Projet SIDES

Politique de Sécurité du Système d'Information
PSSI

V 1.0 – Juillet 2014

Classification	Restreint UJF et Universités membres de SIDES		
Version	V 1.0		
	Nom Prénom	Entité	Date
Propriétaire		Université Joseph Fourier	30 juin 2014
Rédigé par	Martinet Bernard	UJF	30 juin 2014
Validé par			
Historique des mises à jour			
Date	Modifié par	Description du changement	

Table des matières

PSSI du projet SIDES

1. AVANT PROPOS

1.1 Objectifs de la PSSI

Le passage à l'informatisation des épreuves nationales classantes (**ECN**) est à l'origine de deux projets intimement liés. Premièrement, le CNG du ministère de la Santé, qui est en charge des ECN, envisage des épreuves dématérialisées pour mai 2016. Le principe est de réaliser les ECN sur tablettes tactiles avec correction automatique. Deuxièmement, les universités, de leur côté, s'organisent pour proposer à leurs étudiants une préparation adaptée à ce type de support. Pour cela, elles partagent une même plate-forme d'évaluation, intitulée SIDES, avec la constitution d'une base de données docimologique nationale d'entraînement qui est ouverte depuis novembre 2013. Un environnement propre à chaque université est disponible sur cette plate-forme pour la mise en œuvre des examens des formations en santé.

Les Universités qui utilisent SIDES manipulent des éléments potentiellement sensibles en terme de disponibilité, d'intégrité et de confidentialité ; Il est donc nécessaire pour chaque Université de mettre en place un système de gestion de la sécurité de l'information adapté à ces besoins spécifiques.

Pour atteindre cet objectif, l'Université Joseph Fourier – Grenoble 1 s'est donné pour mission de fournir une analyse de risque ainsi qu'une politique de sécurité initiale qui pourra être déclinée dans chaque établissement.

[ISO 27001 - A 5.1.1]	Politique de sécurité de l'information

La Politique de Sécurité des Systèmes d'Information est le document de référence pour l'Établissement, qui énonce les règles opérationnelles de sécurité qui doivent être implémentées. Ces règles découlent des mesures sélectionnées en réponse aux risques évalués sur l'ensemble du périmètre de l'Etablissement.

Les règles de sécurité décrites dans la PSSI sont ordonnées et référencées selon les thèmes ISO-27002 (ou annexe A ISO-27001) afin de faciliter la gestion des risques, leur suivi de mise en œuvre et la conduite d'audit du SI ou SMSI conformément à l'ISO-27001.

La ou les mesures de l'annexe A de la norme ISO-27001 sont rappelées en encadré au-dessus de la ou des règles de sécurité plus précises définies par la PSSI, comme c'est le cas en tête de ce paragraphe.

1.2 Périmètre

La PSSI s'applique à l'ensemble du système d'information du projet SIDES.

Par "Système d'Information", il faut comprendre l'ensemble des moyens mis en œuvre par l'Établissement pour opérer le service. Ainsi, au-delà des matériels informatiques, des logiciels et des données manipulées, la PSSI définit aussi des règles de sécurité relatives à l'organisation, aux personnes opérant ces systèmes et à leurs infrastructures d'accueil.

2. GESTION DE LA POLITIQUE DE SECURITE

2.1 Organisation pour la gestion de la SSI

Une politique de management de la sécurité de l'Information décrit les processus et les rôles et responsabilités des intervenants en matière de gestion de la sécurité.

Un Comité de Sécurité SIDES est mis en place au sein de l'établissement, afin de coordonner les activités liées à la sécurité, de relayer les décisions du Comité de Pilotage Stratégique d'Etablissement et de lui fournir la visibilité nécessaire sur l'état des lieux de la sécurité du système d'information en regard des règles de la PSSI.

2.2 Mise en œuvre de la politique de sécurité

La présente Politique de Sécurité est rédigée sous la responsabilité du Comité de Sécurité SIDES d'Etablissement et fait suite à une analyse de risques menée sur le SI de SIDES. La stratégie de traitement des risques retenues et les règles de sécurité en résultant doivent être mises en œuvre, appliquées et contrôlées par les intervenants concernés.

La mise en œuvre opérationnelle des règles, par les différentes catégories de personnels, est appuyée par des documents d'application.

2.3 Approbation et Diffusion

La PSSI est approuvée par le président de l'établissement. C'est un document à diffusion restreinte à l'établissement et à certains de ses partenaires. Elle est diffusée à tout le personnel de l'établissement ayant le besoin d'en connaître.

2.4 Contrôle et suivi

Des contrôles de mise en œuvre opérationnelle et d'efficacité des règles de sécurité énoncées sont définis et réalisés. Le plan d'audit annuel est proposé par le responsable du Comité de Sécurité SIDES de l'Etablissement et validé par le Comité de Sécurité SIDES de l'Etablissement.

La PSSI sert de référentiel aux audits internes de la Sécurité des Systèmes d'Information. A ce titre, les manquements ou défauts d'implémentation sont identifiés et analysés par le Comité de Sécurité SIDES de l'Etablissement.

2.5 Gestion des évolutions

[ISO 27001 - A 5.1.2]	Revue des politiques de sécurité de l'information

Le Comité de Sécurité SIDES de l'Etablissement procède à la mise à jour de la PSSI en fonction des évolutions du système d'information, des besoins de sécurité, et des risques identifiés.

La PSSI est revue tous les ans par le Comité de Sécurité SIDES de l'Etablissement et soumise à validation par le Comité de Pilotage Stratégique. Le président de l'établissement approuve la version finalisée du document.

3. Organisation Interne

3.1 Fonctions et Responsabilités

[ISO 27001 - A 6.1.1]	Fonctions et responsabilités liées à la sécurité de l'information

Toutes les responsabilités en matière de sécurité de l'information du projet SIDES doivent être définies et attribuées.

3.2 Relations avec les autorités

[ISO 27001 - A 6.1.3]	Relation avec les autorités

Des relations appropriées avec les autorités compétentes doivent être entretenues.

3.3 Relations avec un groupe de travail national

[ISO 27001 - A 6.1.4]	Relation avec des groupes de travail spécialisés

Des relations appropriées avec un groupe de travail national sur l'évolution de la PSSI du projet SIDES doivent être entretenues.

4. Formation et Sensibilisation

La formation et la sensibilisation des personnes à la sécurité de l'information constituent un maillon essentiel de la sécurité. Ainsi, une sensibilisation à la sécurité du projet SIDES doit être mise en place et suivie par tous les acteurs impliqués dans les projets, enseignants, services scolarité, informaticiens.

[ISO 27001 - A.7.2.2]	Sensibilisation, apprentissage et formation à la sécurité de l'information

L'ensemble des acteurs du projet SIDES et, quand cela est pertinent, des sous-traitants, doit bénéficier d'une sensibilisation et de formations adaptées et recevoir régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leurs fonctions.

5. Contrôle d'accès

5.1 Politique de contrôle d'accès

[ISO 27001 - A.9.1.1]	Politique de contrôle d'accès

Une politique de contrôle d'accès doit être établie, documentée et revue sur la base des exigences métier et de sécurité de l'information

5.2 Gestions de l'accès utilisateurs

[ISO 27001 - A.9.2.1]	Enregistrement et désinscription des utilisateurs

Un processus formel d'enregistrement et de désinscription des utilisateurs doit être mis en œuvre pour permettre l'attribution des droits d'accès.

ISO 27001 - A.9.2.2	Distribution des accès aux utilisateurs

Un processus formel de distribution des accès aux utilisateurs doit être mis en œuvre pour attribuer et retirer des droits d'accès à tous types d'utilisateurs sur l'ensemble des services et des systèmes.

ISO 27001 - A.9.2.3	Gestion des droits d'accès à privilèges

L'allocation et l'utilisation des droits d'accès à privilèges doivent être restreintes et contrôlées.

[ISO 27001- A.9.2.4]	Gestion des informations secrètes d'authentification des utilisateurs

L'attribution des informations secrètes d'authentification doit être réalisée dans le cadre d'un processus de gestion formel.

[ISO 27001 - A.9.2.5]	Revue des droits d'accès utilisateurs

Les propriétaires d'actifs doivent vérifier les droits d'accès des utilisateurs à intervalles **réguliers.**

5.3 Contrôle de l'accès au système et à l'information

[ISO 27001 - A.9.4.1]	Restriction d'accès à l'information

L'accès à l'information et aux fonctions d'application système doit être restreint conformément à la politique de contrôle d'accès.

[ISO 27001 - A.9.4.2]	Sécuriser les procédures de connexion

L'accès aux systèmes et aux applications doit être contrôlé par une procédure de connexion sécurisée.

6. Mesures cryptographiques

[ISO 27001 - A.10.1.1	*Politique d'utilisation des mesures cryptographiques*

Une politique d'utilisation des mesures cryptographiques en vue de protéger l'information doit être élaborée et mise en œuvre

Chaque fois que cela sera possible les flux d'information seront chiffrés.

7. Sécurité Physique

Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'organisation

7.1 Zones sécurisées

ISO 27001 - A.11.1.1 Périmètre de sécurité physique

Des périmètres de sécurité doivent être définis et utilisés pour protéger les zones contenant l'information sensible ou critique et les moyens de traitement de l'information.

Un contrôle d'accès renforcé au local de stockage des tablettes numériques doit être mis en place.

7.2 Matériels

ISO 27001 - A.11.2.1	Emplacement et protection des matériels

Les matériels doivent être localisés et protégés afin de réduire les risques d'accès non autorisés.

Les tablettes numériques devront être stockées dans un local spécialisé protégé.

8. Sécurité liée à l'exploitation

Nombre des mesures ci-dessous sont concentrées sur la partie « serveur » du projet SIDES et concernent en premier lieu les équipes de développement et d'exploitation.

8.1 Procédures et responsabilités liées à l'exploitation

ISO 27001 - A.12.1.1	Procédures d'exploitation documentées

Les procédures d'exploitation doivent être documentées et mises à disposition de tous les utilisateurs concernés.

Côté établissement, on insistera particulièrement sur la formation correcte aux usages de la plate-forme SIDES, et on s'assurera que le personnel formé le soit en nombre suffisant.

ISO 27001 - A.12.1.3	Dimensionnement

L'utilisation des ressources doit être surveillée et ajustée et des projections sur les dimensionnements futurs doivent être effectuées pour garantir les performances exigées du système.

8.2 Journalisation et surveillance

ISO 27001 - A.12.4.1	Journalisation des événements

Des journaux d'événements enregistrant les activités de l'utilisateur, les exceptions, les défaillances et les événements liés à la sécurité de l'information doivent être créés, tenus à jour et vérifiés régulièrement. Ces journaux sont conservés pendant une durée conforme à la réglementation en vigueur.

9. Sécurité des communications

9.1 Gestion de la sécurité des réseaux

ISO 27001 - A.13.1.1	Contrôle des réseaux

Les réseaux doivent être gérés et contrôlés pour protéger l'information contenue dans les systèmes et les applications.

ISO 27001 - A.13.1.2	Sécurité des services de réseau

Pour tous les services de réseau, les mécanismes de sécurité, les niveaux de service et les exigences de gestion, doivent être identifiés et intégrés dans les accords de services de réseau, que ces services soient fournis en interne ou externalisés.

ISO 27001 - A.13.1.3	Cloisonnement des réseaux

Les groupes de services d'information, d'utilisateurs et de systèmes d'information doivent être cloisonnés sur les réseaux.

10. Sécurité des processus de développement et d'assistance technique

Nombre des mesures ci-dessous sont concentrées sur la partie « serveur » du projet SIDES et concernent en premier lieu les équipes de développement et d'exploitation.

ISO 27001 - A.14.2.1	Politique de développement sécurisé

Des règles de développement des logiciels et des systèmes doivent être établies et appliquées aux développements de SIDES.

ISO 27001 - A.14.2.2	Procédures de contrôle des changements de système

Les changements des systèmes dans le cadre du cycle de développement doivent être contrôlés par le biais de procédures formelles.

ISO 27001 - A.14.2.3	Revue technique des applications après changement apporté à la plateforme d'exploitation

Lorsque des changements sont apportés, les applications doivent être vérifiées et testées afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.

11. Sécurité dans les relations avec les fournisseurs

Mesures concernant les rapports avec OVH, hébergeur des serveurs SIDES.

ISO 27001 - A.15.1.1	Politique de sécurité de l'information dans les relations avec les fournisseurs

Des exigences de sécurité de l'information pour limiter les risques résultant de l'accès des fournisseurs aux actifs de l'organisation doivent être acceptées par le fournisseur et documentées.

ISO 27001 - A.15.1.2	La sécurité dans les accords conclus avec les fournisseurs

Les exigences applicables liées à la sécurité de l'information doivent être établies et convenues avec chaque fournisseur pouvant accéder, traiter, stocker, communiquer ou fournir des composants de l'infrastructure informatique destinés à l'information de l'organisation.

12. Redondance matériels

Mesures destinées à assurer un minimum de continuité d'activité.

ISO 27001 - A.17.2.1	Disponibilité des moyens de traitement de l'information

Il convient de mettre en œuvre des moyens de traitement de l'information avec suffisamment de redondances pour répondre aux exigences de disponibilité.