

EXTRAIT DU

Procès-verbal de la séance du 5 juillet 2017.

ORDRE DU JOUR :

1

32.- Directive relative à l'utilisation des moyens informatiques au sein de l'Université de Liège.

Les membres du Conseil d'administration ont reçu le document 18.647 reprenant la "Directive relative à l'utilisation des moyens informatiques au sein de l'Université de Liège".

Ce document, qui constitue entre autres une annexe au règlement de travail, vise à confirmer et préciser à chaque utilisateur (tant les membres du personnel de l'Université que les étudiants ou toute autre personne à qui l'Université confie des moyens informatiques) de ces moyens informatiques (définis préalablement) les principes qu'il doit observer dans ce cadre.

La directive énonce également la procédure mise en place par l'Université pour réaliser tout contrôle nécessaire (au regard des finalités définies) de l'utilisation desdits moyens.

Enfin, afin d'assurer la continuité des activités de l'Université tout en préservant la vie privée de ses agents en cas d'absence ou de départ de ceux-ci, la directive prévoit des règles d'accès aux moyens informatiques utilisés par les agents dans le cadre de leur activité professionnelle.

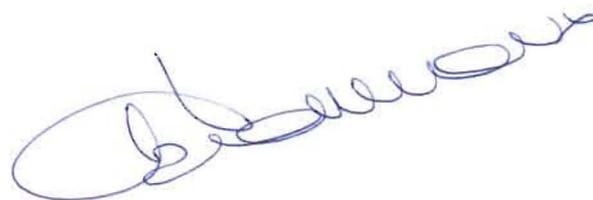
Des corrections formelles doivent être apportées au document.

Le Conseil d'administration, à l'unanimité, adopte la "Directive relative à l'utilisation des moyens informatiques au sein de l'Université de Liège", conformément au document 18.647bis ci-joint.

La Secrétaire
(s) Véronique BOVEROUX

Pour copie conforme,
La secrétaire,

Le Recteur-président,
(s) Albert CORHAY



Directive relative à l'utilisation des moyens informatiques au sein de l'Université de Liège

La présente directive a pour objet de définir les conditions d'utilisation et les règles de bon usage des moyens informatiques de l'Université de Liège, dans le respect des lois et règlements.

Sauf mention contraire, la directive s'applique à l'ensemble des personnes qui, quel que soit leur statut, ont accès aux moyens informatiques de l'Université de Liège (ci-après dénommées «l'utilisateur» ou «les utilisateurs»).

Sont notamment constitutifs de moyens informatiques,

- les stations de travail (ordinateurs fixes, portables, tablettes, smartphones,...) des facultés, instituts, départements, centres, services, laboratoires...
- les serveurs (physiques et virtuels), les applications et services informatiques dont le système de messagerie électronique,
- les réseaux informatiques de l'Université de Liège, les équipements d'infrastructure réseau,
- les périphériques et objets connectés au réseau (téléphones IP, imprimantes, caméras, écrans informatifs, terminaux de paiement, modalités médicales...),
- les périphériques amovibles de stockage (clés USB, CD/DVD, disques durs portables...),
- l'ensemble du parc logiciel, des bases de données, des produits multimédias ou des périphériques affectés au fonctionnement des éléments décrits ci-dessus.

Sont également considérés comme moyens informatiques, les ressources extérieures accessibles par l'intermédiaire des réseaux de l'Université de Liège et notamment le réseau Belnet.

I. Principes relatifs à l'utilisation des moyens informatiques

1. Responsabilité des utilisateurs des moyens informatiques de l'Université

Les utilisateurs sont entièrement responsables de l'utilisation qu'ils font des moyens informatiques de l'Université de Liège.

Les utilisateurs sont responsables des opérations locales ou distantes effectuées depuis leurs comptes, à l'aide de leurs badges ou de leurs accès personnels.

En conséquence, les utilisateurs doivent prendre toute mesure pour limiter les accès frauduleux aux moyens informatiques de l'Université, à ce titre ils doivent **notamment** :

- veiller à la confidentialité des codes, mots de passe, cartes/badges d'accès, clefs ou tout autre dispositif de contrôle d'accès qui leur sont confiés à titre strictement personnel;
- veiller à la confidentialité des comptes utilisateurs qui leur sont attribués ou connus;
- se déconnecter immédiatement après la fin de leur période d'utilisation des moyens informatiques et activer un verrouillage automatique afin de se protéger lorsqu'ils s'absentent pour une courte durée;
- informer immédiatement leur support informatique local (UDI) ou à défaut, le helpdesk général du Service général d'Informatique, de toute tentative d'accès frauduleux ou de tout dysfonctionnement suspect dont ils auraient connaissance;
- changer régulièrement leurs codes et mots de passe d'accès; les modifier immédiatement s'il y a suspicion d'utilisation abusive de ceux-ci;
- s'assurer que les fichiers qu'ils jugent confidentiels ne soient pas accessibles à des tiers;
- déclarer et gérer la détention et l'utilisation de (base de) données à caractère personnel conformément aux législations et règlements internes en vigueur ;
- pour les agents de l'Université, activer le profil sécurisé via myULg.

2. Utilisation des moyens informatiques

L'utilisation des moyens informatiques mis à disposition par l'Université est exclusivement à des fins professionnelles, de formation, de recherche ou toute autre fin ayant justifié l'octroi des moyens informatiques. À cet égard, l'utilisateur observe avec rigueur la politique de sécurité de l'information définie par l'Université.

À titre d'exception, l'Université en tolère l'usage à des fins privées à condition que cet usage :

- soit occasionnel;
- n'entrave pas la bonne conduite des missions de l'Université, ni l'intérêt du Service; et
- ne porte pas atteinte au bon fonctionnement des moyens informatiques de l'Université.

L'utilisateur est invité à différencier ses données privées des données relevant de ses activités au sein de l'Université¹ (adresse électronique, répertoires, données, etc.). À défaut, l'utilisateur est tenu d'indiquer, dans l'identification des données qu'elles ont un caractère privé (à titre d'exemple, dans l'objet d'un courriel, reprendre une mention de type «Personnel», cf. www.ulg.ac.be/securite-informatique). En outre, s'il s'agit d'un courriel, l'utilisateur doit supprimer, dans le corps du message, toute mention relative à l'Université (telle que la signature automatique) et toute autre indication qui pourrait laisser croire que le message est rédigé par l'utilisateur dans le cadre de ses activités au sein de l'Université.

¹ Sont ainsi visées les activités professionnelles, de recherche, d'apprentissage ou toute autre activité ayant justifié l'octroi de moyens informatiques par l'Université.

L'Université n'assume aucune responsabilité relative à la perte ou la destruction partielle ou totale des données privées dont les utilisateurs disposeraient sur les moyens informatiques de l'Université dans le cadre de la présente exception.

En outre, dans le cadre de ses activités professionnelles, l'agent doit veiller à conserver ses données professionnelles sur les moyens informatiques mis à disposition par l'Université et n'utiliser des moyens informatiques personnels que dans le cadre strictement recommandé (ex. smartphones, tablettes et recommandations d'utilisation et de sécurité).

Si, à titre exceptionnel, un agent utilise à des fins professionnelles des moyens informatiques personnels, il doit veiller à transférer, dans les plus brefs délais, les données professionnelles sur les moyens informatiques mis à sa disposition par l'Université.

3. Utilisations prohibées

Tout usage illégal, diffamatoire, contraire aux bonnes mœurs ou susceptible de porter atteinte à la dignité d'autrui, ainsi que tout usage de nature à nuire aux intérêts de l'Université, à ses missions et à sa réputation sont strictement prohibés.

À titre exemplatif, sont interdits à l'utilisateur :

- l'usurpation d'identité ainsi que la divulgation de tout mot de passe, code, compte ou autre dispositif de contrôle d'accès (propre ou d'autrui);
- l'infraction aux législations relatives à la propriété intellectuelle lors de l'utilisation ou de la diffusion de documents écrits, de documents audio ou visuels (musique, films), de logiciels...
- l'accès non autorisé aux ressources (machines, fichiers, bases de données...) des réseaux connectés, internes ou externes à l'Université de Liège, ou l'entrave au bon fonctionnement de ces ressources (piratage...);
- l'envoi massif de courriers électroniques indésirables (spam);
- l'utilisation inutile ou excessive des moyens informatiques : bande passante et services réseau, ordinateurs publics, espace de stockage, ressources humaines...;
- l'exploitation commerciale des moyens informatiques;
- pour l'agent, la consultation, la copie, la reproduction ou la diffusion de données auxquelles l'agent a accès, à des fins non strictement nécessaires à l'exercice de sa fonction.

Dans ce cadre, l'Université se réserve le droit de bloquer à tout moment et sans avertissement préalable l'accès aux sites web ou applications dont elle juge le contenu illégal, offensant ou inapproprié.

II. Contrôle de l'utilisation des moyens informatiques²

A) Principes :

Les traces des activités informatiques à l'Université sont stockées sur ses systèmes informatiques pour une durée de 12 mois maximum. L'Université peut également conserver une capture de toutes les données informatiques utiles à des fins diagnostiques.

Outre les nécessités d'accès visées au point III ci-dessous, l'Université se réserve le droit de contrôler les données informatiques, en vue des finalités évoquées ci-après, et ce qu'il s'agisse de la messagerie électronique, de l'usage de services et applications informatiques, ou de l'utilisation de moyens informatiques (en particulier, le réseau).

La Direction générale du Service général d'Informatique est mandatée pour ce contrôle.

Ce contrôle s'effectue tout en respectant la vie privée de l'utilisateur.

Le respect de la vie privée de l'utilisateur est assuré lors de contrôles grâce à l'application de 3 principes :

1) Principe de finalité :

Le contrôle des moyens informatiques a pour objectif de poursuivre les finalités suivantes :

- a) la prévention, l'identification et la résolution de situations illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui;
- b) la protection des intérêts de l'Université;
- c) la sécurité ou le bon fonctionnement technique des systèmes informatiques en réseau de l'Université, en ce compris le contrôle des coûts y afférents, et la protection physique des installations; et
- d) de façon plus générale, le respect de l'utilisation en bon père de famille des moyens informatiques mis à disposition des utilisateurs.

2) Principe de proportionnalité :

L'Université effectue un contrôle adéquat, pertinent, non excessif et nécessaire au regard des finalités définies ci-avant.

3) Principe de transparence :

L'Université informe les utilisateurs de l'existence du contrôle via son site web.

² L'Université s'inspire en la matière de la CCT n° 81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau.

Les agents sont également informés par le règlement de travail.

B) Individualisation :

Aux fins de la poursuite des finalités énoncées au II, A, 1, a) à d), l'Université est habilitée à retracer l'identité de l'utilisateur qui est à l'origine d'une anomalie. Cette phase est appelée « procédure d'individualisation ».

Si une anomalie est détectée dans le cadre des 3 premières finalités (a, b, c), l'Université peut procéder à une individualisation sans formalité.

Si une anomalie est détectée dans le cadre de la dernière finalité (d), l'individualisation sera réalisée moyennant la communication simultanée à l'utilisateur de l'existence de l'anomalie.

Si une anomalie de même nature est à nouveau constatée, l'Université procède à l'individualisation sans autre avertissement.

C) Procédure :

- 1) Toute anomalie doit être signalée par celui qui la détecte au Recteur;
- 2) Le Recteur fait constater l'anomalie par la direction générale du Service général d'Informatique;
- 3) En accord avec le Recteur, la direction générale du Service général d'Informatique prend les mesures de sauvegarde, en ce compris le blocage des accès. En cas d'urgence impérieuse mettant en péril la sécurité des personnes et des biens, le Service général d'Informatique est habilité à prendre seul les mesures de sauvegarde et en informe le Recteur dans les plus brefs délais.
- 4) L'utilisateur est averti et convié à un entretien avec le Recteur au cours duquel il sera entendu sur ces faits.

D) Mesures techniques :

L'Université se réserve notamment le droit de bloquer les accès d'un utilisateur aux moyens informatiques qu'elle met à disposition de celui-ci.

III. Accès aux données en vue de la continuité du service

Cet article concerne uniquement les agents de l'Université de Liège.

Afin de faire face aux difficultés liées à des situations particulières, les règles de fonctionnement suivantes sont définies³ :

1. Absence planifiée de l'agent

Outre la réponse automatique à l'expéditeur avec indication d'une personne de contact, l'agent convient d'une personne de confiance, au sein du service dont il relève, habilitée à accéder, via les moyens de partage (Zimbra, Cloud ULiège), aux messages et fichiers

³ Cf. Recommandations de la Commission de la Protection de la Vie Privée – 02.07.2011

professionnels en cas de nécessité justifiée et d'urgence ne pouvant attendre le retour de l'agent absent.

À défaut d'une telle désignation, il revient au responsable hiérarchique de l'agent d'accéder aux données professionnelles dans les mêmes conditions.

2. Absence non planifiée de l'agent

Lorsque l'intérêt du service le justifie, pour les agents des services centralisés, le responsable hiérarchique, accompagné d'un membre du Service des Affaires juridiques et d'un membre du Service général d'Informatique, est habilité à accéder aux messages et fichiers électroniques professionnels de l'agent.

Lorsque l'intérêt du service le justifie, pour les agents d'autres services, le responsable hiérarchique, accompagné d'un membre du Service des affaires juridiques et d'un informaticien de l'UDI dont relève l'agent, est habilité à accéder aux messages et fichiers électroniques professionnels de l'agent.

3. Démission, licenciement de l'agent

En cas de préavis presté, à l'issue de celui-ci, outre la réponse automatique à l'expéditeur avec indication d'une personne de contact, l'agent convient d'une personne de confiance, au sein du service dont il relève, habilitée à accéder, via les moyens de partage (Zimbra, Cloud ULiège), aux messages et fichiers professionnels en cas de nécessité. À défaut d'une telle désignation, il revient au responsable hiérarchique de l'agent d'accéder aux données professionnelles dans les mêmes conditions.

A défaut de préavis, le responsable hiérarchique, accompagné d'un membre du Service des Affaires juridiques et d'un membre du Service général d'Informatique, est habilité à accéder aux messages et fichiers électroniques professionnels de l'agent.

4. Suspicion de fraude ou de malveillance dans le chef de l'agent

Le responsable hiérarchique, accompagné d'un membre du Service des Affaires juridiques et d'un membre du Service général d'Informatique, est habilité à accéder aux messages et fichiers électroniques professionnels de l'agent.

IV. Confidentialité

Les membres du Service général d'Informatique (SEGI), des Unités décentralisées d'Informatique (UDI) et du Service des Affaires juridiques (SAJ) sont tenus à la plus stricte confidentialité, notamment dans le cadre de l'application de la présente directive.