AI Tools, Supply Chain and IAM Clauses

Open Procedure for the provision of consulting services on identity and access management for the European University Institute

A. AI Tools Use Clause

Use of Artificial Intelligence (AI) Technologies

1. **Authorisation Requirement**
   The Contractor acknowledges and accepts that **the use of AI tools to perform this mandate requires explicit authorisation from the Institute**. No AI system, service, software, or automated processing capability shall be used in the performance of the contract unless prior written authorisation has been granted by the Institute.
2. **Information to Be Provided by the Contractor**
   Prior to requesting authorisation, the Contractor shall submit to the Institute, in writing, the following information for each AI tool it intends to use:
   a. the **name, version, and provider** of the AI tool;
   b. a detailed description of the **technical and organisational measures** implemented to prevent data sharing, data leakage, or exfiltration;
   c. confirmation that Institute data will **not be used for model training** or transferred to any unauthorised third party;
   d. a clear explanation of **the purpose and scope** of the AI tool's intended use in relation to the mandate.
3. **Institute's Assessment**
   The Contractor acknowledges that **the Institute will perform its assessment before releasing its authorisation**, including evaluations of security, data protection, compliance, and operational risk. Authorisation may be granted, refused, or granted subject to conditions at the sole discretion of the Institute.
4. **Prohibition Pending Approval**
   Until such authorisation is formally issued, the Contractor is expressly prohibited from using any AI tool in connection with the execution of the mandate.
5. **Ongoing Compliance**
   If authorisation is granted, the Contractor remains fully responsible for:
   - ensuring continuous compliance with all security, confidentiality, contractual, and regulatory obligations;
   - notifying the Institute of any changes to the authorised AI tool, its configuration, or its data-handling practices;
   - immediately informing the Institute of any actual or suspected data leakage, breach, or unauthorised disclosure related to the use of the AI tool.
6. **Right to Withdraw Authorisation**
   The Institute reserves the right to **suspend or withdraw** its authorisation at any time should new risks emerge, compliance issues be identified, or contractual obligations not be met.

B. Supply Chain Cybersecurity and Incident Handling Clause

The Contractor shall implement appropriate and proportionate cybersecurity measures to ensure the security of all services provided to the Institute, taking into account the vulnerabilities and cybersecurity practices of its direct suppliers, as required by NIS2 supply-chain obligations.

The Contractor shall:

1. Designate a Security Contact Point and provide the Institute with the name and contact details of the responsible referent for all cybersecurity matters, consistent with NIS2 supplier-coordination requirements.
2. Maintain and provide documented procedures for the detection, escalation, and reporting of cybersecurity incidents, ensuring compatibility with NIS2 flow-down reporting obligations.
3. Ensure all personnel performing the mandate receive regular cybersecurity awareness training, including phishing, malware, intrusion awareness, and internal reporting.
4. Accept the Institute's right to audit the services and related security controls to verify compliance.
5. Notify the Institute's Information Security referent without undue delay of any cybersecurity incident that may affect the Institute, in line with NIS2 expectations for prompt incident communication.

The successful tenderer shall receive the complete EUI security policies to be acknowledged before proceeding with the signature of the contract.

C. IAM Compliance Obligations Clause

The Contractor acknowledges that access to the Institute's systems and resources is strictly governed by the EUI Identity and Access Management (IAM) Policy. Accordingly, the Contractor and all personnel assigned to the mandate shall:

1. Provide accurate personal identification data for each individual requiring access and promptly notify the Institute of any changes affecting their role, function or eligibility.
2. Ensure that employees use only their individually assigned EUI credentials and do not share, disclose, or transfer them to any third party.
3. Ensure that all personnel protect passwords and authentication factors, and immediately report suspected compromise, data leakage, or account misuse to the EUI Helpdesk or reports@eui.eu.
4. Guarantee that access is used solely for the execution of authorised activities and only for the period officially approved by the Institute.
5. Ensure that joiner/mover/leaver changes are communicated promptly to enable correct provisioning and timely removal of access.
6. Ensure that all personnel sign the required confidentiality undertakings and respect all limitations on access and data handling.

Failure to comply may result in suspension or termination of access, removal of personnel from the project, or other contractual remedies.