Gebruiks- en veiligheidsvoorwaarden

1. Definities

"Gebruiker": Elke persoon die door de Klant gerechtigd werd een Eindapparaat te gebruiken.

"Gebruiks- en veiligheidsvoorwaarden": het voorliggende document.

De andere termen met hoofdletter hebben de betekenis die hen wordt gegeven in de Algemene Voorwaarden, behalve wanneer uit de context van een specifieke bepaling ontegensprekelijk blijkt dat er een andere betekenis moet aan worden gegeven.

2. Afkortingen

De onderstaande lijst geeft de afkortingen die het vaakst gebruikt worden in het voorliggende document:

COO: Chief Operations Officer – Operationeel verantwoordelijke.

CSO: Chief Security Officer – Veiligheidsverantwoordelijke.

ACT: Air Connected Terminal.

LCT: Line Connected Terminal.

3. Doelstellingen

De voorliggende Gebruiks- en veiligheidsvoorwaarden zijn bestemd voor de Gebruiker en beogen de volgende doelstellingen:

3.1 Zowel de veiligheid als de betrouwbaarheid waarborgen van de ASTRID-systemen en van de door de Klant gebruikte Eindapparatuur.

3.2 Het afschermen en beveiligen van de gegevens die de Klant opvraagt, bewerkt of opslaat gebruik makend van ASTRID eindapparatuur en/of systemen.

3.3 Een ondubbelzinnige beschrijving geven van de geldende veiligheidsvoorschriften alsook van de rechten en de plichten van iedere Gebruiker die gebruik maakt van door ASTRID geleverde of andere op ASTRID-systemen aangesloten Eindapparatuur.

3.4 Het ontmoedigen van praktijken die de doeltreffendheid van de LCT('s) of ACT('s) verminderen of die de goede werking van de ASTRID-systemen in gevaar zouden kunnen brengen.

3.5 Het voorkomen van onrechtmatig gebruik van en illegale toegang tot persoonsgegevens.

3.6 De Gebruiks- en veiligheidsvoorwaarden definiëren meer bepaald de acties die door ASTRID aanzien worden als misbruik en bijgevolg niet toegelaten zijn. De aangehaalde voorbeelden zijn niet-exhaustief en worden enkel ter informatie vermeld.

4. Toepassingsgebied

4.1 Deze richtlijnen maken deel uit van de totale veiligheidsstrategie van ASTRID en zijn toepasselijk op iedere Gebruiker. Naargelang de Eindapparatuur door ASTRID geleverd werd of niet, kunnen verschillende maatregelen van toepassing zijn. Dit wordt desgevallend vermeld.

4.2 Elke Gebruiker dient de Gebruiks- en veiligheidsvoorwaarden strikt na te leven.

4.3 De Gebruiks- en veiligheidsvoorwaarden zijn van toepassing op elk gebruik van de Eindapparatuur, met uitzondering van de werkstations van de meldkamers (100 en 101).

4.4 De LCT's zijn uitsluitend beschikbaar bij ASTRID. Ze worden slechts voor een bepaalde duur (afhankelijk van de contractueel bepaalde termijn) ter beschikking gesteld van de Klant.

5. Algemeen

5.1 De Gebruiks- en veiligheidsvoorwaarden maken integraal deel uit van de Overeenkomst. De Klant is verplicht deze nauwgezet na te leven en elke onregelmatigheid in de toepassing ervan meteen aan ASTRID te melden.

5.2 Elk gebruik of configuratie-aanpassing van op ASTRID-systemen aangesloten Eindapparatuur dat schade of ongemakken, van welke aard ook, aan andere gebruikers of derden zou veroorzaken is verboden, alsmede elk gebruik dat in strijd is met de instructies in deze Gebruiks- en veiligheidsvoorwaarden.

5.3 Gebruikers mogen niet proberen om de gebruikersidentificatie of beveiliging van een host, netwerk of account te omzeilen. Dit omvat, maar is niet beperkt tot, het opvragen van gegevens die niet bestemd zijn voor de Gebruiker, het inloggen op een server of een account waarvoor de Gebruiker geen toestemming heeft of het testen van een beveiliging zonder de uitdrukkelijke toestemming van ASTRID.

5.4 Een Gebruiker mag geen poging(en) ondernemen om eender welke dienst, host of netwerk te verstoren.

5.5 Een Gebruiker mag geen pogingen ondernemen om het gebruik of de capaciteit van andere Gebruikers opzettelijk in gevaar te brengen door een onverantwoord grote verkeersstroom te veroorzaken, of door de servers te belasten door middel van scripts of programma's die automatisch grote hoeveelheden gegevens uitwisselen.

5.6 Een Gebruiker mag een LCT nooit langdurig verlaten zonder uit te loggen uit de ASTRID-systemen en/of de toepassingen. De LCT('s) moeten steeds worden uitgeschakeld na het beëindigen van de werkzaamheden (systeem en bijbehorend beeldscherm).

6. Onderhoud en beheer

6.1 Onderhoudswerkzaamheden (aan hard- en software) op de LCT eindapparatuur mogen enkel worden uitgevoerd door personeelsleden van ASTRID of haar aangestelden. Andere personen mogen geen wijzigingen aan het systeem of aan de configuratie ervan

aanbrengen.

6.2 De lijst van de personen van ASTRID of haar aangestelden die gemachtigd zijn onderhoudswerkzaamheden uit te voeren op LCT Eindapparatuur kan door elke Klant op aanvraag worden verkregen.

6.3 De Gebruiker moet nagaan of een persoon die zich aanbiedt voor het uitvoeren van onderhoudswerkzaamheden aan een LCT, op deze lijst voorkomt.

6.4 De Gebruiker dient de ter beschikking gestelde apparatuur als een goed huisvader te beheren.

6.5 Enkele voorbeelden van systeemwijzigingen (niet-exhaustieve lijst) die de Gebruiker niet zelf mag uitvoeren op de LCT's:

6.5.1 Een opstartmedium gebruiken om een gelijkaardig of alternatief besturingssysteem te laten opstarten.

6.5.2 De beschermkast (beschermdeksel) van een LCT computer verwijderen.

6.5.3 Andere software installeren dan deze die door ASTRID werd geïnstalleerd.

6.5.4 Gebruikers, gebruikersgroepen, profielen, veiligheidspolicies enz. (her)configureren op het niveau van het besturingssysteem.

6.6 De Gebruiker mag geen extra software installeren op de LCT's. Enkel personeelsleden van ASTRID of haar aangestelden mogen dit doen.

7. Wachtwoorden

7.1 De Gebruikers van de Eindapparatuur moeten er zorg voor dragen dat hun wachtwoord geheim blijft, zowel op het niveau van het besturingssysteem als wat de gebruikerstoepassingen betreft.

7.2 Bij het gebruik van wachtwoorden moeten de volgende richtlijnen worden nageleefd:

7.2.1 Wachtwoorden moeten uit minstens 6 alfanumerieke tekens bestaan.

7.2.2 Wachtwoorden mogen geen normale of gebruikelijke woorden zijn.

7.2.3 Wachtwoorden mogen geen variaties zijn op de naam van de Gebruiker of zijn naaste familieleden, noch van de gebruikers-ID, noch van de servernaam of van de organisatie van de Klant.

7.2.4 De door ASTRID ter beschikking gestelde Eindapparaten zullen wanneer mogelijk voorzien worden van een schermbeveiliger die automatisch na 10 (tien) minuten non-activiteit geactiveerd wordt. Eens de screensaver actief is, zal de gebruiker opnieuw moeten inloggen (invullen van gebruikers ID en wachtwoord) om opnieuw toegang te krijgen tot het toestel. Indien de Gebruiker tot de uitschakeling van deze schermbeveiliger beslist, zal de eventuele schade waartoe deze uitschakeling leidt, niet in aanmerking worden genomen door het onderhoudscontract.

7.2.5 Wachtwoorden moeten geheim blijven. Een Gebruiker mag zijn wachtwoord nergens noteren noch met anderen delen.

8. Privacy en logging

8.1 ASTRID blijft de eigenaar van de door haar geleverde LCT's en staat in voor hun beheer.

8.2 Met het oog op de algemene veiligheid (beschermen van de systemen en gegevens), de bedrijfszekerheid en het controleren van de prestaties van de ASTRID-systemen behoudt ASTRID zich het recht voor om alle netwerkactiviteit te controleren en/of te registreren.

8.3 De Klant mag hierop toezicht uitoefenen overeenkomstig de met ASTRID terzake gemaakte afspraken.

9. Veiligheidsrichtlijnen met betrekking tot de ACT

9.1 Verloren of gestolen terminals

9.1.1 De Klant dient het ASTRID Service Centre (ASC) onmiddellijk op de hoogte te brengen om de terminal onbruikbaar te laten maken.

9.1.2 Er zal aanvankelijk gebruik worden gemaakt van de functiemogelijkheid "temporary disabled ITSI".

9.1.3 Naargelang van de evolutie van de toestand (terminal teruggevonden of definitief verloren/gestolen), moet het ASC opnieuw op de hoogte worden gebracht om de terminal opnieuw op het netwerk toe te laten ("enable") of om hem daarentegen definitief te schrappen ("permanent disable ITSI/TEI").

9.2 Terminals teruggestuurd voor reparatie

9.2.1 Elke terminal die naar de leverancier/service provider voor reparatie wordt teruggestuurd, zal tijdelijk uit het systeem worden geschrapt, d.w.z. de koppeling ITSI – K zal worden verbroken (de combinatie ITSI – REF zal worden geschrapt en de combinatie K – REF zal in de CKS worden opgenomen).

9.2.2 Voor deze ingreep zal de "disable" functie worden gebruikt ("temporary disable ITSI"). De Klant moet aan ASTRID vragen om deze handeling uit te voeren.

9.3 Terminal in een voertuig dat voor reparatie wordt uitgestuurd

9.3.1 Een mobiele terminal die zich in een voertuig bevindt, moet worden gedemonteerd alvorens dit voertuig aan een concessiehouder of aan een koetswerkhersteller wordt toevertrouwd.

9.3.2 Indien het voorgaande niet mogelijk is, moet A.S.T.R.I.D. worden gewaarschuwd zodat deze terminal tijdelijk uit het systeem kan worden gehaald ("disable" functie – zie hoger).

9.4 Mobiele terminals die als vaste post worden gebruikt

9.4.1 Om een periodieke authenticatie van deze terminals mogelijk te maken, wordt aangeraden om ze eenmaal per maand uit- en in te schakelen.

9.5 Gebruik van een PIN-Code

9.5.1 Het toepassen van een PIN-code bij het aanzetten om gebruik te kunnen maken van terminals die over deze functie beschikken, zou veralgemeend moeten worden.

9.5.2 PIN-codes met geringe beveiliging (11111, 123456, …) moeten worden verboden.

10. Veiligheidsverantwoordelijke bij de Klant

10.1 Krachtens artikel 5.3.2 van de Algemene Voorwaarden moet de Klant een veiligheidsverantwoordelijke aanwijzen.

10.2 De veiligheidsverantwoordelijke moet te allen tijde toezien op het correcte gebruik van de eindapparatuur door de gebruikers van zijn organisatie of dienst.

10.3 De veiligheidsverantwoordelijke moet ieder veiligheidsincident melden aan de door ASTRID aangestelde veiligheidsverantwoordelijke (CSO) zodat zij samen de gepaste maatregelen kunnen nemen.

11. Internet- en modemgebruik

11.1 Het is een gebruiker altijd en overal verboden om met een eindapparaat dat geactiveerd werd op de ASTRID-systemen, een rechtstreekse of onrechtstreekse verbinding te maken met het Internet, tenzij deze verbinding als dienst door ASTRID zelf wordt aangeboden.

11.2 Het is de Klant verboden eender welke modem aan te sluiten en te gebruiken op een eindapparaat dat geactiveerd werd op de ASTRID-systemen, tenzij deze verbinding als aanvullende dienst door ASTRID zelf wordt aangeboden of het aansluiten gebeurt op verzoek van personeelsleden van ASTRID of haar aangestelden die hiertoe uitdrukkelijk werden gemachtigd.

12. Sancties

12.1 ASTRID behoudt zich het recht voor om een Klant aansprakelijk te stellen voor de schade toegebracht door één van zijn Gebruikers ingevolge het niet of niet correct toepassen van de Gebruiks- en veiligheidsvoorwaarden.

12.2 Niet-naleving van de geldende Gebruiks- en veiligheidsvoorwaarden kan resulteren in een tijdelijk of permanent verlies van de toegang tot de ASTRID-systemen.

13. Aanvullende informatie –contactpersonen

Alle vragen omtrent deze voorwaarden kunnen schriftelijk aan ASTRID worden gesteld.

13.1 Ofwel per brief ter attentie van Bruno ANTOINE, CSO, 02.500.67.22 of 0496.595.722.

13.2 Ofwel per e-mail aan info@astrid.be.

13.3 Onverminderd de rechten en plichten die voortvloeien uit de Algemene Voorwaarden zullen geschillen omtrent de Gebruiks- en veiligheidsvoorwaarden in eerste instantie behandeld worden tussen de door de Klant aangewezen veiligheidsverantwoordelijke en de CSO en COO van ASTRID.