Politique de sécurité des systèmes d'information LEX 6.5.1

2 juin 2014, état au 1er janvier 2017

La Direction de l'Ecole polytechnique fédérale de Lausanne arrête :

Préambule

Ce document concerne tous les utilisateurs des systèmes d'information de l'EPFL (ci-après, le système d'information), quel que soit le moyen de communication employé pour accéder au système d'information, ainsi que toutes les informations créées par l'EPFL ou qui lui ont été confiées et qui ont été sorties du périmètre du système d'information.

Il est évolutif et sera adapté en fonction des directives de l'EPFL, du CEPF et de la Confédération.

Section 1 Contexte de base

Article 1 Périmètre du système d'information

[1] Le système d'information de l'EPFL est considéré comme une entité constituée de composants de nature et de provenance diverses, centrée sur les besoins des utilisateurs. Il comprend les principales composantes suivantes :

1. infrastructure et équipements mis à disposition des utilisateurs individuellement ou collectivement;
2. données et leurs traitements ;
3. documentation ;
4. utilisateurs et informaticiens.

[2] Son périmètre englobe tous les composants cités ci-dessus possédés ou loués par l'EPFL, sur tous ses sites et quel que soit le moyen d'accéder au composant. En plus des informations créées par l'EPFL, le périmètre comprend aussi celles qui lui ont été confiées par des tiers.

Article 2 Importance de la sécurité de l'information à l'EPFL

[1] Le système d'information de l'EPFL constitue l'un de ses actifs essentiels en contribuant à ses objectifs.

[2] La croissance des besoins, du nombre d'interconnexions et d'interdépendances, de la complexité et de la diversité des systèmes, ainsi que des menaces, contribue à une augmentation rapide des risques auxquels doit faire face l'EPFL.

[3] La sécurité du système d'information de l'EPFL - à savoir sa disponibilité, son intégrité, sa confidentialité et sa traçabilité - doit faire l'objet d'une attention particulière. Elle vise à assurer la poursuite des activités de l'EPFL et à protéger sa réputation en relation avec l'utilisation de l'information et des moyens qui la supportent.

[4] La Direction de l'EPFL est consciente de l'importance de la protection de cet actif et soutient activement sa politique de sécurité du système d'information (PSSI).

[5] Le Vice-président pour les systèmes d'information est chargé de mettre en place la politique de sécurité du système d'information.

[6] Le Responsable de la sécurité des systèmes d'information est chargé de la gestion des crises liées à la sécurité desdits systèmes, outre ses responsabilités directement liées à la sécurité de l'information.

Section 2 Fondements et principes

La politique de sécurité du système d'information repose sur des **piliers** qui sont tous aussi importants et décrits dans les articles suivants.

Article 3 Pilier 1

Le système d'information est un actif essentiel pour l'EPFL. En ce sens, il doit faire l'objet de mesures de protection en rapport avec sa valeur et en rapport avec l'évaluation du risque associé à son indisponibilité, sa perte, son altération ou son vol.

Article 4 Pilier 2

L'EPFL reste propriétaire de ses informations sorties, avec ou sans son consentement, du périmètre de son système d'information. La PSSI, en particulier les articles 6 et 18 de la présente politique, reste applicable.

Article 5 Pilier 3

Toute information sensible fait l'objet d'une classification qui lui est rattachée.

Article 6 Pilier 4

Sauf changement de classification, le niveau de protection de l'information contre les accès non autorisés reste le même tout au long de son cycle de vie, et ce, quel que soit son support (confidentialité et intégrité).

Article 7 Pilier 5

L'information et ses traitements font l'objet de mesures de protection en rapport avec leur valeur, contre les modifications non autorisées, volontaires ou non (intégrité).

Article 8 Pilier 6

Le niveau de protection du système d'information est adapté globalement ou localement en fonction de la valeur / sensibilité de l'information qu'il stocke et traite. Cette adaptation est documentée.

Article 9 Pilier 7

Les utilisateurs du système d'information sont au préalable authentifiés et autorisés (authentification et autorisation). Les accès sont tracés et les traces sont conservées hors de portée des utilisateurs (traçabilité), afin de permettre l'identification des auteurs d'actes délictueux. Les traces sont accessibles dans le cadre prévu par la loi.

Article 10 Pilier 8

L'information utile est disponible au moment opportun pour les utilisateurs (disponibilité).

Article 11 Pilier 9

Les utilisateurs n'accèdent qu'aux informations dont ils ont besoin dans le cadre de leur travail (need-to-know). De même, ils n'opèrent dans le système d'information que des actions correspondant au cadre de leur travail (need-to-do).

Article 12 Pilier 10

Les modifications d'informations sensibles peuvent être attribuées à un utilisateur donné (traçabilité). L'identification de l'utilisateur permet de s'assurer de la validité des mesures de protection.

Article 13 Pilier 11

Les informations financières sont traitées selon le principe de séparation des tâches de manière à éviter les fraudes et les erreurs (4 yeux).

Article 14 Pilier 12

Les accès physiques aux supports informatiques sensibles sont limités au minimum selon les principes need-to-know et need-to-do à des personnes autorisées et identifiées. Les accès sont tracés. Les traces sont accessibles dans le cadre prévu par la loi.

Article 15 Pilier 13

Des contrôles sont mis en place afin de prévenir ou corriger les incidents et de s'assurer du respect de la présente politique.

Article 16 Pilier 14

Chaque utilisateur du système d'information est individuellement responsable du bon usage des moyens et de la protection des informations mis à sa disposition par l'EPFL, dans le respect des intérêts de l'Ecole, des lois, règlements et directives en vigueur et de la présente politique.

Article 17 Pilier 15

La sécurité de l'information est prise en compte dans chaque projet mettant en œuvre des moyens informatiques et tout au long du cycle de vie du système d'information.

Section 3 Parties prenantes

Article 18 Responsabilités

[1] La protection du système d'information est l'affaire de toutes les parties prenantes. Chacun, par son comportement, peut améliorer cette protection ou mettre le système en danger.

[2] L'EPFL veille à mettre à disposition de ses collaborateurs, étudiants, invités et prestataires des moyens performants et en rapport avec leurs besoins. L'EPFL veille aussi à la formation de ses collaborateurs. En échange, elle s'attend à ce que chacun :

1. protège la réputation de l'EPFL ;
2. ne lui fasse pas courir de risque, en particulier financier, légal ou opérationnel, supérieur aux limites qu'elle a définies ;
3. prenne, dans le cadre fixé par l'EPFL, toutes les mesures nécessaires pour protéger le système d'information mis à sa disposition pour son travail ;
4. annonce immédiatement aux instances responsables toute faille dans la sécurité du système d'information ;
5. préserve le secret de failles éventuelles vis-à-vis de tiers non autorisés ;
6. utilise les moyens mis à sa disposition pour accomplir les tâches qui lui ont été confiées dans le cadre de sa relation contractuelle avec l'EPFL ;
7. protège les informations qu'il a sorties du périmètre du système d'information ou auxquelles il accède depuis l'extérieur du périmètre.

Section 4 Entrée en vigueur

Article 19 Entrée en vigueur

[1] La présente politique entre en vigueur le 2 juin 2014, état au 1er janvier 2017.

Au nom de la Direction de l'EPFL:

Le Président :
Patrick Aebischer

La General Counsel :
Susan Killias

Remarque : cette directive a été revue dans le cadre de la réorganisation 2017. Cette revue n'a donné lieu à aucune modification de la directive.

Annexe : Glossaire

Glossaire

Actif	Tout élément représentant de la valeur pour l'organisme.
Authenticité	Caractère de ce qui est exact.
Authentification	Procédé permettant de vérifier l'identité d'une personne.
Autorisation	Procédé permettant d'accorder une permission à une personne.
Classification	Procédé permettant de distribuer les informations suivant un certain nombre de degrés caractérisant leur niveau de protection souhaité, par exemple public, usage interne, confidentiel (salaires, contrats avec l'industrie) et secret (état de santé d'un collaborateur, fiche d'appréciation du Comité de Promotion des professeurs).
Cloud computing	Utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs via Internet.
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.
Donnée (data)	Fait, notion ou instruction représentés sous une forme conventionnelle convenant à une communication, à une interprétation ou à un traitement soit par l'homme, soit par des moyens automatiques.
Fiabilité	Probabilité pour qu'un élément ou un dispositif complet soit utilisé sans défaillance pendant une période de temps déterminée, dans des conditions opérationnelles spécifiées.
Imputabilité	Possibilité d'attribuer à un individu la responsabilité d'une action.
Information	Faits et connaissances déduits des données.
Information sensible	Information confidentielle ou information dont l'altération, volontaire ou non, autorisée ou non, peut conduire à une perte financière pour l'EPFL (p. ex. données transmises à une banque en vue d'effectuer un transfert de compte à compte).
Intégrité	Propriété de protection de l'exactitude et de l'exhaustivité des informations.
Need-to-do	Principe selon lequel l'utilisateur d'un système d'information ne peut interagir avec ledit système que selon ce qui est défini par le cadre de son travail. Ce principe est parfois appelé principe du privilège minimum ou principe de l'autorité minimale.
Need-to-know	Principe selon lequel l'utilisateur d'un système d'information n'accède qu'aux informations dont il a besoin dans le cadre de son travail.
Non-répudiation	Fait de ne pas pouvoir revenir sur le contenu d'un document ou d'une transaction.
Propriétaire de données	Entité ou personne qui autorise ou refuse l'accès à ces données. Elle s'assure aussi de leur exactitude, intégrité et actualité et détermine sa classification.

Propriétaire de système	Entité ou personne qui autorise ou refuse l'accès à ce système. Elle s'assure : 1. de l'exactitude des éléments qui sont fournis au système, 2. de l'exactitude de ce que le système produit, 3. de son intégrité 4. et de ce que le système soit à jour.
Sécurité de l'information	Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information. De plus, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité peuvent également être concernées.
Système d'information	Un système d'information (SI) est un ensemble organisé d'éléments qui permet de regrouper, de classifier, de traiter et de diffuser de l'information sur un phénomène donné. L'utilisation de moyens informatiques, électroniques et la télécommunication permettent d'automatiser et de dématérialiser les opérations telles que les procédures d'entreprise. Ils sont aujourd'hui largement utilisés en lieu et place des moyens classiques tels que les formulaires sur papier et le téléphone et cette transformation est à l'origine de la notion de système d´information.
Traçabilité	Possibilité de suivre une information aux différents stades de son traitement.