

# Conditions d'Utilisation et de Sécurité

## 1. Définitions

"Utilisateur" : Toute personne autorisée par le Client à utiliser un Equipement Terminal.

"Conditions d'Utilisation et de Sécurité" : le présent document.

Les autres termes en majuscules ont la signification qui leur est donnée dans les Conditions Générales, sauf si le contexte d'une disposition démontre incontestablement qu'une autre signification doit leur être donnée.

## 2. Abréviations

La liste ci-dessous reprend les abréviations les plus fréquemment utilisées dans le présent document :

**COO**: Chief Operations Officer – Responsable Opérations.

**CSO**: Chief Security Officer – Responsable Sécurité.

**ACT**: Air Connected Terminal.

**LCT**: Line Connected Terminal.

## 3. Objectifs

Les présentes Conditions d'Utilisation et de Sécurité à l'intention de l'Utilisateur visent les objectifs suivants:

- 3.1 Garantir à la fois la sécurité et la fiabilité des Systèmes Astrid et des Equipements Terminaux utilisés par le Client.
- 3.2 Assurer la protection et la confidentialité des données demandées, traitées ou stockées par le Client lors de l'utilisation des équipements terminaux et/ou des Systèmes Astrid.
- 3.3 Fournir une description explicite des consignes de sécurité en vigueur ainsi que des droits et obligations de chaque Utilisateur d'Equipements Terminaux fournis par Astrid ou d'autres Equipements Terminaux connectés aux Systèmes Astrid.
- 3.4 Décourager les pratiques réduisant l'efficacité des LCT ou ACT ou susceptibles de compromettre le bon fonctionnement des Systèmes Astrid.
- 3.5 Eviter une utilisation illégitime et un accès illégal de données à caractère personnel.
- 3.6 Les Conditions d'Utilisation et de Sécurité définissent notamment les actions considérées comme abusives par Astrid et qui sont, par conséquent, interdites. Les exemples cités ne sont pas exhaustifs, ils sont cités à titre informatif.

#### **4. Champ d'application**

- 4.1 Ces directives s'inscrivent dans la stratégie de sécurité globale d'Astrid et sont applicables à chaque Utilisateur. En fonction du fait que les Equipements Terminaux aient été fournis par Astrid ou non, différentes mesures peuvent être applicables. Il en sera fait mention le cas échéant.
- 4.2 Chaque utilisateur est tenu de respecter scrupuleusement les Conditions d'Utilisation et de Sécurité.
- 4.3 Les Conditions d'Utilisation et de Sécurité s'appliquent à toute utilisation des Equipements Terminaux, à l'exception des stations de travail des dispatching (100 et 101).
- 4.4 Les LCT sont exclusivement disponibles auprès d'Astrid. Ils sont uniquement mis à la disposition du Client pour une durée déterminée (en fonction du délai défini par la Convention).

#### **5. Généralités**

- 5.1 Les Conditions d'Utilisation et de Sécurité font intégralement partie de la Convention. Le Client est tenu de le respecter scrupuleusement et d'aviser immédiatement Astrid de toute irrégularité dans son application.
- 5.2 Toute utilisation ou modification de configuration des Equipements Terminaux connectés aux Systèmes Astrid susceptible de causer des dommages ou des nuisances, de quelque nature qu'ils soient, à d'autres utilisateurs ou tiers est interdite, ainsi que toute utilisation contraire aux instructions dans les présentes Conditions d'Utilisation et de Sécurité.
- 5.3 Toute tentative de contourner l'identification de l'Utilisateur ou la sécurisation d'un hôte, réseau ou compte est interdite aux Utilisateurs. Cela inclut, mais ne se limite pas, à consulter des données qui ne sont pas destinées à l'Utilisateur, à faire un login sur un serveur ou un compte alors que l'Utilisateur n'y est pas autorisé ou à tester une sécurisation sans autorisation expresse d'Astrid.
- 5.4 Il est interdit à l'Utilisateur d'entreprendre toute tentative visant à perturber tout service, hôte ou réseau quel qu'il soit.
- 5.5 Il est interdit à l'Utilisateur d'entreprendre délibérément des tentatives visant à compromettre l'utilisation ou la capacité d'autres Utilisateurs, en produisant un flux de trafic important injustifié, ou en surchargeant les serveurs au moyen de scripts ou de programmes qui échangent automatiquement des quantités importantes d'informations.
- 5.6 Il est interdit à l'utilisateur de quitter pour une période prolongée un LCT sans faire un logoff des Systèmes Astrid et/ou des applications. Les LCT doivent être déconnectés en tout temps dès la fin des activités (le système et l'écran y relatif).

#### **6. Maintenance et gestion**

- 6.1 Les travaux de maintenance (hardware et software) aux équipements terminaux LCT ne peuvent être exécutés que par les membres du personnel d'Astrid ou ses préposés. Il est interdit à d'autres personnes d'apporter des modifications au système ou sa configuration.

- 6.2 La liste du personnel d'Astrid ou de ses préposés habilités à exécuter des travaux de maintenance sur des équipements terminaux LCT est à la disposition de tout Client et ce, sur simple demande.
- 6.3 L'Utilisateur est tenu de vérifier si le nom de la personne qui se présente pour la réalisation de travaux de maintenance sur un LCT figure dans la liste en question.
- 6.4 L'utilisateur est tenu de gérer le matériel mis à sa disposition en « bon père de famille »
- 6.5 Quelques exemples de modifications (liste non exhaustive) au système que l'Utilisateur ne peut pas réaliser lui-même sur les LCT:
  - 6.5.1 Recourir à un media de démarrage pour faire démarrer un système d'exploitation similaire ou alternatif.
  - 6.5.2 Oter le couvercle de protection d'un ordinateur LCT.
  - 6.5.3 Installer d'autres logiciels que ceux installés par Astrid.
  - 6.5.4 Procéder à la (re)configuration d'utilisateurs, groupes d'utilisateurs, profils, politiques de sécurité, etc. au niveau du système d'exploitation.
- 6.6 Il est interdit à l'Utilisateur d'installer des logiciels supplémentaires sur les LCT. Seuls les membres du personnel d'Astrid ou ses préposés y sont autorisés.

## **7. Mots de passe**

- 7.1 Les Utilisateurs des Equipements Terminaux sont tenus de veiller au secret de leur mot de passe, tant au niveau du système d'exploitation qu'au niveau des applications de l'utilisateur.
- 7.2 L'usage des mots de passe est soumis aux directives suivantes:
  - 7.2.1 Les mots de passe seront composés de minimum 6 caractères alphanumériques.
  - 7.2.2 Les mots de passe ne seront pas des mots normaux ou usuels.
  - 7.2.3 Les mots de passe ne peuvent constituer une variante du nom de l'utilisateur ou de membres de sa famille proche, des utilisateurs ID, du serveur ou de l'organisation du Client.
  - 7.2.4 Les Equipements Terminaux mis à la disposition par Astrid seront pourvus, si possible, d'un économiseur d'écran qui est activé automatiquement après 10 (dix) minutes de non-activité. Une fois l'économiseur d'écran activé, l'utilisateur devra à nouveau procéder à un login (compléter l'ID utilisateurs et le mot de passe) pour pouvoir accéder à nouveau à l'appareil. Dans les cas où l'utilisateur impose la désactivation de cet économiseur, les dégâts potentiels engendrés par cette désactivation ne seront pas pris en charge par le contrat de maintenance.
  - 7.2.5 Les mots de passe resteront impérativement confidentiels. Il est interdit à l'Utilisateur de noter le mot de passe ou de le communiquer à d'autres personnes.

## **8. Confidentialité et logging**

- 8.1 Astrid reste propriétaire des LCT fournis par elle et en assure leur gestion.
- 8.2 Pour des raisons de sécurité générale (protection des systèmes et des données), et de fiabilité et de contrôle de performances des Systèmes Astrid, Astrid se réserve le droit de contrôler et/ou d'enregistrer toutes les activités de réseau.
- 8.3 Le Client peut superviser ce contrôle ou ces enregistrements conformément aux accords conclus à ce sujet avec Astrid.

## **9. Consignes de sécurité applicables aux ACT**

### 9.1 Terminal volé ou perdu

- 9.1.1 Le Client est tenu d'informer immédiatement le ASTRID Service Centre (ASC) en vue de rendre le terminal inutilisable.
- 9.1.2 La fonctionnalité « temporary disabled ITSI » sera utilisée dans un premier temps.
- 9.1.3 En fonction de l'évolution de la situation (terminal retrouvé ou définitivement perdu/volé), l'ASC sera à nouveau informé pour autoriser le terminal sur le réseau (« enable ») ou au contraire sa suppression définitive (permanent disable ITSI/TEI).

### 9.2 Terminal envoyé pour réparation

- 9.2.1 Tout terminal renvoyé au fournisseur/service provider pour réparation sera supprimé temporairement du système c-à-d. que l'association ITSI – K sera rompue (la paire ITSI – REF sera supprimée et la paire K – REF reprise dans le CKS).
- 9.2.2 La fonctionnalité « disable » sera utilisée pour cette opération (temporary disable ITSI). Le Client demandera à Astrid de réaliser cette manipulation.

### 9.3 Terminal se trouvant dans un véhicule envoyé en réparation

- 9.3.1 Le terminal mobile se trouvant dans un véhicule sera démonté avant que ce véhicule ne soit confié à un concessionnaire ou à un carrossier.
- 9.3.2 Si ce qui précède ne peut être réalisé, Astrid sera avertie afin que ce terminal soit temporairement supprimé du système (fonctionnalité disable – voir ci-dessus).

### 9.4 Terminaux mobiles utilisés comme poste fixe

- 9.4.1 De manière à permettre une authentification périodique de ces terminaux, il est recommandé de les éteindre et de les allumer une fois par mois.

### 9.5 Utilisation d'un PIN-Code

- 9.5.1 La mise en œuvre d'un PIN code à l'allumage pour utiliser les terminaux qui disposent de cette fonctionnalité devrait être généralisée.
- 9.5.2 Les PIN codes à sécurité faibles (11111, 123456, ...) sont à proscrire.

## **10. Responsable de la sécurité auprès du Client**

- 10.1 Le Client désignera un responsable de la sécurité en application de l'article 5.3.2 des Conditions Générales.
- 10.2 Le responsable de la sécurité veillera en tout temps à ce que les utilisateurs de son organisation ou service réservent une utilisation correcte aux équipements terminaux.
- 10.3 Le responsable de la sécurité est tenu de signaler chaque incident en matière de sécurité au responsable de la sécurité (CSO) désigné par Astrid de sorte qu'ils puissent, ensemble, prendre des mesures adéquates.

## **11. Utilisation de l'Internet et du modem**

- 11.1 L'utilisateur se voit interdire, en tout temps, d'établir, au moyen d'un équipement terminal activé sur les Systèmes Astrid, une connexion directe ou indirecte à l'Internet, à moins que cette connexion ne soit proposée en tant que service par Astrid-même.
- 11.2 Il est interdit au Client de connecter un modem quel qu'il soit et de l'utiliser sur un équipement terminal activé sur les Systèmes Astrid à moins que ce service complémentaire soit proposé par Astrid-même ou que la connexion soit effectuée à la demande des membres du personnel d'Astrid ou ses employés qui sont explicitement habilités à cet effet.

## **12. Sanctions**

- 12.1 Astrid se réserve le droit d'engager la responsabilité du Client pour les dommages causés par un de ses Utilisateurs suite à la non-application ou à l'application incorrecte des Conditions d'Utilisation et de Sécurité.
- 12.2 Le non-respect des Conditions d'Utilisation et de Sécurité en vigueur peut entraîner une privation temporaire ou permanente de l'accès aux Systèmes Astrid.

## **13. Informations complémentaires – personnes de contact**

Toutes les questions relatives à ces conditions peuvent être adressées par écrit à Astrid.

- 13.1 Soit par courrier à l'attention de Bruno ANTOINE, CSO, 02.500.67.22 ou 0496.595.722.
- 13.2 Soit par courrier électronique à [info@astrid.be](mailto:info@astrid.be).
- 13.3 Sans préjudices des droits et obligations qui découlent des conditions générales, les litiges relatifs aux Conditions d'Utilisation et de Sécurité seront en premier lieu traités entre le responsable de la sécurité désigné par le Client et les CSO et COO d'Astrid.