THE GRADUATE INSTITUTE GENEVA

INSTITUT DE HAUTES ÉTUDES INTERNATIONALES ET DU DÉVELOPPEMENT

GRADUATE INSTITUTE OF INTERNATIONAL AND DEVELOPMENT STUDIES

Conditions générales d'utilisation des ressources informatiques de l'Institut

1. Conditions de mise à disposition, but et champ d'application

1.1. Conditions de mise à disposition

L'utilisation des ressources informatiques de l'Institut est une simple faculté octroyée à bien plaire par ce dernier. Cette mise à disposition ne génère aucun droit acquis pour ses utilisateurs.

L'Institut peut donc restreindre, en tout ou en partie, les modalités d'utilisation accordées, sans préavis et sans dédommagement.

1.2. But

Les présentes conditions générales d'utilisation (ci-après « CGU ») a pour but de fixer le cadre des règles d'utilisation et de protéger les intérêts de l'Institut et de l'utilisateur en matière de surveillance des ressources informatiques.

1.3. Champ d'application

Les CGU s'appliquent à toute personne bénéficiant d'un accès à une ressource informatique (personne désignée « utilisateur », ci-après): candidat enregistré étudiant interne ou externe, alumni, participant aux programmes de formation continue, collaborateur interne ou externe, affilié, visiteur, consultant.

Constituent des ressources informatiques tous les équipements et services touchant au domaine informatique (y compris applications dérivées) et mis à disposition de l'utilisateur par l'Institut, quel que soit le lieu d'utilisation et/ou le type d'accès (sur site, à distance, par câble ou par liaison sans fil, etc.).

L'utilisation des ressources informatiques de l'Institut par l'utilisateur entraîne l'acceptation pleine et entière, par ce dernier, des dispositions des CGU et des réglementations en découlant.

2. Intérêts et risques de l'Institut et de l'utilisateur

2.1. Intérêts et risques de l'Institut

L'utilisation, à l'Institut, d'un équipement informatique connecté au réseau (sur site ou à distance) peut porter atteinte à certains intérêts et équipements techniques de l'Institut. Peuvent être affectés notamment :

- la capacité de stockage des fichiers et la bande passante du réseau, suite par exemple à une utilisation excessive d'Internet et du courrier électronique ;
- la sécurité des données et des applications (disponibilité, intégrité, confidentialité), en raison de l'importation de virus, vers, chevaux de Troie ou de l'installation de logiciels étrangers à l'Institut sur des ordinateurs de l'Institut;
- les intérêts financiers (augmentation des coûts pour des moyens et/ou prestations supplémentaires, frais de réseau, etc.);
- d'autres intérêts de l'Institut protégés par la loi, tels que sa réputation, ou encore la confidentialité des données.

2.2. Intérêts et risques de l'utilisateur

Les intérêts de l'utilisateur, liés notamment au surf et au courrier électronique dans le cadre de ses activités à l'Institut (information et communication), peuvent être menacés sur le plan notamment de la protection des données ou sur le plan économique.

3. Mesures de protection techniques et journalisations

3.1. Mesures de protection techniques

L'Institut met en œuvre les mesures de protection techniques suivantes:
- Accès sécurisés aux locaux contenant les serveurs de données ;
- Authentification de l'utilisateur avec mot de passe confidentiel ;
- Protection contre des accès non autorisés (droits d'accès) aux données ou objets dignes de protection ;
- Sauvegarde quotidienne des fichiers (*backup*) sécurisée et gestion des quotas disques ;
- Système de pare-feu (*firewall*) protégeant les données contre les attaques extérieures ;
- Logiciels antivirus permettant de déceler les virus et éléments analogues et en règle générale aussi de les détruire.

Les mesures précitées peuvent être adaptées au gré de l'évolution de la technique.

3.2. Journalisations

La plupart des activités effectuées à l'aide de moyens informatiques de l'Institut sont consignées dans des fichiers journaux. La journalisation est l'enregistrement continu des données d'utilisation de type « qui, quoi, quand». Au sein de l'Institut, elle est effectuée aux endroits suivants:

- Sur les ordinateurs de l'Institut, dans le système d'exploitation (fichiers et applications utilisées), dans le navigateur internet (historique et *cookies*). Le but de ces journalisations est d'améliorer les temps de réponses des applications. Elles sont stockées à titre temporaire (cache).
- Sur les serveurs de l'Institut. Le but de ces journalisations est le contrôle du bon fonctionnement des serveurs. Les journaux ne sont pas conservés au-delà d'un mois .
- Sur les équipements de connexions inter-sites (firewalls, routeurs, switch, etc.). Le but de ces journalisations est le contrôle du bon fonctionnement du réseau et la gestion de la bande passante. Les journaux ne sont pas conservés au-delà de trois mois.

4. Règlement d'utilisation

Les ressources informatiques sont mises à disposition à des fins académiques et professionnelles. Un usage personnel est toléré dans les limites de la bienséance et selon les règles d'utilisation émises par l'Institut. Toute utilisation abusive ou dans des conditions contraires à la loi et aux bonnes mœurs est formellement interdite.

Les ordinateurs de l'Institut contiennent un ensemble d'applications préinstallées. Afin de prévenir tout risque de détérioration du contenu de l'ordinateur, toute installation de nouvelles applications doit être faite par le service informatique de l'Institut.

Les règles d'utilisation sur le plan pratique font l'objet d'un document particulier séparé[1].

En outre, les collaborateurs sont soumis à l'article 8 du règlement interne[2].

5. Règlement de surveillance

5.1. Priorité aux mesures de protection techniques

L'Institut s'engage à privilégier les mesures de protection techniques pour prévenir les abus et les dommages de nature technique. Il actualise régulièrement les mesures de protection techniques en fonction des évolutions de la technologie. Il adapte également ces mesures après un dérangement technique. Il n'a le droit de procéder à une analyse nominative des fichiers journaux que dans les cas où les mesures de protection techniques ne suffisent pas à empêcher un abus. Il n'utilise pas d'espiogiciels.

5.2. Analyse des fichiers journaux

L'Institut peut effectuer des analyses anonymes et pseudonymes des fichiers journaux dans le but de vérifier si le règlement d'utilisation est respecté. L'analyse anonyme est une analyse statistique des fichiers journaux qui s'effectue sur la base de critères tels que les pages web les plus consultées. L'analyse pseudonyme se fait par sondages uniquement.
Les analyses anonymes ou pseudonymes portent sur des échantillons suffisamment grands de personnes pour garantir le caractère confidentiel des analyses.
Si l'Institut constate un abus lors d'une analyse anonyme ou pseudonyme (ou qu'une analyse fait naître un soupçon d'abus), il procède à une analyse nominative des fichiers journaux. Est considéré comme abus toute violation du règlement d'utilisation. Lorsqu'il y a abus, l'Institut peut prononcer une des sanctions visées au point 5.4 des CGU. S'il s'avère qu'un soupçon est infondé, l'Institut interrompt immédiatement l'analyse nominative.
Si l'analyse des fichiers journaux ou d'autres éléments révèle l'existence d'un délit ou fait naître des soupçons d'abus, l'Institut sauvegarde les fichiers journaux concernés. Il se réserve le droit de déposer plainte contre l'utilisateur concerné. La suite de la procédure relève des autorités pénales. L'Institut s'engage à traiter les résultats de l'enquête de manière confidentielle, notamment à l'égard des tiers non

[1] Règles et bonnes pratiques d'utilisation des ressources informatiques
[2] Règlement interne de l'Institut de hautes études internationales et du développement

autorisés (tels que les collaborateurs et étudiants de l'Institut). C'est la direction (ou toute personne qu'elle aura habilitée à cet effet) qui décidera si une plainte est déposée ou non.

5.3. Surveillance exercée pour garantir la sécurité et le bon fonctionnement du système informatique ou sur la base d'autres indices

Si l'Institut ou un partenaire technique (fournisseur d'accès Internet, etc.) constate un dysfonctionnement du système informatique en dépit des mesures de protection techniques prises, l'Institut peut analyser les fichiers journaux pour en déterminer la cause. Si le dysfonctionnement est dû à un abus, l'utilisateur fautif peut faire l'objet d'une des sanctions visées au point 5.4.
Si l'Institut constate un abus ou qu'il pense qu'il y a eu abus parce que d'autres indications le lui font supposer, il peut consulter les fichiers journaux concernés et leurs analyses. En cas d'abus, il peut prononcer l'une des sanctions visées au point 5.4.

5.4. Sanctions en cas d'abus

Si les conditions requises pour la surveillance et les règles qui la régissent ont été respectées, l'Institut est en droit, lorsqu'il constate un abus, de prendre des sanctions disciplinaires contre l'utilisateur fautif. Les sanctions possibles seront décidées par la direction.

5.5. Prétentions de l'utilisateur en cas de surveillance illicite

Si les conditions requises pour la surveillance et les règles qui la régissent ne sont pas respectées, l'utilisateur peut faire valoir les prétentions prévues par les dispositions civiles et pénales applicables.

5.6. Autres dispositions

Le service informatique et la direction de l'Institut prennent toutes les mesures techniques nécessaires pour empêcher que les données personnelles qu'ils traitent dans le cadre d'une surveillance ne tombent entre les mains de personnes non autorisées. Ils veillent en particulier à assurer la confidentialité, la disponibilité et l'intégrité de ces données.
L'utilisateur peut en tout temps demander à l'Institut si des données le concernant sont traitées et, le cas échéant, lesquelles.
Des données personnelles ne peuvent être communiquées à des tiers non autorisés sans motif valable ou sans l'accord de la personne concernée.

6. Responsabilités et exclusions de responsabilité

6.1. Etendue de la responsabilité de l'utilisateur

De manière générale, l'utilisateur est responsable de tout dommage résultant d'une utilisation non conforme des ressources informatiques.

En particulier, l'utilisateur est personnellement responsable notamment de

- La mise en application de la sécurité informatique à son niveau d'utilisateur
- La sauvegarde des données qu'il traite, ainsi que de leur intégrité
- Toute action effectuée sous l'identité de son compte
- Des informations qu'il rend accessible aux autres
- Tout dommage ou pénalités résultant du non-respect de dispositions légales ou réglementaires, notamment de droits de propriété intellectuelle de tiers (p. ex. non-respect de licences de logiciels, etc.).

6.2. Etendue de la responsabilité de l'Institut

L'Institut met en œuvre tous les moyens raisonnables, en l'état de la technique, pour assurer des ressources informatiques performantes ; néanmoins, l'Institut décline toute responsabilité, à quelque titre que ce soit, concernant des dommages, de quelque nature qu'ils soient (directs, indirects, etc.), liés à l'utilisation des ressources informatiques.

De même, l'Institut utilise tous les procédés raisonnables, en l'état de la technique, pour sécuriser les ressources informatiques ; toutefois, l'Institut ne donne aucune garantie, de quelque nature que ce soit, quant à la sécurité et la fiabilité des ressources informatiques mises à disposition et, de ce fait, décline toute responsabilité à ce sujet, cette exclusion étant opérée aux conditions citées au paragraphe précédent.

7. Entrée en vigueur

Les CGU entrent en vigueur le 2 septembre 2009.

8. Mises à jour

V120 - 24.08.2015 : extension du champ d'application aux participants des programmes de la formation continue

V200 - 22.06.2017 : extension du champ d'application à tous les utilisateurs des ressources informatiques de l'Institut. Ajout d'une référence au règlement interne de l'Institut pour les collaborateurs. Nouveau titre avec le remplacement du terme Note par Conditions générales d'utilisation.