MALPENSA "SMART CITY OF GOODS" ECOSYSTEM
TERMS AND CONDITIONS FOR USING THE ECOSYSTEM

FOREWORD
Following the signing, in December 2013, of the Protocol aimed at the creation of an IT platform enabling virtuous communication and the transfer of data necessary for the processing of air cargo at Malpensa airport Lombardy Region, SEA (Società S.p.A. Esercizi Aeroportuali), ANAMA (Associazione Nazionale Agenti Merci Aeree - National Association of Air Cargo Agents) and Assohandlers (Association of Airport Handlers, hereinafter referred to as Promoters) have initiated a series of actions and investments for the implementation of the platform (hereinafter referred to as "Ecosystem").

This document represents and regulates the Terms and Conditions for both participation and use of the Ecosystem in the operational phase and is addressed to all air cargo operators wishing to use it, subject to the principles stated in the above Protocol.

DEFINITIONS

Participant(s)   economic operator, company, public or private entity, participating in the Ecosystem according to specific application conditions and by signing the Participation Agreement

Services   data, information and other functions other than applications created and made available to other Participants of the ecosystem

Promoters   Lombardy Region, ANAMA, ASSOHANDLERS and SEA S.p.A.

Operating Participants   SEA S.p.A. (hereafter SEA)
ANAMA
ASSOHANDLERS

Technological Platform Manager   SEA S.p.A.

Steering Committee is the body charged with the overall governance of the initiative from a strategic point of view and with promoting the development and dissemination of the Ecosystem in terms of new players participating and the publication of an increasing number of services and applications. The body is composed of a representative of the Operational Participants and third parties, if any

Documentation for participating in the ecosystem (Application Documentation) consists of:
- Application form
- Terms and conditions for using the ecosystem
- Use rules
- Technical specifications

1) **ECOSYSTEM OPERATION**

1.a) Operating logic and technological components of the ecosystem
- The Ecosystem is based on the creation of a community of service providers or applications useful for making the cargo services offered at Malpensa airport more efficient and offers users a logically unique landing point for digital information describing the cargo chain at Malpensa.

- In order for it to function, some of the participating operators expose services (functions, real-time information, «information bricks»), while other actors in the supply chain integrate with these services by developing their own applications that enable them to use them.
- The Smart City of Goods Ecosystem is part of the Malpensa Airport's Airport Information Systems and provides support to airport operators in the cargo sector, making available application services for sharing data on the different phases of air cargo transport based at the airport.

1.b) System and core services development
- The definition of the application functions and services to be made available through the Ecosystem is the responsibility of the *Steering Committee* which transmits the needs expressed by users to the *Technological Platform Manager*.
- The *Technological Platform Manager* develops and manages the technological "*core*" of the Ecosystem to which all *Participants* connect to use the services through the integration components developed by each of them or through the use of the portal that allows manual data input.

1.c) Technological system management
The *core* of the Ecosystem is managed within the *Technological Platform Manager*'s Airport Data Centre and is subject to all the security procedures and operating rules provided for airport information systems to support operations (user profile control, prevention of unauthorised access, *firewalls*, etc.).

2) THE TECHNOLOGICAL SYSTEM: SECURITY FEATURES, CONNECTION MODE AND MANAGED DATA

2.a) Asset protection and network communications
- The technological infrastructure is architecturally structured on three levels (presentation, business logic, backend), segregated both at server system and network level
- The FTP/SFTP and WSDL exposure systems are located within a DMZ network protected by Firewall/IPS-IDS installed at a Fastweb provider's farm;
- The presentation site (web server) is CA-certified and allows HTTPS communications;

- Business logic services (Middleware), on the other hand, are located on the SEA Server Farm's internal network and in turn protected by internal firewalls;
- Administrative access takes place only via SSH-type sessions.

2.b) Technical ways of connecting to the system
- The ecosystem can be accessed by one of the following transmission channels:
  - Web-Services (HTTPS = HTTP over Secure Socket Layer),
  - FTP (SFTP = Secure FTP),
  - Portal (HTTPS)
To access the system via any channel, the user must log in with a user name and password.

2.c) Users identification when connecting to the system

- Where the exchange of data between *Participants* and the Ecosystem takes place in FTP/SFTP mode, access is permitted only with the specific credentials
- In the case of WEB Service mode access over HTTPS protocol, user identification is carried out by application recognition of the calling site.

2.d) Data storage and tracking

- Every creation or modification of information managed by the Ecosystem is recorded and stored in a history *database*. The *track record* of each individual data item contains the following information
  - type of status change (e.g. created, updated, deleted)
  - date/time of the change
  - operator and user who made the status change
  - transmission channel used to make the change.
- The history database stores data for twelve months from the date of entry into the system and allows to analyse the history of a specific data item within the Ecosystem.
- In any case, the ecosystem does NOT replace the archives and databases that each user must maintain for legal or commercial and administrative purposes.

3) PARTICIPATION IN THE SYSTEM

3.a) Participation Conditions

- Economic operators in the air cargo community can participate in the Ecosystem (meaning: Air cargo agents, airport handlers, off-airport handlers, ramp handlers, customs and CAD forwarders, air carriers and their agents - GSA/GSSA) who, as part of their business, operate directly or indirectly at Malpensa Airport.
- Public administrations involved in air cargo transport can also participate (by way of example but not limited to: Customs Agency, Guardia di Finanza (Italian Finance Police), Air Health Authorities, etc.).
- In order to use the Ecosystem, it is necessary to participate in the initiative by signing an application form as indicated in the following paragraph.
- Participation in the Ecosystem and its use are free of charge.

3.b) Participation applications

- Economic operators belonging to the categories indicated in section 3.a) associated with one of the Trade Associations that promoted the initiative (Assohandler and ANAMA) and operators not associated with or not represented by any Trade Association must forward their participation applications directly to the *Technological Platform Manager* so that he/she can activate the necessary user account and authorisations.
- The applications must be accompanied by documentation proving entitlement to access the system (documentation proving that the *Participant* is an air cargo economic operator included in the listed categories) and any references of operators *Participating* in the ecosystem on whose behalf the applicants may be authorised to operate.
- The participation application form must specify the list of services to be used and the connection mode that will be used.
- Signing the application form implies explicit acceptance by
  the operator of the conditions and requirements stated in the *Application Documentation*
- This documentation is not only available on the Ecosystem website, but can also be requested from the IT platform manager.

3.c) Withdrawal from use of the system and cancellation of user account

- Operators who have participated in the use of Ecosystem may at any time withdraw from the Ecosystem and request the blocking of their user account, addressing their request to the same body they had applied to for participation. Withdrawal is not subject to any evaluation, takes immediate effect and results in the user account being blocked

from the system and the revocation of the credentials assigned.

- The Steering Committee may, at its sole discretion, request the Technological System Operator to block an operator's user account if the requirements that had allowed them to participate are no longer met or if they jeopardise or endanger the proper functioning of the Ecosystem. The cancellation must be communicated to the person concerned and entails the cancellation of the authorisations and credentials by the *Technological Platform Manager*. An operator whose user account is cancelled may apply again for its activation if it meets the requirements again.

4) USE OF THE SYSTEM: USERS AND DELEGATIONS

4.a) User profiles and system access credentials
- Access security is guaranteed by user IDs and passwords.
- User IDs and passwords are assigned by SEA during registration on the system and may be changed by the persons concerned in accordance with the rules specified in the user manuals of the specific applications, and in any case in compliance with existing data security and confidentiality regulations.
- The characteristics of passwords (e.g. length and composition), their management (e.g. duration and method of allocation/change) and the verification of access to the system by users (e.g. disabling in the event of a predefined period of inactivity, disabling after a few failed connection attempts due to an incorrect password, etc.), ensure the highest security standards in the management of Ecosystem use by authorised users. The rules for defining and managing passwords are contained in the user manuals of the specific applications.
- Each *Participant* is authorised to access one or more of the functions and services supported by the ecosystem. Authorisations to use the functions are associated with the credentials provided to access the system.
- Each *Participant* using the "Web Service" or "FTP" connection mode is allowed to create and manage its own internal users, assigning them an authorisation to use the functions and services they access.
- On the other hand, authorisations to use the portal are given to each user account individually.

4.b) Delegations for data input during the process of uploading information into the Ecosystem
- Each Ecosystem *participating* operator may only enter data into the system for which he/she has been authorised and may not consult or use information/data that are not associated with his/her profile.
- Each operator is entitled to delegate other operators to enter specific information as part of the goods handling process in the event that certain operations (e.g. customs operations, security checks, etc.) are entrusted to them (e.g. a customs agent operating on a specific consignment will only be allowed to add MRN code to a specific AWB on the basis of a previous authorisation notified to the ecosystem).
- In order to be able to proceed with data entry, delegated operators must also have participated in the ecosystem according to the method stated in section 3
- The delegation may only take place for a subset of functions for which both the delegator and the delegatee are entitled to access (e.g. a customs agent cannot be delegated to enter security data, but a regulated agent can be).
- A delegation mechanism between operators performing the same roles is not allowed (e.g. a customs agent cannot delegate another customs agent to act in his/her place).
- It is the responsibility of each operator to activate the delegations for the functions and services to which other operators must be authorised on his/her behalf. There are two modes of delegation:

- **default delegation**: this implies that the delegatee may operate on all the delegator's entities pertaining to it. The delegator may designate one or more persons as the default delegatees for a certain activity, assuming full responsibility for any interference between them.
- **specific delegation**: involves the delegator, for a specific entity and for a specific activity, explicitly designating one or more delegated parties, assuming full responsibility for any interference between them.

- Only cargo handlers operating within the airport can have access, without any delegation, to all data concerning shipments addressed to them.
- Airlines have read-only access to their shipment data
- Freight forwarders and "off-airport" handlers may only enter data on the waybills for which they are responsible and may access all data associated with those waybills in the system. None of these operators may consult data entered by a "competitor" belonging to the same category. Public administrations have read-only access to the information they are responsible for
- The user control and profiling mechanisms ensure the segregation of data so that each authorised operator (information holder or his/her delegate) can only access information for which the relevant authorisation has been registered in compliance with the rules stated in this paragraph.

   For instance, in order to ensure the confidentiality of the information entered into the platform, each AWB/HAWB is associated with:
   - the "agent code" that generated it and that can be managed by it exclusively with the contribution of operators delegated by him/her;
   - the GHA code that can be consulted and taken over.

   No other operator who is not explicitly delegated/authorised may access the data.
   In addition, to further protect access to data and information only by authorised parties, the "IP filtering" function can be activated (accessible from the portal to the administrators of each company), indicating the IP addresses (or Ip ranges) from which it is possible to connect to the Ecosystem to enter or consult the data for which they are responsible. If IP filtering is active, the ecosystem does not handle requests for data entry or consultation by other IPs for that company

- The Ecosystem verifies that each delegation request complies with the requirements stated in the participation rules
- All authorisations and delegations are recorded and stored in the system history.

5) TERMS AND CONDITIONS FOR USING THE SYSTEM

5.a) Legal value of information managed by the ecosystem
- The data transmitted to the Ecosystem is equivalent to a computer document, created, stored and transmitted by telematic tools. They have the same validity as the corresponding paper document and are considered to be directly usable by those concerned for the purposes of the goods management process for which they were uploaded onto the system.
- Each *participating* operator undertakes to enter into the ecosystem the data related to the services it has declared it will use and assumes full responsibility with respect to said entry.
- The correctness and completeness of the data is solely the responsibility of the operator who entered or changed them. These operations can be identified through the data tracking registration provided by the technology platform.
- The ecosystem does not carry out any transformation, change or manipulation of the data entered by the users, but merely stores them and makes them available according to the specifications defined by the *Steering Committee* and in accordance with the previous points.

- Each *participating* operator using the data entered into the ecosystem is fully responsibility for its use.
- Data inaccuracies, omissions or missing entries cannot therefore be attributed to the ecosystem.
- All data used within the Ecosystem are made available for operational purposes only and do not replace or have any priority over official or formally valid data.
- Each participating operator remains responsible for the data it enters in the Ecosystem, which are made available to users solely for the purposes defined for the specific services and do not have priority over data used by operators in the context of their business relations with each other.

5.b) Data confidentiality and privacy
- The *participants* undertake to take all measures to ensure the protection of the information and/or data made available through the Ecosystem and, in particular, to use the data and/or information received exclusively for the uses and purposes permitted by these terms of use.
- The *participants* undertake in particular to ensure the confidentiality of the information and/or data received and in particular to:
  - not to communicate in any way, assign or otherwise disclose, for any reason and at any time, the content of such information to third parties;
  - limit knowledge of or access to the content of the information to its strictly necessary staff, making them individually aware in advance of the confidentiality obligations stated in these terms of use;
- Each *Participant* shall promptly inform the *Technological Platform Manager* in the event that it is obliged, by virtue of an order issued by an Authority vested with appropriate powers, to disclose data or information learned through the use of the Ecosystem.
- The confidentiality obligation will last for the duration of 24 months from the date of withdrawal from the Ecosystem or termination of its use.

5.c) Disclaimer
- The *Technological Platform Manager* provides no guarantee to participants for the quality of the data made available by other participants within the Ecosystem.
- The *participant* assumes full and sole responsibility for the quality of his/her data and indemnifies the Platform Manager from any and all liability and damages arising to other participants or third parties as a result of the data he/she has provided or entered into the Ecosystem.
- The *participant* expressly acknowledges that no charge shall be made to SEA for any loss or damage that the Participant may incur as a result of the changes made by the latter to its systems for communicating with the Ecosystem, or for any temporary or permanent cessation in the transmission of data to the Ecosystem platform and/or in the provision of related services.
- The *Technological Platform Manager* shall be released from any liability or claim for any damages in the event of service suspension due to causes not attributable to SEA and/or force majeure of any nature.
- No charges may be brought against SEA in the event of any service interruptions due to technical faults in the platform. In such cases, SEA is obliged to inform all participants in good time about the duration of the interruption and the expected restoration time. In this circumstance, specific contingency procedures will have to be activated by the participants to enable the smooth management of the flow of goods through the use of paper documentation

5.d) Liability - Indemnity
- The *Technological Platform Manager* will use its reasonable capabilities and due care to make the platform available and efficient on a continuous and regular basis. For this purpose, it has set up an emergency response structure for the resolution of technical problems (hardware and software) with response times similar to those of the most critical ICT airport systems.
- However, the *Technological Platform Manager* cannot guarantee with absolute certainty that no temporary or prolonged interruption of services will occur for any reason that may or may not be its responsibility.
- Therefore, the *participants acknowledge that SEA* shall in no event be liable, except in the case of wilful misconduct or gross negligence, for any kind of damage, direct or indirect, caused to the participants or third parties:
  - from the use or inability to use any of the Services;
  - from any interruption of any Services;
  - from alteration of transmissions or data of the Customer, including, inter alia, any damage, including financial damage, that the Customer may have suffered due to loss of profit, use, loss of data or other intangible elements;
  - from deletion, alteration, failure to store, send or receive transmissions of participants or data obtained through the Services.
- The *participants* undertake to indemnify and hold harmless the Technological Platform Manager against any prejudice, damage, indemnity or expense that the Technological Platform Manager may incur as a result of third party claims, complaints, demands and actions against the Technological Platform Manager relating to, dependent on and/or connected to the services provided through the Ecosystem
- Similarly, SEA acknowledges that no charges may be brought against the participants for any negative consequences that may derive to the management of cargo traffic at Malpensa Airport from their conduct with respect to the use of the Ecosystem.

5.e) Intellectual and Industrial Property
- The *participant* guarantees that he/she has full ownership of all industrial and intellectual property rights or rights of use, including any licences to use the programmes used by him/her, in relation to the services and data shared within the Ecosystem.
- Anything developed by the *participant* to access Ecosystem services remains the exclusive property of the *participant*, in accordance with applicable law.
- The *participant* undertakes to indemnify the IT Platform Manager against any damage or claim brought against it by third parties for infringement of any industrial and intellectual property right in the ownership of such third parties.
- In the event of any dispute raised by third parties, or by other participants for any infringement of their industrial and intellectual property rights in the software components or information managed, the *participant* must inform the IT Platform Manager and the Steering Committee as soon as possible.
- All intellectual and industrial property rights related to the *core* components of the Ecosystem are and remain the property of the *Technological Platform Manager* (SEA).

5.e) Use of the ecosystem's image by participants and the platform manager
- The Ecosystem *participant* and its suppliers, if any, who have developed technological components for connection with the Ecosystem, are entitled to use the Ecosystem logo, subject to the following indications:
  - the logo may only be used by the *participant* and its direct supplier, but not by any third parties in any way involved by the participant in the implementation of the

services or applications.
- by displaying the logo, the *participant* must also publish the link to the Ecosystem website.
- The *participant* hereby grants the *Steering Committee* the right to use its logo for the purposes of communication and promotion of the Ecosystem.