OPEN CALL FOR TENDERS

*concludes with a **single Framework service contract***

Tender Documentation

Web Development services

ENISA F-EDO-23-T06

Part 1 Introduction to ENISA

Part 2 Terms of Reference

Part 3 Tender Specifications

Annex I	Legal Entity & Financial ID Forms
Annex II	Simplified Financial Statement form
Annex III	Declaration on honour on exclusion criteria and selection criteria
Annex IV	Financial Offer form
Annex V	Draft Framework Service contract
Annex VI	Power of Attorney for Consortium Forms
Annex VII	Sub-Contractors Form
Annex VIII	Administrative ID and Declaration form
Annex IX	Daily Allowances
Annex X	Description of tasks per Profile

e-Submission

*Offers via e-Submission portal **ONLY***

CONTENTS

PART 1 ABOUT ENISA

1.1 INTRODUCTION

The European Union Agency for Cybersecurity (ENISA) was established by the European Parliament and the Council Regulation (EU) No 2019/881 of 17 April 2019 (OJ L 151/15, 07.06.2019). ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow.

1.2 SCOPE

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure.

The permanent mandate and enhanced role of the Agency established by the 2019 EU Cybersecurity Act (CSA) and ENISA's new strategy are two milestones that mark an unprecedented and exciting period in the 17 years of the Agency´s life. ENISA aims to build from these two success stories and continue to raise cybersecurity awareness in the EU public fora. In addition, as regards to Article 3 (1c) of the MB decision MB/2020/9 planning, coordinating and implementing communication and outreach activities, the Agency needs to support the necessary activities to fulfil tasks as set out in Art. 21 and 23 of the CSA.

In order to do so the Agency's communications sector supports the implementation of the Agency's Annual Work Programme and has developed a Multi-Annual Communication Strategy and a brand positioning strategy. The strategy lists the steps that the Agency needs to undertake to strengthen its existing communication activities and credibility among its key stakeholders while serving its strategic and policy goals.

1.3 OBJECTIVES

The Agency's objectives are as follows:

- ENISA shall be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks.
- ENISA shall assist the Union institutions, bodies, offices and agencies, as well as Member States, in developing and implementing Union policies related to cybersecurity, including sectoral policies on cybersecurity.
- ENISA shall support capacity-building and preparedness across the Union by assisting the Union institutions, bodies, offices and agencies, as well as Member States and public and private stakeholders, to increase the protection of their network and information systems, to develop and improve cyber resilience and response capacities, and to develop skills and competencies in the field of cybersecurity.
- ENISA shall promote cooperation, including information sharing and coordination at Union level, among Member States, Union institutions, bodies, offices and agencies, and relevant private and public stakeholders on matters related to cybersecurity.

- ENISA shall contribute to increasing cybersecurity capabilities at Union level in order to support the actions of Member States in preventing and responding to cyber threats, in particular in the event of cross-border incidents.
- ENISA shall promote the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market. ENISA shall contribute to the establishment and maintenance of a European cybersecurity certification framework in accordance with Title III of this Regulation, with a view to increasing the transparency of the cybersecurity of ICT products, ICT services and ICT processes, thereby strengthening trust in the digital internal market and its competitiveness.
- ENISA shall promote a high level of cybersecurity awareness, including cyber-hygiene and cyber-literacy among citizens, organisations and businesses.

2. ADDITIONAL INFORMATION

Further information about ENISA can be obtained on its website: www.enisa.europa.eu.

PART 2 TERMS OF REFERENCE

I. SCOPE OF THIS TENDER

By means of this Call for Tenders ENISA seeks to conclude a single framework service contract with an economic operator capable of providing a wide range of web development services to support ENISA's main website and several ENISA portal sites as stipulated in the chapters outlined below.

The prospective contractor is also expected to plan and execute the migration of the main ENISA's websites and portals from the current infrastructure (together with the previous contractor) to a new cloud infrastructure based on Microsoft Azure.

ENISA uses various digital communication channels. The ENISA website is an important communication tool to get its message across to government organizations, businesses and citizens across Europe. The scope of this tender includes ENISA's main website (www.enisa.europa.eu) and several ENISA portal and event sites, i.e. extranets dedicated to specific user groups (for example, working groups, groups of stakeholders, etc.) collaborating with ENISA.

Both the website and the portals are based on the PLONE Content Management System; therefore, the tenderers shall demonstrate experience and have in-depth knowledge of CMS platforms and PLONE in particular. ENISA plans to migrate its websites and portals from PLONE to DRUPAL in the coming years, so additional experience with DRUPAL is also required for possible new developments and support with the migration.

Given the nature of ENISA's work and focus on cybersecurity, the security of the websites is crucial and so security should receive maximum attention).

Subject of the tender	Maximum budget
Web Development Services	A maximum budget of **€2.400.000,00 (two million and four hundred thousand euro)** over the maximum possible period of **4 years**
Last date for dispatch of offers	**31st March 2023 until 18:00 CEST**
PLEASE NOTE: *In the case where unforeseen circumstances result in this contract being consumed faster than originally planned, the Agency reserves the right to consider conducting a 'Negotiated procedure without prior publication of a contract notice' with the existing contractor in order to increase the maximum amount stated above by* ***up to 50%.*** *This procedure being fully in accordance with Article 164(4) and Annex I - point 11.1(e) of the EU Financial Regulation (FR)).* **PLEASE NOTE:** *This tender procedure is limited to tenderers which are legally incorporated or which have an incorporated subsidiary in a member state of the European Union/EEA as well as SAA countries[1] . The Agreement on Government Procurement (GPA) does not apply to EU Regulatory Agencies and as such, ENISA cannot accept offers from legal entities based in 'third countries'.*	

[1] Under the Stabilisation and Association Agreements (SAA) economic operators established in FYROM, Albania, Montenegro, Serbia, Bosnia and Herzegovina and Kosovo have been granted access to procurement procedures of the Union institutions, agencies and bodies.

IMPORTANT: For entities outside the EU (including UK based entities): *The United Kingdom is now considered a 'third country by the European Union'. ENISA cannot therefore accept submissions from legal entities based in the UK, nor can a UK legal entity be nominated as part of a consortium. Subcontracting of UK (and other third country) entities is allowed. In these cases, any transfer of personal data to third countries shall only take place after prior authorisation of ENISA and shall fully comply with the requirements laid down in Chapter V of Regulation (EU)2018/1725.*

Method of submitting tenders: 	***e-Submission portal***	***YES***
	Courier or postal service	*NO*
	By hand	*NO*
	By email	*NO*

1. OVERVIEW OF THE CURRENT ENISA IMPLEMENTATION

DOMAIN, SUBDOMAIN AND URL STRUCTURE

The main ENISA website is at https://www.enisa.europa.eu which is a Plone CMS instance.

The websites and portal under the scope of this FwC are mentioned below:

Category	Number of implementations	URL	Comment
Website	11	https://enisa.europa.eu	Main ENISA website
		https://privacyforum.eu	+ pages for previous years https://2012.privacyforum.eu, ..., https://2021.privacyforum.eu)
		http://ecsc.eu	ECSC Challenge main website
		https://challenges.ecsc.eu	ECSC supporting website
		https://icc-games.com/	ICC main website
		https://csirtsnetwork.eu/	Currently static to be migrated to PLONE
		http://cybersecuritymonth.eu	ECSM main website
		https://resilience.enisa.europa.eu	Community information
		https://ciras.enisa.europa.eu	CIRAS infrastructure for incident reporting (restricted access) and for the public (visual tool)
		Certification website	
		https://opencsam.enisa.europa.eu/	OpenCSAM The Open Cyber Situational Awareness Machine (OpenCSAM) is an innovative tool that has been developed to facilitate the tasks of cyber situational awareness and incident response both for the EU Institutions and the Member States.
		https://staging.infohub.enisa.europa.eu/	Information Hub and prototype portal
Portals	7	https://mbportal.enisa.europa.eu	Restricted for the community
		https://ag.enisa.europa.eu	Restricted for the community
		https://nlos.enisa.europa.eu	Restricted for the community
		https://cyclone.enisa.europa.eu	Restricted portal, hosted by ENISA, need for development and support and maintenance
		https://qcc.enisa.europa.eu	Restricted portal, hosted by ENISA, need for support and maintenance. The same server as the cyclone portal
		https://mmchat.enisa.europa.eu	Restricted portal, hosted by ENISA, associated chat messaging service to the cyclone portal. Need for development, support and maintenance.

		https://collabora.enisa.europa.eu	Restricted portal, hosted by ENISA. Need for support and maintenance. Server used for online editing purposes in the mmchat server.
Web Tools	21	https://www.enisa.europa.eu/tools	21 tools are currently publicly available under enisa.europa.eu

CURRENT HARDWARE INFRASTRUCTURE

The majority of ENISA's websites and portals (including ENISA's main website) are being hosted in servers physically located in a datacenter in Bucharest, Romania in the Agency's current contractor's premises. A number of ENISA's portals (see above) are also hosted directly by ENISA in a cloud infrastructure.

ENISA is currently implementing an infrastructure of two host servers responsible for the production service.

Each of them has the following architecture:

- 2 x 16 Core 3.0Ghz, 155W, 64bit Processors
- 128 GB DDR4 RAM
- 4 x SSD 2 TB
- 2 x Quad Gigabit LAN
- 1000W Redundant (1+1) Power Supplies

TECHNOLOGIES USED

The website and portal servers are built using the following technologies:

Web application firewall:

- FORTINET Web Application Firewall – FortiWeb 400D

Virtualization:

- KVM virtualisation
- VMware (used by ENISA)

Operating system:

- CentOS Linux release 7.7.1908 (Core)

Applications layer specific technologies:

- Monitoring service nrpe (client for Icinga2 monitoring system)
- Zope 4.5.5
- Amavis and Clam deamon as antivirus for uploaded files
- ZEO database
- Apache/ (CentOS)
- Matomo analytics platform

- Maria DB for Matomo
- Docker server / containers (happroxy, Zeo, Zope)
- Plone 5.2.4 built on top of the Zope application server
- ZODB, database used by Zope
- Splunk for logs collection
- Frontend technologies HTML5, CSS3, and JavaScript, REST API.
- Architectures oriented to the Front-end and web products (ex. Angular, NodeJs, Flask).

Integration engines and Big Data infrastructures:

- Container technology (Docker, Docker-compose).
- Continuous integration systems (Jenkins, etc.).
- ElasticSearch/Logstash/Kibana (ELK stack)
- Manipulation of exchange formats (XML, JSON), SOAP web services.

NLP and ML algorithms:

- Machine Learning, Deep Learning, Natural Language Processing, Natural Language Generation, Text Summarization, Text Simplification, etc.
- NLP and ML libraries such as NTLK, Stanford NLP, Spacy, Sklearn and other toolkits.
- Usage of taxonomies/ontologies in data harvesting
- Unstructured textual data.

2. DESCRIPTION OF SERVICES TO BE PROVIDED

The services that may be required during contract implementation are listed in the following paragraphs. They shall be understood as the minimum service requirements.

The tenderer is allowed to propose additional or higher level service requirements in their offer. In this case, should the proposal be accepted, the tenderer will be bound to its proposal of higher service levels (and the tenderer cannot afterwards refer to the minimum requirements as set out in this section).

2.1 WEB HOSTING MANAGEMENT SERVICES (INFRASTRUCTURE MIGRATION AND MAINTENANCE)

The prospective contractor is not expected to offer web hosting services. ENISA's websites and portals (that are not already hosted by ENISA) will be moved within 2023, from their current dedicated infrastructure in Romania to a cloud-based solution (Microsoft Azure) owned by ENISA.

Migration

The current dedicated Virtual Machines, will be rebuilt in an Azure Subscription. Additionally, the setup shall support a Disaster Recovery site in a second Azure Region. The prospective contractor is expected to support the setup of the service in this new Azure based infrastructure (together with the previous contractor).

The new infrastructure shall use Azure native services as much as possible especially regarding to security, networking and availability (Azure firewall, Azure Application gateway with WAF, Azure backup, Azure recovery site, etc.)

The prospective contractor is expected to:

- Review and evaluate the current architecture and propose changes/additions/improvements where/ if applicable to the architecture taking into consideration the advantages and limitations of the new cloud infrastructure and ENISA's security and other requirements.
- Plan and execute the migration from the current infrastructure (together with the previous contractor) and test the service functionality after the migration. A detailed migration plan with a breakdown of the relevant tasks and timeline should be included as part of the offer submitted for this tender.
- Work together with the current ENISA's contractor and ENISA's web project manager(s), ISO, and System Administrator in order to successfully finalise this project fulfilling ENISA's requirements regarding security, downtime etc.

The ability of the prospective contractor to provide assistance on the implementation of a relevant data protection risk assessment for the move to the cloud prior to the migration to the new infrastructure will be considered highly advantageous.

Maintenance

The prospective contractor shall also draft the ICT procedures needed for the operation of the service on Azure as well the day-to-day ICT operations (backups, disaster recovery tests, security updates, other software updates, network and application gateway configuration changes, etc.)

The contractor shall finally also have the full responsibility of the ICT operations related to the service, given that the service will be hosted on Azure cloud.

At least two profiles for a system administrator shall be provided with experience and expertise with Microsoft Azure. Certified Azure engineers CVs, like Microsoft Azure Administrator Associate, Microsoft Azure Developer Associate, Azure Stack Hub Operator Associate, Microsoft Azure Security Engineer Associate, Microsoft Azure Solutions Architect, Microsoft DevOps Engineer, are advantageous to be submitted.

2.2 PRODUCTION AND ACCEPTANCE TEST ENVIRONMENTS

Two separate environments are always required: a production environment and a test environment. The prospective contractor is responsible for making sure that the two environments are identical. In case of real data use on the test environments the security requirements of the test environments are exactly the same as the production environment.

The test environment will be used by ENISA to check and test new developments, changes and bug fixes before deploying them in the production environment. The test environment will also be used by ENISA to run intrusive tests, like vulnerability scans, and performance/load tests.

Logical access to the test environment should be restricted to designated IP addresses.

2.3 AVAILABILITY AND RESPONSE TIME

The minimum service levels for availability and response time shall be as following:

- A minimum availability of 99% must be guaranteed. Availability is to be measured monthly as the number of total available hours divided by the measurement period.
- Planned downtime must be agreed with the Agency at least 3 days prior to the scheduled date, and should be scheduled between 20:00 CET and 06:00 CET. Planned downtime should not exceed two hours per month. For urgent cases, direct contact with ENISA must be made via telephone to the assigned ENISA contact person (or his/her backup) beforehand.
- Average server response time should be less than 1 second (first byte). Average network time should be less or equal to 3 seconds.

The prospective contractor shall measure and report about availability and response times (see Monitoring and reporting) and corrective measures – if applicable should be agreed with ENISA. The measurement of response time should be done in such a way that measurement is representative for normal usage, for example using a probe located in another city or country. Measurements should reveal the average response time

The contractor shall report about these measurements in the monthly reports (see section 2.7 Monitoring and reporting).

2.4 BACKUPS

The minimum backup requirements are the following:

- Daily backups must be made and kept for 8 days.
- Weekly backups must be made and kept for 35 days.
- Monthly backups must be made and kept for 6 months.
- Backup restore requests should be handled within a maximum of 12 hours.

The contractor should test backups regularly by testing the backup restore procedure. The contractor should report about success or failure of these tests in monthly reports (see section 2.7 Monitoring and reporting).

2.5 PATCHING AND UPDATES OF SERVERS

The requirements around patching and updates of servers are described below and are based on ENISA's patching policy:

Scale	Details
Critical	As soon as possible for Internet facing systems/ between 7-14 calendar days for internal systems
High	30 days
Medium	90 days
Low	120 days

In particular, critical OS/Server/Application updates and security patches for publicly facing services must be deployed within 12 hours of their public release.

Normal updates to be performed on a weekly basis. ENISA should be notified prior to each update or patch and all patches and updates should be tested first on a testing environment and then deployed to production.

It is foreseen that the prospective contractor will update on a regular basis outdated libraries and dependencies used by the websites and portals (e.g. JavaScript libraries).

The contractor should report about deployed updates and patches in the monthly reports (see section 2.7 Monitoring and reporting).

Updates/patches to be applied first to the test environment and then to the respective production one.

2.6 TESTING AND SCANNING

The requirements around testing and scanning are the following:

- The contractor shall periodically test for dead links across the website and portals;
- The contractor shall carry out vulnerability scans periodically, to identify software vulnerabilities in the deployed operating systems or applications. The results of these scans must be reported to ENISA within 5 working days. Serious vulnerabilities should be reported to ENISA immediately;
- Independent vulnerability scans will be performed by ENISA annually in consultation with the contractor;
- The contractor shall perform load or performance tests periodically.

The contractor shall report about the results of these tests and scans in the monthly reports (see section 2.8 Monitoring and reporting).

ENISA can also perform penetration tests at a given and predefined time after notifying the contractor. With the penetration testing ENISA will evaluate the security of the IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities may exist in operating systems, service and application flaws, improper configurations etc.

2.7 MONITORING AND REPORTING

The contractor shall monitor service levels continuously and report about them monthly. Indicatively, the service level reports should address the following items – for the website and the portals separately:

- Overall availability;
- Average response time during the day (hourly averages);
- Average response time per day;
- 404 responses (page not found) per day;
- Number of page hits per day;
- Tests;
- Dead links;
- Security scan results;
- Load test results;
- Backups restore test results

In addition to monitoring services performance (eg used CPU, memory, processes etc), the contractor should be able to collect security events and feed with the required logs Azure logs monitoring services like Sentinel, MS Defender.

Alternatively, the tenderer could offer a dashboard, instead of using monthly reports.

2.8 SECURITY

Secure administration

- Access control: Establishing strict access controls to ensure that only authorized individuals are able to access sensitive systems and data. Including implementing multi-factor authentication, role-based access controls, and regularly reviewing and revoking access permissions for former employees or contractors.
- Password management: Having a robust password management policy in place can help to prevent unauthorized access to systems and data. This can include requiring strong, unique passwords for all accounts, regularly updating passwords, and implementing a password manager to securely store and automatically generate passwords.
- Least privilege: The principle of least privilege states that users should only have the access rights and permissions that are necessary to perform their job functions.

Security architecture

- 3-tier architecture must be in place.
- Adequate network segmentation is in place.

Secure code development

- Any custom developed application must be created using well established secure coding guidelines (e.g. Owasp for WebApp, DigIT secure coding guidelines, SDLC, NIST)
- Proof of adherence to the guidelines must be made available after finalization of the development.

Network and application level protection

- Mandatory stateful firewall must be in place.
- Application level protection such as Web Application Firewall must be in place.

- Distributed denial of service must be in place in front of ENISA portals and websites

Security hardening

- Operating system and server software must be hardened according to known security baselines (e.g. CISecurity, Microsoft, NIST)

Mandatory logging and monitoring

- Network, web application firewall, firewall, server and OS level relevant security logs must be centrally collected in SIEM platform.
- The collected logs and alerts must be regularly monitored by a designated person.

Incident response

- The prospective contractor must have well-defined incident response plan in place, that outlines the steps to be taken in the event of a security incident, including reporting procedures and communication protocols.

Penetration testing & red teaming

- The contractor conducts penetration testing and red teaming assessments on their infrastructure as well as on ENISA's.
- Regular penetration tests are foreseen, especially after large development cycles of the Application.

Patching & Vulnerability management

- Periodic vulnerabilities scans are conducted and critical findings are addressed in a timely manner
- Regular patching and maintenance take place.
- Patching of critical/high vulnerabilities are prioritized according to ENISAs patching policy.

Backup and recovery

- Maximum Tolerable Downtime, Recovery Point Object, Recovery Time Objective to be defined with ENISA.
- Business continuity and disaster recovery plans are available and regularly tested.

3 SERVICE REQUIREMENTS FOR WEB DEVELOPMENT

Web development will be requested on a case-by-case basis with requests varying from simple bug fixing, small tasks and enhancements to major web development projects. The contractor shall identify and shall apply appropriate modern technologies and techniques for the web development that will improve and optimize overall, all web-based products of ENISA.

ENISA will provide a functional or technical specification of a new development, new project or a simple change needed and the methodology to be followed will be decided on a case-by-case basis. All basic information, requirements and basic business case will be included as part of the functional specifications sent to the service provider. In each case and depending on the overall complexity of the project, ENISA will provide the service provider, with the project's overall scope, UI general requirements, desired functions, tentative timeline (and required delivery deadline –when relevant)

Web development projects (requests for proposal)

Taking into consideration the complexity of the project, the contractor is expected to provide a preliminary business analysis, a risk assessment, a project plan and a quotation of the amount of work needed (in person hours), a timeline for delivery, and the total costs.

Analysis of business requirements and transposition to technical requirements of most complex tasks/projects (i.e. production of a new tool/web application/website), workflows and wireframes are expected to be done by the contractor as part of the overall web development project. The contractor is also expected to share its expertise on the analysis phase with ENISA project managers in order to facilitate the whole project management flow and assure the end result will reflect all the needs ENISA has on business level. A section that identifies project risks must always be included in the analysis of the contractor at the initial stage.

3.1 DESCRIPTION OF TASKS (WEB DEVELOPMENT PROJECTS)

The contractor will need to perform a number of tasks towards the delivery of each major development (i.e. production of a new tool/web application/website). In this section, a short description of the tasks can be found.

During the project initiation, the contractor will be asked to provide a detailed project plan together with a relevant timeline of the project flow (e.g. Gantt chart) and key milestones that will be agreed with ENISA. Project management methodology (i.e. waterfall or agile methodology) should be the point of reference for all major web development projects. The methodology to be used in each project will be defined by the project manager of ENISA and the contractor should be able to follow both methodologies. Depending on the complexity of the project, all steps of project management shall be followed including validation checks and all have to be applied in every major project depending on the project management methodology.

To this end, the activities mentioned in this section contain an indicative framework for the entire project and will be refined during the project, when deemed necessary.

- **Activity 1:** Set up the project scope
- **Activity 2:** Develop interaction model for the web application/tool – including the development of wireframes/mock ups.
- **Activity 3:** Development of necessary functions
- **Activity 4:** Testing (functional and non-functional)
- **Activity 5:** Deployment
- **Activity 6:** Documentation
- **On-going Activity:** Project Management

In parallel, ENISA will make sure to provide crucial deliverables, feedback, and other necessary information on time for the delivery of web development projects/tasks or to inform the service provider in case of delays.

3.2 SECURITY BY DESIGN

Given the nature of the agency's work/focus, it is of paramount importance that ENISA's environment remains as secure as possible at all times. Security mechanisms, secure functions and security good practices in both coding, configurations and connections shall be utilised to ensure application level security. Corresponding safeguards, e.g., ISO27001 compliance, etc. shall be considered an advantage.

3.3 COMPATIBILITY

Web development shall always apply cross-platform and responsive design, meaning that all ENISA websites and web apps are mobile friendly. The contractor shall use all cutting-edge frameworks or boilerplates to satisfy that need and provide always web solutions that reflect the current trends.

The prospective contractor shall ensure and monitor that the website, portals and tools are accessible from (at least) the top five desktop and mobile browsers and applications. Requirements set in section 2. refer to all these browsers and applications.

Service requirements specified in Section 3 shall be met by the contractor wherever applicable to web development and software, e.g. patching, backups, testing and scanning, monitoring and reporting, availability and response time.

4. PROJECT TEAM

The organisation of the project team is a key feature and it is fundamental for delivering the expected results within the defined timeframe.

The required experience and qualifications of the team members should be explicitly reflected in their CVs, which are to be included in the tenderer's offer (as referred in these Tender Specifications). The tenderers need to ensure that the team has a sufficient number of members and fulfils the requirements listed below in terms of qualifications and experience.

For the duration of this Framework Contract, a management team consisting of ENISA and the contractor's project managers will be established and will be responsible for managing the implementation of the Framework Contract and specific contracts/order forms. This team will work together for establishing common understanding of the specific project scopes, facilitating

communication between ENISA, the contractor and external stakeholders of the project and overall establishing a transparent environment and the conditions for fruitful cooperation.

The day-to-day work regarding the execution of the tasks foreseen under the specific contracts/order forms will be carried out by the contractor and managed by the contractor's project manager. The contractor will be responsible for providing all the necessary resources for carrying out the tasks successfully.

The profiles listed below are the team members the contractor should have available **as a minimum,** at any time during the implementation of the Framework Contract.

4.1 SKILLS OF WEB-DEVELOPERS

The website and portals currently use Plone, Zope, Apache, Varnish, and Pound Load balancer. The tenderer shall demonstrate experience in these tools and applications. Also, as ENISA plans to migrate its websites and portals from PLONE to DRUPAL in the coming years, the tenderer shall demonstrate experience in these tools as well.

For the performance of the above-mentioned activities, the following skills and experience shall be demonstrated by the tenderer in the submitted proposal:

- Proven expertise and experience in programming Python, HTML, and JavaScript;
- Proven experience and expertise in programming PHP, SQL and NoSQL and using the Drupal API (especially DRUPAL 9) (for Drupal Developers)
- Proven skills in creative development of interactive interfaces covering end-user accessibility and functionality requirements in an attractive/innovative manner (user experience);
- Proven experience in transforming user requirements into demonstrable prototypes;
- Experience in systems integration, availability and security of web and mobile infrastructures;
- Experience in testing, optimization and secure software development;
- Experience in automation tools (eg. automated testing, automated deployment) and scripting languages (eg. bash, perl, python, HTML5, CSS3, JavaScript, REST API,Angular, NodeJs, Flask Jenkins, ELK stack, XML, JSON, SOAP web services, NLP and ML libraries such as NTLK, Stanford NLP, Spacy, Sklearn).);
- Experience in relevant tasks in both the private and public sector;
- Good project management, interpersonal and coordination skills;
- Excellent command of written and spoken English.

4.2 DESCRIPTION OF PROFILES

The tenderer shall be able to provide the following requested profiles for web development services.

NOTA BENE: It is acceptable that one team member might cover two roles provided that this member's profile is at the levels described in this section for both roles and there is no overlap in the tasks (e.g. the developer cannot be the same person as the tester).

Project Manager	
Nature of the tasks	• Project management including proposals for project strategies, planning, definition of tasks and deliverables, review of project deliverables, quality control, risk analysis and management, project status reports, problem reporting and management systems, follow up and organisation. • Provide effective leadership for the project team ensuring that team members are motivated and constantly developing their skills and experience. Be in-charge of project activities and review deliverables. • Participate in functional and technical working groups and progress meetings. • Estimate and monitor costs, timescales and resource requirements for the successful completion of each project to agreed terms of reference. • Prepare and maintain project and quality plans and tracks activities against the plan, provide regular and accurate reports.
Education & Experience	• A level of education which corresponds to completed university studies of at least four (4) years attested by a diploma • Minimum 4 years' experience in IT Project Management. Practical experience with software development life-cycle. • Proven experience with quality procedures. (e.g. number of projects overseen and quality assurance methods followed)
Knowledge and skills	• Project management and leadership. • Usage of project management office tools (e.g. Asana, Atlassian / Jira, MS Project or equivalent). • In depth technical knowledge of the project's main aspects and general technical knowledge on the other aspects touched by the project. • Usage of methods and techniques for reporting. • Ability to give presentations. • Participate in meetings and give status report presentations, be a good communicator. • Capability of integration in an international/multi-cultural environment. • Written and oral English at European language level C1 or higher.

Business Analyst	
Nature of the tasks	• Liaise with business managers and end-users to understand and document business requirements • Analyse requirements and transform them into technical specifications • Consultancy studies in a specific technical domain regarding information systems. • Production of use case models, software architecture documentation. • Provide expertise in a specific technical domain regarding information systems. • Technical evaluations and provide expertise on integration of IS into the working environment. • Able to draft all the required documentation.
Education & Experience	• A level of education which corresponds to completed university studies of at least four (4) years attested by a diploma in one of the following fields: Computer Science, Information Technologies, Mathematics, Physics, Engineering, Business Administration, Business Management or equivalent. • A minimum of four (4) years of experience in Information Technology development and/or Information Technology consulting. • Experience with business process analysis, documentation, and change management as well as experience in working with Plone-related methodologies and technologies • Experience in analysis and programming, databases and web application development.
Knowledge and skills	• Knowledge of international standards like W3C, WAI and IPG(desirable) standards • Conceptual understanding of content structuring, storage, access and presentation elements • Strong interest in follow-up of trends in web development • Ability to participate in multi-lingual meetings • Good communicator • Written and oral English at European language level C1 or better

Developer	
Nature of the tasks	• Development of web-enabled applications. • Creating/maintaining web applications. • Development of front-end and back-end systems including database development tasks • Develop both simple and complex solutions. • Translate software requirements into concise and robust programming code. • Increase program operating efficiency and adapt system to new requirements, as necessary. • Report status and flag issues to the ENISA Project/Product Manager.
Education & Experience	• University degree in computer science, mathematics, engineering, physics or similar; alternatively, post-secondary degree plus five (5) years proven experience in IT and software development technologies. • At least five (5) years of experience for senior developers and three (3) years of experience for junior developers, developing in a web environment working with python and PLONE – related technologies
Knowledge and skills	• Top-notch programming skills and in-depth knowledge of modern HTML/CSS • Extensive knowledge of Python, HTML, Javascript and PLONE related technologies (including ZODB) • Experience with version control systems and source code management system for software development, git (preferred) or svn. • Strong interest in follow-up of trends in web development. • Basic knowledge of Search Engine Optimization process • Written and oral English at European language level B2 or higher.

Drupal Developer	
Nature of the tasks	• Development of web-enabled applications. • Creating/maintaining web applications. • Development of front-end and back-end systems including database development tasks • Develop both simple and complex solutions. • Translate software requirements into concise and robust programming code. • Increase program operating efficiency and adapt system to new requirements, as necessary. • Report status and flag issues to the ENISA Project/Product Manager.
Education & Experience	• University degree in computer science, mathematics, engineering, physics or similar; alternatively, post-secondary degree plus five (5) years proven experience in IT and software development technologies. At least five (5) years of experience with PHP, SQL and Drupal
Knowledge and skills	• Top-notch programming skills and in-depth knowledge of modern HTML/CSS • Extensive knowledge of PHP, DRUPAL SQL etc. and the DRUPAL API • Experience with version control systems and source code management system for software development, git (preferred) or svn. • Strong interest in follow-up of trends in web development. • Basic knowledge of Search Engine Optimization process • Written and oral English at European language level B2 or higher.

Graphical Interface Designer	
Nature of the tasks	• Definition and creation of the graphical layout of web pages, prototyping. • Collaborate with ENISA project manager and software and website developers to define and implement innovative solutions • Execute all visual design stages from concept to final hand-off to ENISA • Conceptualize original ideas that bring simplicity and user friendliness to complex design roadblocks • Create wireframes, storyboards, user flows, process flows and site maps to effectively communicate interaction and design ideas • Conduct user research and evaluate user feedback • Establish and promote design guidelines, best practices and standards
Education & Experience	• Course on web design at University, or at a specialized institute/school followed by 3 at least years of experience in the above tasks. • BS/MS in Human-Computer Interaction, Interaction Design, or related will be considered advantageous • Experience working in an Agile/Scrum development process
Knowledge and skills	• Up-to-date with the latest UI trends, techniques, and technologies • Knowledge of international standards like W3C, WAI and IPG (desirable) standards • Demonstrable UI design skills with a strong portfolio • Solid experience in creating wireframes, storyboards, user flows, process flows and site maps • Proficiency in HTML, CSS, and JavaScript for rapid prototyping. • Excellent visual design skills with sensitivity to user-system interaction • Experience in creating vector graphic images –svgs (desirable) • Written and oral English at European language level B2 or better.

Quality Assurance / Tester / Devops	
Nature of the tasks	• Analysis, design, planning and execution of a test strategy for new features and sustaining projects. • Developing and executing automated tests to enable delivery of high-quality software on time and on budget. • Performing functional and non-functional tests in order to ensure the quality and the proper goal of the end product / feature. • Implement test tools and utilities to improve the efficiency and effectiveness of the development life-cycle • Configuration and maintenance of a test lab environment that resembles complex customer environments • File detailed bug reports and follow up on the problems until complete resolution • Comply with good engineering practices, coding standards and contribute to automation code reviews • Collaboration with development team to assure correct replication, integration and deployment on production.
Education & Experience	• University degree in computer science, mathematics, engineering, physics or similar; alternatively, post-secondary degree plus five (5) years proven experience in IT and software development technologies. • At least three (3) years of experience developing/testing in a web environment working with PLONE – related technologies. Experience with working with other technologies e.g. Drupal will be considered advantageous.
Knowledge and skills	• Extensive knowledge of Python, HTML, Javascript and PLONE related technologies • Experience with a Test Automation Framework (e.g. Selenium, QTP, Sikuli) • Experience with QA methodologies • Great understanding of testing throughout the product lifecycle, including unit, integration, regression, component and end-to-end system testing • Familiarity with SSH, and one of the following deployment automation tools (Jira/Bamboo, Jira/Zephyr, Chef, Puppet, Maven, Jenkins, Kubernetes, Capistrano etc.) • Strong scripting programming knowledge (e.g. Shell/Ruby/Python) • Strong system administration knowledge of Linux platforms. • Experience with version control systems and source code management system for software development, git (preferred) or svn. • Written and oral English at European language level B2 or better

System Administrator/Engineer	
Nature of the tasks	• Upkeep, configuration, and reliable operation of ENISA's hosting infrastructure • Apply updates and patches • Check the secure configuration of the tools • Collaboration with development team to assure correct replication, integration and deployment on production.
Education & Experience	• University degree in Computer Science, Information Technology, System Administration, or a closely related field, or post-secondary degree plus five (5) years of proven related experience • At least 3 years of database, network administration, or system administration experience
Knowledge and skills	• Working knowledge of virtualization, VMWare, or equivalent • Working knowledge and experience with Microsoft Azure • Strong knowledge of systems and networking software, hardware and networking protocols • Experience with scripting and automation tools • Expert knowledge of security, storage, data protection, and disaster recovery protocols • Knowledge and experience with helpdesk and IT operations best practices - Certification or familiarity with IT service management methodologies like ITIL • Written and oral English at European language level B2 or better

The **minimum** number of CVs required per profile is presented below:

ID	Profile	
1	Project Manager	2 CVs
2	Business Analyst	1 CV
3	Developer*	5 (Plone Developers) + 2 (Drupal developers) CVs
4	Graphical Interface Designer	2 CVs
5	Quality Assurance/Tester/DevOps	2 CVs
6	System Administrator	2 CVs

*At least three of the five PLONE 'Developers' should be at a senior level, i.e. more than 5 years of experience in web development and database experience, as well as in working with python and Plone-related technologies. The profiles for at least two more senior developers experienced with Drupal are required.

All key roles/resources needed for a project lifecycle shall be used in a web development project to assure quality of end-result (e.g. analyst, designer, developer, tester, pm, etc.). In each phase of the project, the participation in meetings and interaction of the corresponding key expert with ENISA personnel is expected. However not all the roles/resources are needed for helpdesk support and smaller basic tasks and enhancements of the website and portals. The contractor should be able to propose the relevant team members based on the project's/task's requirements.

In case of the departure of one or more members of the proposed team, the contractor is expected to provide ENISA with CVs of replacements with at least the same level of qualifications and similar experience to cover ENISA's needs. ENISA will evaluate the CV and experience in order to decide within 5 working days, whether to accept, or reject and request an alternate replacement candidate.

5. CANCELLATION OF CONFIRMED ASSIGNMENTS

Each request by ENISA will lead to the signature of a dedicated Order Form serving as the legal confirmation of an assignment. In case an assignment is cancelled by ENISA after the signature of an Order Form, liquidated damages will be applied to the contractor as described in the paragraphs below:

6. ORGANISATIONAL ASPECTS

6.1 ISSUE TRACKER – TICKETING SYSTEM

The use of Order Forms will be periodically issued for general development services (e.g. bug fixing, small updates) or for new development projects. Within this legal framework, the contractor is expected to operate a ticketing system (such as redmine, flow etc.) to register bug reports, change requests, requests for information, and so on.

Each ticket, together with approval provided by the ENISA responsible person, shall be referred to in the ensuing invoice, which may be partly or fully issued against the amount of the Order, depending on the mutually agreed periodicity of the invoicing.

The tenderer is free to suggest a regular invoicing period, however the Agency would suggest either bi-monthly or quarterly invoicing, in order to reduce administrative burden on both sides.

6.2 BUGS AND ISSUE REPORTS

The contractor shall respond to bug and issue reports based on their classification as per the following table:

- **Critical:** With descending priority, attacks, security updates, website and portals availability, a critical service of the website/portal (e.g. Submission with deadline, such as procurement and

recruitment or submission of incident report on incident reporting period) – immediate response (within 2 hours)
- **High:** an issue that prevents an application from meeting requirements or carrying out a feature – response within the same day
- **Normal:** a minor defect that it has no direct effect on the general functionality of the application itself – response within the next 2 days
- **Low:** bugs/issues with no real impact on the functionality of an application (design or cosmetic errors – response within 3 days.

The specific response time per category is further defined in a Service Level Requirements (SLR) which will be agreed and annexed to the resulting Framework contract.

6.3 REQUESTS FOR CHANGES

The contractor shall respond to change requests (small enhancements, change of behaviour) at the latest within 3 working days. Request for changes will be reported and monitored using the dedicated ticketing system. The specific response time per type of request or incident will be further defined in the Service Level Requirements (SLR) according to the urgency of the latter.

6.4 REQUESTS FOR INFORMATION AND CONSULTANCY

The contractor may be asked to provide consultancy services on the feasibility of implementing various ideas put forward by the ENISA staff. The contractor should respond to requests for information within 5 working days.

6.5 DESIGN AND WEBSITE STRUCTURE

The contractor will be asked to provide advice and technical support in improving the Information Architecture of ENISA's website and portals. The contractor should have (or collaborate with) skilled designers, architects and web usability experts to respond to such requests.

ENISA always seeks to improve the website's information structure and design. It would therefore be considered advantageous if tenderers are able to demonstrate expertise in this respect

6.6 MIGRATION AND TRANSITION

The prospective contractor will be assigned the task to migrate the website and portals (that may or may not be already hosted by ENISA) from the existing hosting environment to the new cloud environment owned by ENISA. It is expected that this migration should not take longer than one month. The tenderer shall provide:

- A one-off costing for this migration, to be scheduled for the first year of the contract (see Annex IV Financial Offer form).
- The detailed migration plan and timeline for the migration.

7. PLACE OF WORK AND DELIVERY

The implementation of the services will be undertaken at the contractor's premises.

One face-to-face kick off meeting between ENISA and the contractor might be held at ENISA's premises (either in Athens or Heraklion) depending on the needs of the Agency and upon the agreement with the contractor. If a face-to-face meeting is not possible or otherwise will be agreed, the kick off and all other meetings between ENISA and the contractor can be held online.

8. CONTENT AND PRESENTATION OF THE TECHNICAL OFFER

This section is of a great importance in the assessment of the bids, the award of the contract and the future execution of any resulting contract. Attention is also drawn to the award criteria, which define those parts of the technical offer to which the tenderers should pay particular attention. The technical offer should address the tenderer's approach to and solutions for all matters laid down in the technical specifications while the tenderer should be aware, that a simple repetition of the Technical specification will result in a very low technical score. The level of detail of the tender will be very important for the evaluation of the tender.

To ensure equal treatment for all tenders, it is not possible to modify technical offers after their submission. As a consequence, incompleteness in this section can only result in negative impact for the evaluation of award criteria. Please note also, that offers deviating from the Technical Specifications may be rejected for non-conformity.

The Technical Specifications and the tenderer's bid shall be integral parts of the contract and will constitute annexes to the contract, while in case of contradictions the Technical Specifications prevail.

The Tender must demonstrate clear understanding of the objectives and assignments, project management, organisation of the project team and communication, work plan and timelines.

8.1 GENERAL REQUIREMENTS

The tenderer must submit its Technical Offer following the indicative structure described below:

A paper (maximum 30 pages in Arial 11 font size or equivalent) describing and demonstrating:

- Understanding of the issues related to the objectives of the project;
- Methodology for delivering of these services, addressing issues such as testing of new features, automated deployment in the test environment, automated deployment in the production environment, test data to test resolved bugs in the test environment and delivery of documentation;
- The planning and support that will be provided for the migration of ENISA's websites and portals, the setting up and the maintenance of ENISA's new web hosting infrastructure, including technical details about how the detailed requirements will be met (security, availability etc. as well as data protection requirements under Section 11 below).
- The operational structures provided to implement the activities and to fulfil the foreseen tasks, with particular concern on project management, coordination of tasks with sub-contractors (if applicable), coordination of expertise and organisation of the project team required and the strategy to manage different activities and deliver hight quality services in the given timeline;

- Correspondence to scenarios;
- Knowledge about the issues related to the objectives described for this Framework Contract;
- Methodology to be followed: what activities will be implemented to cover the full spectrum of the tasks under this Framework Contract and how they will be implemented;
- Process that will be followed and will ensure that the execution of the tasks meets the requirements of ENISA and will be performed without defects and/or errors and within data protection/privacy policy and/or any other legal and regulatory framework with regard to compliance (quality assurance)
- Process that will be followed and will check if the deliverables meet ENISA's requirements and are flawless; this process should also define the mitigation actions in case the quality control reveals errors in the deliverables (quality control);
- Risk assessment and management process. The contractor will have to describe at least:
  a. The strategy that will be followed and will cope with change requests coming from ENISA;
  b. The strategy that will be followed and will cope with the work under pressure (e.g. tight deadlines, unexpected scarcity of resources);
  c. Management of any other risk envisaged during the implementation of the project.

The organisation of the project team and operational structures the tenderer will put in place to ensure the timely provision of high-quality services listed in Section 2;

***NOTA BENE:** the professional and technical capacity documentation (i.e. CVs etc) and evidences and the correspondence to scenarios are not considered as part of the 30 pages maximum and will be annexed to the technical offer.

8.2 SCENARIOS

The following two scenarios must be assessed and your estimations of volume of work required in 'person hours' per profile and overall project cost shall be entered into the appropriate boxes in the Financial Offer form (Annex IV). These scenarios refer to a possible situation in accordance to ENISA needs, in order to facilitate the tenderer towards building a reliable and comparable financial offer. Hourly rates are also required to be provided in Part B of the Financial Offer form for the various requested profiles, which must then be used as the basis, together with estimation of person hours required for each scenario. The actual projects to be awarded to the successful contractor will have a much more detailed level of technical specifications.

Please note: Failure to provide a technical description and price estimation for scenarios will result in your offer being declared invalid and not further evaluated.

8.2.1 SCENARIO 1: ENISA WEBSITE REVAMP

Based on the findings of an existing user experience exercise and a new one that will include focus groups and/or interviews to establish users' goals, a card sorting exercise, wireframe testing and usability testing, ENISA would like to fully redesign the front- end of its main website www.enisa.europa.eu. The project will include:

- A complete website redesign taking into account current trends in website design, user experience best practices, mobile compatibility, meeting fully accessibility requirements, ENISA's new brand positioning strategy but also new tasks and new areas of work.
- Rethinking and evaluation of the IA and introduction of changes based on the card sorting exercise
- Redesign or new design of styles and features to accommodate new needs, new areas of work e.g. new content libraries, update of existing content types and subscriptions to new content updates

8.2.2 SCENARIO 2: DEVELOPMENT OF AN INTERACTIVE REGISTRY TOOL SUPPORTTING STAKEHOLDERS

According to the NIS 2 (Directive (EU) 2022/2555) article 27, ENISA shall create and maintain a registry for essential and important entities such as DNS service providers, TLD name registries, cloud computing service providers, data centre service providers and content delivery network providers referred, as well as digital providers. This registry will be developed as a web tool/database where users of various roles will be able to insert, edit, view, and search entries. As defined in the NIS2 proposal, the minimum information that will be held for each entity is:

- the name of the entity
- the address of its main establishment and its other legal establishments in the Union or, if not established in the Union, of its designated representative
- up-to-date contact details, including email addresses and telephone numbers of the entities

The main purpose of the tool will be to implement the above registry and search directory so there should be basic and advanced search features. Furthermore, apart from this basic functionality there should be additional options, such as:

- User roles and their access rights management
- Configuration of country profiles
- Ability to manage (e.g add, view, edit, delete) entries for national entities
- Browse entities using different search criteria
- Generate statistics and reports

The interface of the registry and user experience should be as intuitive as possible to facilitate the support to the member states.

9. CONTENT AND PRESENTATION OF THE FINANCIAL OFFER

The Financial offer must be drawn up using the **Financial Offer form (see Annex IV)**.

In order to be considered a valid offer, it must be duly filled in, dated, stamped, and signed by the authorised person.

Please take special care to enter price data **in all boxes as described**. Failure to provide a fully completed form may result in your offer being declared invalid and not being further evaluated.

10. TENDER RESULT AND ESTIMATED CONTRACT VALUES

The result of the evaluation of tenders will be the awarding of a single Framework Service Contract. The estimated overall maximum contract value without this being binding for ENISA is **two million and four hundred thousand Euro (€ 2.400.000)** over a maximum possible period of four (4) years.

(Please note that in the case where unforeseen circumstances result in this contract being consumed faster than originally planned, the Agency reserves the right to consider conducting a 'Negotiated procedure without prior publication of a contract notice' with the existing contractor in order to increase the maximum amount stated above by up to 50%. This procedure being fully in accordance with Article 164(4) and Annex I - point 11.1(e) of the EU Financial Regulation (FR)).

11. DATA PROTECTION AND TRANSPARENCY

Processing of personal data in the context of this contract shall comply with the legal framework on data protection, i.e.:

- **Regulation (EU) 2018/1725[2] ('the EDPR')** as concerns personal data processing by the selected contractor, processing data in execution of the contract with ENISA.

The EDPR constitutes the specific data protection legal framework applicable to institutions, bodies, offices and agencies of the European Union, including ENISA, mirroring the GDPR applicable within the Union.

ENISA is the controller under this Regulation and the prospective contractor is the processor. The processor shall act only under the instructions of ENISA. ENISA's terms and conditions concerning procurement contracts are included in Article II.9.2 of the draft contract in Annex V.

- **Regulation (EU) 2016/679[3] (General Data Protection Regulation – 'the GDPR')** as concerns personal data processing carried out by the contractor on its proper behalf as a controller.

Processing of personal data by ENISA as contracting authority:

Information on the processing of personal data by ENISA as contracting authority in charge of the present procurement procedure is available in the Privacy Statement on the ENISA website as well as in Article II.9.1 of the draft contract in Annex V. In this context, please be informed that ENISA may register your personal data as a tenderer or selected contractors in the Early Detection and Exclusion System (EDES) if you are in one of the situations mentioned in Article 136 of the Financial Regulation. The relevant Privacy Statement is available on the European Commission's website, here: http://ec.europa.eu/budget/explained/management/protecting/protect_en.cfm#BDCE.

Processing of personal data by the selected contractor:

Personal data processing in execution of the contract between ENISA and the selected contractors shall comply with Regulation (EU) 2018/1725 (the EDPR).

[2] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295/39 21.11.2018

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p. 1–88

The processing of personal data shall happen in accordance with Article 29 of the EDPR. In particular, the selected contractor shall comply with the following:

- to process the personal data only on documented instructions of ENISA, in particular with regard to the purposes of the processing, the categories of data that may be processed, the recipients of the data and the means by which the data subject may exercise its rights;
- to abide in particular by ENISA's data protection policies as regards the confidentiality of electronic communications (Section 3 EDPR) and the processing of personal data in web services;
- to ensure that access to personal data is granted to the extent strictly necessary for the implementation of the contract and to ensure that persons authorised to process the personal data have committed themselves to confidentiality;
- to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks, in particular the risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the personal data, processed or stored;
- not to engage another processor of personal data (i.e. by means of a subcontract), without prior written authorisation of ENISA. Where another processor is engaged for carrying out specific processing activities on the personal data, the same data protection obligations as set out in the contract shall be imposed on the other processor;
- to assist ENISA in the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the EDPR;
- to assist ENISA with its obligations with regard to security of processing, the notification obligations in case of a personal data breach, as well as where applicable cooperation in data protection impact assessments (DPIAs) and prior consultations with the European Data Protection Supervisor (the EDPS)[4], outlined in Art. 33 to 40 of the EDPR;
- to make available to ENISA all information to demonstrate compliance with the obligations laid down in the EDPR and to allow for and to contribute to audits, including inspections, conducted by ENISA or another auditor mandated by ENISA;
- As concerns the localisation of and access to the personal data, to comply with the following:
    - the personal data shall only be processed and held in data centres within the territory of the European Union and the European Economic Area and will not leave that territory. This includes also any backup centres and location of backup data.;
    - the contractor may not change the location of data processing without the prior written authorisation of ENISA ;
    - The contractor shall inform ENISA in case of any need for transfer of personal data to third countries or international organisations and will perform such transfer only after written authorisation by ENISA. Any transfer of personal data to third countries or international organisations shall fully comply with the requirements laid down in Chapter V of the EDPR ;
    - The contractor shall notify ENISA without delay of any legally binding request for disclosure of the personal data processed on behalf of ENISA made by any national public authority, including an authority from a third country. The contractor may not give such access without the prior written authorisation of ENISA;

[4] http://www.edps.europa.eu

- To contact the Data Protection Officer (DPO) of ENISA, in charge of monitoring data protection compliance, with any questions arising or in case of need for assistance concerning personal data protection dataprotection@enisa.europa.eu,

In addition, **Article II.9.2 of the draft contract** provided in Annex V is applicable.

Confidentiality:

ENISA will disregard general statements that the whole tender or substantial parts of it contain confidential information. Tenderers need to mark clearly the information they consider confidential and explain why it may not be disclosed. The EU body reserves the right to make its own assessment of the confidential nature of any information contained in the tender.

12. MARKING OF SUBMITTED DOCUMENTS

The tenderer SHOULD NOT mark tender documents (for e.g. the header or footer) with any of the following words: RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET. If the tenderer considers that such markings are required, a prior approval from the ENISA Procurement Coordinator should be obtained BEFORE sending the tender documents. The tenderer should be aware that the information sent to ENISA for procurement purposes is handled in accordance with the governing rules for EU Public Procurement and the EU Financial Regulation framework.

13. PRICE

Prices submitted in response to this Tender must be inclusive of all costs involved in the performance of the contract. Prices shall be submitted only in Euro and VAT excluded.

14. PRICE REVISION

The price quoted must be fixed and not subject to revision during the first year of performance of the contract. From the beginning of the second year of performance of the contract, prices may be revised in accordance with Article I.3.3 of the framework contract.

15. COSTS INVOLVED IN PREPARING AND SUBMITTING A TENDER

ENISA will not reimburse any costs incurred in the preparation and submission of a Tender. Any such costs must be paid by the Tenderer.

16. PERIOD OF VALIDITY OF THE TENDER

Tenderers must enclose a confirmation that the prices given are valid for six (6) months from the date of submission of the tender.

17. PROTOCOL ON PRIVILEGES & IMMUNITIES OF THE EUROPEAN UNION

ENISA is exempt from all taxes and duties, including value added tax (VAT), pursuant to the provisions of Articles 3 and 4 of the Protocol on the Privileges and Immunities of the European Union. Tenderers

must therefore give prices, which are exclusive of any taxes and duties and must indicate the amount of VAT separately.

18. PAYMENT ARRANGEMENTS

Payments under the Contract shall be carried out, subject to prior approval of the report accompanying the invoices, listing the services rendered, within 60 days of submission of an invoice accompanying the final report or deliverable based on the conditions set out in the draft contract.

19. CONTRACTUAL DETAILS

A Framework Service Contract will be proposed to the successful tenderer. Selection of a tenderer and / or signature of the Framework Service Contract imposes no obligation on ENISA to order services.

The contract and its annexes draw up the legal, financial, technical and administrative provisions governing the relations between the Agency and the Contractor during its period of validity.

The tender will conclude, valid as of the date of the last signature, with a one-year Framework Service contract, tacitly renewable up to three times for a maximum of four years.

The Agency reserves the right to end the contract at any time, without any obligation to invoke the reason for it, at one months' notice. The Tenderer's offer must be drafted taking fully into account the provisions of the draft Framework Service contract annexed to this call for tenders (See draft contract, in Annex V).

Please note *that the general conditions of our standard framework service contract cannot be modified. Submission of a tender by a potential contractor implies acceptance of this contract and all of the terms and conditions contained therein.* ***It is strongly recommended*** *that you have this draft contract checked and passed by your legal services before committing to submitting an offer.*

PART 3 TENDER SPECIFICATIONS

1. INFORMATION ON TENDERING

1.1 CONTRACTUAL CONDITIONS

In drawing up their offer, the tenderer should bear in mind the provisions of the draft contract (Annex V) attached to this invitation to tender particularly those on payments, performance of the contract, confidentiality, and checks and audits. Submission of a tender by a potential contractor implies acceptance of this contract and all of the terms and conditions contained therein. Any limitation, amendment or denial of the terms of contract will lead to automatic exclusion from the procurement procedure.

It is strongly recommended that you have this draft contract checked and passed by your legal representative before committing to submitting an offer.

Before the contract is signed, the Agency may decide to abandon the procurement procedure or cancel the award procedure without the tenderers being entitled to claim any compensation.

1.2 JOINT TENDERS (IF APPLICABLE)

A joint tender is a situation where a tender is submitted by a 'group' of economic operators (consortium). Joint tenders may include subcontractors in addition to the joint tenderers.

Tenders can be submitted by groupings of service providers/suppliers who will not be required to adopt a particular legal form prior to the contract being awarded. However, the Agency will require the grouping:

- Either to have the contract signed by all members (partners) of the grouping. In this case, one of them, as 'Lead Partner', will be responsible for the receipt and processing of payments for members of the grouping, for managing the service administration and for coordination of the contract;
- Or to have the contract signed by the 'Lead Partner' only, who has been duly authorised by the other members to bind each of them (a fully completed 'power of attorney' form for each member of the Group will be attached to the contract according to the template provided by the Agency).

In addition, the composition and constitution of the grouping, and the allocation of the scope of tasks amongst the members, shall not be altered without the prior written consent of the Agency, which can be withheld at its discretion.

In case of a joint offer, each member of the grouping shall provide the following:

- a **Legal Entities form** and a **Power of Attorney of each consortium partner**, must be filled in, signed by (an) authorised representative(s), scanned and uploaded in the corresponding section.

- a **Declaration of honour with respect to the Exclusion Criteria and absence of conflict of interest** must be filled in, signed by (an) authorised representative(s), scanned and uploaded in the corresponding section.

1.3 LIABILITY OF MEMBERS OF A GROUP

Partners in a joint offer assume **joint and several liability** towards the Agency for the performance of the contract as a whole.

Statements, saying for instance:

- That one of the partners of the joint offer will be responsible[5] for only one part of the contract and another one for the rest, or
- That more than one contract should be signed if the joint offer is successful

are thus incompatible with the principle of joint and several liability. The Agency will disregard any such statement contained in a joint offer, and reserves the right to reject such offers without further evaluation, because they do not comply with the tendering specifications.

1.4 SUBCONTRACTING

Subcontracting is permitted in the tender but the contractor will retain full liability towards the Contracting Authority for performance of the contract as a whole.

If the tenderer intends to subcontract part of the service, they shall indicate in their offer which part will be subcontracted and to what extent (% of the total contract value).

Tenderers must ensure that Article II.7 of the contract (Annex V) can be applied to subcontractors.

Tenderers must give an indication of the proportion of the contract that they intend to subcontract.

Tenderers are required to identify all subcontractors.

During contract execution, any change of a subcontractor identified in the tender will be subject to prior written approval of the Contracting Authority.

2. STRUCTURE AND CONTENT OF THE TENDER

2.1 GENERAL

Tenders must be written in **one of the official languages** of the European Union. The working language of ENISA is English.

Tenders must be written in a clear and concise manner, with continuous page numbering. Since tenderers will be judged on the content of their written bids, they must make it clear that they are able to meet the requirements of the specifications/terms of reference.

2.2 STRUCTURE OF THE TENDER

Based on the ***e-Submission*** environment[6], all tenders must provide information and supporting documentation in two sections:

[5] not to be confused with distribution of tasks among the members of the grouping

[6] *For detailed instructions on how to submit a tender please consult the e-Submission Quick Guide available at: https://webgate.ec.europa.eu/digit/opsys/esubmission/assets/documents/manual/quickGuide_en.pdf*

1) Qualification - data and documentation;

2) Tender offer - data and documentation.

2.3 QUALIFICATION DATA

a) Identification of the Tenderer

The tenderer must fill in all required fields in the qualification section. In case of a joint tender the consortium name has to be provided and an identification of every party in the consortium needs to be added.

The following information should also be provided:

(i) Legal Entities

In order to prove their legal capacity and their status, all tenderers and identified subcontractors must provide a Legal Entity Form with its supporting evidence.

However, the subcontractor(s) shall not be required to fill in or provide those documents when the services represent less than 20% of the overall contract value.

The Legal Entity Form can be generated via the e-Submission application. Alternatively, a standard template in each EU language is available at:

http://ec.europa.eu/budget/contracts_grants/info_contracts/legal_entities/legal_entities_en.cfm

Tenderers must provide the following information if it has not been included with the Legal Entity Form:

- For **legal persons**, a legible copy of the notice of appointment of the persons authorised to represent the tenderer in dealings with third parties and in legal proceedings, or a copy of the publication of such appointment if the legislation, which applies to the legal entity concerned, requires such publication. Any delegation of this authorisation to another representative not indicated in the official appointment must be evidenced.
- For **natural persons**, where applicable, a proof of registration on a professional or trade register or any other official document showing the registration number.

(ii) Financial identification

The tenderer (or the single point of contact in case of joint tender) must provide a Financial Identification Form and supporting documents. Only one form per offer should be submitted (no form is needed for subcontractors and other joint tenderers). The form is available at:

http://ec.europa.eu/budget/contracts_grants/info_contracts/financial_id/financial_id_en.cfm

Remark: Tenderers that are already registered in the Agency's accounting system (i.e. they have already been direct contractors **with ENISA** in the past) must provide the filled in form but are not obliged to provide the supporting evidence.

The form needs to be printed, filled in and then scanned and uploaded in the Qualification section. In case of a joint tender, it has to be uploaded in the ***"Documents"*** section of the Consortium Leader.

(iii) Power of Attorney

In case of a joint tender, an Agreement / Power of Attorney for each partner must be filled in, signed by (an) authorised representative(s), scanned and uploaded. Please choose 'Model A' for an ad hoc grouping or 'Model B' for a legally constituted consortium - see templates in Annex VI (a) and (b)

(iv) Lots interested in *(only in case the tender has multiple lots)*

The tenderer must indicate for which lots the tender is applicable, by ticking the relevant boxes in the section: ***"Interested in the following lots".***

b) Information regarding exclusion and selection criteria:

The tenderer is requested to submit the following documents:

1. Declaration by the Tenderer relating to the exclusion criteria (see 3.1 below)

   The filled-in Declaration form.

   In case of a joint tender, each member of the consortium has to submit a declaration under the respective party name (see template in Annex III)

2. Documents certifying economic and financial capacity (see 3.2.2 below)

   In case of a joint tender, each member of the consortium has to submit the documents under the respective party name.

3. Proof of technical and professional capacity (see 3.2.3 below)

   In case of a joint tender, each member of the consortium has to submit the documents under the respective party name.

If any of the above documents are associated with a specific Lot, please indicate for which Lot it is applicable inside the document AND in the Description field of the attachment *(only in case the tender has multiple lots).*

2.4 TENDER DATA

a) Technical proposal

The technical section is of great importance in the assessment of the bids, the award of the contract and the future execution of any resulting contract.

The technical offer must cover all aspects and tasks required in the technical specification and provide all the information needed to apply the award criteria. Offers deviating from the requirements or not covering all requirements may be excluded based on non-conformity with the tender specifications, and will not be evaluated.

The technical tender needs to be uploaded in the relevant section:

The tenderer selects the "Technical Tender" document from the dropdown box ("Financial Tender or Technical Tender"). The e-Submission application allows attachment of as many documents as necessary.

b) Financial proposal

- All tenders must contain a financial proposal, to be submitted **using the form attached as Annex IV.**

The tenderer's attention is drawn to the following points:

- Prices must be quoted in **euro**, including the countries that are not in the euro-zone. As far as the tenderers of those countries are concerned, they cannot change the amount of the bid because of the evolution of the exchange rate. The tenderers choose the exchange rate and assume all risks or opportunities relating to the rate fluctuation.
- **Prices must be fixed amounts**.
- **Estimated travel and daily subsistence allowance expenses must be indicated separately**. *(only if applicable to this procedure)*

  This estimate should be based on Articles I.5 and II.22 of the draft framework contract (Annex V). This estimate will comprise all foreseen travel and will constitute the maximum amount of travel and daily subsistence allowance expenses to be paid for all tasks.
- **Prices must be quoted free of all duties**, taxes and other charges, including VAT, as the European Union is exempt from such charges under Articles 3 and 4 of the Protocol on the privileges and immunities of the European Union. The amount of VAT may be shown separately.
- Prices shall be fixed and not subject to revision during the performance of the contract.

The total price needs to be encoded in the e-Submission application[7].

- In the box labelled ***'Total amount exclusive of taxes'*** – please add the amount Total P_B from your Financial Offer form.
- In the box labelled ***'Total taxes amount'*** – please put zero *(if this is not accepted by system then enter 0,01)*
- In the box labelled ***'Total amount'*** – again simply add the amount Total from your Financial Offer form or the maximum budget assigned for this tender

The completed Financial Offer form(s), MUST ALSO be uploaded in the relevant section:

The tenderer selects the "Financial Tender" document from the dropdown box ("Financial Tender or Technical Tender"). The e-Submission application allows attachment of as many documents as necessary.

3. ASSESSMENT AND AWARD OF THE CONTRACT

The assessment will be based on each tenderer's bid. All the information will be assessed in light of the criteria set out in these specifications. The procedure for the award of the contract, which will concern only admissible bids, will be carried out in three stages, normally in the order shown below.

The aim of each of these stages is:

[7] In the case of framework contracts, unless otherwise instructed, please add the maximum budget given for this tender

1) to check on the basis of the ***exclusion criteria***, whether tenderers can take part in the tendering procedure;
2) to check on the basis of the ***selection criteria***, the technical and professional capacity and economic and financial capacity of each tenderer;
3) to assess on the basis of the ***award criteria*** each bid which has passed the exclusion and selection stages.

Only tenders meeting the requirements of each stage will pass on to the next evaluation stage.

3.1 EXCLUSION CRITERIA

Tenders will be rejected if they do not comply with applicable obligations under environmental, social and labour law established by Union law, national law and collective agreements, or by the international environmental, social and labour law provisions listed in Annex X to Directive 2014/24/EU and compliance with data protection obligations resulting from Regulation (EU) 2016/679 and Regulation (EU) 2018/1725".

All tenderers shall provide a 'declaration on their honour' (see Annex III), stating that they are not in one of the situations of exclusion listed.

The 'declaration on honour' is also required for identified subcontractors whose intended share of the contract is above 20%.

The 'declaration on honour' has to be duly signed by parties that are not signing the Tender Preparation Report in *e-Submission*.

The successful tenderer shall be asked to provide the actual documents mentioned as supporting evidence in Annex III before signature of the contract and within a deadline given by the contracting authority. This requirement applies to all members of the consortium in case of joint tender.

Remark:

A tenderer may be waived of the obligation to submit the documentary evidence mentioned above if such evidence has already been submitted for the purposes of another procurement procedure launched by ENISA, provided that the documents are ***not more than one-year-old*** starting from their issuing date and that they are still valid. In such a case, the tenderer shall declare on his/her honour that the documentary evidence has already been provided in a previous procurement procedure, specifying the reference of the call for tender for which the documents have been provided, and confirm that no changes in their situation has occurred.

ENISA will also waive the obligation of the tenderer to submit the documentary evidence if it can access it on a national database free of charge.

Each tenderer (and each member of a consortium) shall declare in the relevant field in Annex VIII (Administrative Identification form) whether it is a Small or Medium Size Enterprise (SME) in accordance with Commission Recommendation 2003/361/EC[8].

As a general guideline, here is an excerpt from the Recommendation:

[8] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF

"*The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.*"

3.2 SELECTION CRITERIA

The following criteria will be used to select the Tenderers for further evaluation. If the Tender is proposed by a consortium, these criteria apply to the tenderer as a whole (unless otherwise stated).

Documentary evidence of the Tenderers' claims in respect of the below-mentioned criteria is required.

3.2.1 LEGAL AND REGULATORY CAPACITY

The Tenderer must provide evidence of enrolment (declaration or certificates) in one of the professional or trade registers related to the subject of this tender, in the country of its establishment.

3.2.2 FINANCIAL AND ECONOMIC CAPACITY

Proof of financial and economic standing shall be furnished by the following documents and minimum requirements:

(a) Copy of the financial statements (balance sheets and profit and loss accounts) for the last two (2) financial years for which accounts have been closed, where publication of the accounts is required under the company law of the country in which the economic operator is established. In case of a consortium, each consortium member shall present their financial statements.

If the tenderer is not obliged to publish its accounts under the law of the state in which it is established, a copy of audited accounts for the last two (2) financial years should be presented. In case of a consortium/grouping, audited accounts for each consortium partner shall be presented.

(b) **Complete (also) the attached Annex II 'Simplified Financial Statement',** which summarises your recent financial capacity. Please note that the average turnover for the last two (2) financial years for which accounts have been closed must meet our **minimum annual average turnover** of **€600.000 (six hundred thousand euro)**:

In case of a consortium/grouping, the annual average turnover for each of the partners shall be presented. The sum of the annual average turnovers of each partner will be taken into account to reach the annual average turnover of **€600.000**.

(c) If tenderers will call on the competences of another entity (for example, a parent company), a written undertaking by the said entity certifying that it will make available to the tenderers the resources required to implement the contract.

If for some exceptional reason which the Contracting Authority considers justified, the tenderer is unable to provide the documentary evidence requested above, he may prove his economic and financial capacity by any other means which the Contracting Authority considers appropriate, but only following a formal request for clarification before the tender expiry date.

3.2.3 TECHNICAL AND PROFESSIONAL CAPACITY CRITERIA AND EVIDENCE

The Tenderers are required to have sufficient technical and professional capacity to perform the contract. Evidence of the technical and professional capacity of the tenderers shall be furnished on the basis of the following requirements:

Criterion T1 The tenderers must demonstrate their experience in the provision of hosting management services (including hosting in a cloud environment such as Microsoft Azure, OVH etc).

Evidence for T1: Reference list (including contact details) of minimum three (3) current and/or past customers to whom the tenderer has supplied the core services, in the past three (3) years; specifying the tenderer's share (at least 50%) in provision of the services and if subcontractors were used for any of the services.

Criterion T2: The tenderer must prove experience in web development services based on the Plone platform as well as other platforms (e.g. Drupal).

Evidence for T2: Reference list (including contact details) of minimum three (3) current and/or past customers to whom the tenderer has supplied the core services, in the past three (3) years; specifying the tenderer's share (at least 50%) in provision of the services and if subcontractors were used for any of the services.

Criterion T3: The tenderer must ensure compliance with the Regulation (EU) 2018/1725 (the EDPR) and the Regulation (EU) 2016/679 ('the GDPR').

Evidence for T3: A signed statement confirming that the tenderer fulfils the general requirements of Regulation (EU) 2016/679 ('the GDPR') and that in particular it will comply with the specific requirements of Regulation (EU) 2018/1725 (the EDPR) in its service provision to ENISA with reference to the obligations on personal data protection listed in Part 2 - Section 11 of these tender specifications;"

Criterion T4: The tenderers must demonstrate the capacity to build, coordinate and manage the team of experts (experiences, skills and competences of the team indicated in Part 2 Terms of Reference - section 4). The team shall be competent to ensure quality of all the expected results and deliverables.

Evidence for T4: The Curricula Vitae (CVs), preferably in the common European format, of the proposed members of the team must be enclosed and showing clearly qualifications, professional experience within the relevant business area with the start and the end date (i.e. from DD.MM.YYYY to DD.MM.YYYY) and the linguistic skills. The form can be downloaded from:
https://europass.cedefop.europa.eu/en/documents/curriculum-vitae/templates-instructions
It is expected the submission of at least the following:

- Project Manager (2 CVs)
- Business Analyst (1 CV)
- Developer (5 CVs)
- Drupal Developer (2 CVs)
- Graphical Interface Designer (2 CVs)
- Quality Assurance/ Tester/ DevOps (2 CVs)
- System Administrator (2CVs)

The successful tenderers may be requested to provide the diplomas and professional qualifications of the persons responsible for providing the services, and/or any other type of relevant work in the field that is the object of this contract.

3.3 AWARD CRITERIA

3.3.1 QUALITY OF THE OFFER

Once the Tenderer has demonstrated the appropriate capacity to perform the Contract on the grounds of the selection criteria, the offer will be assessed based on the award criteria.

No	Qualitative award criteria		Weighting (max. points)
1.	**Quality of the methodological approach and quality control measures**	• Overall methodology and approach to project management for services listed in Section 2 Part 2 • Quality assurance strategy • Overall risk management strategy • Change management strategy • Management of conflicting requirements (working under pressure)	40
2.	**Internal organisation and structure**	• Overall organisation of the project team • Measures to ensure effective communication between team members and between contractor and ENISA • Work plan for implementing the framework contracts and expected requests for services	30
3.	**Response to Scenarios:** **Scenario 1 (max 15 points)** **Scenario 2 (max 15 points)**	Quality of technical proposal for each scenario: • Resource allocation, timing and process organisation; • Implementation of requirements outlined in Section 8.2; • Risk management of specific scenario; • Demonstrated know-how of technical solutions;	30
Total Qualitative Points (QP)			**100**

Minimum attainment per criterion

Offers scoring less than 50% for any criterion will be deemed to be of insufficient quality and eliminated from further consideration.

Minimum attainment overall

Offers scoring less than **60%** after the quality evaluation process will be considered to be of insufficient quality and eliminated from the following phase.

The sum of all criteria gives a total of 100 points. The respective weighting between the different award criteria depends on the nature of the services required and is consequently closely related to the terms of reference. The award criteria are thus quantified parameters that the offer should comply with. The **qualitative award criteria** points will be weighted at **70%** in relation to the price.

3.3.2 PRICE OF THE OFFER

The Financial Offer form (Annex IV) contains price boxes, which shall be completed with a monetary amount by the tenderer.

The total bid price ratio '**P_P**' will be calculated using the following formula and weightings:

$$P_P = [(P_{MC} / P_M) \times 20] + [(P_{SC} / P_{ST}) \times 40] + [(P_{DC} / P_D) \times 40)]$$

where:

P_M = Web hosting management cost

P_D = Web Development consolidated cost/Experts Costs (P_1 +P_2 + P_3 + P_4 + P_5 + P_6 + P_7)

P_{ST} = Total Scenario cost (S_1 + S_2)

P_{MC} = Cheapest P_M

P_{DC} = Cheapest P_D

P_{SC} = Cheapest P_{ST}

Please note: If any price box is left blank by the tenderer then the Financial Offer may be considered to be invalid and will be eliminated from further evaluation.

3.3.3 AWARD OF THE CONTRACT

The contract will be awarded to the offer that is the most cost effective (offers the best value for money) which obtains the highest number of points after the final evaluation, based on the ratio between the **quality criteria (70%) and the price (30%).** The following formula will be used:

$$TWP = (Q_P \times 0.7) + (P_P \times 0.3)$$

where;

Q_P = Qualitative points
P_P = Price points
TWP = Total weighted points score

In case the successful tenderer is unable to sign the contract for any reason, the Contracting Authority reserves the right to award the contract to other tenderers as per the ranking order established following the evaluation procedure.

4. TENDER OPENING

The public opening of received tenders will take place online on **April 2023 at 09:30 CEST Central European Summer Time**.

Please note *that all tenderers may simply request a copy of the Opening Report to be sent to them by email after the conclusion of the Opening Session procedure.*

5. OTHER CONDITIONS

5.1 VALIDITY

Period of validity of the Tender: six months from the closing date stated in Invitation to Tender. The successful Tenderer must maintain its Offer for a further 120 days from the notification of the award.

5.2 LOTS

This Tender is not divided into Lots.

5.3 ADDITIONAL PROVISIONS

- Changes to tenders will be accepted only if they are received on or before the final date and time set for the receipt of tenders.
- Expenses incurred in respect of the preparation and presentation of tenders cannot be refunded.
- No information of any kind will be given on the state of progress with regard to the evaluation of tenders.
- All documents submitted by Tenderers will become the property of ENISA and will be treated as confidential.

5.4 NO OBLIGATION TO AWARD THE CONTRACT

Initiation of a tendering procedure imposes no obligation on the Contracting Authority to award the contract. Should the invitation to tender cover several items or lots, the Contracting Authority reserves the right to award a contract for only some of them. The Contracting Authority shall not be liable for any compensation with respect to Tenderers whose tenders have not been accepted. Nor shall it be so liable if it decides not to award the contract.

6. SPECIFIC INFORMATION

6.1 TIMETABLE

The timetable for this tender and the resulting contracts is as follows:

Title: "**Web Development Services"**

ENISA F-EDO-23-T06

Summary timetable comments

Launch of tender: - Contract notice to the Official Journal of the European Union (OJEU) - Uploaded to e-Tendering website - Uploaded to ENISA website	24th February 2023	
Deadline for request of information to ENISA	27th March 2023	
Last date on which clarifications are issued by ENISA	29th March 2023	
Deadline for **electronic reception** of offers via ***e-Submission***	**31st March 2023**	**18:00 CEST** Central European Summer time
Opening of offers	3rd April 2023	**09:30 CEST** Central European Summer time
Date for evaluation of offers	TBA	
Notification of award to the selected candidate + 10 day standstill period commences	TBA	
Contract signature	end April 2023	Estimated