# CHARTE D'UTILISATION
# DES RESSOURCES INFORMATIQUES D'ESIEE PARIS



## 1. INTRODUCTION

ESIEE Paris met à la disposition des élèves et de certains visiteurs, un ensemble de ressources informatiques logicielles et matérielles exclusivement réservées aux activités pédagogiques, scientifiques, administratives et de recherche et développement.
Les micros et stations de travail sont connectés à un réseau local lui-même relié à Internet via le fournisseur d'accès d'ESIEE Paris : RENATER. L'ensemble de ces ressources ainsi que l'accès au réseau Internet sont exclusivement réservés aux seules personnes ayant obtenu un code d'accès par l'intermédiaire de l'Administration d'ESIEE Paris.

Outre les règles déontologiques et de bonne conduite, l'utilisation d'un système informatique quel qu'il soit est soumis au respect d'un certain nombre de textes de lois. Leur non-respect peut-être passible de sanctions pénales (amendes et peines de prison).

La présente charte n'a pas pour but d'être exhaustive en termes de lois que doit respecter tout usager d'un système informatique mais elle l'informe de leur existence et l'avertit des risques encourus.

Elle s'applique à toute personne (désignée dans ce document par "**utilisateur**") consommant directement ou par l'intermédiaire d'applications des ressources informatiques au sein du réseau informatique d'ESIEE Paris. Les ressources informatiques comprennent l'ensemble des moyens matériels, logiciels et réseaux mis à la disposition des utilisateurs d'ESIEE Paris, y compris les ressources gérées par ESIEE Paris accessibles via le réseau Internet. Par la suite, l'ensemble de ces ressources informatiques sera désigné par le terme de « **système informatique** ».

Le système informatique est gérée par le Service des Moyens Informatiques Généraux d'ESIEE Paris (SMIG) ou par les ingénieurs de laboratoires d'ESIEE Paris. L'ensemble de ces collaborateurs est désigné par le terme « **service informatique** ».

Ces règles s'appliquent aussi implicitement aux personnes extérieures qui utilisent les services en tant qu'invité (le wifi, par exemple) sous la responsabilité du collaborateur d'ESIEE Paris qui a fait la demande de code d'accès (en général l'organisateur d'une réunion).

## 2. AVERTISSEMENT PRELIMINAIRE

Le service informatique met à la disposition des utilisateurs des ressources matérielles et logicielles. L'utilisation de ces ressources est sujette aux conditions suivantes :

- Le service informatique ne saurait être tenu pour responsable des dommages, pertes de données ou d'informations découlant d'une mauvaise utilisation des ressources informatiques.
- Le service informatique effectue des sauvegardes régulières des données des utilisateurs stockées sur les serveurs dans le but de les protéger contre les pannes matérielles et logicielles dans le cadre d'un engagement de moyens. Il subsiste malgré tout une probabilité que ces données n'aient pu être sauvegardées ou ne puissent être restaurées. Le Service des Moyens Informatiques Généraux ne saurait en être tenu pour responsable.
- A son départ de l'établissement, l'utilisateur fait son affaire de l'archivage de ses données personnelles. L'utilisateur ne pourra se prévaloir d'un quelconque dommage en cas d'usage ultérieur de ses données ou au moment de leur effacement.
- Les activités d'ESIEE Paris étant l'enseignement et la recherche, ses systèmes informatiques sont ouverts à un nombre important et à une grande variété d'usagers. Ils nécessitent la mise en place de procédures de sécurité adaptées en conséquence. Bien que les administrateurs des systèmes informatiques prennent en compte et appliquent les diverses recommandations en la matière, il subsiste toujours des possibilités d'intrusion résultant de l'absence ou du dysfonctionnement non répertoriés d'un mécanisme de sécurité. Le service informatique ne saurait en être tenu pour responsable.
- Afin de préserver l'intégrité et la sécurité des ressources informatiques, pour éviter les intrusions, le piratage ou la falsification des données, les administrateurs du système informatique peuvent être amenés à vérifier et examiner le contenu des fichiers des comptes des utilisateurs. De même, dans le cas d'une présomption d'intrusion, de piratage ou de falsification de données, la boîte aux lettres électronique d'un utilisateur pourra être examinée.

## 3. CONDITIONS D'ACCES AUX SYSTEMES INFORMATIQUES

Seuls les utilisateurs autorisés peuvent accéder au système informatique d'ESIEE Paris. Les autorisations sont délivrées par les services administratifs d'ESIEE Paris sous la forme d'un compte informatique identifié par un code d'accès (login) et un mot de passe. Pour les élèves, ces informations sont délivrées lors des formalités d'inscription, au début de chaque année scolaire.

L'autorisation d'accès au système informatique est attribuée individuellement à chaque utilisateur. **Ce droit est personnel et incessible**. Un utilisateur qui ouvrirait l'accès de son compte informatique à une tierce personne est responsable de ses agissements et se verrait endosser la responsabilité des actions malveillantes qui pourraient être intentées à l'encontre des autres utilisateurs ou des ressources informatiques.

Le mot de passe constitue la clé de voûte de la sécurité dans le système informatique. Chaque utilisateur doit choisir un mot de passe suffisamment difficile à découvrir et le modifier régulièrement, en particulier en cas de présomption de tentatives d'intrusion sur son compte par une tierce personne.

Le droit d'accès est accordé pour les activités de l'utilisateur dans l'établissement (recherche, études, enseignement, stages,...). Il disparaît lorsque l'utilisateur quitte définitivement l'établissement.
Il donne accès :

- à au moins un poste de travail, dédié ou partagé ;
- à une adresse de messagerie, cette messagerie est basée sur les services Google Apps ;
- au réseau interne, aux services associés et à l'Internet ;
- aux serveurs d'ESIEE Paris et aux applications qu'ils hébergent ;

Tout utilisateur non-permanent (vacataire, stagiaire, étudiant ou enseignant de passage, intervenant extérieur) doit être recommandé par un enseignant/chercheur permanent ou un responsable administratif d'ESIEE Paris pour pouvoir obtenir l'ouverture d'un compte informatique nominatif.

Les conditions d'accès aux salles informatiques, dans le cadre du libre-service, sont soumises à des règles strictes. En particulier, les clés des locaux ne peuvent être prêtées ou remises à un tiers sans l'accord des personnes en charge de la surveillance du bâtiment ou des responsables des ressources informatiques.

## 4. REGLES D'UTILISATION DES RESSOURCES INFORMATIQUES

L'utilisateur est responsable du poste de travail qu'il utilise. Il doit suivre les consignes de sécurité notamment en matière d'accès et d'anti-virus. L'utilisateur s'engage à ne pas désactiver les logiciels clients installés par le service informatique concernant notamment la mise à jour de l'anti-virus, les mises à jour de sécurité du système d'exploitation, les outils de gestion du parc ou de supervision.

L'utilisateur doit éviter de s'absenter de son bureau de manière prolongée en laissant libre accès à son poste de travail. Il ne doit jamais quitter un poste de travail en libre service sans se déconnecter.

L'utilisateur s'interdit d'apporter volontairement des perturbations au système informatique ou envers un autre utilisateur du système informatique, soit par des manipulations anormales du matériel, soit par des modifications de logiciel, soit par l'introduction de logiciels parasites ou par tout autre moyen. Le service informatique se réserve le droit de désinstaller tout logiciel perturbant le bon fonctionnement du poste de travail.

L'utilisateur s'interdit également de développer des programmes dans le but d'harceler d'autres utilisateurs d'un système informatique, de contourner des mécanismes de sécurité ou de rechercher le mot de passe d'autres utilisateurs. Toute tentative, même à caractère ludique, de récupération de mot de passe et d'usurpation d'identité d'autres utilisateurs est considérée comme un délit.

De même, il s'interdit de développer des programmes de type virus ou ver et de façon plus générale, il s'interdit de se connecter et de lancer des processus sur un ordinateur distant, directement ou via une tierce machine, sans en avoir obtenu une autorisation explicite des collaborateurs concernés au sein de l'établissement.

La connexion au réseau informatique de nouvelles machines (postes de travail, périphériques, imprimantes), le déplacement et/ou la modification de la connexion de machines existantes, l'ajout de commutateurs, de bornes wifi, de modems, … ne pourront être faits que par un représentant du service informatique. Un contrôle est opéré par le service informatique sur la connexion de nouveaux équipements.

De même, l'installation de nouveaux logiciels ou la modification de logiciels existants, ayant un impact sur des programmes ou des bibliothèques utilisés par la communauté des utilisateurs, ne pourra être faite que sous la responsabilité d'un représentant du service informatique.

Les fichiers présents sur un compte utilisateur sont considérés comme une production personnelle, qu'ils soient ou non accessibles par les autres usagers du réseau. En conséquence, l'utilisateur s'engage à ne pas lire, modifier ou détruire d'autres fichiers ou flots d'information que ceux qui lui appartiennent en propre, sans l'accord explicite de son propriétaire.

## 5. RESPECT MUTUEL ET BONNE ENTENTE

L'utilisateur travaille au sein d'une communauté. **Il s'interdit toute utilisation abusive d'une ressource commune** (imprimante, réseau, espace disque, accès Internet, licences flottantes, etc…). Les activités risquant d'accaparer fortement les ressources informatiques (impression de gros documents, calculs importants, utilisation intensive du réseau, etc.) devront être effectuées sur les équipements dédiés à ces activités et/ou à des moments qui pénalisent le moins la communauté :

A cette fin, on veillera à respecter les règles suivantes :

- n'occuper que la quantité d'espace disque strictement nécessaire en supprimant les fichiers devenus inutiles et en utilisant efficacement les moyens de compression et d'archivage,
- n'imprimer les longs documents (rapports de thèse ou de stage, soutenance, …) en dehors des heures d'affluence ou via le service de reprographie de l'établissement,
- ne pas bloquer l'accès à un poste de travail pendant son absence et durant les heures d'affluence.

Les ressources informatiques ne doivent pas être utilisées pour des activités commerciales, de conseil ou de consulting sans l'accord préalable de la Direction d'ESIEE Paris (voir notamment à ce sujet le §11 ANNEXE 2 - MSDNAA - CONTRAT D'UTILISATION ETUDIANT)

La consommation de boissons ou de nourriture est interdite dans les locaux informatiques.

De plus, chacun doit s'attacher à ne pas introduire de nuisances préjudiciables au travail d'autrui :

- se munir d'un casque audio ou d'écouteurs pour l'utilisation des périphériques sonores
- respecter le calme des locaux et le matériel qui s'y trouve
- ne pas s'introduire dans une salle dans laquelle se déroule une activité pédagogique programmée sans avoir obtenu l'accord de l'intervenant

Les jeux informatiques sont strictement interdits durant la journée (8h – 19h). En dehors de cette plage horaire, ils ne sont tolérés qu'à titre exceptionnel et sous conditions :

- priorité absolue aux utilisateurs désirant travailler,
- les activités ludiques ne doivent troubler en aucune manière le travail d'autrui, aussi bien en termes de disponibilité des ressources qu'au niveau des nuisances sonores ou visuelles.

Toute personne ne respectant pas ces règles élémentaires se verra immédiatement exclue de la salle de travail et privée de ses droits d'accès au réseau. Tout abus entraînera l'interdiction totale des jeux informatiques.

Clubs et associations d'élèves : Seuls les clubs ou associations répertoriés et reconnus par le Bureau Des Elèves peuvent obtenir un ou plusieurs comptes informatiques spécifiques. Leur président en exercice endosse la responsabilité de ces comptes qui sont réservés à l'activité du club ou de l'association et ne doivent pas héberger de travaux personnels. D'autre part leur accès est strictement limité aux personnes en charge de leur gestion et de leur animation. En cas de défaillance du président, c'est le Bureau des Elèves qui en assume, en dernier recours, la responsabilité.

En tout état de cause, ESIEE Paris se réserve le droit de bloquer l'accès à des sites ou à des services n'ayant aucun rapport avec l'exercice professionnel ou perturbant le bon fonctionnement du système.

## 6. REMONTEE ET TRAITEMENT DES ANOMALIES

**En cas d'anomalie pouvant mettre en cause la sécurité du poste, des données ou du système informatique ou de compromission ou de risque de compromission de son compte informatique, l'utilisateur préviendra immédiatement le SMIG**, afin que celui-ci prenne les mesures de protection nécessaires.

Lorsque des anomalies mettant en cause le bon fonctionnement ou la sécurité du système informatique sont relevées, ou lorsqu'elles révèlent une méconnaissance des droits de la propriété intellectuelle, le représentant du service informatique signale ces anomalies à l'utilisateur et les élimine avec son accord. En cas d'urgence, le service informatique peut se passer d'un accord préalable.

## 7. ENREGISTREMENT DES TRACES

L'utilisateur est informé que différents dispositifs du système informatique, liés à la gestion de la sécurité et de la qualité de service et à la recherche des pannes et incidents, enregistrent des évènements le concernant. Ces enregistrements, qui n'ont pas par nature vocation à être des outils de surveillance individuelle, peuvent donner lieu à des analyses systématiques de volumétrie ou de détection de comportements anormaux. Ils peuvent à l'occasion être utilisés pour identifier des utilisations manifestement abusives au sens des différentes clauses de cette charte.

L'utilisateur est informé que l'ensemble des traces de connexion à l'internet via la messagerie ou via le web est conservé pendant un an.

## 8. RAPPEL DE LA LEGISLATION EN VIGUEUR

Dans l'exercice de son droit d'accès au système informatique, **l'utilisateur doit s'imposer le respect des lois** et notamment celles relatives aux publications à caractère injurieux, diffamatoire, raciste, négationniste ou celles relatives au harcèlement sexuel ou moral et à la protection des mineurs. L'accès aux sites Internet pénalement répréhensibles est non seulement interdit mais engage la responsabilité pénale de l'utilisateur concerné.

**Loi informatique et Libertés :**
Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers entrant dans le champ d'application de la loi Informatique et Libertés, il devra auparavant en avoir fait la demande à la CNIL, par l'intermédiaire de l'établissement, et en avoir reçu l'autorisation.

> *En application de la loi du 6 janvier 1978 relative à l'encadrement des traitements automatisés de données à caractère personnel.*

**Législation concernant les logiciels :**
Il est strictement interdit à l'utilisateur d'employer des logiciels pour lesquels il ne dispose pas de droit de licence. Il est strictement interdit à l'utilisateur d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit. Seules les copies, notamment de sauvegarde, autorisées par la loi ou par la licence peuvent être faites.

> *En application de la loi du 5 janvier 1985 sur la protection des logiciels*

**Propriété intellectuelle et artistique :**
Il est strictement interdit à l'utilisateur d'utiliser, de reproduire et plus généralement d'exploiter des œuvres protégées par le droit d'auteur sans l'autorisation de l'auteur ou du titulaire des droits, et notamment des documents textes, des images, de la musique, de la vidéo.

*En application de la loi du 11 mars 1957, complétée par la loi 85-660 du 3 juillet 1985 et par la circulaire du 17 octobre 1990, relative aux droits d'auteurs et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes, et des entreprises de communication audiovisuelle qui s'applique de plein droit aux domaines des logiciels informatiques et des oeuvres multimédias.*

**Fraude informatique :**

*En application de la loi du 5 janvier 1988 dite loi Godfrain, ``l'accès ou le maintien frauduleux dans un système informatique (...) la falsification, la modification, la suppression et l'introduction d'information avec l'intention de nuire (...) la modification, la suppression ou l'introduction de traitements dans un système dans le but d'en fausser le comportement (...), sont considérés comme des délits. La tentative de ces délits relève des mêmes peines (...)'' ( voir annexe)*

**Autres Textes de référence en matière informatique**

- La charte Renater ;
- Le code de la propriété intellectuelle ;
- La convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales : notamment l'article 8 sur la protection des données à caractère personnel ;

## 9. RESPECT DE LA CHARTE

**En cas de non respect des présentes règles par l'utilisateur, et indépendamment des éventuelles conséquences civiles et pénales de ses actes, ESIEE Paris se réserve le droit de restreindre ou de suspendre sans préavis son accès au système informatique et de prendre toute autre mesure qu'il jugera nécessaire.**

## 10. ANNEXE 1 : LOI NUMERO 88-19 DU 5 JANVIER 1988 RELATIVE A LA FRAUDE INFORMATIQUE OU LOI GODFRAIN

*La loi du 5 janvier 1988 ou loi GODFRAIN est constituée des articles suivants :*

*Art 462-2 alinéa 1er : délit d'intrusion dans le système d'autrui*
*Art 462-2 alinéa 2 : délit d'intrusion ayant entraîne des dégradations involontaires*
*Art 462-3 : délit d'entrave au système*
*Art 462-4 : délit d'atteinte aux données*
*Art 462-5 : faux informatique*
*Art 462-6 : usage de documents informatises falsifies*
*Art 462-7 : tentatives des délits*
*Art 462-8 : participation à une association délictueuse*
*Art 462-9 : confiscation des matériels*

*Art 462-2 alinéa 1er : délit d'intrusion dans le système d'autrui :*

*Art 462-2 alinéa 1$^{er}$ : "Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de 2 mois à un an et d'une amende de 2 000 F à 50 000 F ou de l'une de ces 2 peines seulement."*

*Art 462-2 alinéa 2 : délit d'intrusion ayant entraîne des dégradations involontaires*

*Art 462-2 alinéa 2 du code pénal : "Lorsque il sera résulté (de l'intrusion ou du maintien non autorisé dans le système) soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de 2 mois à 2 ans et l'amende de 10 000 F à 100 000 F."*

*Art 462-3 : délit d'entrave au système*

*Art 462-3 : "Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de 3 mois à 3 ans et d'une amende de 10 000 F à 100 000 F ou de l'une de ces 2 peines."*

*Art 462-4 : délit d'atteinte aux données*

*Art 462-4 : "Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement introduit des données dans un système de traitement automatisé ou supprimé ou modifié les données qu'il contient, ou leur mode de traitement ou de transmission, sera puni d'un emprisonnement de 3 mois à 3 ans et d'une amende de 2000 F à 500 000 F ou de l'une de ces 2 peines."*

*Art 462-5 : faux informatique*

*Art 462-5 : "Quiconque aura procédé à la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui, sera puni d'un emprisonnement d'un an à 5 ans et d'une amende de 20 000 F à 2 000 000 F."*

*Art 462-6 : usage de documents informatisés falsifies*

*Art 462-6 : "Quiconque aura sciemment fait usage des documents informatisés visés à l'article 462-5 sera puni d'un emprisonnement d'un an à 5 ans et d'une amende de 20 000 F à 2 000 000 F ou de l'une de ces 2 peines seulement."*

*Art 462-7 : tentatives des délits*

*Art 462-7 : "La tentative des délits prévus par les articles 462-2 à 462-6 est puni des mêmes peines que le délit lui même."*

*Art 462-8 : participation à une association délictueuse*

*Art 462-8 : "Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou plusieurs infractions prévues par les articles 462-2 à 462-6 du code pénal sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée"*

*Art 462-9 : confiscation des matériels*

*Art 462-9 : "Le tribunal pourra prononcer la confiscation des matériels appartenant au condamné et ayant servi à commettre les infractions prévues au présent chapitre."*

## 11. ANNEXE 2 - MSDNAA - CONTRAT D'UTILISATION ETUDIANT

En sa qualité de membre de MSDN® Academic Alliance, le département auquel vous êtes inscrit est autorisé à vous fournir des logiciels à utiliser sur votre ordinateur personnel. Vous devez respecter les instructions d'utilisation générales de MSDN Academic Alliance citées précédemment, ainsi que les termes et conditions du Contrat de Licence Utilisateur final (CLUF) MSDN, l'Amendement du Contrat de Licence MSDN Academic Alliance et les conditions imposées par votre département.

L'administrateur du programme MSDNAA de votre département devra consigner toutes les données relatives à l'utilisation des étudiants, fournir des données consolidées à Microsoft® sur demande et s'assurer que tous les utilisateurs au sein du département, notamment les étudiants, les membres du département et le personnel technique, respectent strictement toutes les conditions du programme.

*Par l'installation, la copie ou toute autre utilisation des logiciels, vous acceptez de vous conformer aux modalités du programme stipulées dans le CLUF et l'Amendement du Contrat de Licence. Si vous refusez de vous y conformer ,il vous est interdit d'installer, copier ou utiliser les logiciels.*

Instructions relatives à l'installation

- Pour pouvoir installer des logiciels sur votre ordinateur personnel, vous devez êtes inscrit à au moins un cours dispensé par le département abonné.
- Votre département peut soit vous donner accès à un serveur de téléchargement, soit vous prêter une copie des logiciels de façon temporaire afin que vous l'installiez sur votre ordinateur personnel.
- Dans le cas de certains produits, une clé de produit vous sera remise pour installer les logiciels. Il est interdit de divulguer cette clé à un tiers.

Instructions relatives à l'utilisation

- Vous n'avez pas le droit de donner à un tiers des copies des logiciels empruntés ou téléchargés. Les autres étudiants autorisés doivent se procurer les logiciels conformément aux procédures définies par l'administrateur du programme MSDN Academic Alliance.
- Vous pouvez utiliser les logiciels à des fins non lucratives, notamment à des fins d'enseignement, de recherche et/ou de conception, de développement et de test dans le cadre de projets associés à un cours ou personnels.

Il est interdit d'utiliser les logiciels MSDN Academic Alliance pour le développement de logiciels à but lucratif.

- Lorsque vous n'êtes plus inscrit à aucun cours dispensé par le département abonné, vous ne pouvez plus vous procurer des logiciels MSDN Academic Alliance. Toutefois, vous pouvez continuer à utiliser les produits précédemment installés sur votre ordinateur, à condition de vous conformer toujours aux instructions du programme MSDN Academic Alliance.
- Si vous contrevenez aux termes et conditions stipulés dans le CLUF et l'Amendement du Contrat de Licence, l'administrateur du programme MSDN Academic Alliance exigera la confirmation de la désinstallation des logiciels de votre ordinateur personnel.