UNIL | Université de Lausanne
Direction

Directives de la Direction

Directive de la Direction 6.1 sur l'utilisation de l'infrastructure informatique

La Direction de l'Université de Lausanne (UNIL),

vu l'article 24 alinéa 2, 44 et 48 de la loi du 6 juillet 2004 sur l'Université de Lausanne (LUL),

vu l'article 2 alinéa 2 du règlement d'application du 18 décembre 2013 de la loi sur l'Université de Lausanne (RLUL),

vu l'article 50 de la loi du 12 novembre 2001 sur le personnel de l'Etat de Vaud (LPers-VD),

vu l'article 125 du règlement d'application du 9 décembre 2002 de la loi sur le personnel de l'Etat de Vaud (RLPers-VD),

vu l'article 321a du Code des obligations (CO),

considérant la Stratégie numérique de l'UNIL,

considérant la Politique de sécurité de l'information (PSSI) de l'UNIL,

adopte la Directive suivante.

CHAPITRE 1 DISPOSITIONS GÉNÉRALES

Article 1 But

La présente directive vise à garantir la sécurité de l'infrastructure informatique de l'UNIL, à définir les droits et devoirs des utilisateurs de cette infrastructure et à prévenir les abus.

Article 2 Terminologie

Toute désignation de personne, de statut, de fonction ou de profession utilisée dans la présente directive s'applique indifféremment aux femmes et aux hommes.

Article 3 Champ d'application personnel

La présente directive s'applique à toute personne qui utilise l'infrastructure informatique de l'UNIL qu'elle soit membre du personnel de l'UNIL, étudiant immatriculé à l'UNIL, auditeur ou qu'elle accède à cette infrastructure à un autre titre (ci-après : utilisateurs).

Article 4 Champ d'application matériel

[1] La présente directive s'applique à l'infrastructure informatique de l'UNIL, y compris les machines figurant à l'inventaire centralisé en application de l'art. 9 de la Directive de la Direction 6.6 sur l'équipement informatique.

[2] Elle ne s'applique pas :

a. aux infrastructures centrales gérées par le Centre informatique (Ci) telles que serveurs physiques et virtuels, poste de travail virtuels, stockage centralisé ;

b. à l'équipement informatique acquis à titre privé par les étudiants immatriculés à l'UNIL et les auditeurs ;

c. aux systèmes de vidéosurveillance qui font l'objet d'une directive distincte.

CHAPITRE 2 CONDITIONS D'UTILISATION DES INFRASTRUCTURES INFORMATIQUES

Article 5 Principes généraux

[1] L'utilisation des infrastructures informatiques par les utilisateurs a pour but la réalisation du travail professionnel ou d'étude.

[2] Lors de l'utilisation des infrastructures informatiques, chaque utilisateur veille à respecter :

a. la réglementation interne de l'UNIL, y compris la présente directive ;

b. la législation sur le droit d'auteur et les droits voisins ainsi qu'en matière de protection des données personnelles et de transparence lorsqu'applicable ;

c. toute autre réglementation applicable, en particulier les dispositions réprimant la soustraction de données (art. 143 et 179^{novies} du Code pénal suisse, CPS), la pornographie (art. 197 CPS), les infractions contre l'honneur (injure, calomnie, etc.) ;

d. les notes publiées par le Ci dans le cadre de la Politique de sécurité de l'information (PSSI) de l'UNIL.

[3] Il est interdit aux utilisateurs des infrastructures informatiques d'utiliser celles-ci de manière contraire à leurs buts, notamment en :

a. accédant sans droit à des comptes, données, informations ou tout autre ressource ;

b. contournant ou supprimant des restrictions de sécurité ;

c. exploitant d'éventuelles failles de sécurité ;

d. visant des buts commerciaux sans rapport avec l'UNIL ou nuisant à l'image de celle-ci.

[4] Des exceptions à l'al. 3. peuvent être octroyées par le Ci, en particulier lorsque les activités poursuivies visent le développement de la science par l'enseignement et la recherche.

[5] Chaque utilisateur respecte scrupuleusement les instructions reçues de la part du Ci en matière de sécurité informatique.

Article 6 Signalement

Les utilisateurs sont invités à signaler sans délai au Ci tout problème de sécurité dont ils ont connaissance.

Article 7 Sécurisation des transmissions

Lorsque la sensibilité d'une infrastructure le nécessite, le Ci sécurise la transmission de données sur le réseau interne de l'UNIL par des mesures organisationnelles et techniques appropriées (authentification forte, chiffrement, etc.).

Article 8 Responsabilité

Sauf disposition légale contraire ou garantie expresse, la responsabilité de l'UNIL pour tout dommage direct, indirect ou consécutif à l'utilisation incorrecte par l'utilisateur des infrastructures informatiques de l'UNIL ou de tiers est exclue.

CHAPITRE 3 SÉCURISATION DU POSTE DE TRAVAIL DES MEMBRES DU PERSONNEL

Article 9 Configuration minimale

[1] Le Ci définit et installe la configuration minimale standard des postes de travail (chiffrement des données, sauvegarde automatique des données locales, dispositif antivirus, dispositif de gestion de

parc informatique, etc.).

[2] Avec le concours des correspondants informatiques des facultés et des services centraux, le Ci veille à ce que la configuration minimale ne limite pas la flexibilité et la souplesse dont les membres du personnel de l'UNIL ont besoin pour accomplir leur travail.

[3] Le Ci offre un accompagnement aux membres du personnel de l'UNIL ayant des besoins spécifiques qui rendent difficile le déploiement de la configuration minimale standard. Le Ci veille à ce qu'ils bénéficient d'une configuration assurant un niveau de sécurité équivalent.

Article 10 Devoirs des membres du personnel de l'UNIL

[1] Chaque membre du personnel de l'UNIL est responsable de la mise en application de la sécurité informatique à son niveau. Il veille en particulier à :

a. ne pas interférer avec la configuration minimale de son poste de travail effectuée par le Ci en désactivant, contournant ou modifiant celle-ci de quelque manière que ce soit ;

b. mettre à jour les logiciels et le système d'exploitation de son poste de travail lorsque nécessaire ou recommandé par le Ci ;

c. disposer de mots de passe respectant les recommandations émises par le Ci ;

d. se connecter au réseau de l'UNIL de façon sécurisée lorsque le poste de travail se trouve hors du réseau de l'UNIL, notamment lors d'une formation ou de télétravail. Les outils assurant une connexion sécurisée sont fournis par le Ci ;

e. mener une évaluation du risque de vol de l'équipement informatique si cette attribution lui revient en application de l'art. 14 de la Directive 6.6 sur l'équipement informatique ;

f. annoncer tout vol ou perte d'équipement informatique conformément à l'art. 17 de la Directive 6.6 sur l'équipement informatique ;

g. ne pas utiliser la messagerie électronique de l'UNIL dans le cadre de ses activités pour un autre employeur.

[2] Le Ci, en consultation avec les répondants du système d'information concernés, peut octroyer des dérogations aux exigences qui précèdent, notamment pour des raisons techniques.

Article 11 Utilisation à des fins privées

[1] Une utilisation à des fins privée des infrastructures informatiques par les membres du personnel de l'UNIL est tolérée dans la mesure où :

a. elle n'entraîne que des coûts minimes pour l'UNIL et ne consomme pas de ressources informatiques de manière déraisonnable ;

b. elle ne porte pas atteinte à l'image de l'UNIL ou entre en conflit avec ses intérêts ;

c. elle ne vise aucun but lucratif ;

d. elle ne met pas en danger la sécurité des infrastructures de l'UNIL ;

e. elle est conforme à la loi et à la présente directive, et ;

f. elle ne nuit pas aux obligations professionnelles envers l'UNIL. Est considéré comme nuisible, une utilisation pendant le temps de travail ou qui perturbe le membre du personnel dans l'accomplissement de ses tâches professionnelles.

[2] Les membres du personnel veillent à ne pas enregistrer de données d'ordre privé sur leur poste de travail. Lorsque de telles données sont malgré tout enregistrées, elles ne font pas l'objet d'un traitement spécifique par le Ci et peuvent être copiées à des fins de sauvegarde.

[3] L'utilisation à des fins privées de la messagerie électronique est signalée par les utilisateurs par une nomenclature claire (répertoire dans la messagerie électronique ou dans le système de stockage

identifié dans son nom comme « privé »). Les données identifiées comme privées ne font pas l'objets d'analyses.

Article 12 Poste de travail privé

Tout poste de travail privé utilisé professionnellement par un membre du personnel de l'UNIL ou mis à l'inventaire selon l'art. 11 de la Directive 6.6 sur l'équipement informatique est chiffré et équipé par son utilisateur de logiciels ayant des fonctionnalités similaires à ceux mis à disposition par le Ci. Chaque utilisateur veille en particulier à ce que les outils informatiques utilisés dans ce cadre respectent ses obligations en matière de confidentialité. Lorsque nécessaire, le Ci assiste les membres du personnel de l'UNIL par le biais de son helpdesk.

CHAPITRE 4 ASSISTANCE, SENSIBILISATION ET FORMATIONS

Article 13 Assistance aux étudiants et auditeurs

[1] Sur demande, le Ci fournit par le biais de son helpdesk une assistance aux étudiants et auditeurs pour la gestion de leur équipement informatique (installation, utilisation, sécurisation).

[2] Une offre de cours et de formations est proposée aux étudiants et auditeurs.

Article 14 Sensibilisation et formation

Chaque membre du personnel de l'UNIL suit un cours sur la sensibilisation aux bonnes pratiques concernant la sécurité informatique et la protection des données personnelles.

CHAPITRE 5 TRAITEMENT DE DONNÉES PERSONNELLES ET ANALYSES

Article 15 Traitement de données personnelles

Le Ci peut collecter et traiter des données personnelles liées à l'utilisation de l'infrastructure informatique de l'UNIL dans les buts suivants :

a. toutes les données personnelles, y compris celles se rapportant au contenu de la messagerie électronique, pour en garantir la sécurité (copies de sauvegarde) ;

b. les données résultant de l'utilisation de l'infrastructure informatique :

    1. pour maintenir la sécurité de l'information et des services ;
    2. pour assurer l'entretien technique de l'infrastructure informatique ;
    3. pour contrôler le respect de la présente directive ou de toute autre réglementation applicable ;
    4. pour retracer l'accès aux fichiers ;
    5. pour facturer les coûts à chaque unité d'imputation.

Article 16 Analyse ne se rapportant pas aux personnes

[1] Les données enregistrées peuvent être analysées sans rapport avec des personnes dans les buts mentionnés à l'art. 15.

[2] Le Décanat ou le chef de service est compétent pour ordonner l'analyse, il peut charger un tiers d'y procéder.

Article 17 Analyse non nominale se rapportant aux personnes

[1] Les données enregistrées peuvent être analysées en rapport avec des personnes mais de manière non nominale lorsque l'analyse a lieu par sondage et dans le but de contrôler l'utilisation de l'infrastructure électronique.

[2] Le Décanat ou le chef de service est compétent pour ordonner l'analyse, il peut charger un tiers d'y

procéder. Il veille à ce que les mesures nécessaires pour que les personnes ne soient pas identifiables soient prises.

Article 18 Analyse nominale se rapportant aux personnes

[1] Les données enregistrées peuvent être analysées en rapport avec des personnes et de manière nominale dans les buts suivants :

a. élucider un soupçon concret d'utilisation abusive ou poursuivre un cas d'utilisation abusive ;

b. analyser les perturbations de l'infrastructure électronique, y remédier ou parer aux menaces concrètes qu'elle subit ;

c. fournir les prestations indispensables ;

d. saisir les prestations effectuées et les facturer.

[2] Une analyse de données selon l'al. 1 let. a ne peut être effectuée que :

a. si elle est approuvée au préalable par la Direction de l'UNIL ;

b. le ou les membres du personnel sont informés préalablement par écrit ;

c. l'analyse porte sur une période limitée et, sauf exception justifiée par les circonstances du cas d'espèce, postérieure à l'annonce.

[3] Les mesures pouvant être prises sur la base des contrôles effectués sont, selon les circonstances du cas d'espèce, celles découlant du droit du travail et de la présente directive, notamment la suppression ou la restriction des accès octroyés aux infrastructures informatiques. Le service des ressources humaines (SRH), après consultation du Ci et validation de la Direction de l'UNIL, est compétent pour la détermination d'une telle sanction.

Article 19 Durée de conservation des données et déroulement des analyses nominales

[1] La durée de conservation et la destruction des données visées par les dispositions du présent chapitre font l'objet d'une annexe à la présente directive.

[2] Le déroulement des analyses nominales concernant les membres du personnel de l'UNIL fait l'objet d'une procédure établie par le SRH.

CHAPITRE 6 DISPOSITIONS DIVERSES

Article 20 Départ, décès ou disparition

[1] Sous réserve des dispositions qui suivent, l'accès aux infrastructures informatiques de l'UNIL des utilisateurs est supprimé :

a. au moment de la cessation effective de la prestation de travail pour les membres du personnel de l'UNIL ;

b. six mois après la décision d'exmatriculation ou de la fin du programme de mobilité pour les étudiants ;

c. à la fin de la durée fixée lorsqu'un accès a été accordé pour une durée déterminée.

[2] Sur demande de l'utilisateur et pour autant que les circonstances le justifient, une durée d'accès à la messagerie électronique plus longue peut être accordée par le Ci.

[3] Dans la mesure où les missions de l'UNIL l'exigent, le SRH peut ordonner l'accès aux données, documents et courriels professionnels d'un membre du personnel lorsque ses rapports de travail avec l'UNIL ont pris fin, en cas de décès ou lorsqu'il est déclaré absent.

Article 21 Abus et sanctions

[1] Toute violation grave de la présente directive par un utilisateur peut conduire à la suppression ou à la restriction des accès octroyés aux infrastructures informatiques.

[2] Toute violation de la présente directive peut être dénoncée aux autorités compétentes en vue d'éventuelles sanctions disciplinaires, pénales ou administratives.

Article 22 Procédures judiciaires et administratives

Le traitement des demandes relatives aux infrastructures informatiques émises par des autorités judiciaires ou administratives est de la compétence du Service juridique.

CHAPITRE 7 DISPOSITIONS FINALES

Article 23 Exécution

[1] Sauf disposition contraire, l'exécution de la présente directive incombe au Ci.

[2] Le Ci, si nécessaire avec l'assistance des services compétents, peut émettre des conditions d'utilisation spécifiques applicables à un logiciel ou à une catégorie d'utilisateurs.

[3] Les recommandations et instructions émises par le Ci sont publiées sur le site internet de l'UNIL ou adressées directement aux utilisateurs concernés.

Article 24 Adoption et entrée en vigueur

[1] La présente directive a été adoptée par la Direction de l'UNIL le 22 novembre 2022.

[2] Elle entre en vigueur le 1er décembre 2022.

Article 25 Abrogations

Par son entrée en vigueur, la présente directive abroge :

a. la Directive de la Direction 6.1 sur les conditions d'accès à l'intranet administratif ;

b. la Directive 6.2 sur l'utilisation d'internet, de la messagerie électronique, des réseaux sociaux, de la téléphonie et du poste de travail, et ;

c. la Directive de la Direction 6.7 sur l'utilisation des services informatiques centraux.

Annexe 1 Conservation et destruction des données

Article 1 Définitions

Au sens de la présente annexe, on entend par :

a. *données administrées* : les données personnelles qui sont enregistrées lors de l'utilisation de l'infrastructure informatique et qui sont régulièrement utilisées, analysées ou effacées volontairement ;

b. *données non administrées* : les données personnelles qui sont enregistrées lors de l'utilisation de l'infrastructure informatique mais qui ne sont pas ou qui ne sont pas régulièrement utilisées, analysées ou effacées volontairement.

Article 2 Durée de conservation des données administrées

Lorsque les finalités de traitement l'exigent, les données administrées peuvent être conservées :

pour toutes les données personnelles, y compris celles se rapportant au contenu de la messagerie électronique, pour garantir leur sécurité (copies de sauvegarde)	jusqu'à l'archivage par le service compétent des informations qui sont à leur source, mais deux ans au plus si elles ne sont pas reprises pour archivage
pour les données résultant de l'utilisation de l'infrastructure électronique	deux ans au plus

Lorsqu'il s'agit de données d'analyses, elles doivent être détruites au plus tard trois mois après la fin de l'analyse ou dans les 30 jours suivant la notification d'une décision définitive et exécutoire rendue dans la procédure dans laquelle elles sont utilisées.

Article 3 Durée de conservation des données non administrées

La durée de conservation des données non administrées dépend de la capacité de mémoire de l'appareil considéré, à moins qu'il ne soit techniquement possible de les détruire rapidement et automatiquement après leur utilisation.

Les données non administrées sont détruites de manière irréversible au plus tard lorsque l'appareil sur lequel elles sont enregistrées est cédé ou éliminé.

*****