UNIL | Université de Lausanne
Centre informatique
bâtiment Amphimax
1015 Lausanne

Politique de sécurité de l'information de l'Université de Lausanne

Type de document : Politique de sécurité.
Version : 1.7
Classification : Publique

Sommaire

Versions

Version	Auteur	Sujet	Date
0.1	Y. Ghennai	1ère version.	28/03/2018
0.2	Y. Ghennai	Changement pour une politique de l'université, pas seulement pour le Ci.	23/08/2018
0.3	G. Bellezanne	Adaptation de la politique aux exigences du standard et aux besoins UNIL.	20/11/2018
0.7	Y. Ghennai	Revue avec Adriano Barenco	24/04/2019
1.0	Y. Ghennai	Mise-à-jour, définitions…	03/06/2019
1.1	A. Barenco	Révision	26/07/2019
1.2	E.Milhomme	Première relecture SJ	20/08/2019
1.3	E.Milhomme	Seconde relecture SJ après réunion Ci	25/09/2019
1.4	H. Hussain-Kahn	Relecture	29/11/2019
1.5	A. Barenco	Relecture	20/12/2019
1.7	Y. Ghennai	Revue de la direction de l'université, changements mineurs	28/01/2020

1. Objet

1.1. Pourquoi une politique de sécurité du système d'information (PSSI) à l'Université de Lausanne?

L'Université de Lausanne est une institution de recherche et de formation. Son activité première est de créer, mettre à disposition et transmettre de l'information et des connaissances. Elle travaille en bonne intelligence avec les nouvelles technologies. La réussite de sa mission d'enseignement dépend directement de la sécurité de son système d'information.

A ce titre, l'Université prend en compte toutes les dimensions de la sécurité de l'information : elle sensibilise à la sécurité de l'information et développe une politique effective de sécurité de l'information pour l'ensemble de ses membres et partenaires.

En intégrant la sécurité au sein de tous ses nouveaux projets et en évaluant continuellement les risques sur le système d'information de l'institution, notamment au moyen d'une analyse de risques, l'Université souhaite disposer d'une vision pertinente et précise de sa posture de sécurité.

1.2. Une PSSI, pour qui?

L'objectif de la présente Politique de Sécurité du Système d'Information (PSSI) est d'exprimer la stratégie de sécurité de la direction de l'Université de Lausanne relative à son système d'Information (SI), pour l'ensemble des personnes et institutions en relation avec l'Université de Lausanne.

Cette politique de sécurité s'adresse en particulier à ceux qui utilisent, mettent en œuvre, créent ou modifient une partie du SI de l'Université de Lausanne.

Le cadre général décrit ci-dessous est basé sur le standard ISO/IEC 27001. Il sera ensuite précisé par service et par faculté selon l'applicabilité des thématiques évoquées ci-après.

1.3. Quels moyens pour cette PSSI?

Afin d'assurer l'adéquation des mesures mises en œuvre avec les bonnes pratiques, l'Université se base sur des standards internationaux reconnus, notamment les standards de la famille ISO/IEC 27001.

L'Université de Lausanne a décidé de mettre au cœur de sa stratégie de sécurité la protection des données personnelles qui lui sont confiées, notamment en mettant en place des mesures techniques et organisationnelles appropriées.

L'évolutivité de la démarche est un élément crucial afin de s'assurer que les vulnérabilités et menaces récentes soient prises en compte par le plan de gestion de la sécurité de l'information. Pour atteindre cet objectif, l'Université de Lausanne, notamment grâce à l'appui de son Centre informatique, organise des audits internes de sécurité et met en place une démarche d'amélioration continue afin de revoir régulièrement les différents éléments de sécurité et les évolutions au sein de l'Université de Lausanne.

La Direction, par l'entremise du Ci, effectuera une actualisation et une revue régulière de ce document.

2. Définitions

Dans le présent document, les termes et abréviations suivants signifient :

- **SI :** Système d'Information. Ensemble d'éléments humains, techniques et procéduraux permettant la manipulation de tous les types d'informations.
- **CISO ou RSSI :** Chief Information Security Officer (Directeur de la sécurité de l'information). En français le Responsable Sécurité du Système d'Information.
- **Communauté universitaire :** la communauté universitaire se compose du corps enseignant, du personnel administratif et technique, des collaborateurs engagés sur des fonds extérieurs à l'Etat ainsi que des étudiants comme définis dans la loi sur l'Université de Lausanne.[1]
- **SMSI :** Système de management de la sécurité de l'information (Outil de gestion de la sécurité).
- **PSSI :** Politique de Sécurité du Système d'Information. C'est le 1er élément d'un SMSI.
- **ISO 27'000 :** Norme internationale sur la sécurité du système d'information dont nous nous inspirons pour notre gestion de la sécurité.
- **PI :** Propriété intellectuelle, travaux de recherches, brevets, droits d'auteurs…
- **PII :** Informations permettant l'identification d'une personne.

3. Périmètre et applicabilité

Cette politique, et l'ensemble des mesures qui en découlent, s'appliquent :

- Dans l'intégralité des locaux et espaces ouverts de l'Université de Lausanne,
- A toute la communauté universitaire, quel que soit le lieu de l'activité en lien avec l'Université de Lausanne,
- A toute personne externe qui utilise le système d'information de l'Université de Lausanne, quel que soit le lieu de l'activité.

4. Objectifs de sécurité

Cette PSSI réaffirme la volonté de la Direction de l'Université de Lausanne de:

- Protéger les données[2], les droits d'auteur et la propriété intellectuelle (PI).
- Protéger les données personnelles confiées à l'Université de Lausanne.
- Garantir en tout temps et à tout membre de la communauté universitaire un accès à ses données et aux services de l'Université de Lausanne.
- Sensibiliser les utilisateurs à la sécurité de l'information et aux risques inhérents à l'utilisation des technologies de l'information.
- Protéger la réputation de l'Université de Lausanne.

5. Principes fondamentaux de sécurité

L'objectif principal de la sécurité de l'information consiste à protéger celle-ci selon les trois critères de sensibilité énumérés ci-dessous.

---

[1] Article 13 LUL et 9 RLUL (cf. §6)
[2] Tout type de données de recherche, personnelles, sensibles au sens de la loi (Définitions cf. art. 4 LPrD).

- La **confidentialité** est le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé.
- L'**intégrité** est la protection de l'exactitude et de l'intégralité de l'information et des méthodes de traitement de celle-ci.
- La **disponibilité** est l'aptitude d'un système à assurer ses fonctions sans interruption, délai ou dégradation, au moment où la sollicitation en est faite.

Des mesures sont mises en place pour protéger ces composantes pour les informations manipulées par l'Université de Lausanne.

Chacun, dans le cadre de ses activités pour l'Université de Lausanne, est responsable d'observer un comportement de bon sens afin de préserver en tout temps l'information dans ces trois dimensions.

6. Lois et règlements

L'Université de Lausanne s'engage au respect de l'ensemble des textes normatifs qui lui sont applicables, notamment dans la mise en place et le maintien de la Sécurité du SI. Elle porte une attention toute particulière aux textes suivants :

Externes

Lois fédérales:

- Constitution Suisse, RS 101 CST
- Code Civil, RS 201 CC
- Loi fédérale sur la recherche sur l'être humain, RS 810.30 LRH
- Loi fédérale sur la recherche, LERI
- Loi fédérale sur le droit d'auteur et les droits voisins, RS 231.1 LDA
- Ordonnance sur le droit d'auteur et les droits voisins, RS 231.11 ODAu
- Loi fédérale contre la concurrence déloyale, RS 241 LCD

Lois cantonales de l'État de Vaud :

- Loi sur l'information, RS 170.21 Linfo
- Loi sur la protection des données personnelles, RS 172.65 LPrD
- Règlement d'application de la LPrD, RS 172.65.1 RLPrD
- Loi sur le personnel de l'Etat de Vaud, RS 172.31 LPers-VD
- Règlement d'application de la LPers-VD, RS 172.31.1 RLPers-VD
- Loi sur l'archivage, RS 432.11 LArch
- Règlement d'application de la loi sur l'archivage, RS 432.11.1 RLArch

Internes

L'Université de Lausanne est régie par :

- Loi sur l'Université de Lausanne, RSV 414.11 LUL
- Règlement d'application de la loi sur l'Université de Lausanne, RSV 414.11.1 RLUL

Au niveau de l'Université de Lausanne, de nombreux règlements et directives sont applicables.

Ils sont consultables librement à l'adresse suivante :

https://www.unil.ch/interne/home/menuinst/documents---formulaires/textes-legaux/directives-internes-de-lunil.html#table_277

Règlements sur les données personnelles

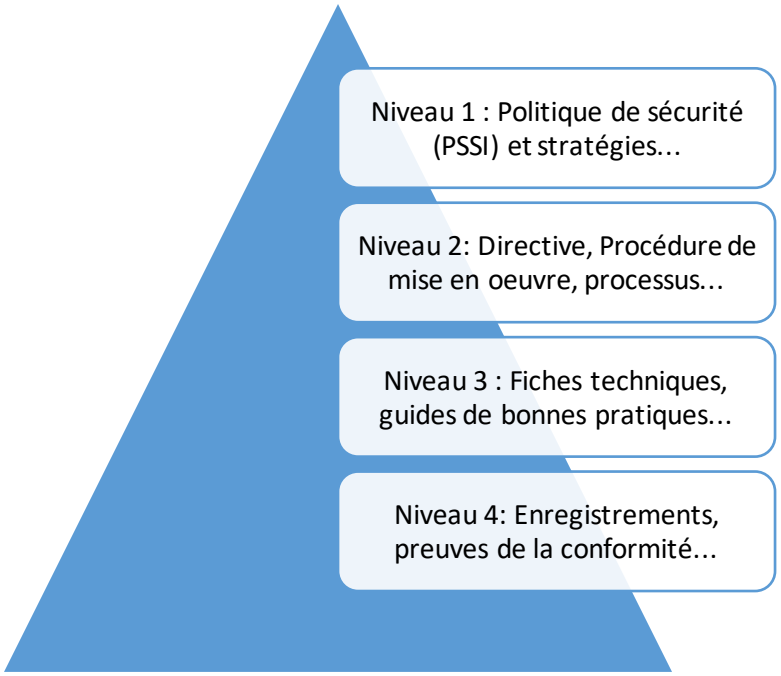
La Loi vaudoise sur la protection des données personnelles (LPrD) est appliquée en tout point.

Lorsque les conditions de son application sont réunies, le Règlement général sur la protection des données (RGPD) est mis en œuvre.

7. Organisation de la sécurité de l'Information

La sécurité de l'information à l'Université de Lausanne est un processus dynamique qui nécessite la formation, l'information et la sensibilisation de toute la communauté universitaire. Ces actions s'appuient sur une documentation adaptée, variée et cohérente. Une telle documentation permet d'offrir un cadre à chacune des actions menées en lien avec la sécurité. Cette documentation est hiérarchisée du texte le plus général au plus détaillé.

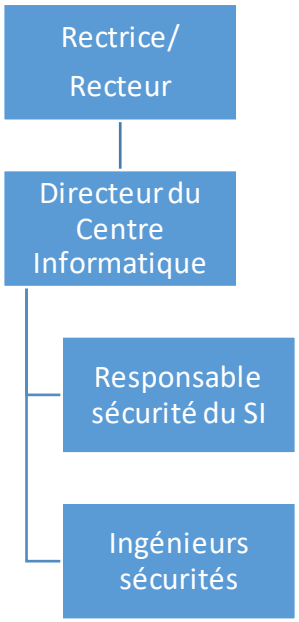
Structure de la documentation :



Niv. 1	Politique de la sécurité des systèmes d'information	Déclaration de la volonté de la Direction de l'Université de Lausanne. Il décrit le cadre de la gouvernance de la sécurité IT de l'Université.
Niv. 2	Directives	Déclaration de la volonté de la Direction dans le contexte d'une thématique en particulier. Comme par exemple les processus et les contrôles de sécurité.
Niv. 3	Procédures, fiches techniques, recommandations	Mise en application de la volonté de la Direction (appliquée à un ou plusieurs services). Documentations techniques, recommandations…
Niv. 4	Enregistrements, contrôles, « preuves »…	Rapport d'audit interne ou externe, fichiers journaux, etc… Preuves que des mesures sont mises en place, et que des vérifications sont faites.

8. Responsabilités

Les responsables dans la mise en place de la sécurité de l'information au sein de l'Université de Lausanne sont :



- Rectrice/Recteur de l'université.
- Directeur du Centre informatique (Ci).
- Le responsable sécurité du Ci,
  niveau gouvernance.
- Les ingénieurs sécurité du Ci,
  niveau opérationnel.

9. Processus décisionnel

Toute nouvelle mesure de sécurité est définie et mise en place selon les étapes décrites ci-dessous:

1. La Direction de l'Université de Lausanne ou le Ci propose des nouvelles mesures de sécurité
2. Le Ci analyse la nouvelle mesure et sa mise en œuvre en considérant les coûts et bénéfices
3. La Direction valide la mesure et sa mise en œuvre
4. Le Ci met en place la mesure si validée

10. Démarches de sécurité entreprises

Gestion du risque du SI

La gestion de la sécurité est orientée par les risques sur le *système d'information (SI).*

Les mesures de sécurité mises en place par suite de cette analyse visent à améliorer *de manière proportionnée* la sécurité sans alourdir inutilement ni pénaliser les activités "métiers" de l'Université.

Tout risque résiduel identifié sera documenté et communiqué à la Direction de l'Université.

Amélioration continue

L'amélioration continue de la sécurité se base sur :

- Des revues régulières de la part des responsables.
- Une surveillance régulière de la sécurité.
- Des audites internes et externes.
- Des propositions émises par des employés.

Audit et revue

Les documents de support à la sécurité de l'information seront revus tous les 2 ans.

Un audit interne de sécurité, sera effectué sur un périmètre défini avec les responsables de la sécurité (i.e. tout ou partie du système d'information, dans une faculté, un service, un groupe de recherche…), à une fréquence fixée, au minimum tous les deux ans. L'audit interne de sécurité est réalisé par des employés de l'université.

Ces audits pourront être réalisés dans le cadre des démarches qualité qui sont déjà organisés à l'Université de Lausanne dans chaque service et chaque faculté.

Annuellement, la nécessité d'un audit externe de sécurité (technique ou organisationnel) sera considérée, et au besoin celui-ci sera planifié tant sur son étendue que sur ses dates de réalisations. L'audit externe de sécurité est réalisé par une société externe mandatée et spécialisée dans le domaine ciblé.

La direction de l'université doit être partie prenante et recevoir les résultats, les analyser, et décider de toute action à entreprendre (P. ex. acceptation du risque, traitement du risque, refus du risque).

Conduite du changement du SI

Chaque changement dans un SI existant ainsi que tout nouveau projet est revu par le CISO.

Préalablement il sera demandé :

- Une analyse d'impact sur la sécurité du système d'information.
- Une validation par la Direction compétente.

11. Thématiques prises en compte

Les thématiques de la sécurité de l'information sont nombreuses et couvrent de nombreux domaines d'activités.

Les points ci-dessous sont extraits de la norme ISO27002 – 2013. Ce standard permet de couvrir tous les domaines de la sécurité de manière exhaustive.

Orientation et management	Un système de management de la sécurité des systèmes d'information (SMSI) est établi avec la Direction. Certains documents comme la PSSI sont rédigés avec la Direction pour donner une « orientation » générale à la sécurité mise en place.
Organisation interne	Une organisation et des mesures pour aider à la sécurité au travail sont définies.
Ressources humaines	Les risques liés aux personnes sont réduits. Les responsabilités sont connues et les connaissances relatives à la sécurité sont en adéquation avec ces dernières.
Gestions des actifs	L'information est inventoriée, qualifiée et affectée à un responsable.
Contrôle d'accès	L'accès à l'information est limité, par des moyens techniques adéquats, aux seules personnes ayant des besoins métiers de les consulter.
Cryptographie	Des mesures cryptographiques sont mises en place et les usages dans le domaine sont établis. Par exemple pour les groupes de recherche qui traitent des données sensibles.
Sécurité physique et environnementale	La sécurité physique est assurée afin de protéger les éléments des systèmes d'information contre les menaces extérieures et environnementales. La gestion des accès du personnel aux différents locaux est contrôlée.
Sécurité liée à l'exploitation du SI.	L'exploitation des systèmes d'information est maîtrisée et est surveillée pour répondre aux besoins.
Sécurité liée aux réseaux.	L'information est transférée de manière sécurisée aux destinataires.
Services IT et applications	Les services fournis par l'Université de Lausanne et les procédés pour les mettre en place sont sécurisés. La composante sécurité est incluse dès le début dans tout nouveau projet.
Relations avec les fournisseurs	Les prestataires externes doivent suivre les exigences de sécurité dans le cadre de leurs activités avec l'Université de Lausanne.
Gestion des incidents	La gestion des incidents est formalisée, encadrée par un processus respectueux de la loi, et adhérent au principe d'amélioration continue.
Continuité de l'activité	Des mesures sont en place pour assurer que l'activité de l'Université de Lausanne est pérenne, quels que soient les évènements.
Juridique et réglementaires	Les obligations légales et réglementaires sont identifiées et intégrées dans le SI.

12. Traitement en cas de violations

En cas de violation de la sécurité de l'information, l'incident fera l'objet d'un processus de gestion complet décrit dans le niveau 2 de la documentation.

Il sera demandé d'effectuer une analyse exhaustive documentée de l'incident en présence des protagonistes et, si nécessaire, des autorités compétentes, qu'elles soient internes ou externes.

L'Université de Lausanne prononcera des sanctions en fonction de la gravité de l'incident, selon la réglementation qui sera mise en place.