ADIGIP

Association **D**es **I**nvestisseurs en **G**irardin **I**ndustriel **P**hotovoltaïque
37 rue des Mathurins 75008 Paris

Charte d'utilisation des ressources informatiques et réseau de l' ADIGIP

Préambule : le cadre juridique

Toute organisation doit vérifier que ses membres respecte son règlement et tout acte illégal effectué par un de ses membre entraîne la responsabilité pénale de celui-ci. Concernant la sécurité informatique, plusieurs types de risques peuvent être retenus :

- Les risques touchant à la sécurité du réseau et des applications
- Les risques d'atteinte à la propriété intellectuelle
- Les risques relatifs à la pornographie, la pédophilie, la diffamation et les injures raciales
- Le blanchiment d'argent et le financement du terrorisme

L' ADIGIP n'échappe pas aux risques potentiels et se doit de faire respecter la réglementation en ce domaine, notamment au vu des données fiscales échangées et particulièrement confidentielles.

La présente charte a pour objet de préciser aux adhérents de l' ADIGIP, leur responsabilité en tant qu'utilisateur des applications informatiques de l' ADIGIP afin d'assurer un usage correct des ressources informatiques et des services réseau avec des règles minimales. Elle fait également connaître aux utilisateurs les mesures de sécurité adoptées.

Article 1er - Définitions

Le terme *ressources informatique* désigne les moyens de traitement de l'information disponibles à l'ADIGIP, en incluant ceux qui offrent une possibilité de connexion à distance.

Le terme *ressource réseau* désigne tous les moyens de communication informatique offerts par l'ADIGIP, incluant notamment tous les services réseaux et Internet (par exemple, Messagerie, serveur de fichier FTP, forums), ainsi que tout équipement de transmission de données.

Le terme *utilisateur* désigne toute personne ayant accès ou utilisant les ressources informatiques ou réseau de l'ADIGIP.

Le terme *services Internet* désigne tout service réseau offert par l'infrastructure de l'ADIGIP, et en particulier, la messagerie électronique, les services d'hébergement de pages Web et l'accès distant.

Article 2 - Règles d'accès aux ressources

Les ressources de l'ADIGIP sont exclusivement réservées à une utilisation dans le cadre :

- De l'activité associative de l' ADIGIP
- De l'activité professionnelle du personnel de FIDAL, tout en restant exclusivement liée à la mission de FIDAL envers les adhérents ADIGIP

Les ressources de l'ADIGIP sont interdites à toutes autres personnes sauf accord écrit de l' ADIGIP.
Les utilisateurs doivent être membres de l' ADIGIP ou FIDAL. Un utilisateur perd son habilitation à utiliser les ressources de l'ADIGIP dès lors qu'il perd son statut d'adhérent ADIGIP ou d'employé FIDAL.

Article 3 - Règles de sécurité

La sécurité des infrastructures informatiques et Internet, nonobstant les dispositifs techniques que l'ADIGIP installe, est l'affaire de tous les utilisateurs. Ceux-ci doivent donc respecter un certain nombre de règles de base destinées à garantir la sécurité de tous et l'intégrité des infrastructures :

- Les comptes ouverts aux utilisateurs sont rigoureusement personnels
- Ceux-ci doivent être protégés par un mot de passe qui respecte les règles de mise en place des mots de passe (voir annexe A)
- Les utilisateurs ne doivent communiquer leurs mots de passe sous aucun prétexte
- **Toute tentative d'intrusion, attaque/piratage informatique, accès illégal dans le Système d'Information de l'ADIGIP constatée par un utilisateur doit être signalée dans les plus brefs délais aux responsables du bureau de l'ADIGIP**
- **Conformément à l'article 2, les autorisations d'accès aux ressources de l'ADIGIP seront retirées à toute personne perdant son statut d'adhérent.**
- **Tout événement ou incident ou dommage qui pourrait compromettre la confidentialité ou la sécurité des données de l' ADIGIP ou nuire à son image doit être signalée dans les plus brefs délais aux responsables du bureau de l'ADIGIP**
- Toute recommandation du bureau ou support ADIGIP, concernant notamment la mise à jour de logiciels pouvant présenter des failles de sécurité, doit être suivie dans les plus brefs délais
- **Les utilisateurs ne doivent jamais quitter un poste de travail sans se déconnecter de l'application et du réseau**
- Les utilisateurs s'engagent à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes, au réseau ou à des données à travers des matériels dont ils ont l'usage.
- Tout matériel informatique ne peut être relié au réseau ADIGIP que par un personnel habilité
- Il est interdit de mettre en place des programmes destinés à contourner les mesures de sécurité
- Des fichiers ne peuvent être déposés sur un serveur ADIGIP que dans des conditions prévues par le responsable ADIGIP du serveur.
- L'ouverture des fichiers joints aux emails doit être particulièrement surveillée

Article 4 - Règles de déontologie

L'utilisateur s'engage à ne pas effectuer d'opération qui pourraient conduire à :

- Masquer son identité
- Usurper l'identité d'autrui
- S'approprier le mot de passe d'un autre utilisateur
- Perturber le fonctionnement normal du réseau
- Utiliser les ressources informatiques et en particulier le réseau de façon irrationnelle et déloyale dans le but de les saturer ou de les détourner à des fins personnelles
- Modifier ou détruire des informations présentes sur un système
- Se connecter sur un site ou une machine sans y être autorisé.
- Réduire l'espace de stockage des données ADIGIP sauf nécessité absolue dans le cadre de l'activité associative de l' ADIGIP ou de l'activité professionnelle du personnel de FIDAL

L'adhérent ADIGIP s'engage à ne pas utiliser l'espace de stockage ADIGIP pour y déposer des données qui seraient pas directement liés à la défense de son dossier par FIDAL.

Article 5 - Utilisation des logiciels

L'installation de logiciels sur le poste de travail d'un adhérent est sous la responsabilité de chaque adhérent.
L' ADIGIP décline donc toute responsabilité en cas de non respect des brevets, marques, licences logicielles sur les sur les postes de travail des adhérents ou tout dommage direct ou indirect liée à l'installation, la configuration ou l'utilisation de logiciels pour accéder aux ressources informatiques ADIGIP distantes.

L' ADIGIP décline toute responsabilité en cas de dysfonctionnement ou interruption de services réseaux, d'accès à internet, ou de tous autres services utilitaires, notamment de type hébergement dès lors qu'ils n'ont pas été confiés à l' ADIGIP et que les dysfonctionnements ou interruptions de services ne relèvent en aucune manière de la responsabilité de l'ADIGIP.

Article 6 - Rappel des lois spécifiques au Droit de l'Informatique et des dispositions du code pénal concernant les infractions en matière informatique

Loi 78-17 du 6 janvier 1978 sur l'Informatique, les fichiers, les libertés
Elle crée la Commission Nationale Informatique et Libertés et met en place des procédures de contrôle des traitements informatisés des données nominatives.

Loi du 3/07/85 sur la protection des logiciels – Elle interdit à l'utilisateur d'un logiciel toute reproduction autre que l'établissement d'une copie de sauvegarde.

Loi du 5/01/88 (loi GODFRAIN) relative à la fraude informatique
Elle vise à lutter contre la fraude informatique en réprimant :

- les accès ou le maintien frauduleux dans un système informatique
- les atteintes accidentelles ou volontaires au fonctionnement
- la falsification de documents informatisés et leur usage
- la tentative de ces délits
- l'association ou l'entente en vue de les commettre

Les dispositions du code pénal :

Article 323-1 (Ordonnance no 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)
Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15000 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 est de deux ans d'emprisonnement et de 30000 euros d'amende.

Article 323-2 - (Ordonnance no 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)
Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45000 euros d'amende.

Article 323-3 - (Ordonnance no 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002) 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 trois ans d'emprisonnement et de 45000 euros d'amende.

Article 323-4 - 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 des infractions prévues par les articles 323-1 à 323-3 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-7 - La tentative des délits prévus par les articles 323-1 à 323-3 est punie des mêmes peines.

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 civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
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 ou à l'occasion 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 établissements de l'entreprise ayant servi à commettre les faits 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 7 Sanctions encourues

L'utilisateur qui enfreint une des règles de la présente charte encourt d'éventuelles sanctions disciplinaires et pénales et/ou la suppression de son accès aux ressources informatiques et réseau de l'ADIGIP.

ENGAGEMENT PERSONNEL DE L'UTILISATEUR :

Nom :
Prénom :
Téléphone :
Email :

Je soussigné (e) …..... déclare avoir pris connaissance des dispositions de la présente charte ainsi que de la note d'information CNIL ci-dessous, et m'engage à les respecter.

Fait à …..... le …../...../....

Signature

ENGAGEMENT DU PRESIDENT D'ASSOCIATION

Je soussigné Wai-Hong Tchen, Président de l'association ADIGIP reconnaît avoir pris connaissance des dispositions de la présente charte, et m'engage à les respecter et à les faire respecter par les membres de l'association.

Fait à Paris le 15/05/2012

Le président de l'association

En conformité avec les dispositions de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et à la Directive Européenne 95/46/CE du 24 Octobre 1995 et 2009/136/EC du 25 Novembre 2009, le traitement automatisé des données nominatives réalisé à partir des sites web "www.adigip.info" "www.adigip.com" et "www.adigip.fr" ont fait l'objet d'une déclaration auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL) enregistrée sous le n° 1544700.

L'utilisateur dispose d'un droit d'accès, de modification, de rectification et de suppression des données qui le concernent (article 34 de la loi "Informatique et Libertés") en adressant un email à donnees-personnelles@adigip.com ou en s'adressant au secrétariat de l'association.

Les informations enregistrées sont destinées à l'association "ADIGIP" pour faciliter le traitement du dossier de chacun de ses adhérents et au personnel FIDAL afin de traiter le dossier de chacun de ses clients-adhérents à l' ADIGIP ; sans que cela vous décharge des transmissions de documents que vous devrez assurer auprès du cabinet d'avocats que vous aurez choisi pour votre défense, l'association déclinant toute responsabilité dans le cas ou un ou plusieurs documents transmis seraient illisibles ou non transmis aux avocats.

"ADIGIP" ne vend pas et ne loue pas les adresses de messagerie et les informations personnelles de ses membres.

Annexe A. Règles de création de mots de passe

Les mots de passe doivent êtres robustes :

- Comporter au moins 9 caractères
- Dont au moins 3 lettres majuscules et 3 lettres minuscules
- Ne pas être un mot présent dans un dictionnaire (quelle que soit la langue)
- Ne pas être une permutation d'un mot présent dans un dictionnaire (quelle que soit la langue)
- Ne pas être une information se rapportant directement au titulaire du compte (date de naissance, etc ...)
- Comporter au moins 2 chiffres
- Comporter au moins 1 caractère spécial (?, ;. :!)