Annex A: Service Level Requirements

Open Call for Tenders:

F-SRAD-17-T28

Provision of Web Hosting and (PLONE) Web Development Services”

1. Overview

This document sets out the Service Level Requirements, for which acceptance by the service provider is mandatory. It is complementary to the tender technical specifications and aims to provide a more detailed overview of the minimum services, the associated procedures and service levels, the service reports as well as the applicable liabilities/penalties in case of non-fulfilment.

1.1. SLR purpose and scope

The purpose of this document is to ensure that proper mechanisms are in place to provide high quality service and support to ENISA. An SLA is an agreement between parties that defines the services provided, the indicators associated with these services, acceptable and unacceptable service levels, liabilities on the part of the services provider and the customer, and actions to be taken in certain circumstances. This SLR provides a clear description of roles and responsibilities, service quality metrics, and available support.

The objectives of this SLR are as follows:

- **Better communication:** It facilitates two-way communication between the parties. The parties involved come together in order to understand each other's needs, priorities and concerns, and to gain an insight into the problems which may be faced by each party through the failure of each party to fulfil their obligations.
- **Mutually agreed standards:** It sets an agreed standard against which performance may be measured. It identifies customer expectations, defines the boundaries of the service provision and clarifies responsibilities.
- **A process for gauging service effectiveness:** As the SLA defines standards against which the service may be measured and evaluated, it provides the basis for performing an assessment of the effectiveness of the service.

1.2. Terminology and conventions

Within this SLR, the following conventions and terminology are used:

- This SLR uses Eastern European Time (EET) – UTC+2 time zone
- Times expressed as a number of “office hours” or “working day” include business hours, Monday to Friday, excluding public holidays.
- ENISA’s public holidays will be communicated to the service provider at the beginning of each year.

It is expected that the service provider shall be able to handle emergencies that occur in the timeframe outside of office hours and during public holidays.

A permanent team backup procedure should be established, ensuring full time support provision. All designated members of the team working for ENISA should be able to have constant visibility on all support/helpdesk/development tasks so that they are constantly able to respond promptly. The team backup procedure should assure continuity of the services in case of any issues occurring outside business hours or during public holidays.

2. Services and service level

2.1. Service level guaranteed for the availability of hosting services

Availability is measured for a month for each website individually, excluding maintenance periods agreed with ENISA. This document defines the required service level for the hosting of ENISA websites. Other services provided, e.g. development, will have their own guaranteed service levels (see below).

Indicator	Specifications	Typical	Guaranteed	Unit
Availability	For each website	**99.3%**	**99.0%**	Uptime/month
Response time	For each website		1 sec (first byte)	Seconds
Network time	For each website (average)		<= 3 sec	Seconds

Uptime is the total time during which the services are available. For example, the 99 guaranteed percent in a 30-day month is 712.8 hours out of 720 hours. This guaranteed uptime covers all cases of downtime, including ISP's downtime(s), unless Force Majeure applies (i.e. any unforeseeable and exceptional situation or event beyond the control of the contracting parties which prevents either of them from performing their obligations. Force Majeure is further defined in the General Conditions of the Framework Service Contract).

Network time refers to the time it takes the server to answer to the request of a browser.

It is the responsibility of the service provider to continually measure and monitor the availability of the services and report monthly whether they meet the agreed service level (see section 2.8 of the Tender Specifications)

ENISA will also conduct its own independent vulnerability tests yearly in co-ordination with the service provider.

2.2. Service level guaranteed for response and implementation time

2.2.1 Helpdesk & web development tasks

ENISA appointed users should be able to introduce new requests or report bugs by adding corresponding tickets on the dedicated ENISA helpdesk- ticketing system.

The acceptance time in case of a helpdesk request (e.g. a bug) should be at maximum the following working day, and the ticket should be resolved in maximum 3 working days (except in cases of low importance requests - see below). Critical bugs related to web hosting will be handled on the same day (see below) they were reported. Critical bugs related to web development will be

handled on the same day they were reported if reported before 16.30 p.m. For other requests and new tasks (e.g. bigger web development projects, new features, enhancements etc.) implementation time should be predefined and communicated to ENISA upon acceptance of the task by the service provider.

Acceptance Time refers to the time that the service provider needs to acknowledge that the service provider has received the request and is going to start handling the issue.

Resolving Time refers to the time that a fix is deployed to the test server and is ready for acceptance by ENISA or the time where the fix is deployed directly in production (in case of e.g. critical bugs). When complete resolution is not possible, at least a temporary solution should be provided within the relevant timeframe, decreasing the severity of the issue, until a permanent fix is ready for deployment to production.

This workflow is the same both for web development and web hosting tickets.

The service level guaranteed values as describe below apply to the implementation time only. They are not associated with the service level guaranteed values applied for the availability of hosting services. The hosting services in the table below refer to helpdesk issues- both normal and critical ones.

Please refer to chapter 1.2 Terminology and conventions for business hours intervals.

Service	Specifications	Acceptance Time	Target Resolving Time	Measurement Unit
Web Hosting	Helpdesk-normal issues	Same day 8 hours	3 days	Days
Web hosting	Helpdesk-critical issues	Same day 1 hour	Same day 8 hours	Hours
Web development	Helpdesk-Low importance requests	3 days	5 days	Days
Web development	Helpdesk-Normal requests	12 hours	24 hours	Hours
Web development	Helpdesk-High importance requests	Same day 8 hours	16 hours	Hours
Web development	Helpdesk-critical requests	Same day 2 hours	8 hours	Hours
Web development	Other requests/web development tasks	3 days	Planned	

Critical: Critical web hosting requests, with descending priority, attacks, security updates, website and portals availability. Web development critical issues are considered bugs related to 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) not more than 7% of all helpdesk requests are expected to be marked as critical.

High: an issue that prevents an application from meeting requirements or carrying out a feature – response within the same day (e.g. Administrator unable to add a new user to the portal.) Around 15% of the helpdesk requests are expected to be marked with high priority.

Normal: a minor defect that it has no direct effect on the general functionality of the application itself – response within the next 2 days (e.g. Getting an error when loading the page but without affecting the functionality of the page.) Around 55% of the helpdesk requests are expected to be marked with normal priority.

Low: bugs/issues with no real impact on the functionality of an application (design or cosmetic errors and issues affecting the usability of the accessibility of an application– response within 3 days. (e.g. Change the text of a button on a custom plone application.) Around 23% of the helpdesk requests are expected to be marked with low priority.

Order of priority for recovery of web services in case they are offline or under attack:

1. ENISA website
2. ENISA resilience portal (Incident Reporting tools)
3. MB portal
4. Other portals (CyberSecMonth, Annual Privacy Forum etc.)

The order of priority for recovering ENISA's web services might be adjusted by ENISA during certain periods of time (e.g. during the European Cyber Security Month) and shall be communicated in advance to the service provider.

Response and resolving time to helpdesk requests will be evaluated per invoicing period by ENISA using the dedicated ticketing system (issue tracker) provided by the service provider for handling ENISA's requests. The service provider should be able to propose ways for facilitating this process e.g. with automated reports.

2.2.2 Web Development projects - Requests for proposal:

Except for introducing tickets for helpdesk requests; smaller changes and web development tasks, ENISA appointed users will also introduce requests for web development projects as described in section 3 of the Tender Specifications.

After acknowledging ENISA's notification for a request for proposal, ENISA is interested in the period of time that the service provider needs before responding with a detailed offer.

The service provider must send a technical offer detailing at least the following:

- the business analysis
- a risk assessment

- the Project proposed start date and main milestones
- an estimation of person/days per profile
- a financial offer based on these estimations

Minimum response times to web development project requests are further defined as follows depending on the request's complexity:

Service	Specifications	Response time	Measurement Unit
Web development	Low Complexity – e.g. Introduction of a set of new features (1-3 pages)	3 days	Business days
Web development	Medium Complexity – e.g. Upgrade of an existing tool (4-7 pages)	7 days	Business days
Web development	High Complexity- e.g. Development of a new tool, website redesign (More than 7 pages)	10 days	Business days

Priority of the projects shall be indicated by ENISA. In case of projects whose implementation is of low priority, new indicative response times shall be specified and agreed between ENISA and the service provider in writing.

Should the service provider require genuine clarification, the measure of the time to prepare and respond will be suspended until ENISA responds to the request for clarification.

2.2.3 Web development – Quality & Error Rate

It should be assured that the quality of new projects' code has been tested and measured using dedicated tools such as CodeClimate, Codacy, or similar. Any reported bugs or issues should be resolved by the service provider at no additional cost before the project's finalisation or liquated damages might apply (see section 2.4.5).

It should be assured that 95% of newly developed pages have no more than two errors per page as this is reported by dedicated tools such as PhantomJS or similar. Any bug or other issue reported which is affecting the page's performance is classified as an error and should be resolved by the

service provider at no cost before the project's finalisation or liquated damages might apply (see section 2.4.5).

Code performance should also be taken into account in the implementation phase of each project development. At least 95% of newly developed pages should have a loading time smaller of equal to 7 sec/per page. In cases where performance is slower ENISA reserves the right to request liquidated damages as described below.

Page Loading time refers to the time it takes between when the server receives the request to serve a web page and the client (the browser) has fully loaded the page for the client. Page loading time consist of the network time and browser time.

Testing of newly developed code will be requested by ENISA on a case by case basis as part of the overall offer for new web development projects. The service provider should be able to propose appropriate tools to be used and set them up at the beginning of the contract.

2.3. Service level guaranteed for notification time and procedure

Notification Time is defined as the amount of time between when one agreement party detects an issue which impacts on the service and the time that the other agreement party is notified on it.

Indicator	Specifications	Typical	Measurement Unit
Notification Time	High	1	hour
Notification Time	Medium	2	hour
Notification Time	Low	4	hour

The service provider should immediately notify ENISA in case of a serious security threat (attacks, vulnerabilities etc.) as well when the web services are offline and in the event of any other critical issue, using a dedicated e-mail address.

The service provider is also supposed to inform ENISA and apply critical and regular 3rd party (e.g. Linux, Plone, open source libraries) patches when necessary. The service provider should also send monthly reports in which patches notifications will be included.

The notification procedure is the agreed procedure between ENISA and the service provider needed to be accomplished when any emergency occurs, according to the table indicators below:

Indicator	Specifications	Notification Channel
Emergency HIGH	Availability of any website is below 40%	Call and e-mail to dedicated ENISA account
Emergency MEDIUM	Availability of any website is below 60%	Sms and e-mail to dedicated ENISA account
Emergency Low	Availability of any website is below 90%	e-mail to dedicated ENISA account

Emergency HIGH: At least one of ENISA's websites and portals is not available or at least one of ENISA's servers is down for more than 1 hour.

2.4 Liquidated damages

Evaluation of contractual performance will be carried out by ENISA every month for web hosting services and per invoicing period for web development services.

Failure to fulfil the required service levels for one or more SLA indicators shall entitle ENISA to request liquidated damages hereafter described in % of the relevant service fee for e.g. web hosting or of the actual value for replying to a helpdesk issue, small change or big web development project.

2.4.1 Services Availability

Except under special conditions clearly specified the framework service contract (force –majeure), the service provider is supposed to deduct from the upcoming invoice 5% of the web hosting monthly fee of the affected service for each 30 minutes of downtime (up to 100% of customer's monthly fee for the affected service). The penalty will be waived for duly documented force-majeure.

2.4.2 Response and implementation time (help desk)

For each hour increment that the response or implementation time is above the time set for a reported bug of priority 1 (critical) liquidated damages of 2% of the actual request value (up to 50% of the actual value) will apply.

For each hour increment that the response or implementation time is above the time set for a reported bug of priority 2 (high) liquidated damages of 1% of the actual request value (up to 50% of the actual value) will apply.

For each 8-hour increment that the response or implementation time is above the time set for a reported bug of priority 3 (normal), liquidated damages of 0.5% of the actual request value (up to 50% of the actual value) will apply.

No liquidated damages are due for delays in the response time for incidents of priority 4 (low).

Any penalty will be waived for duly documented force-majeure or when the reasons for any delay are documented and previously agreed with ENISA. In addition, no penalties will be imposed when any delay is caused by ENISA's e.g. delayed response to a genuine request for clarification or feedback. Classification of incidents will be subject to mutual approval based on the classification as this is documented in this SLA.

2.4.3 Response time (request for proposals)

ENISA will record the send date and time of the acknowledgement email and the send date and time of the email containing the service provider's offer to a request for proposal.

ENISA will also record the time when requests for clarifications are received and when ENISA's email clarifications are delivered so that the time taken to provide clarifications can be deducted.

- A credit of 2% of the value of the request for service proposal for each day in addition to the response time agreed with ENISA but under 10 business days.
- A credit of 5% of the value of the request for service proposal for each day in addition to 10 business days (starting on the 11th business day) up until the 15th business day included

- A credit of 25% of the value of the request for service proposal for each day past the 15th business day (starting in the 16th business days)

The penalties will be credited to ENISA against future use of services. Again, the time taken by ENISA to respond to genuine request for clarifications will not be accounted for. No penalties will be imposed in case a delay has been previously agreed in writing between the service provider and ENISA or in case the service provider replies negatively to a request for proposal (e.g. because of the lack of resources.) The penalty will also be waived for duly documented force-majeure.

2.4.4 Delivery time (web development projects)

ENISA reserves the right to request liquidated damages in case the delivery and/or performance of services is delayed further from the deadlines which were agreed by both parties upon the signature of any purchase contract based on 'ENISA General Conditions'.

Any purchase contract associated with the framework contract related to this SLR is governed by the current 'ENISA General Conditions' published on the ENISA website and available for download at: http://www.enisa.europa.eu/procurement/related/procurement_gen_terms_conditions.pdf

The penalty will be waived for duly documented force-majeure or in cases where the extension is agreed by both parties in writing.

2.4.5 Service Quality

ENISA reserves the right to request liquidated damages before the finalization of a project in case the quality of a delivered service/product is deemed to be low. The quality will be measured using the relevant tools and indications mentioned in section 2.2.

Liquidated damages will be calculated based on the following formula:

AV= Average number of seconds above 7sec per page
AVE =Average number of errors above 5 errors per page
PG = Number of pages affected above 5% of total pages
V= 0.1 % of total project value

- Penalty = AV + PG * V
- Penalty = AVE+ PG * V

The penalty will be calculated once for pages which have more than 5 errors and loading time more than 7sec. The penalty will also be waived in special cases where different thresholds (e.g. a different loading time) are previously communicated, well documented and agreed by ENISA and the service provider in writing.

2.4.6 Notification time

Except under special conditions clearly specified in the framework service contract (force –majeure), the service provider is supposed to refund the customer 0.5% of the web hosting monthly fee for each hour of delay in notification time. The penalty will be waived for duly documented force-majeure.

3. Maintenance

3.1. General provisions

Maintenance operations that do not impact on the service will be done, when considered necessary, upon notification and agreement with ENISA.

This concerns in particular the server maintenance at operating system and application software level.

3.2. Scheduled maintenance

ENISA will be informed of any scheduled maintenance that may affect the service provided to ENISA. The service provider and ENISA will agree on the timing and nature of scheduled maintenance a minimum of two working days prior to the work taking place.

3.3. Emergency maintenance

Emergency maintenance means any time outside a scheduled maintenance window when the service provider needs to apply urgent patches or fixes, or undertake other urgent maintenance activities.

If Emergency maintenance is required, the service provider will contact ENISA and provide the expected start time and the planned duration of the Emergency Maintenance, and state whether it is expected that the Service will be unavailable during the Emergency Maintenance.

4. Procedures for the hosting and web development services provisioned

4.1. Procedure for damaged hard disks

Damaged hard disks and destroyed media will be shipped by the service provider by courier to ENISA, in order to be destroyed at ENISA's premises, as soon as it is certified that they are irretrievably damaged.

4.2. Disaster recovery

The service provider shall ensure that actual mechanisms are used to guarantee that the customers' data is available (online or offline) in case of failures forbidding access to it.

For example, in order to minimize downtime and assure the continuity of services, a mirroring solution with overnight syncs should be set up and be operational (to secure the operability of all services) in maximum one business day after the disaster strikes (the time it takes for restoring backups, DNS updates, IP relocations).

The Servers Room (s) should be locked, and access to it is only provided to the system administrator's team. All servers inside the Servers Room should have an Uninterruptible Power Supply unit attached.

The priority of recovery of web services as mentioned in section 2.2 will be followed.

4.3. Procedure for storage media handling

Back-up media should be encrypted and put in secure off-site storage. All information and media is considered as sensitive and should be kept secure and encrypted.

4.4. Security reports

The service provider will periodically send reports of the tests of systems integrity to the email address provided by ENISA.

The service provider should also send monthly reports about the attacks and incidents faced, both successful and unsuccessful attempts, and potential attacks and vulnerabilities, plus vulnerability assessment report every 6 months, to the same email address as stated above.

[Note: See 2.3, Service level guarantee for notification time and procedure]

5. Data Handling

Data portability

The service provider shall provide capabilities to export data, so it can still be used by the customer e.g., in the event of terminating the contract.

Accountability

The service provider should demonstrate that all appropriate steps have been taken in order to ensure that data protection principles have been implemented.

IT accountability is particularly important in order to investigate personal data breaches; to this end, the platform should provide reliable monitoring and logging mechanisms.

Data minimization

The service customer is responsible for ensuring that personal data are erased (by the provider and any subcontractors) from wherever they are stored as soon as they are no longer necessary for the specific purposes. On a case by case basis ENISA will request from the service provider to ensure that such temporary data are effectively deleted after a predefined period.

Standards and certification mechanisms

The service provider shall provide a list of the data protection codes of conduct, standards and certification mechanisms that the provider complies with.