niveau de sécurité

6.1.4 Revue de l'Analyse de risques

La revue annuelle de l'analyse de risque permet de suivre le niveau de risque résiduel, en prenant en considération les évolutions du contexte, l'évolution de la menace, et l'état des mesures de sécurité existantes à mesure de leur déploiement.

6.2 Amélioration du processus SMSI

6.2.1 Indicateurs et tableaux de bord sécurité

Le Comité de Pilotage Stratégique analyse l'ensemble des Tableaux de Bords fournis par le Comité de Sécurité Opérationnelle. Il dispose également d'indicateurs sur les procédures du processus de management de la sécurité. Ces mesures permettent d'identifier d'éventuelles pistes d'amélioration du SMSI.

6.2.2 Audits

Le Comité de Pilotage Stratégique fait réaliser à intervalles réguliers des audits, afin de vérifier le bon fonctionnement du SMSI. Les rapports d'audit sont étudiés lors des revues de direction, et les plans d'actions sont décidés et suivis.

6.3 Gestion du document de politique SMSI

La présente politique SMSI a été établie par le Comité de Sécurité Opérationnelle et validée par le Comité de Pilotage Stratégique. Elle est approuvée par la Direction, et diffusée à l'ensemble des personnels et intervenants présents au sein de l'établissement, pour application.

Cette politique est revue de façon au moins annuelle, et chaque fois qu'un changement majeur dans le contexte de l'établissement l'imposerait, sous la responsabilité du Comité de Sécurité Opérationnelle (ou le RSSI).

Un corpus documentaire accompagne et soutient la présente Politique de Management. Il est constitué par les documents indiqués au chapitre 1.2 du présent document.

7. Glossaire

Dans ce document, les acronymes et abréviations suivants sont utilisés :

SMSI Système de Management de la Sécurité de l'Information

ISO 27001 Norme ISO-27001:2005 / SMSI - Exigences

CNIL Commission Nationale Informatique et Liberté

EBIOS Expression des Besoins et Identification des Objectifs de Sécurité

(EBIOS est une méthode d'Analyse de Risques).

PSSI Politique de Sécurité des Systèmes d'Information

PMSI Politique de Management de Sécurité de l'Information

ISO International Standard Organisation, organisme international collaboratif élaborant et diffusant des normes et standards dans tous domaines.

Composante Au sein d'un établissement, terme désignant les instituts, écoles, unités de formation et de recherche (U.F.R.), départements, laboratoires et centres de recherche, etc…