

Règlement d'utilisation des systèmes d'information et du réseau de l'ULB



Table des matières

| | | |
|-------|---|---|
| 1 | DEFINITIONS | 3 |
| 2 | PREAMBULE..... | 4 |
| 3 | CONTEXTE | 4 |
| 4 | OBJECTIFS | 5 |
| 5 | DOMAINE D'APPLICATION..... | 5 |
| 6 | PRINCIPES GENERAUX | 5 |
| 6.1 | <i>FINALITES D'UTILISATION</i> | 5 |
| 6.2 | <i>LICEITE DU CONTENU ECHANGE</i> | 6 |
| 6.2.1 | <i>Respect du droit à la propriété intellectuelle</i> | 6 |
| 6.2.2 | <i>Respect des droits et des personnes</i> | 6 |
| 6.2.3 | <i>Respect de l'ordre public</i> | 6 |
| 6.2.4 | <i>Confidentialité</i> | 7 |
| 6.3 | <i>PRINCIPES D'UTILISATION</i> | 7 |
| 6.4 | <i>PRINCIPE DE SECURITE</i> | 8 |
| 7 | SIGNALER LA FUITE DE DONNEES | 9 |

1 Définitions

| | |
|--|---|
| AUP (Acceptable Use Policy) | Ensemble de règles relatives à l'utilisation de services Internet et Réseau. |
| Belnet | Réseau national belge fournisseur de service Internet à haute vitesse notamment aux universités, hautes écoles, centres de recherche et services publics belges. |
| Communauté universitaire | À l'ULB, le terme englobe tout le personnel académique, le personnel scientifique, le personnel administratif, technique, de gestion et spécialisé (PATGS) mais aussi les étudiants, visiteurs et bénévoles, qu'ils soient membres de l'Université ou de ses établissements fédérés (p. ex. : la VUB). |
| Eduroam | De l'anglais « Educational roaming », Eduroam est un service offrant un accès WiFi sécurisé à l'Internet, au personnel et aux étudiants des établissements d'enseignement supérieur et de recherche. Les utilisat.eur.rice.s d'un établissement membre d'Eduroam disposent d'un accès sécurisé à l'Internet dans tous les autres établissements membres en utilisant leurs identifiants personnels. |
| ULBID (anciennement NetID) | De l'anglais « N etwork I dentit y », il s'agit de l'identité réseau d'un utilisat.eur.rice lui permettant d'accéder aux ressources informatiques et réseau de l'Université. |
| Ressources informatiques | Ensemble des moyens matériels (serveurs, logiciels, stations de travail, postes de consultation, ordinateurs portables, périphériques...), des données (en ce compris les données contenues dans des bases de données) et des ressources extérieures (ex. : Internet) accessibles depuis le réseau de l'ULB. |
| Ressources TIC | Toute ressource ou matériel informatique, serveur physique ou virtuel, dispositif de stockage de données ou de réseau, support magnétique ou de réseau ainsi que tout autre dispositif de communication exploité ou géré par l'Université, concédé sous licence à l'Université ou exploité par une organisation externe pour le compte de l'Université. |
| Systèmes d'information | Ensemble d'applications, services, ressources informationnelles ou autres composants permettant de gérer l'information. |
| TIC | Les T echnologies de l' I nformation et de la C ommunication (TIC) regroupent l'ensemble des outils permettant de produire, manipuler, gérer, transmettre ou de retrouver une information et de la communiquer (ex. : Internet). |
| Utilisat.eur.rice | Toute personne, quel que soit son statut, appelée à utiliser les ressources informatiques et le réseau de l'Université. |

| | |
|--|--|
| <p>Les droits d'auteur ¹</p> | <p>Une œuvre est protégée par la législation belge sur le droit d'auteur (intégrée dans le Code de droit économique) s'il s'agit d'une création littéraire ou artistique originale et qu'elle a été mise en forme. La protection du droit d'auteur existe sans qu'aucune formalité ne doive être remplie. Dès sa création, une œuvre qui répond aux conditions d'originalité et de mise en forme est protégée par le droit d'auteur.</p> |
| <p>La propriété intellectuelle ²</p> | <p>La propriété intellectuelle désigne les œuvres de l'esprit, notion qui recouvre non seulement les œuvres d'art et les inventions, mais aussi les programmes informatiques et les marques et autres signes commerciaux.</p> |

2 Préambule

Le présent règlement représente le cadre général régissant l'interprétation et l'application de tous les autres règlements de l'institution en matière d'utilisation et de sécurité des technologies de l'information. Il a pour but d'édicter les règles d'utilisation des systèmes d'information et du réseau de l'Université libre de Bruxelles (ULB).

Les dispositions du présent règlement ne constituent pas et ne sauraient être interprétées comme limitant l'exercice normal du droit à la liberté d'expression, à la liberté syndicale, à l'exercice des droits résultant de l'organisation démocratique interne de l'Université ou à la liberté académique. Elles n'entendent pas non plus limiter la protection dont doivent jouir les lanceurs d'alerte ou restreindre le bénéfice par les membres de la communauté universitaire des exceptions aux droits de la propriété intellectuelle.

3 Contexte

Dans le cadre de ses activités, l'ULB acquiert, développe et maintient plusieurs ressources informatiques et de communication (ou ressources TIC) destinées au soutien direct et indirect des missions d'enseignement, de recherche, des fonctions administratives et de service à la collectivité et à la société qui lui reviennent.

Le réseau universitaire RESULB est raccordé à Internet via le réseau **Belnet**, qui constitue son fournisseur. Chaque utilisateur s'engage à se conformer aux normes et protocoles régissant l'utilisation du réseau et des services Belnet et que Belnet porte à la connaissance de chacun de ses clients dans sa « Politique d'utilisation acceptable (AUP) des services internet de Belnet »³. Ces normes et protocoles sont repris dans le présent règlement.

¹ <https://economie.fgov.be/fr/themes/propriete-intellectuelle/droits-de-pi/droits-dauteur-et-droits/les-droits-dauteur>

² <https://economie.fgov.be/fr/themes/propriete-intellectuelle>

³ BELNET (2020). Politique d'utilisation acceptable ("AUP") des services internet de Belnet. www.belnet.be/fr/politique-dutilisation-acceptable-aup-des-services-internet-belnet

4 Objectifs

Par le présent règlement, l'Université :

- reconnaît l'importance de sécuriser ses systèmes d'information et s'engage à préserver la confidentialité et l'intégrité de ses ressources informatiques et de communication (TIC) qu'elle met à la disposition de la communauté universitaire ;
- met en œuvre les mesures nécessaires pour assurer la protection et la sécurité de l'utilisat.eur.rice ;
- porte à la connaissance de l'utilisat.eur.rice les obligations lui incombant ainsi que les conduites appropriées à suivre, sans être exhaustives, dans le cadre de l'utilisation des ressources informatiques et de l'accès au réseau de l'Université.

5 Domaine d'application

Les dispositions du présent règlement s'appliquent à l'ensemble des utilisat.eur.rice.s des systèmes d'information et du réseau de l'ULB et en particulier à :

- tout membre du personnel ;
- tout membre du personnel (pré)retraité ou (pré)pensionné ;
- tout.e étudiant.e inscrit.e ou en cours d'inscription pour l'année académique en cours ;
- tout.e étudiant.e diplômé.e « alumni » conservant pour une période temporaire son adresse email « @ulb » ;
- tout.e visiteu.r.se, bénévole ainsi que toute personne membre d'une organisation externe autorisée à utiliser les ressources ou réseaux informatiques de l'Université.

6 Principes généraux

6.1 Finalités d'utilisation

Les systèmes d'information et le réseau de l'ULB peuvent être utilisés pour des activités rentrant dans le cadre des missions fondamentales et interdépendantes que sont l'enseignement, la recherche et le service à la collectivité et à la société. L'utilisation à des fins commerciales est interdite. Une utilisation à des fins privées limitée est toutefois autorisée pour autant qu'elle ne nuise pas aux systèmes d'information et au réseau. L'utilisat.eur.rice est tenu.e d'utiliser le réseau et les systèmes d'information de l'ULB uniquement à des fins strictement légales, et en accord avec les dispositions réglementaires de l'Université.

6.2 Licéité du contenu échangé

6.2.1 Respect du droit à la propriété intellectuelle

L'utilisat.eur.rice n'utilisera pas les systèmes d'information et le réseau de l'ULB d'une façon qui pourrait diluer, détourner ou enfreindre le droit à la propriété intellectuelle, notamment le droit d'auteur ainsi que des lois protégeant les brevets, marques et secrets de fabrication.

Tous les logiciels achetés par l'Université ou développés par ses employés ou des entrepreneurs pour le compte de l'Université sont protégés par le droit d'auteur. Par conséquent, l'utilisation ou la reproduction de ces logiciels nécessite une autorisation écrite des titulaires de ces droits.

L'utilisat.eur.rice veillera à :

- utiliser les logiciels sur le réseau ou sur des dispositifs indépendants conformément aux termes des licences souscrites ;
- respecter les droits de propriété intellectuelle d'œuvres protégées (livres, logos, pièces musicales, images, logiciels...), qui interdisent de reproduire et d'exploiter ces œuvres sans l'autorisation explicite de l'auteur ;
- se préserver de toute tentative de reproduction, de téléchargement ou de distribution de matériel protégé par une marque de commerce, un secret commercial ou tout autre droit de propriété intellectuelle sans autorisation appropriée et explicite des titulaires de ce droit.

6.2.2 Respect des droits et des personnes

Il est interdit de diffuser des informations qui seraient en opposition avec les dispositions légales et réglementaires de l'Université, notamment en ce qui concerne la protection de la personne, des individus et des biens, le respect de la vie privée, et le droit à l'image.

L'utilisat.eur.rice s'engage à s'abstenir de porter atteinte par la nature de ses communications à l'image et aux intérêts de l'ULB ou de toute personne morale ou physique.

6.2.3 Respect de l'ordre public

L'utilisat.eur.rice s'engage à respecter l'ordre public et les bonnes mœurs⁴ et s'interdit de commettre des actes ou de tenir des propos troublant ceux-ci, notamment via des messages diffamatoires, d'incitation au terrorisme, racistes, xénophobes, sexistes, constituant un outrage à la pudeur ou encore une diffusion de fausses nouvelles.

⁴ <https://www.justice-en-ligne.be/Ordre-public>

6.2.4 Confidentialité

L'utilisat.eur.rice s'engage à respecter toute donnée ou information à caractère confidentiel et, en particulier, à :

- ne pas lire, copier, divulguer ou modifier les fichiers d'un.e autre utilisat.eur.rice sans son autorisation explicite même si les fichiers lui sont accessibles ;
- ne pas intercepter les communications privées de type messagerie électronique d'un.e autre utilisat.eur.rice ;
- ne pas s'approprier ou déchiffrer les informations d'authentification d'un.e autre utilisat.eur.rice ;
- ne pas limiter ou interdire l'accès aux systèmes d'information d'un.e autre utilisat.eur.rice, sans la décision de l'autorité compétente ;
- ne pas divulguer ou diffuser, sans y être habilité, des renseignements qui sont la propriété de l'Université ;
- sauvegarder et protéger par tout moyen approprié les informations critiques dont ils seraient auteurs ou auxquelles ils auraient accès. Par « informations critiques », on entend toute information ou donnée dont la perte ou la diffusion involontaire pourrait causer un préjudice financier ou moral à l'Université.

6.3 Principes d'utilisation

L'utilisation des systèmes d'information et du réseau de l'Université doit se limiter aux activités universitaires mentionnées au point 6.1 et ne doit en aucun cas perturber le bon fonctionnement du système d'information, ou d'une manière générale, porter atteinte au fonctionnement de l'Université.

Tout utilisat.eur.rice veillera à employer les ressources informatiques mises à sa disposition par l'Université de manière modérée de sorte à ne pas compromettre l'utilisation ou la performance des services des systèmes d'information et du réseau au plus grand nombre.

Une vigilance particulière est requise lors du téléchargement ou du transfert de fichiers volumineux. L'Université se réserve le droit de restreindre voire d'interdire le téléchargement ou le transfert de certains fichiers fortement consommateurs de ressources réseau et risquant de compromettre la performance de ses services.

De plus, tout utilisat.eur.rice du réseau informatique s'engage à ne pas effectuer d'opérations qui entraîneraient :

- l'accès non consenti, la modification ou la destruction de données d'un tiers utilisant le réseau ;
- le gaspillage des ressources (humaines, de réseaux, informatiques) ;

- lors de l'utilisation de ressources informatiques partagées, la monopolisation des systèmes ; la surcharge des réseaux de données excessives ; la dégradation des services ou le gaspillage de temps machine, du temps de connexion ou d'espace disque de tout autre matériel informatique donné ;
- la dégradation des systèmes par l'utilisation d'un espace de données injustifié ;
- l'établissement de connexions réseau sans surveillance ;
- l'interruption du fonctionnement normal du réseau ou d'un des systèmes connectés au réseau par la mise hors tension ou le redémarrage d'un système dont il n'est pas le gestionnaire ;
- la nécessité de mettre en place des moyens humains ou techniques supplémentaires pour son contrôle et sa destruction.

6.4 Principe de sécurité

L'Université s'engage à prendre et maintenir les mesures nécessaires afin d'assurer la sécurité de ses systèmes d'information et de protéger ses utilisat.eur.ice.s en contrant les virus, bloquant les courriers indésirables et surveillant le trafic réseau pour détecter toute activité malveillante éventuelle.

Cependant, l'Université ne peut pas garantir le succès absolu et total de ces mesures et l'utilisat.eur.ice doit accepter le risque inhérent à l'utilisation de la technologie.

Il est interdit de porter atteinte à la sécurité de l'infrastructure informatique de l'ULB, à partir de systèmes connectés à Belnet ou de tout autre système informatique externe ou interne.

Le droit d'accès aux ressources des systèmes d'information et au réseau de l'Université est personnel et incessible.

Afin d'assurer la sécurité des accès aux ressources du système d'information, l'utilisat.eur.ice est tenu.e de :

- protéger son « identité réseau » (« ULBID (anciennement NetID »), son mot de passe et son système contre toute utilisation abusive ou malveillante. Elle est aussi responsable de toutes les activités émanant de son compte ou de ses dispositifs ;
- sécuriser ses équipements informatiques lorsqu'ils sont laissés sans surveillance (ex : verrouillage automatique). Les dispositifs nomades comme les clés USB ou les disques durs externes doivent demeurer en la possession de l'utilisat.eur.ice et être sécurisés.

Pour la sécurité des systèmes informatiques et du réseau, l'utilisat.eur.rice est tenu.e de ne pas effectuer d'actions malveillantes. Par exemple (liste non exhaustive) :

- la tentative de forcer l'accès à des systèmes sans y être autorisé.e ou habilité.e, quel que soit le niveau de sécurisation de ces systèmes ;
- la tentative de contourner la sécurité des systèmes et du réseau interne et / ou externe ;
- la tentative d'intercepter des informations destinées à des tiers, par exemple par la capture de trafic réseau via une connexion réseau fixe ou via un équipement sans fil ;
- l'utilisation d'identifiants d'autrui pour accéder à des ressources informatiques ;
- l'utilisation du réseau pour effectuer une connexion non autorisée à d'autres dispositifs d'information ou de communication ;
- la destruction partielle ou complète de données informatiques ;
- l'usage de matériel ou de logiciel d'une manière qui empêche ou détourne la finalité et les responsabilités de l'ULB dans son usage de Belnet et la mise à disposition d'un réseau dans un cadre public. Nous pensons par exemple à la transparence demandée dans la sphère judiciaire relative au trafic internet, laquelle peut être compromise par des configurations dark web, browser TOR ou Opera (ou tout autre type de connexion anonymisée), etc. ;
- l'introduction et la diffusion de virus et autres codes informatiques malveillants dans les systèmes informatiques.

7 Signaler la fuite de données

Tout utilisat.eur.rice doit avertir son responsable et le RSSI en cas de fuite de données ou tout autre dysfonctionnement du système d'information ou du réseau via l'adresse rssi@ulb.be.

Les incidents informatiques, comme le vol de matériel, le vol de mots de passe, la présence de virus et programmes malveillants ainsi que toute autre type de cyberattaque doivent également être signalés dès leur détection.