Université de Lille

Délibération n°CA-2020-033 de la séance du conseil d'administration du 12 mars 2020 relative à la politique de sécurité des systèmes d'information

LE CONSEIL D'ADMINISTRATION

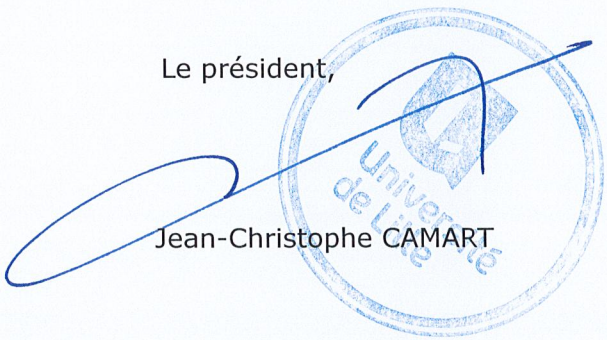
Vu le code de l'éducation, notamment ses articles L712-3 et suivants,
Vu les statuts de l'université de Lille,

APRES EN AVOIR DELIBERE, à l'unanimité avec 33 voix pour

APPROUVE la politique de sécurité des systèmes d'information telle que présentée dans le document annexé à la présente délibération.

Fait à Lille, le 12 mars 2020

Le président,



Jean-Christophe CAMART

Politique de Sécurité du Système d'Information (PSSI)

Document d'orientation de la sécurité des systèmes d'information de l'Université de Lille

V 20200121

Table des matières

Domaine d'application

Contexte

L'Université de Lille (ci-après dénommé l'Université) est un Établissement Public à Caractère Scientifique, Culturel et Professionnel (LRU, Article L123-3).

L'Université est répartie sur plusieurs sites, situés principalement sur les communes de la Métropole Européenne de Lille : Lille, Roubaix, Tourcoing, Villeneuve d'Ascq.

Ces sites hébergent parfois des entités autonomes mais partageant des ressources matérielles avec l'Université (bâtiments et infrastructures) : École Centrale de Lille, Institut Mines-Télécom, Centre Hospitalier Régional Universitaire, etc.

Les chercheurs de l'Université sont principalement employés par l'Université, le CNRS, l'INRIA, l'INSERM et l'INRA.

Périmètre

La PSSI de l'Université s'applique à la totalité de son système d'information, c'est-à-dire à toutes ses données et à toutes les ressources humaines, matérielles et logicielles nécessaires à la bonne gestion de ces données, quelle que soit leur localisation.

L'ensemble de ces éléments sera appelé « actifs (du système d'information) » dans la suite du document.

Liste non exhaustive de sous-ensembles du système d'information :

- les actifs nécessaires à la gestion de l'établissement (RH, finances, scolarité, …) ;
- les actifs des services numériques institutionnels (messagerie, applications et publications Internet, stockage, sauvegarde…) et ceux propres aux composantes (applications scientifiques, traitement des données, bureautique…) ou aux laboratoires (contrats, brevets et publications) ;
- les actifs hors du champ informatique s'appuyant néanmoins sur ses ressources (ToIP/VoIP, visioconférence, vidéosurveillance, contrôle d'accès…) ;
- les interconnexions avec les autres organismes et établissements.

Les données ou ressources externalisées dans le cadre d'une sous-traitance sont aussi concernées par la PSSI.

Cas des unités multi-tutelles ou hébergées

Le système d'information des unités de recherche multi-tutelles est également concerné par la PSSI de l'Université, sauf si un avis contraire a été exprimé dans le cadre des contrats de partenariat passés entre l'Université et une ou plusieurs autre(s) tutelle(s) de l'unité.

Si plusieurs PSSI sont applicables, la PSSI la plus exigeante s'appliquera.

Expression du besoin de sécurité

Nécessité de protection

Le système d'information de l'Université est indispensable pour les activités d'enseignement, de recherche et de gestion. Ce système d'information est susceptible de présenter de nombreuses vulnérabilités d'origines diverses : structures organisationnelles insuffisamment robustes, routines de gestion ou procédures défaillantes, pannes d'équipements, environnement physique mal contrôlé, multiplicité des intervenants,

dépendance de tiers défaillants, assemblage de composants dont la compatibilité n'est pas garantie, défaillance humaine, etc.

Ces vulnérabilités, si elles sont « exploitées », peuvent avoir des conséquences dommageables en termes de temps de travail, de perte d'information, de coût financier, de réputation...

Le système d'information doit donc être protégé des menaces internes et/ou externes. Des mesures de sécurité suffisantes doivent être définies et mises en œuvre afin de réduire à un niveau acceptable les risques d'atteinte à la confidentialité, l'intégrité et la disponibilité des actifs du système d'information.

Obligation de légalité des règles de sécurité

Le règlement intérieur de l'université et les mesures de protection mises en œuvre doivent être respectueux du cadre législatif et réglementaire (cf. annexe « LOIS-0-liste_des_lois_et_règlements_pour_la_ssi-v20191202.pdf » et « LOIS-*.pdf »).

Les lois et règlements sont destinés, entre autres, à interdire les accès frauduleux, à protéger les droits de propriété intellectuelle (droits d'auteurs, brevets...), à respecter la vie privée (fichiers nominatifs, cybersurveillance…) et à assurer la protection du patrimoine scientifique et technique de la Nation.

Méthodologie de sécurisation du système d'information

Prérequis : établir un système de gestion de la sécurité du système d'information à amélioration continue

L'Université établit, met en œuvre, surveille et améliore de façon continue le processus de gestion de la sécurité de son système d'information (SMSI, Système de Management de la Sécurité de l'Information).

Ce processus, itératif, s'appuie 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 » (cf. annexe « DEFINITION-iso_27001-SMSI-introduction.pdf »).

Basée sur la détermination de niveaux de sécurité suffisant à la protection de chaque constituant du système d'information et sur des analyses de risques, les règles de sécurité et les mesures correspondantes sont optimales (ni trop, ni trop peu).

Source des règles et des mesures de sécurité : du spécifique au général

La protection de chaque actif du système d'information consistant à respecter un ensemble de règles de sécurité, il convient de définir leurs sources, de provenance locale et adaptée aux besoins de l'Université, ou provenant de documents plus généraux.

Les sections suivantes définissent la priorité des sources.

Résultats d'analyses de risques (concerne en priorité la protection des "biens essentiels")

Pour protéger les « biens essentiels » de son système d'information, l'Université procède à des analyses de risques en utilisant les outils préconisés par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), et met en œuvre les mesures de sécurité qui en découlent. Les actions prioritaires seront celles destinées à réduire les risques les

plus élevés, risques déduits de l'importance de la menace et de la gravité des conséquences d'une attaque.

Un « bien essentiel » est un ensemble de données et de fonctions de traitement dont le défaut de sécurité aurait des conséquences catastrophiques ou très graves pour l'Université. La liste des biens essentiels est une information à diffusion limitée, et ne peut pas être publiée dans ce document public.

Règlement intérieur de l'université et chartes

Le chapitre 7 du règlement intérieur de l'université, *dispositions régissant l'usage du système d'information*, s'applique à tous les usagers, quel que soit leur statut.

Le respect des règles de sécurité qui y sont exprimées est impératif, sans que le consentement individuel de l'usager (signature) soit nécessaire.

Cf. annexe « REGLEMENT-reglement_interieur_universite_de_lille-partie_ssi.pdf ».

En complément du règlement intérieur de l'Université, opposable à tout utilisateur du SI, une charte s'adresse spécifiquement aux administrateurs de systèmes informatiques, sachant que cette population qui dispose de droits d'accès privilégiés aux actifs du SI doit respecter des obligations (devoirs) supplémentaires (secret professionnel, désignation officielle, qualité de service, …). Cf. annexe «CHARTE-universite_de_lille-ssi-charte_administrateur.pdf ».

Fiches de recommandations

Au fil du temps, les personnels en charge de la sécurité du SI établissent des fiches de recommandations. Il s'agit de documents moins formels que les analyses de risques mais validés par la gouvernance de l'Université. Les recommandations énoncées sont des mesures organisationnelles et/ou techniques adaptées à l'Université et suffisamment détaillées pour pouvoir être mises en œuvre pratiquement.

En l'absence d'une analyse de risque spécifique, mais en présence d'une fiche de recommandations, on respectera cette dernière (ex : *Sécurité des boites aux lettres partagées*, *Sécurité des équipements informatiques contenant des données en cas de réaffectation*, etc.).

Cf. Annexes « RECOMMANDATION-*.pdf ».

Bonnes pratiques du Guide d'hygiène informatique de l'ANSSI ou de la PSSI de l'Etat

En l'absence de règles et mesures de sécurité spécifiques, l'Université s'attachera à respecter un « socle de sécurité » permettant d'obtenir, sinon un niveau de sécurité optimal, tout au moins un niveau de sécurité suffisant pour se protéger de la plupart des risques informatiques usuels et non ciblés.

À ce jour, deux documents établis par l'ANSSI et fort semblables sur le fond pourront indifféremment être utilisés :

- la PSSI de l'Etat, Politique de sécurité des systèmes d'information (PSSIE) portée par la circulaire du Premier ministre n° 5725/SG du 17 juillet 2014. la PSSIE est un ensemble de règles détaillées, regroupées selon la maîtrise d'œuvre chargée de l'application des règles de sécurité : Organisation, Sécurité physique, Réseau, Exploitation, Gestion du poste de travail, Développement, etc. (cf. annexe « PSSIE-cir_38641-PSSI_de_l_Etat-20140717.pdf »)
- le Guide d'Hygiène Informatique constitué de règles macroscopiques, regroupées selon le besoin de sécurité, à destination des maîtrises d'ouvrage et des usagers (cf. annexe « GUIDE-guide_hygiene_informatique_anssi.pdf »),

Le choix d'utiliser l'une ou l'autre des références (ou les deux) sera laissé à l'appréciation de chacun. Par exemple, on pourra communiquer aux usagers ou aux personnels une règle du Guide d'Hygiène Informatique et, en même temps, confier aux personnels spécialisés la mise en œuvre de cette règle de façon détaillée grâce à la PSSI de l'Etat (cf. annexes « GUIDE-comparaison_regles_PSSIE_et_Guide_d_hygiene_de_l_ANSSI-* »).

Responsabilités et Organisation

Responsabilités

Au sein de l'Université, la responsabilité formelle de la sécurité des systèmes d'information relève de son président, en tant que Personne Juridiquement Responsable (PJR) et qu'Autorité Qualifiée pour la Sécurité des Systèmes d'Information (AQSSI).

Pour les unités mixtes de recherche (UMR), la responsabilité formelle de la sécurité du SI relève du Directeur d'Unité (DU), PJR pour son unité.

La mise en œuvre des mesures de protection des systèmes d'information relève de la responsabilité de la chaîne organique (présidence de l'université, direction générale des Services, directions des composantes, directions des unités de recherche, directions des services) avec l'accompagnement des pôles spécialisés (DSI, RSSI et experts SSI, services informatiques des composantes ou des laboratoires, autres services informatiques), et en collaboration avec le Fonctionnaire de Sécurité et de Défense (FSD) dans ses missions de protection du patrimoine scientifique et technique de la Nation.

Comité de Pilotage de la SSI

La définition des orientations techniques de la PSSI est assurée par un Comité de Pilotage de la SSI (COPILSSI).

Ses missions principales sont les suivantes :

- assurer la diffusion et la révision de la PSSI ;
- définir et maintenir la liste des biens essentiels ;
- planifier les analyses de risque selon des critères d'importance du risque et de la possibilité financière de les réaliser ;
- valider les mesures de sécurité résultant des analyses de risques, ou proposées par les RSSI, ou énumérées par le socle de sécurité
- proposer et promouvoir des actions de sensibilisation ou de communication.

L'annexe « ORGANISATION-comite_de_pilotage_de_la_SSI.pdf » définit la constitution et les règles de fonctionnement du COPILSSI.

Chaîne fonctionnelle spécialisée de la sécurité des systèmes d'information

Pour conduire la politique de sécurité des systèmes d'information et faciliter sa mise en œuvre, l'Université s'appuie sur une chaîne fonctionnelle interne spécialisée en SSI qui s'inscrit elle-même dans la chaîne fonctionnelle nationale animée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

La chaîne fonctionnelle SSI de l'Université de Lille est composée comme suit :

- du fonctionnaire de sécurité de défense (FSD) ;

- de deux responsables de la sécurité des systèmes d'information (RSSI), nommés par le président de l'Université. Correspondants auprès des structures nationales de la SSI, ils contribuent activement à l'élaboration d'une politique de sécurité cohérente et à sa mise en œuvre ;
- dans les entités, des « Correspondants Sécurité des Systèmes d'Information » (CSSI) qui relaient les informations de sécurité émises par les RSSIs, recensent et signalent les incidents de sécurité « informatique » (piratage, virus, hameçonnage, vol, etc…) à leur Direction et à l'Université (via les RSSI), et si possible apportent une assistance technique pour traiter ces incidents.

Règles de communication interne/externe

Cf. annexe « ORGANISATION-universite_de_lille-ssi-organisation_et_flux.pdf »

Arbitrages et sanctions

Mesures applicables par les responsables informatiques d'entités

Les responsables informatiques et réseaux peuvent en cas d'urgence user de mesures conservatoires :

- déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation ;
- suspendre l'activité d'un processus qui nuirait au bon fonctionnement des systèmes d'information ;
- isoler un système informatique du réseau si celui-ci présente un comportement qui mettrait en péril la sécurité des systèmes d'information ;
- isoler ou neutraliser provisoirement toute donnée ou fichier qui mettrait en péril la sécurité des systèmes d'information.

Ils doivent en informer le CSSI de l'entité concernée et les RSSI. Ils ont un devoir de confidentialité et ne doivent communiquer sur l'incident que le nécessaire. Ils doivent veiller au mieux à ne pas modifier un environnement pour le recueil de preuves, si l'incident détecté nécessite ultérieurement un dépôt de plainte.

Mesures applicables par les RSSI

À la suite d'un manquement observé au Règlement intérieur de l'Université (chapitre 7 : dispositions régissant l'usage du système d'information), les RSSI peuvent appliquer ou demander d'appliquer les mesures décrites au paragraphe précédent à tout utilisateur ou à tout système de l'Université.

De plus, sur la base des analyses d'activités, de la détection de comportement atypique, d'avis des CERT (Computer Emergency Response Team) ou d'autres autorités reconnues, les RSSI peuvent être amenés à alerter les utilisateurs concernés ou à requérir des informations auprès d'eux.

Celles-ci peuvent être assorties du blocage des flux réseaux partiels ou totaux provenant d'un ou plusieurs systèmes d'information, ou d'un sous-réseau, ou de la suspension des accès aux systèmes d'information.

En cas d'incidents graves, comme ceux susceptibles d'entraîner le dépôt d'une plainte ou entachant l'image de l'Université ou de l'une des tutelles d'une entité, mais aussi une récidive à un manquement à la PSSI ou une non réponse à une requête d'information, les RSSI peuvent demander à ce qu'un utilisateur soit convoqué.

Cette convocation se traduit par un entretien entre l'utilisateur concerné, son N+1, la DRH ou la DGS de l'Université ou encore la Direction des Affaires Juridiques pour certaines catégories d'utilisateurs. La présence du RSSI, notamment à des fins techniques et afin de rappeler les conditions de l'incident et, si nécessaire, les règles de

la PSSI en vigueur et pour discuter des mesures devant être prises, peut-être envisagée. À l'issue de celui-ci, les RSSI peuvent proposer une ou plusieurs des mesures suivantes à l'autorité hiérarchique de l'agent concerné :

- considérer l'incident comme clos et sans suite ;
- demander l'application de mesures spécifiques et maintenir, s'il y a lieu, l'application de la suspension du droit d'usage des systèmes d'information à l'Université jusqu'à la réalisation de ces mesures ;
- rappeler les obligations en vigueur à l'utilisateur. Une information est alors faite à la chaîne hiérarchique et à la chaîne fonctionnelle ;
- remettre le traitement de l'incident à la chaîne hiérarchique. Une information est alors faite à la chaîne fonctionnelle.

En cas d'incidents portant préjudice à l'Université ou à l'une des entités du périmètre de la PSSI, les RSSI peuvent proposer le dépôt d'une plainte auprès du procureur de la République.

En cas d'incidents susceptibles d'entraîner des mesures disciplinaires, les règles en vigueur s'appliquent.

Modalités de publication et de révision de la PSSI

Création : définition des acteurs et de leurs tâches

Rédaction : RSSI assistés des membres du COPILSSI

Validation : Comité de Direction

Approbation : Conseil d'Administration

Révision

Le circuit de révision est similaire à celui de création.

Ceci implique que toute révision nécessite d'être validée et approuvée.

Le processus étant assez complexe, la probabilité de devoir modifier la PSSI a été réduite en évitant de faire référence à des concepts ou des technologies trop rapidement obsolètes, mais certaines situations nécessiteront néanmoins de revoir la PSSI.

On notera cependant que cette possibilité (ou nécessité) de révision n'est absolument pas en contradiction avec le principe d'évolution continue intégré au SMSI, bien au contraire.

Situations qui nécessiteront une révision de la PSSI :

- évolution des stratégies politiques ;
- évolution de la culture d'établissement ;
- évolution du contexte : noms des entités, nouvelles lois ou règlements, nouveaux partenariats, nouvelles normes, nouveaux socles de sécurité, etc. ;
- évolution des capacités humaines, techniques ou financières permettant ou nécessitant une évolution à la hausse ou à la baisse des prétentions (ex : analyse de risque systématiques ou abandon des analyses de risques).

Liste des annexes

CHARTE-universite_de_lille-ssi-charte_administrateur.pdf
DEFINITION-iso_27001-SMSI-introduction.pdf

GUIDE-comparaison_regles_PSSIE_et_Guide_d_hygiene_de_l_ANSSI-1.xls
GUIDE-comparaison_regles_PSSIE_et_Guide_d_hygiene_de_l_ANSSI-2-commentaires_et_conclusion.pdf
GUIDE-guide_hygiene_informatique_anssi.pdf
LOIS-0-liste_des_lois_et_rŠglements_pour_la_ssi-v20191202.pdf
LOIS-1-FRAUDE-1-loi_Godfrain-code_penal.pdf
LOIS-1-FRAUDE-2-loi_Godfrain-loi-JO198800231.PDF
LOIS-2-DROITS_D_AUTEUR-code_de_la_propriete_intellectuelle-Loi_92-597_du_1_juillet_1992.pdf
LOIS-3-PRIVACY-1-RGPD-CELEX_32016R0679_FR_TXT.pdf
LOIS-3-PRIVACY-2-loi_informatique_et_libert,-20181212.pdf
LOIS-3-PRIVACY-3-Decret_2019-536_du_29_mai_2019_pour_application_de_la_loi_informatique_et_libertes.pdf
LOIS-4-INTERNET-1-loi_LCEN_20040621.pdf
LOIS-4-INTERNET-2-LOI_2016-1321_du_7_octobre_2016_pour_une_Republique_numerique.pdf
LOIS-5-RECHERCHE-1-3415_SGDSN_AIST_PST_du_7_novembre 2012-cir_36329.pdf
LOIS-5-RECHERCHE-2-20170919_Note_PPST_SSI-1-NoteHFDS_SIGNEE.pdf
LOIS-5-RECHERCHE-3-20170919_Note_PPST-2-SSI_Guide.pdf
ORGANISATION-comite_de_pilotage_de_la_SSI.pdf
ORGANISATION-universite_de_lille-ssi-organisation_et_flux.pdf
PSSIE-cir_38641-PSSI_de_l_Etat-20140717.pdf
RECOMMANDATION-boites_de_service-SSI.pdf
RECOMMANDATION-coffre_fort_de_mots_de_passe.pdf
RECOMMANDATION-copieurs_multifonctions-1-analyse_de_risque.pdf
RECOMMANDATION-copieurs_multifonctions-2-recommandations-mis_en_forme.pdf
RECOMMANDATION-universite_de_lille-politique_d_acces_aux_donnees_professionnelles_d_un_personnel_indisponible.pdf
RECOMMANDATION-universite_de_lille-securite_des_equipements_informatiques_contenant_des_donnees_en_cas_de_reaffectation.pdf
REGLEMENT-reglement_interieur_universite_de_lille-partie_ssi.pdf