UNIL | Université de Lausanne
Direction

Directive de la Direction 6.2. Utilisation d'Internet, de la messagerie électronique, des réseaux sociaux, de la téléphonie et du poste de travail

1° Base

La présente directive est prise en application de l'article 125 du Règlement général du 9 décembre 2002 d'application de la loi du 12 novembre 2001 sur le personnel de l'Etat de Vaud (Rglpers).

2° But

Le but de la présente directive est de définir les droits et les devoirs des utilisateurs des moyens de communication (Internet, messagerie électronique, réseaux sociaux et téléphonie) et des postes de travail informatiques mis à leur disposition dans le cadre professionnel.

3° Champ d'application

La présente directive s'applique à tous les collaborateurs de l'Etat, y compris à ceux du Centre Hospitalier Universitaire Vaudois de l'Université de Lausanne (ci-après : UNIL), du Tribunal cantonal et du Tribunal administratif.

Pour le Centre Hospitalier Universitaire Vaudois et l'UNIL, les compétences conférées à la Direction des systèmes d'information (ci-après : DSI) et à l'unité télécom du centre d'exploitation sont exercées par l'Office informatique des Hospices, respectivement par le Centre informatique de l'UNIL.

Sont réservées des dispositions particulières justifiées par la nature des activités (par ex. à l'UNIL et à la Police cantonale). Ces dispositions sont préalablement soumises au SPEV, au SJIC, à la DSI et à l'organe Auditeur de la sécurité des systèmes d'information et de télécommunication (ASSIT)

4° Utilisation

4.1 Internet

a) Internet doit être utilisé pour la recherche et la diffusion d'informations à but professionnel que ce soit sur des réseaux sociaux ou autres. Une utilisation

privée est admise à titre exceptionnel, en dehors des heures de travail, dans la mesure où elle ne constitue pas un abus, notamment qu'elle ne surcharge pas l'infrastructure informatique (stockage ou transfert de fichiers, connexion à des sites radiophoniques ou utilisation de messageries instantanées, par ex. CHAT) et ne vise aucun but lucratif, sous réserve de l'accès à des réseaux sociaux qui ne peut se faire que dans le cadre professionnel.

b) Les collaborateurs ne consultent, ne stockent, ni ne diffusent des documents qui, sous quelque forme que ce soit, constituent une participation à un acte illicite et qui, en particulier, portent atteinte à la dignité de la personne, présentent un caractère pornographique, incitent à la haine raciale ou constituent une apologie du crime ou de la violence. De même, il est interdit de communiquer des données confidentielles par le biais notamment des réseaux sociaux.

c) Les collaborateurs s'engagent à ne pas copier illégalement des logiciels, à ne pas diffuser des informations appartenant à des tiers sans leur autorisation et à mentionner les sources lors de l'utilisation d'information en provenance de tiers.

d) Les collaborateurs ne sont pas autorisés à s'abonner à des services d'information payant sauf accord par le chef d'unité.

e) Le devoir de loyauté auquel est soumis tout collaborateur s'applique également aux réseaux sociaux. Les collaborateurs ont le devoir de protéger les intérêts de l'Université de Lausanne dans tous les commentaires qu'ils peuvent notamment émettre sur des réseaux sociaux.

4.2 Messagerie électronique

a) L'utilisation du courrier électronique comme instrument de communication est réservée aux besoins professionnels. Une utilisation privée est admise à titre exceptionnel, en dehors des heures de travail, dans la mesure où elle ne constitue pas un abus, notamment qu'elle ne surcharge pas l'infrastructure informatique (stockage ou transfert de fichiers) et ne vise aucun but lucratif.

   Les collaborateurs ne participent pas à des chaînes de distribution.

b) L'utilisation de fonctionnalités spéciales pour la messagerie (envoi automatique de notification de réception de messages, envois de SMS, etc.) est réservée exclusivement à des buts professionnels, justifiée et tolérée à titre exceptionnel, dans la mesure où elle ne surcharge par l'infrastructure informatique.

c) Les collaborateurs ne consultent, ne stockent, ni ne diffusent des documents qui, sous quelque forme que ce soit, constituent une participation à un acte illicite et qui, en particulier, portent atteinte à la dignité de la personne, présentent un caractère pornographique, incitent à la haine raciale ou constituent une apologie du crime ou de la violence.

d) Chaque collaborateur s'engage à ne pas modifier les paramètres techniques, ni la liste de contrôles d'accès de sa messagerie personnelle.

e) Sous réserve des dispositions de la loi sur l'information, les collaborateurs s'engagent à ne pas diffuser des informations qui peuvent porter atteinte à la réputation de l'Etat de Vaud ou être contraires aux normes en vigueur (lois, règlements, etc.) sur n'importe quel support que ce soit.

f) A moins d'être cryptées, les données personnelles jugées sensibles (cf. art. 101 Rglpers) ne sont pas transmises par la messagerie électronique.

La conservation des données personnelles est interdite.

4.3 Téléphonie

a) L'utilisation de la téléphonie fixe ou mobile est réservée aux besoins professionnels. L'utilisation de la téléphonie à usage privé est tolérée en respectant les points b) et c).

b) Pour les communications privées, à partir d'appareils mobiles fournis par l'employeur ou d'un téléphone fixe, de même que les conversations professionnelles à partir d'appareils privés, elles sont autorisées, selon les modalités prévues dans la Directive Direction y relative.

c) Dans tous les cas, les collaborateurs privilégient les appels depuis et vers les postes fixes avant de composer le numéro du mobile.

d) L'utilisation de services payants et la commande de biens passée au moyen du mobile et portée directement en compte sur la facture téléphonique, sont interdites sauf autorisation écrite délivrée par le chef de service et envoyée au préalable au Centre informatique.

e) L'utilisation de la téléphonie (fixe et mobile) comme moyen de connexion à un autre réseau externe (Internet, etc.) est interdite, sauf autorisation expresse de l'ASSIT.

f) La définition de la zone géographique d'appel relève de la compétence du chef de service.

4.4 Poste de travail et stockage des données

a) Le poste de travail est un élément constitutif du système informatique de l'Etat. La modification de son contenu et/ou un usage inapproprié peuvent avoir des effets sur le fonctionnement global du système. Le poste de travail doit être utilisé pour accomplir des tâches à buts professionnels. La gestion des postes est effectuée par des personnes autorisées, sur le site ou à distance, en tout temps.

   Lorsque, dans le cadre d'une intervention, des collaborateurs de l'Etat ont eu connaissance de données à caractère confidentiel, ils sont tenus aux mêmes règles de confidentialité que l'utilisateur du poste.

b) Une utilisation privée des applications installées sur le poste de travail est tolérée à titre exceptionnel, en dehors des heures de travail, dans la mesure où elle ne constitue pas un abus, notamment qu'elle ne surcharge pas l'infrastructure informatique (stockage ou transfert de fichiers) et ne vise aucun but lucratif.

c) Sauf raison professionnelle justifiée et approuvée par le Centre inforamtique (aspects techniques et sécuritaires), il est notamment interdit de :
   - connecter au poste de travail ou sur le réseau des appareils électroniques non homologués par le CI (agendas électroniques, téléphones portables, pocket PC, etc.).

d) Les modifications effectuées et qui sont interdites en vertu de la lettre c) ci-dessus, seront supprimées sans préavis.

e) Les collaborateurs s'engagent à ne pas gêner les opérations découlant des besoins de gestion des postes de travail (activation d'outils d'inventaire et de diagnostic, de prise de main à distance, de télédistribution de logiciels, etc.).

f) Les collaborateurs s'engagent à traiter leur mot de passe personnellement et de manière confidentielle.

g) Les collaborateurs s'engagent à ne pas désactiver la protection antivirus.

h) De manière générale, les collaborateurs stockent leurs données sur les serveurs prévus à cet effet. Ils sont tenus de les épurer régulièrement.

5° Contrôle du respect de la directive et sanctions

5.1 Dispositions générales

a) Les chefs de Service informent leurs collaborateurs des obligations contenues dans la présente directive.

b) Les chefs de Service s'assurent de l'exécution de la présente directive et de son respect.

c) L'application de la présente directive aux chefs de Service est de la compétence du chef de Département.

5.2 Données privées

Les données des collaborateurs sont propriété de l'Etat, sauf si elles sont explicitement et distinctement présentées comme des données privées. Celles-ci ne sont accessibles que par les personnes expressément autorisées par le chef de Service.

L'ouverture directe de fichiers ou de messages explicitement désignés comme données privées n'est pas autorisée, sauf accord du collaborateur.

5.3 Contrôle général

a) Le chef de Service est seul habilité à décider d'un contrôle général anonyme au sein de son service. Il en informe préalablement ses collaborateurs. En principe, sauf décision contraire du chef de Service, le contrôle général porte sur une période postérieure à l'annonce.

b) A cet effet, le chef de Service mandate l'ASSIT, qui assume la responsabilité de l'exécution de ce contrôle. Il peut solliciter les correspondants sécurité informatique décentralisés.

c) L'ASSIT communique au chef de Service les résultats de ce contrôle.

d) Au besoin, l'ASSIT sauvegarde les données le temps nécessaire.

e) Le chef de Service informe les collaborateurs du résultat des contrôles effectués.

f) Sur cette base, le chef de Service peut soit :
- opérer un nouveau contrôle, général ou particulier, et l'annoncer;
- intervenir auprès du collaborateur (mise en garde, demande de mise en conformité, restriction des droits, etc.);
- décider d'une mesure au sens de la Lpers (par ex. avertissement ou résiliation avec effet immédiat pour justes motifs).

5.4 Contrôle particulier

a) Le chef de Service peut décider de procéder à un contrôle particulier personnalisé.

b) Le collaborateur est informé du contrôle particulier, sauf lorsqu'un abus a déjà été constaté lors d'un contrôle général ou lors d'un contrôle informatique technique ou de sécurité, ou encore s'il y a soupçon concret qu'un acte délictuel a été commis. En principe, sauf décision contraire du chef de Service, le contrôle particulier porte sur une période postérieure à l'annonce.

c) A cet effet, le chef de Service mandate l'ASSIT, qui assume la responsabilité de l'exécution de ce contrôle.

d) L'ASSIT communique au chef de Service les résultats de ce contrôle.

e) Au besoin, l'ASSIT sauvegarde les données le temps nécessaire.

f) Selon les résultats du contrôle, le chef de Service examine, avec l'appui du SJIC, si les agissements du collaborateur sont de nature pénale. Dans l'affirmative, le SJIC dépose plainte au nom de l'Etat.

   Dans ce cas, le chef de Service prend les mesures adéquates en application de la Lpers.

g) Sous réserve de la lettre f) ci-dessus, le chef de Service peut soit :
   - opérer un nouveau contrôle, général ou particulier, et l'annoncer;
   - intervenir auprès du collaborateur (mise en garde, demande de mise en conformité, restriction des droits, etc.);
   - décider d'une mesure au sens de la Lpers (par ex. avertissement ou résiliation avec effet immédiat pour justes motifs).

5.5 Divers

Le Conseil d'Etat ou le chef du Département peuvent mandater l'ASSIT afin de procéder à un contrôle transversal, pour s'assurer du respect de la présente directive. Les collaborateurs en sont préalablement informés.

La procédure prévue pour le contrôle général est applicable.

Modifications de la Directive adoptées par la Direction dans ses séances
du 10 octobre 2011 et du 16 juin 2014