ENSIAS

Politique de Sécurité du Système d'Information

Introduction

l'ENSIAS considère que son Système d'Information est indispensable à l'accomplissement de ses missions et a décide d'établir, de mettre en œuvre, de surveiller et d'améliorer de façon continue un « processus de gestion de la sécurité de l'information ».
Les premières étapes consistent à définir le domaine d'application et la politique de sécurité du Système d'Information. Ces étapes sont décrites dans le présent document, plus communément appelé « Politique de Sécurité du Système d'Information (PSSI) ».

1. Définitions

- *Actif* : tout élément représentant de la valeur pour l'organisme **[ISO/CEI 13335-1:2004]** ; on distingue les actifs primordiaux (l'information) et les actifs de support (ressources permettant de traiter l'information : matériels, personnels, réseaux, …)
- *Confidentialité* : propriété selon laquelle l'information n'est pas rendue accessible ou divulguée à des personnes, entités ou processus non autorisés
- *Disponibilité* : propriété d'être accessible et utilisable à la demande par une entité autorisée
- *Intégrité* : propriété de protection de l'exactitude et de l'exhaustivité des actifs.

2. Domaine d'application

2.1. Contexte

Fondé e en 1992, l'École Nationale Supérieure d'Informatique et d'Analyse des Systèmes (ENSIAS) est l'un des dix établissements de l'Université Mohammed V – Souissi. C'est une grande école d'ingénieurs spécialisée en Technologies de l'Information et de la

Communication. Elle a pour missions la formation d'ingénieurs d'état et la recherche en vue du développement technologique et économique du Maroc.

La formation d'ingénieur à l'ENSIAS est organisée en deux premières années d'études communes à l'ensemble de la promotion (Tronc Commun). La troisième année de spécialisation est dispensée en six options :

- Génie Logiciel,
- Business Intelligence,
- E-logistique,
- Ingénierie des Télécommunication et Réseaux,
- Systèmes Embarqués et Mobiles,
- Sécurité des Systèmes d'Information.

L'ENSIAS dispose en outre d'une formation doctorale en informatique proposée par son Centre des Etudes Doctorales ST2I (Sciences et technologies de l'Information et de l'Ingénieur).

2.2. Actifs vitaux du Système d'Information de l'ENSIAS

Les éléments du Système d'Information (SI) que l'ENSIAS considère comme essentiels (« vitaux ») à ses missions :

- les actifs de la fonction Finance,
- les actifs de la fonction Gestion du Personnel,
- les actifs de la fonction Scolarité,
- les actifs vitaux pour la recherche : gestion des contrats, des brevets et des publications.

3. Politique de Sécurité du Système d'Information

3.1. Objectifs principaux de sécurité

L’ENSIAS décide que son système d’information doit posséder les caractéristiques suivantes :

- être capable de fournir l’Information uniquement à ceux qui en ont besoin (Confidentialité) ;
- être capable de fournir l’Information en temps utile (Disponibilité) ;
- être capable de fournir de l’Information juste (Intégrité).

Pour atteindre et maintenir ses objectifs principaux de sécurité, l’ENSIAS mettra en œuvre les mesures de sécurité nécessaires, sans que ces mesures soient en contradiction avec ses principes de gouvernance et le cadre législatif.

3.2. Détail des objectifs de sécurité

3.3.1. Propriétaire des actifs

Etant donné qu’il s’agit d’une condition nécessaire à la gestion des droits d’accès aux actifs, il convient de désigner les propriétaires des actifs et de préciser les responsabilités de ces propriétaires.

Pour l’ENSIAS, les propriétaires sont désignés par le directeur de l’école, dans le respect des dispositions légales (par exemple, le propriétaire pour la fonction Finances est nécessairement l’agent comptable).

Le terme « propriétaire » identifie une personne ou une entité ayant accepté la responsabilité du contrôle de la production, de la mise au point, de la maintenance, de l’utilisation et de la protection des actifs (informations et ressources). Ce terme ne signifie pas que la personne jouit à proprement parler de droits de propriété sur le bien **(ISO 27002)**.

3.3.2. Gestion des utilisateurs

L’ENSIAS décide qu’il convient d’authentifier les utilisateurs du S.I., afin de permettre les contrôles d’accès et la journalisation ; il convient également de gérer le « cycle de vie » de ces utilisateurs pour réévaluer régulièrement leurs droits d’accès.

3.3.3. Propriétés de sécurité des actifs

L'ENSIAS décide qu'il convient d'attribuer à chaque actif un degré de confidentialité, de disponibilité et d'intégrité ; le triplet (C,D,I) résultant est indispensable à l'évaluation de la valeur de l'actif dans le processus d'analyse et d'évaluation du risque et aux mesures de sécurité devant être appliquées.

3.3.3.1. Degrés de confidentialité de l'information

Les degrés de confidentialité sont déterminés par les conséquences résultant d'une divulgation de l'information à des personnes non autorisées. Les degrés de confidentialité retenus par l'ENSIAS sont les suivants :

- **`Secret`** : perte de confidentialité grave (pertes financières importantes, sanctions administratives),
- **`Restreint`** : perte de confidentialité dommageable (atteinte à l'image de marque, baisse de confiance des partenaires, poursuites judiciaires, pertes financières faibles) ; exemple : données nominatives, sujets ou notes d'examen, données d'appels d'offre, données de recherche, supports de cours,
- **`Publique`** : perte de confidentialité sans conséquence ; exemple : sites WEB.

3.3.3.2. Degrés de disponibilité d'un actif

Les degrés de disponibilité sont déterminés par les conséquences résultant de l'impossibilité d'accéder ou d'utiliser un actif au moment désiré. Les degrés de disponibilité retenus par l'ENSIAS sont les suivants :

- **`Haute`** : indisponibilité grave ; exemple : arrêt du réseau, arrêt de la messagerie, données vitales non disponibles,
- **`Moyenne`** : indisponibilité gênante ; exemple : imprimante, accès à l'Internet,
- **`Faible`** : indisponibilité concernant des éléments de confort ou pour lesquels il existe des solutions de remplacement ; exemple : sites WEB informatifs.

3.3.3.3. Degrés d'intégrité d'un actif

Les degrés d'intégrité sont déterminés par les conséquences résultant de la modification accidentelle ou volontaire non autorisée d'une information. Les degrés d'intégrité retenus par l'ENSIAS sont les suivants :

- **Grave** ; exemple : coordonnées bancaires de tous les fournisseurs,
- **Dommageable** ; exemple : article de recherche,
- **Sans conséquence** ; exemple : coordonnée téléphonique.

3.3.4. Confidentialité

3.3.4.1. Accès logique

L'ENSIAS décide qu'il convient d'associer à chaque actif des listes de contrôles d'accès sous la forme de triplets Information/Droit d'accès/Utilisateur et qu'il est de la responsabilité du propriétaire d'un actif d'établir et maintenir ces listes de contrôle d'accès

3.3.4.2. Accès physique

L'ENSIAS décide qu'il convient de limiter l'accès physique aux ressources matérielles du S.I. afin d'être en conformité avec les critères de confidentialité définis pour les actifs hébergés par ces ressources matérielles.

3.3.5. Disponibilité et Intégrité

3.3.5.1. Conformité des sauvegardes

L'ENSIAS décide qu'il convient de vérifier que les sauvegardes des informations sont conformes aux niveaux de confidentialité, de disponibilité et d'intégrité exigés pour ces informations.

3.3.5.2. Plan de reprise d'activité

L'ENSIAS décide qu'il convient de définir, mettre en œuvre et tester un plan de reprise d'activité pour les informations jugées critiques en matière de disponibilité.

3.3.6. Respect des obligations légales de journalisation et d'archivage

3.3.6.1. Journaux

Il convient de mettre en œuvre des mécanismes de journalisation des accès aux ressources du S.I. et de gérer les durées de conservation des journaux.

3.3.6.2. Droits des utilisateurs

Il convient d'informer les utilisateurs des actions de journalisation.

3.3.7. Respect des lois

3.3.7.1. Chartes

Il convient de diffuser et de faire accepter des chartes informatiques « Utilisateurs », « Administrateurs » et « Syndicats ».

3.3.7.2. Sensibilisation

Il convient d'informer et de sensibiliser toutes les catégories d'utilisateurs sur les risques encourus par le SI.

3.3.8. Respect des « bonnes pratiques »

Indépendamment des choix politiques et des priorités d'action définis par la PSSI, l'ENSIAS décide qu'il convient de respecter au moins les recommandations « métier» en matière de SSI. Ces recommandations, appelées « bonnes pratiques » sont détaillées dans la norme

internationale ISO 27005 (Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour la gestion de la sécurité de l'information-), mais nécessitent d'être adaptées aux spécificités de l'école (**voir section 4**).

3.3.9. Processus continu de gestion de la sécurité du S.I.

3.3.9.1. Gestion continue de la sécurité

L'ENSIAS doit établir, mettre en œuvre surveiller et améliorer de façon continue un processus de gestion de la sécurité du SI.

3.3.9.2. Normes

L'ENSIAS doit s'appuyer sur les recommandations présentées dans les normes **ISO 27001 « Technologies de l'information - Techniques de sécurité - Systèmes de gestion de la sécurité de l'information - Exigences »**.

3.3. Les besoins de sécurité

- **Protection de l'outil de travail** : les postes informatiques, les réseaux, les applications et les données, constituent « le Système d'Information » de l'ENSIAS. Cet ensemble est indispensable à la fois pour les activités nécessaires à la formation et la recherche, mais aussi pour la gestion des entités. La disponibilité et l'intégrité de cet outil doivent donc impérativement être placées à l'abri de menaces internes ou externes.

- **Protection des données :** dans quelques cas il peut s'agir de « données classifiées de défense », mais le plus souvent il s'agit de « données sensibles » telles que :

    - Les données scientifiques : liées à des contrats industriels, à un savoir-faire interne, expérimentales, liées à des coopérations nationales ou internationales, scientifiques, techniques, économiques, liées à la formation des élèves ingénieurs ou la recherche au centre doctorale.
    - Les données de gestion : authentification, gestion comptable et financière, gestion des ressources humaines, documents contractuels.

- Les données nominatives : liées à la vie privée des étudiants, liées à l'enseignement (notes, adresse, contacts, etc).
- Les données stratégiques : informations d'ordre politique ou stratégique ou touchant des questions de défense, informations sécurité…

La protection des données sensibles suppose l'identification préalable de ces données, la détermination du type de protection nécessaire (confidentialité, disponibilité, intégrité) et l'évaluation de leur degré de sensibilité (quantification des besoins de sécurité).

La sensibilité des données est appréciée lors d'un inventaire au cours duquel des questions touchant à « la vie de la donnée » doivent être posées :

Quel est son type ?
Où réside t-elle ?
Par qui est-elle partagée (« besoin d'en connaître ») ?
Quelle(s) menace(s) est-elle susceptible de subir ?

- **Protection juridique :** la mise en œuvre des systèmes d'information s'inscrit dans un cadre législatif et réglementaire destiné en particulier à protéger les droits de propriété intellectuelle et industrielle et ceux de la vie privée (fichiers nominatifs, cyber surveillance…). Dans ce cadre, la responsabilité administrative et pénale de la hiérarchie et des administrateurs systèmes et réseaux peut être recherchée.

3.4. Les Menaces et les impacts

3.4.1. Les menaces :

La mise à exécution de menaces volontaires ou involontaires, humaines ou matérielles peut porter atteinte au SI, aux personnels et à l'organisme. Il convient de distinguer ce qui relève **d'attaques délibérées (agressions)** et ce qui relève de **sinistres naturels** (incendie, explosion, inondations…).

Dans le cadre d'une étude de risques, il est possible de considérer les menaces comme la méthode EBIOS (*) le préconise, c'est-à-dire inventorier les menaces en considérant la probabilité que la menace devienne réalité; la menace est prise en compte en fonction des critères suivants :

- Type d'élément menaçant : environnemental ou humain ou naturel;
- Cause d'élément menaçant : délibérée ou accidentelle;
- Potentiel d'attaque : opportunités ou ressources limitées, accidentel et aléatoire, haut degré d'expertise d'opportunité et de ressources.

(*) EBIOS : *« Expression des Besoins et Identification des Objectifs de Sécurité »* : démarche d'analyse de sécurité élaborée par la Direction Centrale de la Sécurité des Systèmes d'Information du SGDN en france.

3.4.1. Les impacts :

Les impacts des attaques sur les critères de sécurité peuvent se traduire ainsi :

Critères	Attaques	Impacts
Confidentialité	**Divulgation**, accès par des tiers non autorisés et **détournement** à des fins délictueuses, de données confidentielles (touchant des travaux confidentiels, des données scientifiques ou technologiques, des données personnelles telles que médicales ou financières…), que ces données soient stockées ou échangées (messagerie)	Pertes du patrimoine scientifique ; pertes d'avance technologique et technique ; pertes financières ; contentieux juridique
Disponibilité	**Vol de matériel**, **émission de malware** (virus, ver, déni de service…)	Interruption de service ; paralysie ou désorganisation conduisant à l'incapacité opérationnelle de fonctionnement, de décision, de gestion, de sécurisation ; saturation de ressources, de systèmes d'alerte ; perte de données précieuses (scientifiques ou de gestion) par absence ou insuffisance de sauvegarde ; atteinte à la sécurité du personnel, des usagers ; perte d'image de marque
Intégrité	**Modification accidentelle ou délibérée** (défiguration de sites Web…), **piégeage** de systèmes d'information, **émission de malware** (bombes logiques, chevaux de Troie, sniffeurs…), **vol** ou **détournement** de moyens informatiques à des fins délictueuses (compromission de serveurs…)	Résultats de fonction incomplets ou incorrects ; expérimentations non crédibles ; prises de décisions inadaptées ; appropriation frauduleuse de biens ; prise de contrôle d'un système physique ; perte du patrimoine scientifique ; perte d'image de marque ; atteinte à des libertés individuelles (cybersurveillance indue…)

À partir des menaces retenues, il convient d'évaluer les risques pour chacune d'entre elles (probabilité d'occurrence et mesure des conséquences).

Les parades viseront donc à peser sur ces deux facteurs : réduire la probabilité d'occurrence, atténuer l'impact en cas de réalisation effective de la menace.

Inversement des éléments tels que la négligence, l'insuffisance de formation ou d'information, les insuffisances de management de la sécurité, l'absence de consignes claires… sont des facteurs aggravants du risque, en amplifiant la probabilité d'occurrence de la menace ou la conséquence de l'incident survenu. En conséquence il est nécessaire de procéder à une analyse de risques.

4. Règles de sécurité

Afin de protéger le patrimoine de l'ENSIAS et d'en maîtriser les risques de sécurité de l'information, les règles suivantes doivent être appliquées par les personnes concernées :

Thème (EBIOS 2010)	Mesure de sécurité
5.1. Politique de sécurité de l'information	Une politique de sécurité de l'information doit exister La politique de sécurité de l'information doit être révisée au moins une fois par an
6.1. Organisation interne	La direction doit soutenir la sécurité de l'information Les responsabilités en matière de sécurité de l'information doivent être définies Les exigences en matière d'engagement de confidentialité doivent être définies
6.2. Tiers	Les visiteurs dans les locaux doivent être systématiquement accompagnés Les visiteurs doivent être systématiquement enregistrés Un engagement de confidentialité doit être signé par les cotraitants, la maintenance, le personnel de nettoyage et les partenaires
7.1. Responsabilités relatives aux biens	Les documents liés aux notes et aux dossiers d'inscription des étudiants, ainsi que les publications/résultats de recherches doivent être systématiquement rangés dans un meuble fermé à clef Les documents de sécurité de l'information ainsi que l'architecture réseau et service installés doivent être rangés dans un meuble fermé à clef Un inventaire des biens sensibles doit être réalisé
7.2. Classification des informations	Le besoin de confidentialité des documents électroniques liés aux dossiers d'inscription des étudiants, notes et diplômes ou attestations doit être marqué Le besoin de confidentialité des documents papiers liés aux dossiers d'inscription des étudiants, notes et diplômes ou attestations

	doit être marqué
9.1. Zones sécurisées	L'accès aux locaux doit être interdit à toute personne (dont le personnel de nettoyage) sans la présence de membres du personnel Des dispositifs de lutte contre l'incendie doivent être mis en place Une alarme anti-intrusion doit être activée durant les heures de fermeture Les locaux doivent être fermés à clef en cas d'absence de personnels
15.1.3 Protection des enregistrements de l'organisme	Une sauvegarde régulière des données avec des processus de restauration validés doit être mise en place.
15.1.4 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.
11.2. Gestion de l'accès utilisateur	Une politique de moindre privilège doit être adoptée
11.4. Contrôle d'accès au réseau	Seuls les services nécessaires doivent pouvoir être accédés
11.5. Contrôle d'accès au système d'exploitation	Un contrôle d'accès par mot de passe doit être mis en place sous Windows XP pour les ordinateurs utilisés dans les salles des TPs L'identifiant des utilisateurs doit être unique
11.6. Contrôle d'accès aux applications et à l'information	Les accès nécessaires pour la maintenance doivent être restreints
12.2. Bon fonctionnement des applications	Un système RAID logiciel doit être mis en place pour assurer le bon fonctionnement utilisé lors des travaux pratique des étudiant.
10.2. Gestion de la prestation de service par un tiers	Un accord sur le niveau de service de l'hébergeur doit être établi
10.10. Surveillance	Les événements informatiques (accès, erreurs…) doivent être journalisés
9.2. Sécurité du matériel	Une climatisation doit être installée. Des antivols doivent être utilisés pour matériel des TPs
10.6. Gestion de la sécurité des réseaux	L'accès en entrée (messagerie, services WEB…) doit être restreint Le WPA2 doit être activé pour le réseau WIFI de l'ENSIAS

Annexe I : description des premières étapes à mettre en œuvre

- **Sensibiliser les utilisateurs aux « risques informatiques » et à la loi « informatique et libertés » :**

Le principal risque en matière de sécurité informatique est l'erreur humaine. La formation, la sensibilisation et l'information des utilisateurs sont donc cruciales pour la sécurité. Cette sensibilisation peut prendre la forme de formations, de séminaires, de diffusion de notes de service, ou de l'envoi périodique de fiches pratiques. La sensibilisation se fait de manière permanente. Elle sera également formalisée dans un document, de type « charte informatique », qui pourra préciser les règles à respecter en matière de sécurité informatique. Ce document

devrait également rappeler les conditions dans lesquelles un utilisateur peut créer un fichier contenant des données personnelles, par exemple après avoir obtenu l'accord du CIL de l'établissement.

- **Nommer un Correspondant Informatique et Libertés (CIL) :**

Le CIL permet de garantir la conformité de l'organisme à la loi « informatique et libertés ». Cette maîtrise des risques juridiques est d'autant plus importante que certains manquements à la loi du 6 janvier 1978 sont pénalement sanctionnés. La désignation d'un CIL entraîne la dispense de déclarations des traitements auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL). Le CIL est alors chargé de tenir un registre des traitements, mis à disposition du public et de la CNIL. L'une des missions du CIL est de s'assurer que toutes les précautions utiles ont été prises pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des personnes non autorisées y aient accès.

- **Diffuser et faire accepter une charte informatique « Utilisateur » :**

Préalablement à son accès aux outils informatiques, l'utilisateur doit obligatoirement prendre connaissance des droits et devoirs que lui confère la mise à disposition par l'Université Lille1 de ces outils. Cette information se fait au travers d'une charte informatique, qui énonce la « loi commune » régissant l'utilisation des moyens informatiques ; elle est intégrée dans le règlement intérieur.

- **Identifier précisément qui peut avoir accès aux données :**

L'accès aux données traitées dans un fichier doit être limité aux seules personnes qui peuvent légitimement y avoir accès pour l'exécution des missions qui leur sont confiées. De cette analyse, dépend « le profil d'habilitation » de l'agent concerné. La clarification du processus d'arrivée, de déménagement et de départ d'un agent, permet au supérieur hiérarchique concerné d'identifier le ou les fichiers auxquels celui-ci a besoin d'accéder et faire procéder à la mise à jour de ses droits d'accès. Une vérification périodique des profils des applications et des droits d'accès aux répertoires sur les serveurs est donc nécessaire afin de s'assurer de l'adéquation des droits offerts et de la réalité des fonctions occupées par chacun.