PUBLIC

SECURITY CONVENTION

FOR CARRIERS REMOTE ACCESS

Convention N°: <eu-LISA acronym>.<serial number>

_____
<company name>

whose registered office is at _____ ,
<company address>

represented by _____ ,
<name of company representative>

_____ ,
<function of company representative>

Hereinafter called "the Carrier",

Agreed as follows:

Table of Contents

1. OBJECT

The present document establishes the security rules for the Carrier to access the Carrier's interface under the provisions of Commission Implementing Regulations 2021/1224 and 2021/1217. This access is enabled in order Carriers can execute the tasks defined in the EES Regulation 2017/2226 and in the ETIAS Regulation 2018/1240.

2. RULES

In order to perform the remote connection, the Carrier must comply with the rules defined below. Failure to comply with those rules may result in Carrier disconnection and/or Carrier deregistration from the Carrier Interface.

2.1. Obligations of Carriers

Carriers shall ensure that only duly authorised staff have access to the carrier interface. The carriers shall put in place at least the following mechanisms:

(a) physical and logical access control mechanisms to prevent unauthorised access to the infrastructure or the systems used by the carriers;

(b) authentication;

(c) logging to ensure access traceability.

Carriers shall provide means to ensure compliane with the following security objectives:

(a) identifying and managing security risks related to the connection to the carrier interface;

(b) protecting the ICT environments and the devices connected to the carrier interface;

(c) detecting, analysing, responding to and recovering from cyber security incidents.

2.2. Authentication Scheme

When carriers access the carrier interface using the Application Programming Interface, the authentication scheme shall be implemented by means of mutual authentication in accordance with Art 45 paragraph 3 of the ETIAS Regulation 2018/1240.

2.3. Authorised Staff

(1) The Carrier shall ensure that the tasks entrusted to them are carried out only by authorised staff.

(2) The Carrier must keep a register of the members of the authorised staff.

(3) The Carrier shall instruct the Authorised staff to comply with the security rules set out in the current text.

2.4. Authentication / Identification of the Authorised Staff

(1) Each member of the Authorised staff using technical equipment connected to the Carrier Interface must be clearly identified and authenticated.

(2) The Carrier is responsible for the internal management and assignment of the Authentication / Identification mechanism(s) for its staff.

(3) The Carrier is legally, jointly and severely liable for the consequences of the misuse or loss of the Authentication / Identification mechanism(s) allowing the use of the Carrier Interface by persons not belonging to the Authorised staff.

2.5. Carrier specific duties

The Carrier undertakes:

(1) To use the information provided by eu-LISA for no other purpose than to execute the tasks based on the EES 2017/2226 and ETIAS Regulation 2018/1240 and shall not reproduce, publish or otherwise disclose such information to any third party;

(2) To destroy all data, transferred to premises of the Carrier in order to perform the tasks required once they are no longer needed;

(3) To remedy as soon as possible and on best effort basis any fault, problem or weakness that could appear and for which the Carrier is responsible;

(4) To comply with new security rules at the request of eu-LISA, for example if eu-LISA implements new Authentication and Access control mechanisms for the connection to the Carrier Interface.

(5) Conduct a risk assessment and implement a security plan for ensuring the security of the Carrier connection to the Carrier interface

2.6. Members of the authorised staff duties

The members of the authorised staff shall be informed by the Carrier's Single Point of Contact (SPOC) on the following rules:

(1) To comply with the security rules and policies of the Carriers realted to the connection to the Carrier Interface;

(2) Not to disclose information held by the Carrier on behalf of eu-LISA to third parties, except on a need-to know basis where authorised;

(3) To make reasonable use of all available means of controlling access provided by the Carrier and in balance with the sensitivity of the information

concerned to prevent unauthorised persons from using the resources at their disposal, in particular by ensuring that computer terminals are not accessible during absences;

(4) Not to disclose authentication procedures or share them with third parties unless required to do so by the needs of the service and after obtaining the Carrier approval;

(5) To be responsible for action taken in their name;

(6) Not to install or use on computers (work stations, local or central servers, etc.) any equipment or programmes, from portable storage media (diskettes, optical disks, etc.) or downloaded from electronic bulletin boards, e-mail systems or telecommunications networks belonging to third parties, unless explicitly authorised by the Carrier;

(7) Not to install or have installed connections with networks without explicit authorisation from the Carrier;

(8) Not to set up electronic bulletin boards, e-mail systems, modem connections or any other type of information communication system that could enable unauthorised persons to gain access to the eu-LISA systems without explicit authorisation from the Carrier;

(9) Not to use equipment or software that is their private property when connected to the Carrier's and / or eu-LISA's network without prior explicit authorisation from the Carrier;

(10) To notify their superior in the Carrier as soon as they suspect any failure or incident affecting the security of their own environment or of other systems;

(11) To take all possible steps in respect of availability, confidentiality and integrity to safeguard the security of their working environment, particularly as regards working methods they have introduced or developed themselves.

2.7. Prohibited uses

Any party is prohibited from using the interface or its content:

(1) For any unlawful purpose;

(2) To solicit others to perform or participate in any unlawful acts;

(3) To violate any international, federal, provincial or state regulations, rules, laws, or local ordinances;

(4) To infringe upon or violate eu-LISA intellectual property rights or the intellectual property rights of others;

(5) To harass, abuse, insult, harm, defame, slander, disparage, intimidate, or discriminate based on gender, sexual orientation, religion, ethnicity, race, age, national origin, or disability;

(6) To submit false or misleading information;

(7) To upload or transmit viruses or any other type of malicious code that will or may be used in any way that will affect the functionality or operation of the Service or of any related website, other websites, or the Internet;

(8) To collect or track the personal information of others;

(9) To spam, phish, pharm, pretext, spider, crawl, or scrape;

(10) For any obscene or immoral purpose;

(11) To interfere with or circumvent the security features of the Service or any related website, other websites, or the Internet.

eu-LISA reserve the right to terminate use of the service or any related website for violating any of the prohibited uses.

SIGNATURE

Signature: _____

Done at _____ , on _____