SMART
ENERGY
LAB

Request for Proposal (RFP)

SEL Platform Cybersecurity:

Implementation of Foundational Framework Initiatives

17/03/2026

By Smart Energy Lab

Request for Proposal (RFP)
SEL Platform Cybersecurity:
Implementation of Foundational Framework Initiatives

Issued by:

Smart Energy LAB – Association

Av. 24 de Julho, 12, 1249-300, Lisboa - Portugal

procurement@smartenergylab.com

Date Issued: ***17/03/2026***

Table of contents

1. Introduction

1.1 Introduction to the RFP Document

The purpose of this Request for Proposal (RFP) is to select a qualified supplier to implement a prioritized set of foundational cybersecurity initiatives within Smart Energy Lab (SEL), in accordance with the requirements described in this document.

This RFP supports the implementation of Phase 1 of SEL's cybersecurity roadmap, aligned with internationally recognized standards and frameworks, including ISO/IEC 27001 and the NIST Cybersecurity Framework (NIST CSF 2.0), while taking into consideration the evolving regulatory landscape applicable to the energy sector.

The engagement focuses on operationalizing high-impact governance, risk management and technical control mechanisms that strengthen the cybersecurity posture of the SEL Platform, a cloud–edge energy management platform designed to support the deployment and operation of digital energy services across distributed energy environments.

This RFP does not aim to implement the full cybersecurity framework nor to achieve ISO 27001 certification or full NIST CSF 2.0 compliance within the duration of the contract. Instead, it establishes the foundational elements required to support long-term cybersecurity maturity, scalability and certification-readiness.

By executing this Phase 1 foundational framework initiative, SEL intends to enhance the platform's operational resilience, reinforce stakeholder trust and support its strategic positioning in an increasingly digital and regulated energy ecosystem.

This document is organized into the following chapters:

- **Chapter 1: Introduction**

  This chapter provides an overview of the Request for Proposal (RFP), outlining its purpose, structure and strategic context. It also presents Smart Energy Lab (SEL), its mission, and the background that motivates the present cybersecurity initiative.

- **Chapter 2: Instructions to Tenderers**

This chapter defines the administrative and procedural framework of the RFP process. It details eligibility conditions, exclusion grounds, pricing structure, submission requirements, and evaluation and award criteria.

- **Chapter 3: Scope of Work**

  This chapter describes the technical and operational requirements of the assignment. It defines the project's objectives, scope of services (Fixed and Variable), responsibilities of the Contractor and SEL, execution timeline, and expected deliverables.

In addition to these chapters, this RFP includes annexes that form an integral part of the tendering process and provide supplementary contractual information.

1.2 Smart Energy Lab

Smart Energy Lab (SEL) is a non-profit association that brings together science, technology, and industry in the energy sector, with renowned partners EDP Comercial and Accenture, and academic institutions such as Instituto Superior Técnico and INESC TEC. Through a collaborative model, SEL accelerates the development, implementation, and adoption of solutions to address the challenges of the energy transition.

Using innovation processes that include validation through market testing and pilots, SEL stands out by seeking competitive advantages that ensure market success, ranging from technological adaptation to cost reduction. Its main goal is to deliver products and services that promote the business of energy transition products offered by market players and their role in helping clients achieve carbon neutrality

1.3 "SEL Platform" development history and context

The energy sector is undergoing rapid transformation driven by renewable integration, electrification and the increasing decentralization of energy systems. As distributed energy resources (DERs), such as photovoltaic systems, batteries, electric vehicle chargers and heat pumps, become more widespread, both end-users and energy service providers face growing challenges in integrating, coordinating and optimizing these assets in real time, while ensuring alignment with corporate systems, energy markets and grid operators.

In response to these market dynamics, SEL progressively developed a portfolio of digital energy products and services designed to accelerate the energy transition. Although different in their specific applications, these solutions share common characteristics: enabling intelligent energy management, controlling local flexibility and supporting user-centric optimization strategies.

The initial drivers for the development of what would later become the SEL Platform included:

a) Accelerating the delivery of SEL's digital energy solutions and streamlining the implementation of new energy use cases;

b) Providing internal teams with a scalable and unified technological foundation through the reuse of previously developed technological assets and building blocks;

c) Strengthening control over hardware streams, cost efficiency and operational reliability, particularly regarding edge devices and embedded systems.

To address these needs, reusable technological building blocks were progressively developed and consolidated, ultimately leading to the creation of the SEL Platform.

Over time, the platform evolved from a set of internally developed components into a structured, service-oriented architecture with an API based approach, designed to enhance modularity, scalability and development efficiency. This architectural refactoring enabled clearer separation of core services and facilitated integration with external systems and third-party platforms.

The SEL Platform combines cloud-based orchestration and data services with edge-level control capabilities deployed in local facilities. This hybrid cloud–edge architecture enables:

- Real-time monitoring and control of distributed energy assets;
- Execution of energy optimization algorithms either centrally in the cloud or locally at the edge;

- Secure communication between edge devices and centralized services;
- Integration with corporate IT systems, operator platforms, aggregators and market interfaces;
- Centralized device fleet management, including remote configuration, monitoring and updates;
- Collection, storage and analysis of operational and energy-related data to support advanced energy services.

In parallel with the cloud architecture, SEL undertook efforts to standardize its local IoT controller devices to ensure consistency in hardware specifications, firmware management and operational oversight at the edge level.

Given its modular design, integration capabilities and intended scalability, the SEL Platform is structured to support diverse deployment scenarios and to serve as a foundational infrastructure for current and future digital energy services.

1.4 Strategic Opportunity

As an innovation-driven organization operating at the intersection of technology and the energy sector, SEL recognizes cybersecurity as a foundational enabler of the SEL Platform’s reliability, regulatory alignment and market credibility.

Through its technical expertise, sectoral engagement and interaction with key stakeholders, including potential adopters and alternative solution providers, SEL has identified a significant global market opportunity for the SEL Platform, particularly among organizations seeking to develop and deploy digital energy management products and services.

Several strategic factors reinforce the need for a structured and robust cybersecurity framework:

A. **Internal Use:** The SEL Platform is systematically reused to support the development and deployment of new digital energy products and services.

B. **Commercial Positioning:** The Platform is increasingly central to SEL’s commercial offering and must demonstrate compliance, security and deployment readiness in corporate environments.

C. **Market Transformation:** The rapid expansion of distributed energy resources, including electric vehicles, heat pumps, batteries and solar PV, is increasing the complexity of energy management systems across residential, commercial and industrial segments.

In response to these strategic drivers, SEL has previously undertaken a dedicated cybersecurity strategy definition phase, which established a structured roadmap aligned with internationally recognized standards and best practices.

The effective operationalization of that roadmap represents a critical next step to ensure the long-term resilience, scalability and competitiveness of the SEL Platform.

2. Instructions to Tenderers

2.1 General provisions

This section establishes the following general rules applicable to this Request for Proposal (RFP), complementing the specific instructions and requirements detailed throughout the document:

- The purpose of this RFP is to select a qualified supplier to implement prioritized cybersecurity initiatives within a three (3) month execution period, as described in the Scope of Work.
- This engagement does not aim to achieve full ISO 27001 certification or full NIST Cybersecurity Framework (CSF) 2.0 compliance, but to establish foundational governance, control and operational capabilities contributing to that objective.
- This RFP constitutes an open tender procedure. Participation is open to all entities that demonstrate compliance with the eligibility, qualification and experience requirements set forth herein.
- Intellectual property rights arising from the work performed under the resulting contract, including, without limitation, documentation, templates, processes and configuration deliverables, shall belong to Smart Energy Lab upon full payment in accordance with the terms and conditions defined in Annex I.
- This RFP does not oblige Smart Energy Lab to award a contract or to reimburse any costs related to the preparation and submission of proposals.
- Communication shall be carried out in Portuguese or English; proposals and deliverables shall be submitted in English. All prices shall be expressed in euros (€).
- This RFP and any resulting contract shall be governed by Portuguese law. Any dispute arising from the interpretation, validity or execution of the contract shall fall under the exclusive jurisdiction of the District Court of Lisbon, with express waiver of any other jurisdiction.

2.2 Timeline for the RFP

Smart Energy Lab has established the following preliminary milestones for the process of the RFP, which are subject to modifications by Smart Energy Lab:

Table 1 – Milestones of the RFP Process

Milestone	**Dates**
Publication of the RFP	17/03/2026
Deadline for the submission of questions by the Tenderers	21/03/2026, until 12:00 GMT+0
Deadline for issuing responses to the Tenderers' questions	24/03/2026, until 23:59 GMT+0
Deadline for the Submission of Proposals	28/03/2026, until 23:59 GMT+0
Deadline for the correction of formal irregularities by the Tenderers	30/03/2026, until 23:59 GMT+0
Deadline for the Publication of the Preliminary Report (**estimated**)	03/04/2026
Deadline for Tenderers to submit their observations to the Preliminary Report	5 calendar days after publication of the Preliminary Report
Deadline for the Publication of the Final Report (**estimated**)	08/04/2026
Deadline for the submission of the Qualification Documents by the Tenderer (**estimated**)	13/04/2026
Project start (**estimated**)	17/04/2026

2.3 Requests for clarification

From the date of the publication of the Request for Proposals until the 21st of March of 2026, 12h00 (Lisbon time, GMT+0), interested parties may submit any requests for clarification necessary for a proper understanding and interpretation of the RFP, to the following email address:

- **procurement@smartenergylab.com**

Requests for Clarification should be submitted with the following subject line:

- ***Request for Clarification – RFP SEL Platform Cybersecurity [Tenderer Company Name]***

Clarifications are notified by SEL within a reasonable time to all interested parties.

2.4 Submission Instructions

Tenderers may submit their Proposals until the 28th of March of 2026, 23:59 (Lisbon time, GMT+0), to the following email address:

- **procurement@smartenergylab.com**

For the submission of proposals, the following subject line should be used:

- ***Proposal Submission – RFP SEL Platform Cybersecurity [Tenderer Company Name]***

For the submission of Proposals, Tenderers must follow what is requested in the following section of this document (2.5 Proposal Organization and Content).

2.5 Proposal Organization and Content

Aligned with the defined Criteria Award (Section 2.8 of this RFP), this section establishes the mandatory requirements regarding the structure and content of the proposals to be submitted by the Tenderers.

For technical scope and detailed service description, Tenderers must refer to Section 3 Terms of reference.

1. **Tenderer Presentation and Relevant Experience**
   a) Document containing the Company background, organizational structure and core areas of expertise in cybersecurity framework implementation (preferably for similar projects).
   b) Structured portfolio evidencing compliance with the experience requirements defined in Section 2.7, including **at least eight (8) relevant** cybersecurity framework implementation projects completed **within the last four (4) years**.
   For each referenced project, the Tenderer must provide:
      - Identification of the client sector (with explicit indication of projects in energy, utilities, telecommunications or other critical infrastructure sectors) and approximate organizational size (e.g. EBITDA);
      - Project duration and implementation timeline;
      - Detailed project scope and implementation challenges;
      - Clear identification of the role performed by the team members;
      - Description of implemented frameworks and controls (including ISO 27001 and/or NIST CSF where applicable);
      - Outcomes and measurable impact achieved.

   The portfolio must clearly identify which projects correspond to:
      - ISO 27001 implementation or certification-readiness operationalization;
      - NIST Cybersecurity Framework implementation or structured alignment (including NIST CSF 2.0);
      - Implementation of one or more of the foundational initiatives defined in this RFP scope (Section 3).
2. **Proposed Team**
   a) Description of the governance and organization of the proposed team, including key roles and responsibilities.

b) Identification of key experts and confirmation of their direct involvement throughout the project execution period.

c) Sanitized CVs of the proposed team members, including:
- Academic and professional background;
- Relevant professional certifications (e.g., ISO 27001 Lead Implementer, ISO 27001 Lead Auditor, CISSP, OSCP, CEH, CISM or other relevant certifications);
- Years of relevant professional experience;
- Direct participation in ISO 27001, NIST 2.0 and prioritized domain implementations;
- Experience in projects conducted in energy, utilities, telecommunications or other critical infrastructure environments (where applicable).

3. Methodology, Work Plan and Feasibility

a) Document containing the proposed implementation methodology, including:
- Technical and operational approach;
- Implementation phases and sequencing;
- Operationalization mechanisms (e.g., structured workshops, governance embedding, process integration, validation sessions, configuration support);
- Clear demonstration of understanding of SEL's technological platform context and its cybersecurity exposure;
- Consideration of regulatory exposure and sector-specific risks;
- Assumptions, identified risks and mitigation strategies;
- Deliverables and validation mechanisms;
- Knowledge transfer activities and mechanisms to ensure long-term sustainability of implemented controls beyond the execution period.

b) Detailed work plan including:
- Description of activities and tasks;
- Allocation of team members per workstream;
- Milestones and Gantt Chart;
- Confirmation of delivery within the three (3) month execution period;
- Description of proposed acceleration strategies and delivery assurance mechanisms.

4. **Financial Proposal**
    a) Document indicating the detailed pricing structure, specifying:
    - Fixed Service total price (which **may not exceed 95,000.00 €, under penalty of exclusion**);
    - Unit price per penetration test (which **may not exceed 7,000.00 €, under penalty of exclusion**);
    - Blended hourly-based technical support rate (which **may not exceed 100.00 €/hour, under penalty of exclusion**).

Due to the nature of this RFP procedure, proposals will be shared amongst all the tenderers.

For commercial, industrial or other confidentiality reasons, tenderers may request, when submitting their proposal, that certain documents which constitute the proposal be classified in accordance with the law, for the purpose of restricting or limiting access to them to the extent strictly necessary.

SEL will decide on the classification of the documents that constitute the proposal and will notify the tenderers when the proposals are opened.

2.6 Formal Irregularities

If any formal irregularities in the proposals received are encountered, Smart Energy Lab will request Tenderers to remedy them within two (2) days. Those remedies must not change the content of the proposals or beach the principles of equal treatment and fair competition. Those irregularities may include the failure to submit or incorrect submission of documents that merely prove facts or qualities prior to the date of submission of the application or tender.

2.7 Exclusion Grounds

The proposal will be excluded, if the company does not comply with the following requirements:

a) The price of Fixed Service, exceeds 95,000.00€ (ninety five thousand euros).
b) The unit prices for the Variable Services exceed the following limits:

- Penetration Testing: 7,000.00 € (seven thousand euros) per system application tested;
- Hourly-Based Technical Support: 100.00 € (one hundred euros) as blended hourly rate.

c) The proposal includes minimum service commitments, bundled quantities, or pricing structures for Variable Services that may result in a total amount exceeding 30,000.00 € (thirty thousand euros) during the contract duration.

d) The proposed timeline exceeds the maximum delivery period of three (3) months from the project start.

e) Lack of portfolio documentation evidencing at least eight (8) relevant Cybersecurity framework implementation projects (not solely advisory or assessment) in technological platforms, completed within the last four (4) years.

From those eight (8) projects, at least:

- Four (4) **must involve** ISO 27001 implementation or certification-readiness operationalization;
- Four (4) **must involve** NIST Cybersecurity Framework implementation or structured alignment (including NIST CSF 2.0 or equivalent updated versions);
- Four (4) **must demonstrate** practical implementation of the prioritized domains defined in section 3 of this this RFP.

Each referenced **project must include**:

- Description of client type (sector and approximate size: e.g: EBITDA);
- Project dates and duration;
- Project scope and implementation challenges;
- Role performed by the bidder;
- Outcomes and measurable impact;
- Indication of whether the project involved international or cross-border context (where applicable).

f) Terms and Conditions of the project delivery, including warranties, limitations, exclusions and support terms that are not compatible with the critical imperative conditions presented in Annex I - Imperative conditions to be respected by the winning tenderer.

2.8 Criteria Award

Proposals will be evaluated based on the following factors:

Table 2 – Criteria award factors

Factor	Criterion	Weight (%)
A	Team experience and qualifications	35%
B	Technical project quality	35%
C	Cost	30%

The award will be made to the proposal with the highest Final Score (FS), calculated using the following formula:

$$FS = [0{,}35 \times A] + [0{,}35 \times B] + [0{,}30 \times C]$$

Where:

- FS – Final score of the bidder's proposal;
- A – Score obtained in factor A, *"Team experience and qualifications"*;
- B – Score obtained in factor B, *"Technical project quality"*;
- C – Score obtained in factor C, *"Cost"*.

Factor *A*: "Team experience and qualifications" score

The score for each proposal under Factor A will be calculated as follows:

$$A = [0{,}25 \times A1] + [0{,}20 \times A2] + [0{,}20 \text{ x } A3] + [0{,}15 \text{ x } A4] + [0{,}20 \text{ x } A5]$$

Where:

Table 3 – Criteria award subfactor A

Subfactor	Subcriteria	Descriptor	Weight
A1	ISO 27001 Operational Implementation Experience	Assess the project team's relevant **participation in ISO 27001 implementation** or certification-readiness projects. Emphasis will be placed on **operational implementation (not solely advisory)**, role performed by proposed team members, complexity of projects, measurable outcomes achieved, and on concrete and recent experience (in the last 4 years).	**25%**
A2	NIST Cybersecurity (CSF 2.0) Framework Implementation Experience	Assess the project team's effective participation in NIST Cybersecurity Framework implementation or structured alignment projects **(including NIST CSF 2.0,** in the last 4 years). Emphasis on integration with governance and risk management, demonstrated maturity uplift, and on concrete and recent experience (in the last 4 years).	**20%**
A3	Implementation of Prioritized Domains	Assess the project team's practical experience in implementing Governance, Risk Management, IAM, Secure SDLC, BC/DR, and Third-Party Risk Management.. Emphasis is placed on concrete and recent experience (in the last 4 years). Evidence of direct operational involvement of proposed team members will be particularly valued.	**20%**
A4	Sector Experience	Assess the project team's experience in projects conducted in the energy sector, utilities, critical infrastructure, or telecommunications. Greater relevance will be attributed to direct participation in energy or utilities environments.	**15%**
A5	Qualifications and Certifications	Assess project team's academic and professional background, professional seniority, and cybersecurity certifications of the proposed team members (e.g., ISO 27001 Lead Implementer, ISO 27001 Lead Auditor, CISSP, OSCP, CEH, or other relevant).	**20%**

The scores for subfactors A1 through to A5 will be assigned based on a rating scale from 0 to 10, where 0 represents the lowest score and 10 the highest.

Factor B: "Technical project quality" score

The score for each proposal under Factor B will be calculated as follows:

$$B = [0{,}25 \times B1] + [0{,}20 \times B2] + [0{,}20 \text{ x } B3] + [0{,}15 \text{ x } \mathrm{B4}] + [0{,}10 \text{ x } \mathrm{B5}] + [0{,}10 \text{ x } \mathrm{B6}]$$

Where:

Table 4 – Criteria award subfactor B

Subfactor	Subcriteria	Descriptor	Weight
B1	Clarity and Robustness of Implementation Methodology	Assess the logical structure, sequencing and internal coherence of the proposed implementation methodology. Evaluation will consider the definition of workstreams, alignment between objectives and deliverables, **feasibility within the three (3) month execution period**, and evidence of structured implementation logic rather than generic consulting narratives.	**25%**
B2	Adequacy to SEL's Context and Technological Platform	Assess the bidder's understanding of SEL's technological platform environment and its cybersecurity exposure. Evaluation will consider adaptation of frameworks to digital and platform-based environments, regulatory awareness, and degree of contextualization versus generic framework application.	**20%**
B3	Operationalization Approach	Assess the existence of concrete mechanisms to operationalize the prioritized initiatives during the execution period. Evaluation will consider structured workshops, governance activation, process embedding, validation sessions and practical enablement activities. Proposals predominantly focused on documentation production will receive a reduced score.	**20%**

Subfactor	**Subcriteria**	**Descriptor**	**Weight**
B4	Risk Mitigation and Delivery Assurance	Assess identification of implementation risks, mitigation strategies, milestone control mechanisms and realism of workload planning within the defined timeframe. Proposals underestimating complexity or lacking delivery control will receive a reduced score.	**15%**
B5	Knowledge Transfer and Sustainability	Assess the approach to ensure long-term sustainability of implemented controls, including knowledge transfer, usability of deliverables, responsibility assignment within SEL and continuous improvement mechanisms.	**10%**
B6	Resource Allocation and Delivery Commitment	Assess the credibility of the proposed team allocation model, workload distribution, availability of key profiles and assurance of their continuous involvement throughout the engagement.	**10%**

The scores for subfactors B1 through to B6 will be assigned based on a rating scale from 0 to 10, where 0 represents the lowest score and 10 the highest.

Factor C: "Cost" score

The score for each proposal under Factor C will be determined as follows:

C = [0,60 × $C1$] + [0,15 × $C2$] + [0,25 × $C3$]

Where:

C1: Score for Fixed Service Price (Price$_{C1}$) of the foundational Cybersecurity initiatives (described in section 3)

The score for each proposal under Subfactor C1 will be calculated as follows:

- If Price$_{C1}$> 95.000,00 €, then the proposal will be excluded;
- If Price$_{C1}$≤ 95.000,00 €, then:

$$C1 = -0,\ 36 \text{ x Price}_{C1} + 35{,}20$$

C2: Score for Variable Service Unitary Price (Price$_{C2}$) of Cybersecurity- Penetration Testing (Individual System Application Security Testing)

The score for each proposal under Subfactor C2 will be calculated as follows:

- If Price$_{C2}$> 7.000,00 €, then the proposal will be excluded;
- If Price$_{C2}$≤ 7.000,00 €, then:

$$C2 = -4{,}5 \text{ x Price}_{C2} + 32{,}5$$

C3: Score for Variable Service Unitary Price (Price$_{C3}$) of Cybersecurity- Hourly-Based Technical Support

The score for each proposal under Subfactor C3 will be calculated as follows:

- If Price$_{C3}$> 100,00 €, then the proposal will be excluded;
- If Price$_{C3}$≤ 100,00 €, then:

$$C3 = -0{,}18 \text{ x Price}_{C3} + 19$$

2.9 Panel or jury composition

The proposals submitted in response to this Request for Proposals will be evaluated by an evaluation jury composed of a minimum of four (4) members designated by SEL. The jury members will be selected based on their relevant expertise and experience to ensure an objective, fair, and comprehensive evaluation of the proposals. SEL reserves the right to modify the composition of the jury, including the number of members, as deemed necessary to support the evaluation process.

2.10 Preliminary and final reports

After evaluating the proposals, SEL will issue a preliminary report, in which it will propose the admission/exclusion of proposals according to section 2.7 of this RFP, and classifying the admitted proposals, according to the award criteria established in section 2.8.

SEL will notify all tenderers of a preliminary report, together with the proposals submitted.

The tenderers may submit their observations on the preliminary report in writing, using the e-mail address procurement@smartenergylab.com within 5 days after the publication of the Preliminary Report.

SEL issues a final report in which it considers the observations made by the tenderers and notifies it to all the tenderers.

When the final report results in a change to the ordering of the tenders contained in the preliminary report, SEL proceeds to a new prior hearing.

2.11 Qualification documents

SEL notifies the winning Tenderer to submit within 5 calendar days after the publication of the Final Report the following qualification documents:

1) The certificate of commercial registry ("*Certidão Permanente do Registo Comercial*") or equivalent document in the State of which it is a national or in which its main establishment is located.

2) Documentation proving that the winning Tenderer is not in breach of its obligations relating to the payment of taxes in Portugal or, where applicable, in the State of which it is a national or in which its main establishment is located.

3) Documentation proving that the winning Tenderer is not in breach of its obligations relating to the payment of social security contributions in Portugal or, where applicable, in the State of which it is a national or in which its main establishment is located.

The deadline for submission of qualification documents may be extended, at the request of the winning Tenderer, for a period not exceeding 5 days.

Failure to submit the required qualification documents within the established deadline will result in the contract not being awarded to the winning Tenderer, in which case Smart Energy Lab may award the contract to the next highest Tenderer.

2.12 Price and payment method

2.12.1 Price

The **total price indicated in the awarded proposal may not exceed 125,000.00 €** (one hundred and ninety-five thousand euros), plus VAT at the rate in force on the date of payment.

The total price comprises the following parcels, categorized as **i) Fixed Service** and **ii) Variable Services**

i) **Fixed Service**

Maximum price for Fixed Service:

The Fixed Service price may not exceed 95,000.00 € (ninety-five thousand euros) for the delivery of the cybersecurity initiatives defined in the section 3 of this RFP.
Proposals exceeding this amount shall be excluded.

Abnormally low price for Fixed Service:
The total price proposed for the Fixed Service included in the Contract is considered abnormally low if it is less than 70,000.00 € (seventy thousand euros).
If the price submitted is abnormally low, Smart Energy Lab will ask the respective tenderer to provide clarifications, within an appropriate time limit, regarding the relevant components of their proposal.
Proposals containing an abnormally low price, for which no supporting explanations have been submitted or which are not considered sufficient, will be excluded.

ii) **Variable Service**:

Optionality character:

The Variable Services shall be payable exclusively in proportion to the services effectively requested in writing by SEL, duly executed by the Contractor, and validated in accordance with the contractual requirements.

Given their optional nature, no minimum volume of Variable Services is guaranteed under the Contract.

The total cumulative amount payable under all Variable Services shall not exceed 30,000.00 € (thirty thousand euros) during the contract duration.

The Variable Services comprise:

a) Penetration Testing (Individual System Application Security Testing);
b) Hourly-Based Technical Support.

Maximum Price for Variable Services

a) Penetration Testing Maximum unit price

This service corresponds to the individual Application Security Testing.

The bidder must present a unit price per system application tested.

The **unit price per system application tested may not exceed €7,000.00 (seven thousand euros), individually**.

Proposals exceeding this amount shall be excluded.

Abnormally low price for Penetration Testing:

The total price proposed for the Penetration Testing included in the Contract is considered abnormally low if it is less than 5,000.00 € (five thousand euros). If the price submitted is abnormally low, Smart Energy Lab will ask the respective tenderer to provide clarifications, within an appropriate time limit, regarding the relevant components of their proposal.

Proposals containing an abnormally low price, for which no supporting explanations have been submitted or which are not considered sufficient, will be excluded.

b) Hourly-Based Technical Support Maximum hourly rate

This service corresponds to operational and technical support activities, including but not limited to:

- Support to Secure Software Development Lifecycle (SDLC) practices and validation of security mechanisms.
- Configuration and tuning of cybersecurity tools and security controls.
- Technical adjustments related to the cybersecurity controls implemented under the Fixed Service.
- Support to the configuration and implementation of specific technical security measures (e.g., VPN access rules, network security configurations, access control mechanisms).
- Support to the implementation of additional cybersecurity initiatives or adjustments not explicitly covered under the Fixed Service.

The **blended hourly rate may not exceed 100.00 €/hour (one hundred euros)**.

Proposals exceeding this rate shall be excluded.

Abnormally low price for Hourly-Based Technical Support:
The total price proposed for the Hourly-Based Technical Support included in the Contract is considered abnormally low if it is less than **50.00 €/hour (fifty euros per hour)**.
If the price submitted is abnormally low, Smart Energy Lab will ask the respective tenderer to provide clarifications, within an appropriate time limit, regarding the relevant components of their proposal.
Proposals containing an abnormally low price, for which no supporting explanations have been submitted or which are not considered sufficient, will be excluded.

2.12.2 Payment Schedule

The price will be paid by Smart Energy Lab upon formal validation and acceptance of the following milestones:

i) Fixed Service

- Project kick-off – **34% of the total fixed price**

- After steering review confirming the delivery and validation of the outputs related to the following initiatives, detailed in section 3 of the RFP:

  - Governance, Operating Model and Organization
  - Policies and Standards
  - Identity and Access Management
  - Risk Management

  – **33% of the total fixed price**

- After final project steering and validation of the outputs related to the remaining initiatives of section 3 of the RFP and project handover completion – **33% of the total fixed price**

ii) Variable Service

a) For each System Application Security Testing requested:
   - 100% of unit price upon delivery of test results.

b) Hourly-Based Technical Support
   - Payment will be made based on the number of hours effectively requested and validated by Smart Energy Lab.

3. Terms of Reference

3.1 Background

Smart Energy Lab (SEL) has defined a cybersecurity strategy for the SEL Platform, aligned with internationally recognized standards and frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework (NIST CSF 2.0).

During the cybersecurity strategy definition phase, several foundational elements of the cybersecurity framework were initially defined and documented. These include, among others, the cybersecurity governance model, an Information Security Policy, Secure Software Development Lifecycle (SDLC) strategy and supporting training materials, as well as initial penetration testing assessments. These elements serve as a baseline for the implementation activities and may be refined or adapted during the execution of the project as required.

This Request for Proposal focuses on the implementation of phase 1 of the cybersecurity roadmap defined for the SEL Platform. The objective of this assignment is to operationalize, refine and integrate the existing cybersecurity framework elements into SEL's operational processes, strengthening the platform's security posture and establishing the foundations for long-term cybersecurity maturity.

3.2 Main Objective of the Project

The main objective of this project is to strengthen the organization's overall security posture and establish a solid foundation for long-term cybersecurity maturity, by implementing a set of fundamental foundational cybersecurity framework initiatives.

These initiatives focus on the following domains:

I. Governance, Operating Model and Organization

II. Policies and Standards

III. Identity and Access Management

IV. Secure Software Development Management

V. Risk Management

VI. Business Continuity Plan

VII. Third Party and Supply Chain Risk Management

More specifically, the project aims to operationalize cybersecurity governance, strengthen risk management practices, implement structured access management mechanisms, reinforce secure development processes, improve organizational resilience and ensure adequate oversight of third-party cybersecurity risks.

The activities described in this section build upon the cybersecurity strategy and initial framework elements previously developed by SEL.

3.3 Scope of Work

The scope of this collaboration includes **strategic, analytical, and execution-oriented activities** required to design, implement and support the defined initiatives across governance, policies, resilience, risk management, software development, identity and access management and third-party risk domains.

Throughout the project, the selected organization is expected to work closely with SEL's internal teams and relevant stakeholders providing both strategic guidance and implementation capabilities to ensure effective delivery, sustainable adoption and measurable improvement of the organization's cybersecurity maturity.

Deliverables produced under this assignment must be properly documented, operationalized and validated in collaboration with SEL.

Responsibilities of the Contractor

The Contractor shall be responsible for:

- Delivering all activities described in the Scope of Work and associated deliverables.
- Ensuring alignment with the cybersecurity strategy previously defined by SEL.
- Providing the required technical expertise and implementation support across the defined cybersecurity domains.
- Maintaining clear communication regarding project progress, risks and implementation challenges.
- Supporting the validation and operationalization of implemented controls and processes.

Responsibilities of Smart Energy Lab

Smart Energy Lab shall:

- Provide access to relevant documentation, systems and internal stakeholders required for the implementation of the project.
- Review and validate deliverables produced during the project.
- Facilitate coordination with internal teams and the appointed CISO.
- Provide feedback and approval within the defined project governance framework.

3.3.1 Governance, Operating Model and Organization

Key objectives:

- Support on the SEL's CISO onboarding process and assuring the activation of the defined governance model, by clarifying roles and responsibilities across the organization, establishing clear ownership, accountability and integration into business operations.
- Enhance the implementation of structured risk oversight and reporting mechanisms, including KPIs and governance reporting to support informed decision-making.

Mandatory Deliverables:

- Implement the SEL's existing **cybersecurity governance model**, operationalizing the accountabilities, responsibilities of the established roles, committees and decision flows.
- **Governance reporting framework** and **security KPIs** implemented.
- **Governance activation workshops/training and establishment of the reporting routines**.

3.3.2 Policies and Standards

Key objectives:

- Support and refine the development of the existing SEL's cybersecurity policy framework aligned with organizational objectives and regulatory requirements covering all relevant security domains according to the ISO 27001 and NIST CSF 2.0 frameworks. This includes access controls, training and awareness, asset and vulnerability management, business continuity, backups, platform and application security, data classification and protection, incident response and vendor requirements.

- Ensure organization-wide communication and acknowledgment of cybersecurity policies to promote awareness, accountability, and compliance.
- Establish enforcement and compliance mechanisms, including audits, monitoring activities, and disciplinary measures for policy violations.
- Implement a structured review and update process to keep policies current with evolving technologies, regulatory changes, and business developments.

Mandatory Deliverables:

- Report a **consolidated and updated cybersecurity policy framework** aligned with SEL's objectives and applicable regulations.
- Document **policy communication templates** and enforcement procedures across the organization.
- Process implementation for **annual review and update reporting** to ensure continuous awareness and effectiveness of cybersecurity policies.

3.3.3 Identity and Access Management

Key objectives:

- Establish a structured identity and access governance framework to manage user access across SEL's organizational tools and platforms.
- Define and operationalize identity lifecycle management processes (Joiner, Mover, Leaver) to ensure consistent access provisioning, modification and revocation.
- Strengthen access control mechanisms by enforcing least-privilege principles, structured role models (RBAC) and clear access request and approval workflows.
- Improve visibility and oversight of user entitlements across organizational tools through periodic access reviews and segregation-of-duties validation.
- Strengthen password management practices, particularly for shared or privileged accounts, through appropriate password policies and the use of password vault mechanisms.

Mandatory Deliverables:

- **Support the Identity and access governance framework definition**, including processes for access request, approval, provisioning, modification and revocation.
- IAM governance guidelines and configuration documentation delivered to support operational continuity.
- Role-based access control (RBAC) model definition for selected organizational tools.
- Password management practices define and support, including password generation standards and password rotation policies for all company accounts.
- Support in the Joiner–Mover–Leaver (JLM) processes definition, aligned with HR onboarding and offboarding procedures.
- Support provided to SEL teams in configuring roles, groups and permissions across selected organizational tools, ensuring alignment with the defined access governance model.
- Access review procedures established, and initial access review conducted for selected systems.

3.3.4 Secure Software Development Management

Key objectives:

- Ensure development and operational activities are driven by identified risks and approved treatment plans, reinforcing accountability and traceability.
- Maintain comprehensive and auditable evidence of requirements, testing, reviews, approvals, and continuous improvement actions.
- Support the implementation of DAST, SAST and SCA ensuring the alignment of software development activities with risk and compliance requirements.

Mandatory Deliverables:

- **Support the refinement and improvement of secure SDLC management framework, and governance guidelines** including recommended security checkpoints, validation procedures, documentation practices for development activities, exception criteria and approval process.
- **Support and validation of the integration of SAST, DAST and SCA** mechanisms into the existing software development lifecycle.
- Provide training workshops on SDLC defined procedures and support the establishment of monitoring and improvement routines.

3.3.5 Risk Management

Key Objectives:

- Establish a structured and standardized risk management methodology, aligned with the organization's overall risk strategy and governance framework.
- Systematically identify and assess threats and vulnerabilities affecting critical assets and processes, leveraging both internal monitoring and external intelligence sources.
- Prioritize mitigation efforts based on business impact, using BIA outputs and consistent risk scoring or quantification models.
- Integrate risk insights into executive reporting and decision-making, ensuring that risk exposure directly informs resource allocation and strategic planning.
- Implement formal mechanisms for lessons learned and continuous improvement, incorporating findings from incidents, audits, and reviews into process and control enhancements.
- Ensure transparency and accountability through documented tracking, defined ownership, and regular reporting to governance bodies.
- Create feedback loops between risk metrics and control improvements, ensuring that performance indicators actively drive security posture enhancement.

Mandatory Deliverables:

- Document a **risk assessment framework**, delineating methodologies and assessment templates.
- **Inventory** of all critical assets and cybersecurity vulnerabilities.
- Document both **risk scoring and evaluation methodologies.**

3.3.6 Business Continuity Plan

Key objectives:

- Conduct a comprehensive Business Impact Analysis (BIA) to identify critical services, systems, and dependencies, defining and documenting Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) aligned with business priorities and with a risk assessment to evaluate potential disruption scenarios and their impact.
- Design and document a formal Business Continuity Plan (BCP) covering essential processes and operational continuity strategies, a transversal incident recovery framework that clearly defines roles, responsibilities and escalation paths. Align BCP with risk management and incident management processes to ensure a coordinated response model, ensuring all recovery strategies are consistent with critical business objectives.
- Conduct structured simulations and exercises to validate preparedness for disruption. Assure and prepare regular continuity and recovery testing to assess plan effectiveness and identify gaps.
- Document execution results of BCP tests and real recovery events. Conduct structured post-incident and post-test reviews to evaluate performance and identify improvement actions, updating recovery plans and strategies based on lessons learned.

Mandatory Deliverables:

- **Business Impact Analysis** report, documenting critical services, systems, dependencies and approved RTO/RPO.

- Document a **Business Continuity Plan** assuring coverage of recovery and escalation procedures
- Report **BCP testing results** and a consequent improvement action plan.
- Document **improvement guidelines** for continuous iteration of resilience's procedures and strategies.

3.3.7 Third-Party and Supply Chain Risk Management

Key Objectives:

- Define and formalize a Cyber Supply Chain Risk Management (C-SCRM) strategy, establishing responsibilities and a structured approach to managing risks introduced by external partners and suppliers.
- Implement a risk-based vendor assessment framework, identifying critical third parties and/or suppliers. Assure integration of cybersecurity and regulatory requirements into procurement processes and contracts.
- Establish continuous oversight mechanisms, including periodic reassessments, security attestations, and threat intelligence monitoring to maintain visibility over supplier risk exposure.
- Strengthen incident and vulnerability management across the supply chain, ensuring timely reporting, coordinated response and mitigation of third-party security issues.
- Enforce mandatory cybersecurity risk evaluations prior to onboarding new vendors, systems, or services, preventing unmanaged risk from entering the environment.

Mandatory Deliverables:

- **Document a C-SCRM strategy** and governance model implemented
- **Vendor risk assessment framework**, including evaluation methodology and templates.
- Document **third-party cybersecurity requirements** for procurement and onboarding, monitoring procedures and incident reporting templates.

Note to Respondents: The listed objectives and deliverables represent SEL's mandatory objectives and deliverables for the Scope of work. Respondents are welcome to propose enhancing methodologies to deliver the required outcomes and additional deliverables that can boost the overall quality of the mandatory targets delivery and add confidence to the results. Any additional element should be clearly identified and should not.

3.4 Project Execution Timeline and Deliverables

The project shall be completed within a maximum period of three (3) months from the contract start date.

Given the multi-domain nature of the cybersecurity initiatives covered by this assignment, the activities described in this RFP may be executed in parallel, according to the methodology proposed by the Contractor and validated by Smart Energy Lab.

Tenderers shall present a proposed work plan including the sequence of activities, allocation of resources and expected timeline for the implementation of the defined initiatives.

The work plan shall ensure that all mandatory deliverables described in this Terms of Reference are completed within the maximum execution period.

The Contractor shall submit a detailed project plan during the project initiation phase, including the proposed timeline, milestones, governance model and communication schedule.

The Contractor shall ensure that **intermediate outputs related to the different cybersecurity initiatives are progressively delivered throughout the project duration to enable validation and feedback by Smart Energy Lab.**

3.5 Expert Team

The Tenderer shall propose a multidisciplinary **Expert Team** with the combined technical and managerial competencies required to ensure the successful and timely implementation of the services described in this RFP.

The proposed team shall be capable of supporting both the **Fixed Service activities** and the potential **Variable Services**, including penetration testing and technical cybersecurity support.

The Expert Team shall, at a minimum, include the following key roles:

- **One Project Manager / Cybersecurity Lead**, responsible for overall project coordination and engagement with Smart Energy Lab.
- **One Senior Cybersecurity Expert**, with relevant experience in cybersecurity frameworks implementation (e.g., ISO/IEC 27001, NIST Cybersecurity Framework CSF 2.0).
- **One Cybersecurity Technical Specialist**, supporting the operational implementation of the cybersecurity initiatives and potential technical support activities.
- Senior experts are expected to dedicate, on average, **at least 20% of their working time to the project** over its duration.

Tenderers may propose additional roles or an alternative team composition, provided that the minimum requirements outlined above are fully met and the proposed structure demonstrably supports the effective delivery of the services defined in this RFP.

Experience

- The **Project Manager** must have proven experience in managing at least one cybersecurity project of similar scope and dimension in the last five (5) years.
- The proposed team must demonstrate **relevant experience in cybersecurity framework implementation and operational support**, particularly in areas such as governance, risk management, identity and access management, secure software development lifecycle, business continuity, third-party risk management, and security testing.

Communication

- The team should be fluent in **Portuguese and English**, and capable of producing documentation and deliverables in English.

3.6 Reporting and Communication

The Contractor shall ensure continuous and transparent communication with the Smart Energy Lab (SEL) project team throughout all phases of the assignment. Regular monitoring and reporting are required to ensure that progress, risks, and deliverables remain aligned with the approved work plan.

Meetings

- A bi-weekly meeting (remote or in-person) shall be held to review progress, discuss ongoing activities, and address potential risks or deviations.
- Ad-hoc meetings may be scheduled at SEL's request, particularly for deliverable validation or technical reviews.

Communication Channels

All formal communications shall be made via email and through the designated SEL contact point, defined at project start.

Informal or day-to-day exchanges may occur directly between technical counterparts using mutually agreed tools (e.g. Teams), provided that key decisions are documented and shared formally.

Deviations

Any deviation from the agreed scope, schedule, or deliverables shall be immediately communicated in writing to SEL. SEL will review and decide on the necessary corrective actions, which must be documented and approved before implementation.

Annex I – Imperative conditions to be respected by the winning tenderer

Clause 1

(Intellectual and Industrial Property)

1. All inventions, suggestions for technical improvements, and/or other similar creative activities, created or developed by the collaborators assigned by the winning tenderer or for the execution of the Contract, including all creations subject to registration of industrial property rights and copyrights (“Intellectual Property Creations”) that are in any way relevant to SEL's activities must be immediately communicated to SEL.

2. The winning tenderer undertakes to obtain from its collaborators assigned to the service provision all necessary authorizations and declarations, so that the intellectual property belongs to SEL, and the winning tenderer is responsible for providing adequate compensation for this purpose.

3. Likewise, the winning tenderer undertakes to agree with the collaborators assigned to the provision of services on a clause that allows SEL to hold ownership of the rights over the Intellectual Property Creations, even if they have been developed outside the scope of the services provided by the winning tenderer.

4. The Parties expressly agree that the aforementioned Intellectual Property Creations are the exclusive property of SEL and that all intellectual property rights and economic copyrights will be assigned to SEL, with the winning tenderer obliged to obtain from the collaborators assigned to the service provision the necessary documentation for this purpose.

5. The winning tenderer agrees and declares that, at SEL's request, they will sign, acknowledge, and prepare all documents, and will obtain from the staff assigned to the service provision all documents necessary for obtaining industrial property rights and copyrights in any country or countries, with all costs being borne by the winning tenderer.

6. The winning tenderer undertakes to agree with the collaborators assigned to the provision of services that the remuneration of these collaborators already includes special compensation for any creative activity, with the collaborators not entitled to any additional remuneration, indemnity, or compensation in this regard from SEL.

7. The winning tenderer undertakes to agree with the collaborators assigned to the provision of services that they are obliged to comply with all internal rules and policies

regarding intellectual and industrial property rights in force at any time at SEL, particularly the Intellectual Property policy.

Clause 2

(Distinctive Signs)

1. The winning tenderer is prohibited from using any distinctive signs of trade that are the property of SEL, or that SEL is authorized to use by any other title, namely trademarks, logos, or internet domain names, in public dissemination channels such as social media or news outlets, in the name of SEL, or if such use could easily be identified by third parties as belonging to or being directly or indirectly under the responsibility of SEL.

2. Non-compliance with the provisions of the above paragraph may constitute grounds for immediate termination of this Contract, granting SEL the right to compensation for damages resulting from such breach.

Clause 3

(Confidentiality)

1. All information to which the winning tenderer and any personnel assigned by them to the provision of the contracted services have access as a result of the execution of the Contract, regardless of the format in which it is found, shall be considered confidential, except for information that is public knowledge or that reaches the winning tenderer through third parties who have lawfully obtained and disclosed it ("Confidential Information").

2. Confidential Information includes all information relating to the business, whether technical, commercial, or financial in nature, including trade secrets, and information about clients, suppliers, partners, and marketing plans.

3. The winning tenderer and the personnel assigned to perform the services under the Contract are bound by the obligation of confidentiality regarding the Confidential Information. They may not disclose it, in any way, directly or indirectly, communicate it to unauthorized third parties, or use it for their own purposes without the prior written authorization of SEL.

4. The winning tenderer undertakes to adopt security measures in relation to the Confidential Information and to ensure that the personnel assigned to the execution of the Contract adopt similar measures, with the aim of preventing unauthorized access by third parties as well as disclosure of such information. In particular, the Service Provider is obliged to implement any measures SEL imposes through instructions issued to protect the Confidential Information.

5. The above obligation remains in effect beyond the duration of the Contract. Upon termination of the Contract, the winning tenderer must return all Confidential Information in their possession to SEL, regardless of the format in which it is held.

Clause 4

(Personal Data and Privacy)

1. For the purposes of the Contract, the winning tenderer understands that "personal data" is any information relating to an identified or identifiable natural person ("the data subject"); and that an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, electronic identifiers, or one or more specific factors relating to that person's physical, physiological, genetic, mental, economic, cultural, or social identity.

2. For the purposes of the Contract, the winning tenderer understands that the processing of personal data refers to any operation performed on personal data, whether automated or not, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, comparison or interconnection, restriction, erasure, or destruction.

3. The winning tenderer acknowledges that, during the provision of its services, it may be necessary to access or process personal data for which SEL is responsible, or personal data of third parties who are clients or suppliers of SEL.

4. Thus, any personal data processed or merely accessed by the Service Provider during the provision of services to SEL shall be treated as confidential unless expressly indicated otherwise by SEL.

5. The winning tenderer and any personnel assigned to the execution of the contracted services may not copy, transfer, or disclose any personal data for which SEL is responsible, nor use them for any purposes other than those expressly indicated by SEL.

6. The winning tenderer must inform SEL immediately if there is reason to suspect that personal data for which SEL is responsible have become known to or accessed by an unauthorized person.

7. SEL reserves the right to issue additional instructions at any time to ensure the confidentiality and integrity of the personal data for which it is responsible, as well as to establish control procedures to ascertain the degree of compliance with such instructions.