Haute école pédagogique
Comité de direction

Directives du Comité de direction
Chapitre 4 : Systèmes d'information

Directive 04_01 Politique de sécurité de l'information (PSSI)

Le Comité de direction de la Haute école pédagogique (ci-après : HEP),

- vu la Loi sur la Haute école pédagogique (LHEP), état le 01.08.2018,
- vu le Règlement d'application de la LHEP (RLHEP) , état le 01.08.2018,
- vu la Loi fédérale sur la protection des données (LPD), état le 01.01.2014,
- vu la Loi cantonale sur la protection des données personnelles (LPrD), état le 01.09.2007,

arrête la Politique de sécurité de l'information suivante :

Article premier — Résumé exécutif

[1] Le système d'information (SI) est devenu un levier incontournable de la performance, de l'innovation et de la transformation de l'entreprise. Assurer la sécurité du SI, c'est assurer la survie et la compétitivité de l'entreprise (qu'elle soit publique ou privée).

[2] La présente politique de sécurité de l'information (PSSI) définit la stratégie, le cadre, les grandes orientations, l'organisation et les responsabilités en matière de sécurité de l'information à la HEP, conformément aux lois, règlements et engagements (accords) contractuels, et en alignement avec la stratégie de la HEP. Elle s'inscrit dans une démarche globale de système de management de la sécurité de l'information (SMSI). La protection de l'information ou sécurité de l'information ou sécurité du SI est caractérisée par les 3 critères fondamentaux suivants: confidentialité, intégrité et disponibilité.

[3] Le chapitre 1 rappelle les enjeux, le concept de sécurité du SI, les principes de mise en oeuvre, ainsi que l'engagement de la Direction. A travers cette démarche de sécurité du SI, la Direction s'engage à soutenir toute mesure proportionnelle aux risques encourus visant à assurer la protection appropriée du SI de l'institution contre les menaces externes ou internes, naturelles ou accidentelles ou délibérées.

[4] Le chapitre 2 rappelle les normes internationales (notamment les normes ISO 2700x) et les référentiels de bonnes pratiques (en particulier COBIT5 et BCI) dans le domaine de la sécurité du SI qui sous-tendent la présente PSSI.

[5] Le chapitre 3 définit les principes fondamentaux de sécurité du SI, à savoir: défense en profondeur, moindre privilège, ségrégation / séparation des tâches, renforcement (*hardening*) des systèmes et protection de la sphère privée.

[6] Le chapitre 4 définit l'organisation, les rôles et responsabilités permettant d'assurer la sécurité du SI:

- La Direction est responsable de l'entier de la sécurité de l'information (et de la sécurité du SI).
- Les entités métier (UER, filière, unité de service) sont « maître » des fichiers et « responsable du traitement » dans leur domaine métier.
- L'unité Informatique est garante de la mise en oeuvre de la sécurité du SI.

[7] Le chapitre 5 fixe le périmètre, les objectifs et les mesures de sécurité de l'information, conformément aux normes ISO 2700x. Tous les domaines de sécurité de l'information sont considérés dans la présente PSSI.

[8] Tout-e collaborateur-trice, toute entité, tout partenaire ou intervenant-e externe doivent être conscient-e-s de leur responsabilité lors de l'utilisation (ou de la gestion) de l'information et des systèmes d'information. Car la sécurité du SI, c'est l'affaire de tous.

hep/

Art. 2 — Politique de sécurité de l'information (PSSI)

Table des matières

Chapitre 1 Pourquoi une Politique de sécurité du SI (PSSI)?

La sécurité du SI, indispensable à la HEP pour mener à bien ses activités

La norme internationale ISO/CEI 27000 (chap.3.1) constate et rappelle que:

« Des organisations de toutes catégories et de toutes tailles:

a) collectent, traitent, stockent et transmettent de grandes quantités d'informations ;

b) reconnaissent que les informations et les processus associés, les systèmes, les réseaux et les gens qui s'y rattachent sont des actifs importants pour la réalisation des objectifs de l'organisation ;

c) font face à un éventail de risques qui peut avoir des répercussions sur le fonctionnement des actifs ;

d) et modifient les risques en mettant en œuvre des mesures de sécurité de l'information.

Toutes les informations détenues et traitées par une organisation sont exposées à des menaces d'attaque, d'erreur, d'évènement naturel [...], etc. et sont exposées à des vulnérabilités inhérentes à leur utilisation. Le terme sécurité de l'information repose, en général, sur le fait que l'information est considéré comme un actif qui a une valeur et qui, en tant que tel, nécessite une protection appropriée contre, par exemple, la perte de disponibilité, de confidentialité et d'intégrité. Permettre aux personnes qui en ont l'autorisation et le besoin de disposer d'informations précises et complètes en temps utile est un catalyseur pour l'efficience de l'organisation.

Pour qu'une organisation puisse atteindre ses objectifs, se mettre en conformité avec la loi et valoriser son image, il lui est essentiel de protéger ses actifs. Protéger les actifs d'information en définissant, accomplissant, maintenant et améliorant efficacement la sécurité de l'information est essentiel pour permettre à une organisation d'atteindre ses objectifs et maintenir et améliorer sa conformité légale et son image. Ces activités coordonnées visant à orienter la mise en œuvre de mesures appropriées et du traitement des risques inacceptables liés à la sécurité de l'information, sont connues généralement comme éléments de management de la sécurité de l'information. »

Ainsi l'information et *de facto* le système d'information sont indispensables pour une entreprise (qu'elle soit privée ou publique, comme la HEP) pour mener à bien ses activités. Il est donc essentiel d'en assurer la sécurité.

Nota, par système d'information (SI), on entend:

1. « Ensemble des moyens (organisation, acteurs, processus, procédures, données, systèmes informatiques) nécessaires à l'acquisition, au traitement, à la retransmission et à la conservation des informations pour assurer les missions et les prestations de l'Administration.»

   Source: Règlement relatif à l'informatique cantonal (Etat de Vaud), RIC 172.62.1

2. « *Information systems (IS) are defined as the combination of strategic, managerial and operational activities involved in gathering, processing, storing, distributing and using information and its related technologies. (IS) are distinct from information technology (IT) in that an information system has an IT component that interacts with the process components.*
   IT is defined as the hardware, software, communication and other facilities used to input, store, process, transmit and output data in whatever form. »

   Source: ISACA CISA, Review Manual, 26th Edition, p32

1.1 … En conformité avec les exigences légales, statutaires, règlementaires, contractuelles

Cadre juridique intercantonal et fédéral:

- Accord intercantonal sur le hautes écoles spécialisés (AHES)
- Convention scolaire romande
- Loi fédérale sur la recherche (LERI)
- Ordonnance fédérale sur la formation professionnelle (OFPr)

Cadre juridique cantonal:

- Loi sur l'enseignement obligatoire (LEO)
- Loi sur l'enseignement secondaire supérieur (LESS)
- Loi sur la pédagogie spécialisée (LPS)
- Loi sur le personnel de l'Etat de Vaud (LPers-VD)
- Règlement d'application de la LPers-VD (RLPers-VD)

Cadre juridique spécifique à la HEP Vaud:

- Loi sur la haute école pédagogique (LHEP)
- Règlement d'application de la LHEP (RLHEP)
- Règlement sur les assistants à la HEP Vaud

En matière de protection des données:

- Constitution Suisse, RS 101 CST
- Code Civil, RS 201 CC
- Loi fédérale sur la protection des données, RS 235.1 LPD + Ordonnance RS 235.11 OLPD
- Loi fédérale sur la surveillance de la correspondance par poste et télécommunication, RS 780.1 + Ordonnance RS 780.11 OSCPT
- Loi fédérale sur le droit d'auteur et les droits voisins, RS 231.1 LDA + Ordonnance RS 231.11 ODAu
- Loi fédérale contre la concurrence déloyale, RS 241 LCD
- Ordonnance concernant la tenue et la conservation des livres de comptes, RS 221.431 Olico
- Code pénal, RS 311.0, Infractions
- [VD] Loi sur l'information, RS 170.21 LInfo
- [VD] Loi sur la protection des données personnelles, RS 172.65 LPrD
- [VD] Règlement d'application de la LPrD, RS 172.65.1 RLPrD
- [VD] Loi sur le personnel de l'Etat de Vaud, RS 172.31 LPers-VD
- [VD] Règlement d'application de la LPers-VD, RS 172.31.1 RLPers-VD

En matière d'archivage:

- [VD] Loi sur l'archivage, RS 432.11 LArch
- [VD] Règlement d'application de la loi sur l'archivage, RS 432.11.1 RLArch

1.2 But de la PSSI - Engagement de la Direction

La Politique de sécurité du SI (PSSI), soutenue, partagée et avalisée par la Direction, fixe la stratégie, le cadre et les responsabilités en matière de de sécurité du SI au sein de la HEP:

1. conformément aux lois, règlements et engagements contractuels, et
2. en alignement à la stratégie et aux exigences métier de l'institution.

La PSSI est communiquée à -- et respectée par -- l'ensemble des parties prenantes des systèmes d'information. Elle est complétée par des directives et des procédures. Elle est suivie de plan d'actions spécifiques. Elle s'incrit dans une démarche globale d'amélioration continue de (système de) management de la sécurité du SI (SMSI).

A travers cette démarche de sécurité du SI, la Direction s'engage à soutenir toute mesure proportionnelle aux risques encourus visant à assurer la protection appropriée du SI de l'institution contre les menaces externes ou internes, naturelles ou accidentelles ou délibérées.

Dans ce document, on utilisera indifférement les termes «sécurité du SI», «sécurité de l'information», «protection du SI», et «protection de l'information» pour désigner l'ensemble des mesures au niveau technique, organisationnel et humain pour assurer la sécurité de l'information et du système d'information (SI) tant d'un point de vue stratégique, tactique qu'opérationnel.

La protection de l'information est caractérisée par les 3 critères fondamentaux suivants (cf. ISO/CEI 27000):

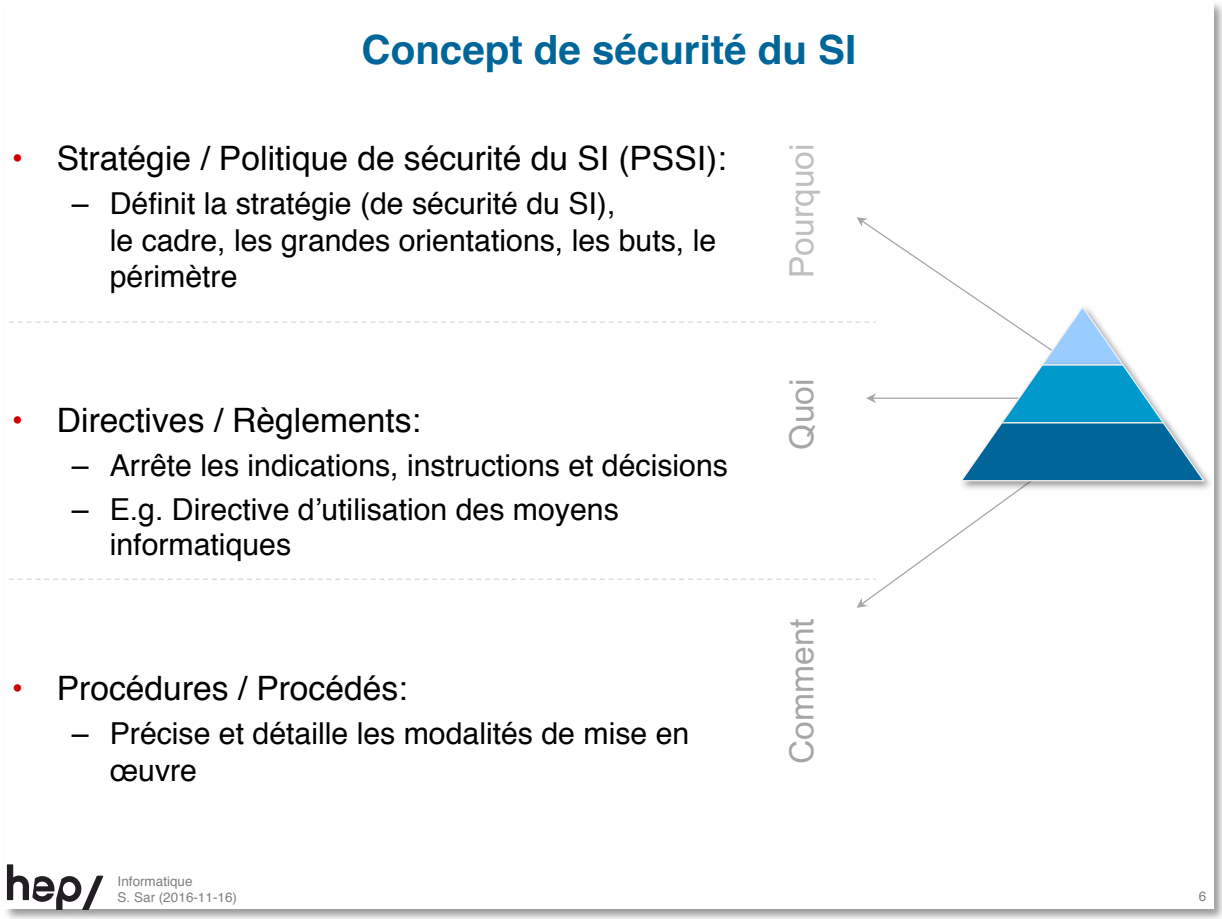
- Confidentialité (« propriété selon laquelle l'information n'est pas rendue disponible ou divulguée à des personnes, des entités ou des processus non autorisés »)
- Intégrité (« propriété de protection de l'exactitude et de la complétude des actifs »)
- Disponibilité (« propriété pour une ressource d'être accessible et utilisable à la demande par une entité autorisée »)

D'autres critères peuvent également être importants selon le contexte:

- Authenticité («propriété selon laquelle une entité est ce qu'elle revendique être »)
- Imputabilité (« responsabilité d'une entité par rapport à ses actions et décisions»)
- Non-répudiation (« capacité à prouver l'occurrence d'un événement ou d'une action donnée et des entités qui en sont à l'origine »)
- Fiabilité (« propriété relative à un comportement et des résultats prévus et cohérents »)

1.3 Concepts et démarche de la sécurité du SI

La sécurité, c'est l'affaire de tous, à tous les niveaux hiérarchiques de l'institution. Le concept de sécurité du SI distingue 3 différents niveaux de documents:



La PSSI est un élément constitutif et fondateur de la sécurité du SI. Elle fixe la stratégie, le cadre et les responsabilités en matière de de sécurité du SI. La PSSI est un document relativement stable dans le temps; elle est revue et mise à jour régulièrement (toutes les années ou tous les 2 ans).

Les Directives déclinent la PSSI dans des domaines spécifiques et arrêtent les instructions, exigences et décisions dans ces domaines. Elles sont revues et mises à jour régulièrement.

Les Procédures (ou Procédés ou Modes opératoires) sont en général des documents au niveau opérationnel précisant les modalités de mise en oeuvre de la sécurité du SI dans un domaine spécifique. Les Procédures décrivent les activités (et flux y relatifs) à réaliser par qui, comment et avec quoi. Elles nécessitent des revues et mises à jour plus fréquentes.

L'ensemble des documents sur la sécurité du SI et des mesures y afférentes participent de la démarche globale (ou du système) de management de la sécurité de l'information.

Le Système de management de la sécurité de l'information (SMSI) fournit un « modèle destiné à l'établissement, à la mise en oeuvre, à l'exploitation, à la surveillance, au réexamen, à la mise à jour et à l'amélioration de la protection des actifs informationnels afin d'atteindre les objectifs métier en se fondant sur l'appréciation des risques et sur les niveaux d'acceptation des risques définis par l'organisation pour traiter et gérer efficacement les risques. » (Source: ISO/CEI 27000, chap.3.1)

1.4 Principes de mise en oeuvre de la sécurité du SI

Pour atteindre les objectifs de sécurité du SI (définis dans le chapitre Chapitre 5), l'institution s'appuie sur les principes de mise en oeuvre suivants:

Principe 1: Le système de management de la sécurité de l'information (SMSI) est conforme aux lois, règlements, et meilleures pratiques.

Le SMSI est élaboré, mis en oeuvre, exploité, surveillé, mis à jour et amélioré en continu conformément aux lois, règlements et meilleures pratiques, notamment celles des normes ISO/CEI 2700x, de COBIT 5, de ISO 22301 et de BCI.

Principe 2: La gestion des risques en matière de sécurité du SI est régulière, alignée aux objectifs stratégiques de l'institution, et proportionnée.

L'identification, appréciation et traitement des risques sont effectués régulièrement. Les mesures de réduction des risques sont mises en oeuvre en s'assurant que leurs coûts sont proportionnels aux bénéfices obtenus. La gestion des risques est revue régulièrement dans une optique d'amélioration continue de la sécurité.

Principe 3: La mise oeuvre de la sécurité du SI est progressive et pragmatique.

La mise en oeuvre des mesures de sécurité (qui découlent de la gestion régulière et proportionnée des risques) est réalisée de manière pragmatique, en traitant en priorité les risques les plus importants, et ce, dans une optique d'amélioration continue.

Chapitre 2 Normes et Référentiels de sécurité du SI

La présente démarche de sécurité de l'information (la présente PSSI et le SMSI) repose sur les normes internationales et les référentiels de bonnes pratiques suivants:

- ISO/CEI 27000:2016, Systèmes de management de la sécurité de l'information - Vue d'ensemble et vocabulaire
- ISO/CEI 27001:2013, Systèmes de management de la sécurité de l'information - Exigences
- ISO/CEI 27002:2013 (ISO/CEI 17799), Code de bonne pratique pour la gestion de la sécurité de l'information
- ISO/CEI 27005:2011, Gestion des risques liés à la sécurité de l'information
- ISACA, COBIT 5 - Processus facilitants - AP013 Gérer la sécurité:
    - Description du processus: Définir, explorer et surveiller un système de management de la sécurité de l'information.
    - Objectif du processus: Maintenir l'impact et l'occurrence des incidents de sécurité de l'information dans les limites de l'appétit de l'entreprise pour le risque.
- BCI (Business Continuity Institute), Guide de bonnes pratiques (de continuité d'activité) 2013, en alignement avec ISO 22301:2012.

La présente PSSI s'inspire de la politique générale de sécurité des systèmes d'information (PGSSI) de l'Etat de Vaud, de la politique de sécurité des SI (PSSI) de l'Etat de Vaud, et de la politique de sécurité de l'information (PSI) de l'Etat de Genève.

Nota bene: les normes en matière de *Records Management* (RM) sont référencées dans les documents *ad hoc* dans le cadre des mesures de "Conformité aux obligations légales et règlementaires" (cf. objectif de sécurité A18.1 et mesures y relatives).

Chapitre 3 Principes fondamentaux de sécurité du SI

3.1 Défense en profondeur

Plusieurs lignes de défense sont mises en place afin d'assurer la sécurité du SI. Elles couvrent tous les aspects de l'information (et du SI). Aussi peuvent-elles être d'ordre humain (notamment la sensibilisation des employés à la sécurité du SI), organisationnel ou technique. Le concept de défense en profondeur permet de construire une défense globale en coordonnant plusieurs lignes de défense qui doivent être cohérentes entre elles et adaptées aux enjeux.

3.2 Moindre privilège (droits d'accès minimum)

Toute personne n'accède qu'aux informations ou ressources strictement nécessaires à l'acomplissement de son travail, en conformité avec les lois, règlements et directives.

3.3 Ségrégation (ou séparation) des tâches

Pour réduire les opportunités de vol, de consultation, d'altération, ou d'usage non autorisés d'informations, les rôles et responsabilités y relatifs sont assignés à des personnes distinctes, permettant ainsi de prévenir les erreurs et les irrégularités dans le traitement des actifs.

Cette séparation des tâches évite qu'une même personne puisse avoir le contrôle sur tout le cycle de vie d'un système (depuis son développement ou modification jusqu'à sa mise en production) ou d'une transaction (depuis sa saisie jusqu'à son approbation).

3.4 Renforcement (« hardening ») des systèmes

Pour réduire les vulnérabilités et l'exposition aux menaces, la configuration des -- et l'accès aux -- différents systèmes (réseaux de télécommunication, serveurs, logiciels, postes de travail) sont limités au strict nécessaire.

3.5 Protection de la sphère privée

Les données des employés, étudiants ou autres bénéficiaires des prestations de la HEP sont protégées conformément aux lois, règlements et directives.

Chapitre 4 Organisation et Responsabilités

- La Direction est responsable de l'entier de la sécurité de l'information (et de la sécurité du SI). La Direction décide de, approuve, et communique la politique de sécurité du SI.
- Les entités métier (UER, filière, unité de service) sont « maître » des fichiers et « responsable du traitement » dans leur domaine métier. Notamment elles ont la responsabilité:
    - d'identifier les besoins de sécurité et les exigences légales dans leur domaine;
    - d'identifier les actifs, les menaces et les vulnérabilités propre à leur domaine;
    - d'analyser, d'évaluer et de suivre les risques afin de déterminer les niveaux de sécurité requis et la protection la plus appropriée;
    - d'assurer l'application de la PSSI dans leur périmètre, et auprès de leurs bénéficiaires, usagers, partenaires et fournisseurs;
    - d'assurer l'utilisation des systèmes d'information conformément aux politiques, directives et procédures de sécurité.
- L'unité Informatique est garante de la mise en oeuvre de la sécurité du SI. Notamment elle a la responsabilité:
    - de mettre en place l'organisation, les processus et les outils nécessaires à la mise en oeuvre et à l'amélioration continue de la politique de sécurité du SI et du système de management de la sécurité du SI (SMSI);
    - de proposer à la Direction un arbitrage du plan d'actions général et de traitement des risques de la sécurité du SI;
    - de soutenir et de conseiller les entités métier dans toutes les activités de gestion des risques de sécurité dans leur domaine, ou dans l'application des mesures de sécurité;
    - de coordonner les activités des parties prenantes en matière de sécurité;
    - de sensibiliser le personnel, les bénéficiaires et les tiers aux risques encourus et aux mesures de sécurité correspondantes;
    - d'acquérir, de développer, de mettre en oeuvre, d'exploiter, de faire évoluer, de surveiller les SI conformément aux politiques et directives de sécurité.
- Tout bénéficiaire du SI (employé-e-s de la HEP, intervenants externes, fournisseurs, étudiants et partenaires de l'institution) est responsable:
    - de réaliser ses activités, de faire usage de ses droits d'accès, d'utiliser les moyens informatiques et de traiter les informations conformément aux politiques, directives et procédures de sécurité de la HEP;
    - de signaler à l'unité Informatique tout fait ou comportement anormal qu'elle-il pourrait observer dans le domaine de la sécurité du SI.

On entend par:

- *Fichier*, tout ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée (cf. RS 235.1 LPD);
- *Maître du fichier*, la personne privée ou l'organe qui décide du but et du contenu du fichier (cf. RS 235.1 LPD);
- *Responsable du traitement*, toute personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine le contenu, ainsi que les finalités du fichier (cf. RS VD 172.65 LPrD);

Chapitre 5 Déclaration d'applicabilité (Objectifs de sécurité du SI)

Tous les domaines de sécurité de l'information sont considérés dans la présente PSSI. Ces domaines ainsi que les objectifs y relatifs en matière de sécurité du SI reposent sur la famille de normes ISO/CEI 27000x:

- Politiques de sécurité de l'information
- Organisation de la sécurité de l'information
- Sécurité des ressources humaines
- Gestion des actifs
- Contrôle d'accès
- Cryptographie
- Sécurité physique et environnementale
- Sécurité liée à l'exploitation
- Sécurité des communications
- Acquisition, développement et maintenance des systèmes d'information
- Relations avec les fournisseurs
- Gestion des incidents liés à la sécurité de l'information
- Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
- Conformité

Approuvé par le Comité de direction

Lausanne, le 1er octobre 2018

(s) Vanhulst G.

Guillaume Vanhulst
recteur

Diffusion :

- Membres du CD
- Site internet, espace réglementation