Nom du signataire de cette charte : .....
.....
Date d'entrée à l'Institut d'Optique : .....
Durée du séjour à l'Institut d'optique : .....

Charte d'utilisation des moyens informatiques au sein de L'Institut d'Optique Graduate School

Cette charte s'applique à l'ensemble des composantes de l'Institut d'Optique ainsi qu'aux entités hébergées dans le bâtiment 503 Orsay et sur le site de Palaiseau.

Institut d'Optique	**MASTER**
Laboratoire Charles Fabry	**SFO**
IOTech	**Associations…**
	Jeunes pousses……

1 Domaines d'application :

Le but de cette charte est d'établir des règles pour une bonne utilisation des moyens informatiques de l'Institut d'Optique et des composantes qu'il abrite. Ces règles complètent et explicitent celles énoncées dans le Code Pénal Français (loi 88-19 du 5 janvier 1988 relative à la fraude informatique, notamment). En particulier, certains des actes décrits ci-après sont répréhensibles au sens de la Loi Française et peuvent donner lieu à des poursuites devant les tribunaux.

Ces règles s'appliquent à toute personne utilisant les systèmes informatiques de l'Institut d'Optique, de quelque nature qu'ils soient (micro ordinateur, station de travail serveurs ou autre), les systèmes informatiques auxquels il est possible d'accéder à partir de l'Université Paris Sud ainsi que les systèmes informatiques d'organismes extérieurs à l'Université Paris Sud et accessibles par réseau depuis l'Université Paris Sud.

2 Conditions d'accès aux systèmes informatiques :

Le droit d'accès à un système informatique est *personnel* et *incessible*. Il ne doit être communiqué à personne que ce soit explicitement en donnant votre mot de passe ou implicitement en donnant un droit d'accès à votre compte.

L'utilisation des moyens informatiques de l'Institut d'Optique doit être limitée à des activités de recherche et d'enseignement. Sauf autorisation préalable, ils ne peuvent être utilisés pour des projets faisant l'objet d'un financement extérieur.

3 Respect du caractère confidentiel des informations :

Les fichiers possédés par les utilisateurs doivent être considérés comme propriété privée. Les utilisateurs ne doivent pas tenter de lire, de copier ou de modifier les fichiers d'un autre utilisateur sans son autorisation (verbale ou écrite). Le fait d'avoir la possibilité de lire ou de modifier ne signifie pas que l'on a le droit de le faire.

Les utilisateurs doivent également s'abstenir de toute tentative d'intercepter les communications privées entre utilisateurs, qu'elles se composent de courrier électronique ou de dialogue direct.

4 Respect des droits de propriété :

Les utilisateurs doivent s'abstenir de faire des copies de tout logiciel autres que ceux du domaine public. Les utilisateurs ne doivent pas tenter de contourner les protections des logiciels.

Les licences de certains logiciels comprennent des contraintes restreignant leur utilisation à certaines tâches. Les utilisateurs doivent respecter ces contraintes. Le non respect de ces règles est un vol.

…/…

…/…

5 Respect des principes de fonctionnement des systèmes informatiques :

Les utilisateurs ne doivent pas utiliser de comptes autres que ceux auxquels ils ont légitimement accès. Ils ne doivent pas non plus effectuer de manœuvre qui aurait pour but de méprendre les autres utilisateurs sur leur identité.

Ils doivent s'abstenir de toute tentative de s'approprier ou de déchiffrer le mot de passe d'un autre utilisateur, de modifier ou de détruire des fichiers d'un autre utilisateur et de limiter ou d'interdire l'accès aux systèmes informatiques d'un utilisateur autorisé. La conception d'un programme ayant de telles propriétés est également interdite sans autorisation préalable.

La modification délibérée de fichiers système est considérée comme un acte de vandalisme.

6 Utilisation des réseaux informatiques :

Tout utilisateur d'un réseau informatique s'engage à ne pas effectuer d'opérations qui pourraient avoir pour conséquence :

- D'interrompre le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau
- D'accéder à des informations privées d'autres utilisateurs sur le réseau
- De modifier ou de détruire des informations sur un des systèmes connectés au réseau
- De nécessiter la mise en place de moyens humains ou techniques supplémentaires pour son contrôle et sa destruction.

La conception d'un programme ayant de telles propriétés est également interdite sauf autorisation préalable.

Les utilisateurs ne doivent pas se connecter sans autorisation sur des systèmes distants. La possibilité de se connecter sur un ordinateur ne signifie pas que l'on en ait le droit.

7 Accès aux salles contenant le matériel informatique :

Les utilisateurs s'engagent à respecter les règles d'accès aux salles contenant le matériel informatique.

8 Respect mutuel des individus entre eux :

Les utilisateurs ne doivent pas persécuter un individu à l'aide d'outils électroniques.

Tout utilisateur n'ayant pas respecté les "règles de bonne conduite" énoncées ci-dessus est passible de poursuites, internes à l'Institut d'Optique ou pénales (articles 462-2 à 462-9 du code pénal - en annexe -) suivant le cas.

Je soussigné(e) ……certifie avoir pris connaissance des règles de bonne conduite énoncées ci-dessus et m'engage à m'y conformer,

A Palaiseau, le

…/…

…/…

ANNEXE

Code Pénal

(Partie Législative)

Chapitre III : Des atteintes aux systèmes de traitement automatisé de données

Article 323-1

(Ordonnance n°2000-916 du 19 septembre 2000 art.3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

(Loi n° 2004-575 du 21 juin 2004 art. 45 I Journal Officiel du 22 juin 2004)

Le fait d'accéder ou de soutenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 Euros d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine de trois ans d'emprisonnement et de 45000 Euros d'amende.

Article 323-2

(Ordonnance n°2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

(Loi n° 2004-575 du 21 juin 2004 art. 45 II Journal Officiel du 22 Juin 2004)

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 Euros d'amende.

Article 323-3

(Ordonnance n°2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

(Loi n° 2004-575 du 21 juin 2004 art. 45 II Journal Officiel du 22 Juin 2004)

Le fait d'introduire Frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 Euros d'amende.

(Inséré par la Loi n° 2004-575 du 21 juin 2004 art. 46 I Journal Officiel du 22 Juin 2004)

Le fait, sans motif légitime, d'emporter, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-4

(Loi n° 2004-575 du 21 juin 2004 art. 46 II Journal Officiel du 22 Juin 2004)

La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou par l'infraction la plus sévèrement réprimée. …/…

…/…

Article 323-5

Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1° L'interdiction, pour une durée de cinq ans au plus, des droits civique et de famille, suivant les modalités de l'article 131-6 ;

2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle l'infraction a été commise ;

3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;

4°La fermeture pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissement de l'entreprise ayant servi à commettre les incriminés ;

5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;

6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131 - 35.

Article 323-6

Les personnes morales peuvent êtres déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.

Les peines encourues par les personnes morales sont :

1° L'amende, suivant les modalités prévues par l'article 131-38 ;

2° Les peines mentionnées à l'article 131-39.

L'interdiction mentionnée au2°de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Article 323-7

(Loi n° 2004-575 du 21 juin 2004 art. 46 II Journal Officiel du 22 Juin 2004)

La tentative des délits prévus par les articles 323-& à 323-3-1 est punie des mêmes peines.