

CONFIDENTIALITY & NON-DISCLOSURE AGREEMENT

EIT Manufacturing issued the Request for Proposal entitled “Content Quality Check in Skills.move” published on the website of the EIT Manufacturing on June 26th which contains sensitive information regarding quality check service for EIT Manufacturing’s Skills.Move platform. EIT Manufacturing is willing to protect the shared information through the RfP process from being disclosed to third-parties.

THIS AGREEMENT is hereby executed between

EIT Manufacturing an association (Registration number W913012329, SIRET 88077857600012, VAT FR62 880778576) registered under French law, with its office at 2, Boulevard Thomas Gobert, 91120 Palaiseau, France (hereinafter refer to as **EITM** or **Disclosing Party**)

And

_____ having its principal place of business at
_____ (hereinafter “**Recipient Party**”),

in relation to Request for Proposal entitled “Content Quality Check in Skills.move,” (hereinafter “RFP”).

Affirmation

The Authorized Representative, by signing this Agreement in the name and on behalf of the Recipient Party, subscribes and affirms the following:

1. that he/she is the authorized representative of Recipient Party which is qualified to respond to the above referenced RFP;
2. that he/she is signing this Agreement on behalf of and as the act and deed of the Recipient Party named below intending to bind said Recipient Party to the representations made herein;
3. that the Recipient Party will comply with all requirements of this Agreement; and
4. that the Recipient Party will return or destruct the Confidential Information.

PART 1. DEFINITIONS

A. Confidential Information

‘Confidential Information’ (hereinafter “Confidential Information”) shall be defined to include:

1. any document or information that EITM, regardless of form or medium of disclosure (e.g., verbal, hard copy, or electronic) or source of information provides to Recipient Party, or which Recipient Party obtains, discovers, derives or otherwise becomes aware of solely as a result of this RFP other than:
 - (a) information that is previously rightfully known to the Recipient Party without restriction on disclosure;
 - (b) information that is shared via the website of EITM with the public; and
 - (c) Information that is independently developed by the Recipient Party without the use of Confidential Information.

Title to all Confidential Information remains the property of the EITM. Confidential Information is provided on an “as is” basis, and the EITM makes no warranties, guarantees or representations of any kind express or implied, or arising by custom or trade usage, as to any matter whatsoever, without limitation, and specifically makes no implied warranty of fitness for any particular purpose or use, including but not limited to adequacy, accuracy, completeness or conformity to any representation, description, sample or model.

B. Authorized Use

“Authorized Use” shall be defined as the use of Confidential Information by Recipient Party, its employees, consultants and subcontractors, solely for the purpose of submitting a proposal to the RFP and, studying pertinent documents and information for this purpose. Disclosure, display, use, duplication, storage or transmittal of Confidential Information, in any form, for any purpose other than that set forth in the engagement, including extrapolation or retention of summary information, data or business processes, even if without specific identifiers, shall be deemed an “unauthorized use”.

C. Authorized Person

“Authorized Person” shall be defined as those persons within Recipient Party’s employ or control identified by Recipient Party to EITM as having a need to receive, possess, store, access, or view Confidential Information for an Authorized Use.

PART 2. CONFIDENTIALITY & NON-DISCLOSURE REQUIREMENTS

A. Duty to Protect Confidential Information

Upon proper execution of this Agreement, Recipient Party will be granted a non-exclusive, non-transferable license to storage and view Confidential Information only for an Authorized Use. Recipient Party shall safeguard all Confidential Information which is delivered from the EITM to the Recipient Party to insure its authorized use and to protect and prevent its unauthorized use or disclosure.

“Safeguard all Confidential Information” shall be defined as Recipient Party taking either one, or a combination of the following security measures, whichever standard is higher:

- (1) Where Recipient Party has established security procedures for its own confidential, sensitive business information which impose security requirements for the protection of its own trade secret, proprietary or confidential information, Recipient Party shall protect the Confidential Information using the same means; and/or
- (2) Where the Recipient Party has not established such internal procedures, Recipient Party shall take the commercial measures defined below, to protect the Confidential Information.

Commercial Measures to Protect Confidential Information

For purposes of this Agreement, “commercial measures” shall be defined to include all of the following responsibilities to be undertaken by the Recipient Party. Recipient Party shall take all of the following “commercial measures” to protect the Confidential Information:

I. Use Restriction

Confidential Information shall only be received, possessed, stored, accessed and/or viewed by Authorized Persons.

II. Access by Authorized Person(s)

- a. Recipient Party shall be responsible for identifying those persons within its employ or control who have a need to receive, possess, store, access, or view Confidential Information for an authorized use (hereinafter “Authorized Person(s)”).

- b. The Recipient Party shall be required to take commercially reasonable steps to inform each Authorized Person of their individual obligation to protect the security of Confidential Information in accordance with the requirements of this Agreement.
- c. The Recipient Party shall not permit Confidential Information to be received, possessed, stored, accessed, or viewed by any Authorized Person until such person has agreed to comply with the required security obligations set forth below.

III. Access by Subcontractors and Consultants

- a. The Recipient Party shall be responsible for identifying those consultants and subcontractors who have a need to receive, possess, store, access, or view Confidential Information for authorized use.
- b. Recipient Party shall not permit Confidential Information to be received, possessed, stored, accessed, or viewed by any consultant or subcontractor until such entity's legal representative has been made aware of and has agreed to comply with the required security obligations of this Agreement.
- c. Consultants and subcontractors shall not be allowed to further disseminate or distribute Confidential Information, other than to provide access by Authorized Person(s) within consultant's or subcontractor's control and oversight.

IV. Security Obligations Regarding Confidential Information

Any person(s) who receive, possess, store, access, or view Confidential Information from either the Recipient Party or its approved Subcontractor or Consultant shall be subject to the following security obligations:

- a. The Recipient Party must approve any process used to duplicate, distribute or otherwise transmit Confidential Information to Authorized Person(s), and may NOT approve or use any process which involves the use of any public internet or other non-secure medium.
- b. Confidential Information may NOT be stored on personal (non-business) computing or other electronic devices or taken or removed in any form outside of the physical premises of Recipient Party.
- c. Upon termination of employment, Authorized Person(s) shall be required to return Confidential Information to Recipient Party's legal representative, and/or to affirm that all electronic, optical or other copies have been destroyed within any electronic storage or other medium.

V. Chain of Custody

Recipient Party shall be required to keep a record of all copies of the Confidential Information that have been made and distributed to those persons within the employ of Recipient Party, and to those consultants or subcontractors who have a need to access Confidential Information for such authorized use.

Those consultants or subcontractors which receive Confidential Information from the Recipient Party shall, as a condition of accessing such information, affirm that such entity shall keep a record of all copies of the Confidential Information that have been made and distributed to those persons within the employ of such entity.

Termination

The license to use Confidential Information terminates automatically upon the occurrence of any of the following: (a) Breach of this agreement; or, (b) Closure of the RFP; or (c) Non-award of a Contract pursuant to the RFP.

Compliance

The failure of the Recipient Party to furnish the required compliance with the terms of this Agreement will be

deemed a breach of the Agreement. Breach of this Agreement may be considered by the EITM as an issue of responsibility as to such entity in future contracting opportunities with the Recipient Party.

In addition to the foregoing, if Recipient Party breaches or threatens to breach this Agreement, the EITM shall have all equitable and legal rights (including the right to obtain injunctive relief) to prevent such breach and/or to be fully compensated (including reasonable attorney's fees) for losses or damages resulting from such breach. The Recipient Party is deemed to acknowledge that compensation for damages may not be sufficient and that injunctive relief to prevent or limit any breach of confidentiality may be the only viable remedy to fully protect the Confidential Information.

Governing Laws

This Agreement shall be governed by and construed in accordance with the laws of France. If any provision of Agreement is declared by a court of competent jurisdiction to be invalid, illegal, or unenforceable, the other provisions shall remain in full force and effect.

IN WITNESS WHEREOF, this Non-Disclosure Agreement is signed as of the date set forth below.

By: **Recipient Party**

Print Name: _____

Title: _____

Date: _____

By: **EIT Manufacturing**

Print Name: _____

Title: _____

Date: _____