Annex 13 - Distinctive Technical Requirements

The following technical requirements apply for the required services. These technical requirements are distinctive. The quality of the response provided will be awarded.

|  |  |  |
| --- | --- | --- |
| **Interfaces** | **Yes/No/NA** | **Explanation**   * Explanation is **mandatory,** * A **maximum** of **200 words** per explanation is allowed * S**creenshots** are **allowed** |
| Interfaces between trusted and non-trusted networks must preferably be secured in the following way:  - Channel encryption by means of a PKI-SSL certificate  - Device authentication by means of a PKI certificate  - Filtering based on IP-numbers  - Segmentation of networks with different security levels  - Intrusion detection  - (Technical) logging |  |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| **Access Rights** | **Yes/No/NA** | **Explanation**   * Explanation is **mandatory,** * A **maximum** of **200 words** per explanation is allowed * S**creenshots** are **allowed** |
| The Tender shall provide upon request a description of the qualifications of the personnel that has access to or can have access to the systems where data of FMO are present. |  |  |
|  |  |
| There shall be a strict segregation of duties between e.g. a person that has both regular access and system administration access. Administration and functional usage should be separated. |  |  |
| There are measures applied to prevent the threat of information misuse by personnel and (sub-)contractors e.g. the illicit access to services and data should be prevented. |  |  |
| The Tender shall have demonstrable controls in place concerning strong user authentication for access to data. Tenderer shall demonstrate upon request a description of the means of user authentication for access to data (username/password/additional authentication/SMS/token/biometrics) and to which specifications these comply (password maximum 7 characters, capitals, lower case, numerical or special characters). |  |  |

|  |  |  |
| --- | --- | --- |
| Security | Yes/No/NA | Details / Explanation   * Explanation is mandatory, * A maximum of 200 words per explanation is allowed * Screenshots are allowed |
| There are measures applied to prevent the threat of information disclosure to unauthorized parties. |  |  |
| Direct connections with local hardware during remote sessions is not allowed e.g. no use of usb ports during remote sessions |  |  |
| There are measures in place to mitigate the threat of a hacker or malware. The Tender provides upon request a copy of the maintenance and/or licensing agreements with suppliers concerning Antivirus, Firewall, IDS, IPS, Encryption software |  |  |
| Tenderer will provide periodically an overview of the license-compliancy for the environments that are used by FMO. |  |  |
| The Tender will provide upon request information about process hardening (for example disabling unused services, etc.) so that all ICT-components are hardened against attacks. |  |  |
| The Tender shall apply up-to-date e-mail (and DNS) security measures, like specified by IBD and NCSC. Standards are amongst others (but not limited to) TLS, DKIM, DMARC, DANE, DNSSEC |  |  |
| The Tender has demonstrable measures in place to minimize the chance of interception of data in transit by unauthorized parties. |  |  |
| SSL2/SSL3 security protocols are not allowed (also not from IBD), the current demand is in the direction of TLS (1.0/1.1/1.2 and later) security protocols. Currently TLS 1.0 is sufficient. |  |  |
| When FMO finds it necessary the use of certificates shall be supported |  |  |
| The applications and data of FMO shall at all times be separated of the applications and data of other parties. |  |  |
| Prior to implementation the requirements concerning confidentiality, integrity and availability (CIA) need to be adapted between FMO and supplier. In this way appropriate controls and service levels can be established and maintained. |  |  |
| Tenderer has demonstrable operational controls to tackle the risk of theft or loss of data. Tenderer shall provide upon request a description of active controls for access management (e.g. who has physical access to servers/applications/data, which access controls are in place, is there monitoring and alerting) and possible fire prevention for the IT systems used in the execution of this task. Tenderer shall provide upon request a description of the back-up procedure wherein is clear that data loss can amount to maximum one working day. |  |  |
| If there is personal data involved in using cloud services, the Tender shall comply with GDPR. |  |  |
| Generic accounts shall be limited as much as possible. For administrator tasks with administration rights and possible high risks the 4-eyes principle needs to be applied. |  |  |
| Passwords shall be stored safely. |  |  |
| The cooperation with value chain partners will become more important. The exchange of information (files) and access to data-sources shall be managed properly. For confidential information, encryption is optional. For secret data, encryption is mandatory. |  |  |
| The Tenderer shall provide upon request a detailed description about their definition of an incident. |  |  |
| The Tenderer is obliged to report high risk security incident within one day to FMO. The provider is obliged to provide upon request information about specifics that have occurred. |  |  |
| The Tenderer is obliged to solve security incidents as soon as possible, however at a maximum of 5days. |  |  |
| Software licenses - what is licensed and is it allowed to use this license in the cloud - shall be clear upfront. The Tenderer shall provide upon request an overview of the license compliancy of the systems where FMO data is located. |  |  |
| Conversion of data: data shall be offered in an open standard format, like defined upfront by the requestor of FMO. |  |  |
| The sanitization of data after contract termination shall only be executed with prior approval of FMO. |  |  |
| FMO has the right to access logging data. When FMO uses a central logging infrastructure the logging of the Tenderer shall - where possible - have the possibility to interface with the central logging of FMO. |  |  |
| The Tenderer and (when applicable) the data hosting party shall not have ties/locations based in the United States. When this is the case, the parties shall comply to the EU/US Privacy Shield or similar/successive alternatives. Information shall be provided which governments or jurisdictions can claim the data of FMO. The Tenderer shall communicate relevant laws. |  |  |
| Tenderer shall provide upon request a schematically, technically complete description of the needed connections between FMO and users and the environment of the Tenderer (as well as the possible hosting provider / datacenter) |  |  |
| Tenderer shall provide upon request a schematically, technically complete description of the needed connections. This consists of which connections are established, way of access, names of servers, type encryption on these connections (e.g. TLS with certificates), over which ports the traffic is routed, IP-addresses, encryption of stored data. |  |  |
| Tenderer shall provide upon request a schematical overview of the cloud components and their coherence. It must be clear where the data is located (in Europe) and where applications are running. A division is essential in this sense. Cloud services where data and applications are intertwined are not allowed. A cloud service should be fully replaceable while the same data is being used. |  |  |
| Tenderer shall perform an annual disaster test and present the results to FMO. |  |  |
| Tenderer shall not make radical changes to the architecture without prior notice (and approval) of FMO (e.g. change of the back-up procedure or the location where the back-ups are stored). |  |  |