**ANNEX II**

**TECHNICAL PROPOSAL FORM**

The technical proposal must be consistent with the Terms of Reference (see **Section B.1 of the tender specifications**). In preparing the technical proposal the tenderers should bear in mind the award criteria against which it will be evaluated (see **Section B.7 of the tender specifications**).

Tenderers shall use the following format to submit their technical proposals.

Name of the tenderer \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Signed (authorised signature) on behalf of the Tenderer | |
| Name |  |
| Position |  |
| Signature |  |
| Date |  |

The tenderers shall answer the questions below and shall provide the required information in the text boxes provided. Tenderers can extend the answers to questions in the Technical Proposal form on as many pages as needed and there is no restriction on how long the answers can be. The text boxes can be expanded for as long as needed and additional information/documents can be attached if necessary. In case additional information is provided as annex(es) to this technical proposal form, a reference to the annex(es) should be included in the box corresponding to the relevant question.

This technical proposal form is divided in two parts, as follows:

**Part 1: Mandatory Requirements Compliance Matrix**

**Part 2: Technical proposal – description of the proposed services**

**Part 1: Mandatory Requirements Compliance Matrix** \*

\* Important: Please note that the questions in the Mandatory Requirements Compliance Matrix require an unconditional answer. In order for your tender to be evaluated against the award criteria, it should first meet all minimum (mandatory) requirements.

|  |  |  |  |
| --- | --- | --- | --- |
| **Mandatory Requirements Compliance Matrix** | | | |
| **Ref No.** | **Mandatory Requirement Description** | **Compliant Yes / No** | **Please explain briefly how compliance is achieved and, where applicable, make reference to the relevant section of the Part 2 of the technical proposal or annexed document where detailed description is provided** |
| **1** | **Migration from current contractor** | | |
| 1.1 | The contractor shall migrate/move the current e-Net platform to their new environment with maximum downtime of 48 hours, no loss of data and within 40 calendar of signature of the specific contract. |  |  |
| **2** | **Hosting** | | |
| **2.1** | **General requirements** | | |
| 2.1.1 | The contractor shall provide a hosting solution with dedicated server(s) for the CEPOL e-Net system. e-Net must be hosted in a European Union Member State |  |  |
| **2.2** | **Physical environment** | | |
| 2.2.1 | The contractor should ensure that all systems are housed in a secure and redundant environment |  |  |
| 2.2.2 | The contractor should provide a physical environment that is either certified to be ISO 27001 compliant or that conforms to the standards. In the case that the Data Centre is not certified, then the contractor should provide evidence of conformance to recognised industry standards |  |  |
| 2.2.3 | The contractor shall ensure that the hosting platform is backed-up to a remote location which is located in EU and can be restored when required |  |  |
| 2.2.4 | The contractor shall have established processes and procedures to ensure the security of the hosting physical environment and that covers at least the following :  • Power supply;  • Environmental conditions;  • Security and Access Control;  • Fire / Flood suppression |  |  |
| **2.3** | **Capacity Management** | | |
| 2.3.1 | CEPOL requires that the contractor have sufficient hosting capacity to meet required performance as defined in the service level requirements |  |  |
| 2.3.2 | The contractor shall ensure that the capacity at each layer of the platform is proactively monitored and managed. |  |  |
| 2.3.3 | The contractor shall ensure that prompt adequate actions are taken before thresholds are reached |  |  |
| **2.4** | **Hardware** | | |
| 2.4.1 | The contractor shall provide the necessary hardware adequate to host the e-Net Platform. |  |  |
| **2.5** | **Data Centre/ Server connectivity** | | |
| 2.5.1 | The contractor shall provide multiple connections between their Data Centre and the internet in particular ensuring failover if the connection fails. The Datacentre should have adequate bandwidth in order to meet the needs of e-Net. |  |  |
| 2.5.2 | The contractor shall provide at least a 100mbps unmetered connection per server |  |  |
| **2.6** | **Security** | | |
| 2.6.1 | The contractor shall ensure the security of all e-Net layers |  |  |
| **2.7** | **Availability** | | |
| 2.7.1 | CEPOL requires that all components comprising the e-Net platform be available 24/7/365, except for scheduled maintenance. |  |  |
| **3** | **Support and Maintenance** | | |
| **3.1** | **Support** | | |
| 3.1.1 | The contractor shall provide 1st and 2nd level support services for a limited number of CEPOL staff (Working hours: 07:00 to 18:00 Budapest Time). |  |  |
| 3.1.2 | Contractor shall use an automated tool for the registration, management and reporting of support requests (ticketing system). Incident Requests and Change Requests should both be handled by the same tool. |  |  |
| 3.1.3 | The contractor shall provide the means for CEPOL staff to report new support requests outside of the stated office hours. |  |  |
| 3.1.4 | The contractor shall provide the necessary support and ensure that the following types of reported Incidents are addressed.  • Low;  • Medium;  • High/Critical.  Average Response time to open support ticket  • Low: 4 working hours;  • Medium: 3 hours;  • High/Critical: 1 hour. |  |  |
| 3.1.5 | The resolution time is the elapsed time between the contractor responding to a support ticket opened by CEPOL and the contractor successfully resolving the Incident. The maximum resolution times are:  • Maximum resolution time (reported during working hours) for a Low priority incident is: 48 hours  • Maximum resolution time (reported during working hours) for a Medium priority incident is: 12 hours.  • Maximum resolution time (reported during working hours) for a High/Critical incident is: 4 hours. |  |  |
| **3.2** | **Maintenance** | | |
| 3.2.1 | The contractor shall maintain and update throughout the duration of contract:  • any virtualisation technology (if applicable);  • the operating system (security patches, bug fixes, updates);  • the component applications of e-Net (security patches, bug fixes, updates) |  |  |
| 3.2.2 | The contractor shall liaise with CEPOL for the planning of scheduled downtime. Scheduled downtime should not exceed 4 occasions a year for a maximum of 6 hours |  |  |
| **3.2.3** | **Systems administration** | | |
| 3.2.3.1 | The contractor shall apply, throughout the duration of the contract, server system administration policies and procedures including software upgrade and patch application, capacity monitoring/management and change control. |  |  |
| 3.2.3.2 | The contractor shall apply, throughout the duration of contract, server system administration policies and procedures that govern the backup/restore processes including, backup tools used, retention cycles and policies, frequency, restore procedures, backup validation procedures, and off-site storage facilities and processes |  |  |
| 3.2.3.3 | The contractor shall apply, throughout the duration of contract, policies and procedures to ensure that the administration of the CEPOL e-Net is sufficiently protected from unauthorised access and system attacks |  |  |
| 3.2.3.4 | The contractor shall ensure that all webservers have Extended Validation SSL certificates. |  |  |
| **3.2.4** | **Network administration** | | |
| 3.2.4.1 | The contractor shall provide, throughout the duration of the contract, a managed network supported by defined policies and procedures to ensure the security and availability of the CEPOL e-Net |  |  |
| 3.2.4.2 | The contractor shall provide, throughout the duration of the contract, network monitoring and the supporting processes and procedures for the assessment of network capacity and ensuring sufficient capacity |  |  |
| **3.2.5** | **Application Management** | | |
| 3.2.5.1 | The contractor shall provide user rights administration services for the designated CEPOL staff |  |  |
| 3.2.5.2 | The contractor shall maintain and update the component applications of e-Net throughout the duration of contract (security patches, bug fixes, updates) |  |  |
| 3.2.5.3 | The contractor shall apply component application updates in a coordinated and planned maintenance approach |  |  |
| 3.2.5.4 | The contractor shall ensure that all updates of the component applications are tested before rolling out into production |  |  |
| 3.2.5.5 | The contractor shall advise on upgrades. The contractor shall proactively monitor open source application (TYPO3, Moodle, DSpace, CAS) websites and advise on the impact/benefit to CEPOL |  |  |
| 3.2.5.6 | The contractor shall implement upgrades only on approval of CEPOL |  |  |
| 3.2.5.7 | The contractor shall ensure that application change control is conducted according to defined processes and procedures |  |  |
| **3.3** | **Service Level Requirements** | | |
| 3.3.1 | The contractor shall ensure the achievements of the defined Service Level performance indicators |  |  |
| **3.4** | **Reporting** | | |
| 3.4.1 | The Contract shall provide monthly reports to be submitted on the hosting, support and maintenance of the e-Net system |  |  |
| 4 | **Carry-over of services at the end of the contract - Succession** | | |
| 4.1 | The contractor shall undertake to support transition at the end of the contract (mandatory requirement). The foreseen services shall include supporting the migration of data to the next version of e-Net. |  |  |
| **Number of mandatory requirements with confirmed compliance** | |  |  |
| **Number of mandatory requirements with non- compliance** | |  |  |
| **Signature of authorised tenderer representative** | |  | |

**Part 2: Technical proposal – description of the proposed services**

**1. MIGRATION FROM CURRENT CONTRACTOR**

|  |  |
| --- | --- |
| **Ref.** | **Description of the proposed services** |
| 1.1. | Please describe below the approach and methodology that will be used to manage the migration of the e-Net from the current supplier to your new environment and the entry into service. Please explain how “no loss of data” and “maximum scheduled downtime of 48 hours” requirements will be ensured. |
| 1.2. | Please provide a migration plan covering in particular the following aspects:  - Definition of migration roles, responsibilities and milestones;  - Migration time-frame in calendar days. |

**2. HOSTING**

|  |  |
| --- | --- |
| **Ref.** | **Description of the proposed services** |
| **2.1. Hosting solution** | |
| 2.1.1 | Please describe the hosting solution offered. |
| 2.1.2. | Please provide the address of the Data Centre where the e-Net will be hosted. |
| 2.1.3. | Please state the service restore time in the event that restoration of a back-up is required (the service restore time is the time needed by the contractor to provide a solution to restore the service). |
| **2.2. Physical environment** | |
| 2.2.1. | Please describe the Data Centre physical environment offered and demonstrate how it meets and exceeds (if applicable) the requirements specified in Section B.1.3.a. “Main services” paragraph 2.3 “Physical environment” of the tender specifications. |
| **2.3. Capacity management** | |
| 2.3.1. | Please describe the capacity management provisions offered and demonstrate how they meet and exceed (if applicable) the requirements specified in Section B.1.3.a. “Main services” paragraph 2.4 “Capacity management” of the tender specifications. |
| **2.4. Hardware** | |
| 2.4.1. | Please detail the hardware specifications for the proposed hosting solution. |
| 2.4.2. | Please describe the policy applied for maintaining the proposed hardware. |
| **2.5. Data Centre connectivity** | |
| 2.5.1. | Please detail and quantify the Data Centre connectivity including the bandwidth plan for unexpected traffic surges. |
| **2.6. Security** | |
| 2.6.1. | Please describe which documented security policies and procedures you will apply to ensure the physical and technical security of the data centre facilities; this should include firewall(s), vulnerability management, intrusion detection and denial of service attacks (both DOS and DDOS). |
| 2.6.2. | Please describe the measures adopted to ensure that blacklisting is avoided and the countermeasures available in the case of another datacentre user undertaking activity that leads to host blacklisting. |

**3. Support**

|  |  |
| --- | --- |
| **Ref.** | **Description of the proposed services** |
| 3.1. | Please describe how the support to CEPOL staff will be organised and demonstrate how the offered service meets and exceeds (if applicable) the requirements specified in Section B.1.3.a. “Main services” paragraph 3.1 “Support to CEPOL staff” of the tender specifications. |
| 3.2. | Please describe your incident management policies and procedures in place that detail how problem/issue escalation is handled and measured. |

**4. Maintenance**

|  |  |
| --- | --- |
| **Ref.** | **Description of the proposed services** |
| 4.1. | Please describe how the maintenance will be organised and demonstrate how the offered service meets and exceeds (if applicable) the requirements specified in Section B.1.3.a. “Main services” paragraph 3.2. “Maintenance” of the tender specifications. |
| 4.2 | Is the development/test environment separated from the production environment? Is access for the designated CEPOL staff to the development/test environment provided? |
| **4.2. Systems administration** | |
| 4.2.1. | Please describe the server system administration policies/procedures, including software upgrade and patch application, capacity monitoring/management and change control, which will be applied throughout the duration of the contract. Please describe your backup policy. |
| **4.3. Network administration** | |
| 4.3.1. | Please describe how you will provide network monitoring and the supporting processes and procedures for the assessment of network capacity and ensuring sufficient capacity. Is read access to system/network monitoring tools provided? If yes, please provide details. |
| **4.4. Application Management** | |
| 4.4.1. | Please describe your approach to the maintenance and update of the component applications of e-Net throughout the duration of contract (security patches, bug fixes, updates). |
| **4.5. Application Management** | |
| 4.5.1. | Please explain how you will ensure that application change control is conducted according to defined processes and procedures. |
| **4.6. Production/Development/Test environment** | |
| 4.6.1. | Please explain how your production environment will be separated from development/test environment. |
| **4.7. Access to Development/Test environment** | |
| 4.7.1. | Please describe how access to development/test environment will be provided to designated CEPOL staff. |

**5. Service Level Requirements**

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref.** | **Performance indicator** | **Required by CEPOL** | **Offered by tenderer** |
| **5.1 Performance indicators** | | | |
| 5.1.1. | Effective (Application) Availability | 99% per month |  |
| 5.1.2. | System Availability | 99.50% per month |  |
| 5.1.3. | Server Availability | 99.70% per month |  |
| 5.1.4. | Network Availability | 99.80% per month |  |
| 5.1.5. | Scheduled downtime window | * Friday 23:59 to Sunday 23:59 (Budapest Time) |  |
| 5.1.6. | Average Response time to open support ticket | * Low: 4 working hours * Medium: 3 hours * High/Critical: 1 hour |  |
| 5.1.7. | Maximum resolution time | * Low – 48 hours * Medium – 12 hours * High/Critical – 4 hours |  |
| 5.1.8. | Server connectivity | * At least 100 mbps per server unmetered traffic |  |
| 5.1.9. | Performance:  Response time  (The contractor shall measure responsiveness of the hosting components within the data centre in front of the application. The reference pages shall be the main CEPOL page.) | * Average response time less than 1 sec * A maximum of 5% of the requests may exceed 2 sec |  |

**6. Reporting**

|  |  |
| --- | --- |
| **Ref.** | **Description of the proposed services** |
| 6.1. | Please describe how the reporting will be organised and demonstrate how the offered service meets and exceeds (if applicable) the requirements specified in Section B.1.3.a. “Main services” paragraph 3.4. “Reporting” of the tender specifications. |
| 6.2. | Will access to online reporting systems that will allow it to view the applications’ performance including statistics relating to hits, unique visits per page etc. be provided to designated CEPOL staff? If yes, please provide details. |