AGREEMENT FOR REMOTE CONNECTION

VOTRE RÉSEAU SÉCURITÉ
COMMUNICATIE VOOR VEILIGHEID

BETWEEN

.....

With registered office address at .....

Represented by .....

In his/her capacity as .....

Referred to below as '**the Tenderer**'

AND

A.S.T.R.I.D., a limited company under public law with registered office address at Regentlaan 54, 1000 Brussels,

Represented by Salvator Vella, in his capacity as Director General,

Referred to below as '**A.S.T.R.I.D.**'

The Tenderer and A.S.T.R.I.D. are also each referred to individually as '**Party**', and together as '**the Parties**'

FOR THE PURPOSES OF THIS PUBLIC CONTRACT

.....

Referred to below as 'the **Performance**'

WHEREAS:

1. This agreement records the conditions for access by the Representative to the Infrastructure belonging to or entrusted to ASTRID within the scope of the Performance;
2. The following terms used in this agreement have the following definitions:
   Client: *Any service, institution, company, or association as defined in Article 3 §1 of the statute of 8 June 1998 on the radio communications of emergency and security services;*
   Code: *The information necessary to obtain a remote connection to the Infrastructure;*
   Community: *A group of persons sharing common interests;*
   Agreement: *This Agreement for remote connection;*
   Extended Confidentiality Agreement: *Agreement setting out the conditions for the exchange of Information between the Parties (see astrid.be/rfp);*
   Information: *All information or data, irrespective of its form or nature, that belongs to or is entrusted to A.S.T.R.I.D. and that is of importance to A.S.T.R.I.D. and its users, including personal data, technical knowledge, specifications, plans, models, software, techniques, drawings, schedules, procedures, industrial and intellectual property rights, commercial information, information about the suppliers and clients of A.S.T.R.I.D. and, in general, all information that for the account of A.S.T.R.I.D., its employees, sub-contractors, or other parties it engages, is shared with or disclosed to the Tenderer, and/or processed;*
   Infrastructure: *The systems of A.S.T.R.I.D. or any infrastructure in which these systems are located, including cloud solutions, exploited, developed, maintained, or that are required to be installed, combined, adapted or expanded, and in which Information is stored, processed, handled, added to, or made available;*
   Security Officer: *The security officer of ASTRID or their official representative;*
   Partners: *Persons or groups of associated persons who carry out a project;*
   Third parties: *Persons or groups of persons that are not parties to this Agreement;*
   Information Owner: *The Party that holds the intellectual property rights to Information;*
   Intelligence: *The information pertaining to the Representative that is shared with the Security Officer;*
   Representative: *Each employee that is allocated or seconded to ASTRID by the Tenderer;*
   Subcontractors: *Persons that perform work on behalf of either Party;*
   Tenderer: *The Tenderer, including its Representatives, its employees and where relevant its Third Parties and Subcontractors;*
   User: *Any member of staff of the Client who utilises the systems and services of A.S.T.R.I.D.;*
3. A.S.T.R.I.D. is the operator of the emergency and security networks (cf. Articles 102 and 103 of the Royal Decree of 16 January 2017 establishing the third management contract of A.S.T.R.I.D.). Information is sent via these networks which, in the event of any kind of incident, could be released;
4. The '**98 Statute**' means the 'Statute of 11 December 1998 on classification and security clearances, certificates and advisory notices' together with the relevant Royal and ministerial decrees, and including all legislative amendments thereto;
5. All Information classified as 'CONFIDENTIAL - 98 Statute', 'SECRET - 98 Statute' or 'TOP SECRET – 98 Statute' may be exchanged between A.S.T.R.I.D. and the Tenderer in accordance with the rules stipulated by the 98 Statute;
6. A.S.T.R.I.D. classifies its Information in accordance with the Traffic Light Protocol (TLP, https://www.first.org/tlp/) standard:

TLP:CLEAR:	*The recipients may distribute the information globally; there are no restrictions on its distribution;*
TLP:GREEN :	*Restricted disclosure; the recipients may distribute this Information within their Community;*
TLP:AMBER :	*Restricted disclosure; the recipients may only distribute this Information on the basis of a 'need to know' within their organisations and amongst their clients;*
TLP:AMBER+STRICT :	Distribution strictly restricted to ASTRID;
TLP:RED :	*For the eyes and ears of individual recipients only; no other distribution;*

7. The Tenderer should be able to access the Information communicated by A.S.T.R.I.D., its employees, Third Parties, Subcontractors, or Users;
8. The conditions under the Extended Confidentiality Agreement, which is annexed to the specifications for the Performance, are strictly binding;

TLP:AMBER - LIMITED DISCLOSURE, RESTRICTED TO PARTICIPANTS' ORGANIZATIONS

AGREEMENT FOR REMOTE CONNECTION

VOTRE RÉSEAU SÉCURITÉ
COMMUNICATIE VOOR VEILIGHEID

9. The Representative must have installed in advance the Microsoft Authenticator application on their smartphone;
10. The Tenderer that is given access to the Information or to the Infrastructure, should comply strictly with the following conditions;

THE FOLLOWING CONDITIONS STRICTLY APPLY

11. The Tenderer will only appoint as Representative one or more persons who fully satisfy the conditions under the Extended Confidentiality Agreement pertaining to the Performance;
12. The Tenderer shall apply to the Security Officer to obtain a list of the necessary Intelligence and share these Intelligence with the Security Officer in respect of each of its Representatives;
13. The Security Officer of A.S.T.R.I.D. may be contacted via e-mail (sec.advice@astrid.be);
14. After checking the Intelligence, the Security Officer will ask the Representative to attend a physical or remote meeting to share with such Representative the Codes;
15. Physical meeting
    i. Any physical address validated and accepted by the Security Officer is deemed acceptable as the location for a physical meeting;
    ii. The identity of the Representative shall first and foremost be checked by the Security Officer on the basis of an official identity document;
    iii. The Code is activated in the Microsoft Authenticator application on the basis of a QR code disclosed by the Security Officer to the Representative;
    iv. The disclosed Code is strict confidential information for which the Representative is entirely responsible;
16. Remote meeting
    v. Only the Microsoft Teams application may be used for video conferences;
    vi. Teams meetings are only permitted if they have been set up by the Security Officer;
    vii. Only the Representative may participate in a remote meeting;
    viii. The entire meeting shall be recorded and stored by the Security Officer, and is regarded as evidence of the correct delivery of the Codes by the Security Officer to the Representative;
    ix. The Code is activated in the Microsoft Authenticator application on the basis of a QR code disclosed by the Security Officer to the Representative;
    x. The disclosed Code is strict confidential information for which the Representative is entirely responsible;
17. In the event of any breach of this Agreement
    xi. In the event of any breach of this Agreement of any kind, ASTRID will immediately suspend access to its Infrastructure by the Representative who is in breach of the requirements of this Agreement, and the Tenderer will be informed accordingly;
    xii. The Tenderer will be required by the Security Officer to explain the breach;
    xiii. Depending on the explanation given by the Tenderer to the Security Officer, access to the Infrastructure may be reinstated or the suspension of access to the Infrastructure made permanent and definitive;
    xiv. The Security Officer may request the Tenderer to propose to ASTRID another Representative. In such a case, the conditions of this Agreement will strictly apply;
    xv. The definitive suspension of access to the Infrastructure may also lead to the immediate termination of the Performance, in a way that is to the detriment of the Tenderer;
18. This Agreement sets out all obligations of the Parties concerning confidentiality and replaces all previous obligations between the Parties in this regard;
19. This Agreement is governed by Belgian law;
20. Any disputes arising between the Parties under this Agreement shall be brought exclusively before the competent courts in Brussels;
21. The Agreement comprises all the conditions set out in this document;
22. The Tenderer is liable on behalf of its employees, Third Parties and Subcontractors for strict compliance with this Agreement.

Signed in .....

On ..... , in duplicate,

For **A.S.T.R.I.D.**
Represented by: **Salvator Vella**
Position: **Director-General**
Signature:

For : .....
Represented by: .....
Position: .....
Signature:

TLP:AMBER - LIMITED DISCLOSURE, RESTRICTED TO PARTICIPANTS' ORGANIZATIONS