

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER



Ex-Ante cybersecurity Federated Digital Twin-based Cyber Range and managed security services for offshore wind farms

Annex 2

Version 1.0

AENAON GUIDELINES FOR APPLICANTS

JULY 2026

This document is published in the context of and for the objectives of the AENAON project. AENAON is funded by the European Union under the DIGITAL Europe Programme, Grant Agreement No. 101249723. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

Table of Contents

1. Introduction	2
1.1. Context	2
1.2. The AENAON project	3
1.3. Source-of-truth rule	4
2. AENAON Innovation Calls for Cybersecurity Preparedness	4
2.1. Objectives	5
2.2. Main Characteristics	6
2.3. Proposal Requirements and Services	8
2.4. Funding Scheme	9
2.5. Timeline	11
2.6. Applicant KPI Framework	13
3. Eligibility Criteria	13
3.1. Applicants and Consortium Eligibility	14
3.2. Role and Responsibilities of the Lead Beneficiary (Small Consortia)	15
3.3. Eligible Countries	15
3.4. Proposal Eligibility	16
3.5. Financial Eligibility	17
3.6. Language	17
3.7. Impartiality, Applicant Declarations and Process-Side Conflicts of Interest	18
3.8. Documentation Format	18
4. Proposals – Process for Submission, Evaluation and Selection	18
4.1. Proposal Preparation and Submission	19
4.1.1 Proposal package	19
4.2. Submission Rules	20
4.3. Resubmission and Correction before the Deadline	20
4.4. Late Submissions and Portal Failure	20
4.5. Proposal Evaluation and Selection	20
4.5.1. Stage 1 – Admissibility and Eligibility Check	20
4.5.2. Stage 2 – Quality Evaluation by Independent Experts	21
4.5.3 Scoring Scale	24
4.5.4 Individual Evaluation, Consensus and Evaluation Summary Report (ESR)	24
4.5.5 Ranking, Tie-Breaks and Reserve List	25
4.5.6 Evaluator Recruitment and Selection	25
6. Notification, Feedback and Redress	25

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

6.1. Notifications	26
6.2. Redress Procedure.....	26
7. Contract Preparation and Sub-Grant Agreement	27
7.1. Contract Preparation Phase	27
7.2. Failure to Complete Contracting.....	27
7.3. Sub-Grant Agreement	28
8. AENAON Funding Programme: Implementation, Technical Support and Reporting	28
8.1. Implementation Phases	28
8.2. Deliverables, Milestones and Linked Payments — Summary	30
8.3. Technical Support and Guidance	31
8.4. Reporting Requirements.....	31
8.5. Monitoring and KPI Framework.....	31
9. Financial, Cost and Audit Rules	32
9.1. Funding Model and Payment Basis.....	32
9.2. Eligible Activities and Cost Principles.....	32
9.3. Ineligible Costs and Activities	34
9.4. Audit, Record-Keeping and Access Rights	35
9.5. Recoveries, Suspension and Termination	35
9.6. Non-Performance Escalation Procedure.....	35
10. Ethics, Security, Confidentiality and Data Protection	35
10.1. Ethics and EU Values	36
10.2. Cybersecurity, Sensitive Information and Responsible Disclosure	36
10.3. Data Protection	36
10.4. Confidentiality Duration.....	37
11. IPR, Background, Results and Access Rights	37
11.1. Background	37
11.2. Ownership of Results.....	37
11.3. Use of AENAON Background	37
11.4. Open-Source Software and Third-Party Rights	38
11.5. Exploitation Obligation	38
11.6. Publication Review.....	38
12. Governance, Roles and Procedural Principles	38
12.1. Core Principles.....	39
12.2. Conflict of Interest and Confidentiality for Open Call Process Actors	40
13. Communication, Dissemination and Visibility	40

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

13.1. Acknowledgement of EU Funding	40
13.2. Visibility of AENAON	40
13.3. Disclaimer	40
13.4. Publication of Results and Security Clearance	41
13.5. Participation in AENAON Dissemination Activities	41
13.6. Publication of Call Outcome on Recipient's Own Website	41
13.7. Minimum Communication and Dissemination Requirements	41
14. Records Management, Audits and Retention	42
15. Responsibilities of Beneficiaries	42
15.1. Compliance with Sub-Grant Agreement Conditions	42
15.2. Timely Reporting	42
15.3. Gender Equality	42
15.4. Ownership and Control Safeguards	42
15.5. Cooperation with AENAON	43
16. Applicant Integrity and Relationship Disclosure	43
17. Support, Contact and Clarifications	43
17.1. Applicant Support Resources	43
17.2. Clarification Requests	44
17.3. Contact Information	44
18. Protection of Applicant and Participant Confidential Information	44
18.1. Why Confidentiality Matters in This Context	44
18.2. Legal Basis: Article 13 of the Grant Agreement	44
18.3. What Applicants Can Designate as Confidential	45
18.4. How to Designate Confidential Information	45
18.5. How AENAON Handles Designated Confidential Information	46
18.5.1. Access restriction	46
18.5.2. Evaluator binding obligations	46
18.5.3. Publication controls	46
18.5.4. Cybersecurity-specific safeguards	47
18.5.5. Obligations during monitoring and audit	47
18.6. Duration of Confidentiality Obligations	47
18.7. What Applicants Should Know Before Submitting	48
18.8. Reporting Breaches and Escalation	49

1.Introduction

This document serves as the Guidelines for Applicants for the AENAON Innovation Calls for Cybersecurity Preparedness, providing comprehensive information on the applicable participation rules, procedures, requirements and conditions for the two Open Call rounds. In addition, this document presents the funding framework of the AENAON Open Calls and provides prospective applicants with the information needed to understand the objectives, scope, eligibility and admissibility requirements, proposal preparation and submission process, evaluation, ranking, selection and redress procedures, contracting arrangements, implementation and technical monitoring requirements, reporting and payment conditions, and the main contractual, regulatory and project-specific obligations applicable to selected recipients of financial support.

Through this guidance, AENAON seeks to ensure a transparent, fair, effective and audit-ready Open Call process, enabling external stakeholders to contribute to the validation, uptake and wider deployment of AENAON cybersecurity preparedness solutions in real-life offshore wind farm environments and across the broader offshore wind ecosystem.

1.1. Context

The AENAON project is launching two Innovation Calls for Cybersecurity Preparedness to enhance the cybersecurity resilience and digital infrastructure of offshore wind farms. In a context where offshore wind energy operators and related critical energy stakeholders are increasingly exposed to complex cyber threats, AENAON aims to support the validation, customisation, uptake and scaling of advanced cybersecurity solutions tailored to the specific operational needs of the offshore wind sector.

The AENAON Innovation Calls will provide Financial Support to Third Parties (FSTP) through two Open Call rounds:

- Open Call 1 – Cybersecurity Technology Enhancement for Offshore Wind Energy Operators
- Open Call 2 – Scaling Cybersecurity Resilience across the Offshore Wind Ecosystem

Through these Open Calls, AENAON will support selected third parties in validating and scaling solutions that address the specific cyber threats and operational requirements of the offshore wind sector, making use of AENAON's Federated Digital Twin-based Cyber Range Platform. By fostering technological innovation and collaboration, AENAON seeks to empower relevant stakeholders, including offshore wind energy operators, service providers, technology providers, SMEs, research and innovation organisations, and other actors across the offshore wind ecosystem, with advanced cybersecurity tools and services.

To maximise impact, reach and uptake within the offshore wind ecosystem, the AENAON Open Calls are designed to attract and support external entities, including operators, technology providers, SMEs and research and innovation actors, in order to pilot, validate and extend AENAON capabilities in realistic environments and foster cross-sector collaboration in cybersecurity preparedness for critical energy infrastructures.

1.2.The AENAON project

The AENAON project is a Digital Europe action funded under the call DIGITAL- ECCC-2024-DEPLOY-CYBER-07-LARGEOPER Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations. The project addresses the growing cybersecurity challenges faced by offshore wind farm operators and related energy-sector organisations, which need to strengthen their preparedness, resilience and capacity to respond effectively to increasingly complex cyber threats and incidents.

AENAON aims to reinforce the cyber-resilience of offshore wind installations and interconnected grid energy infrastructures by establishing a Federated Digital Twin-based Cyber Range Platform, an interactive cyber range training programme, and a set of cybersecurity preparedness support (ex-ante) services. These services include, among others, penetration testing, threat and risk assessment, risk monitoring, cybersecurity awareness and

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

coordination support among offshore wind farm operators. Through these assets, AENAON supports the offshore wind energy sector in enhancing cybersecurity preparedness and resilience, while also facilitating alignment with relevant regulatory frameworks, including the NIS2 Directive.

The project's overall approach combines technological development, operational validation, training, mentoring, knowledge sharing and market uptake. It seeks to customise preparedness support services according to the specific organisational needs of offshore wind energy stakeholders and to develop cybersecurity skills through dynamic attack-and-defence scenarios, red-team/blue-team exercises and interactive training activities. The platform will be evaluated through internal and external pilot operations involving organisations from advanced offshore renewable energy regions in Europe, including the North Sea and the Baltic Sea.

AENAON focuses on several key areas of activity, including:

- the specification of requirements and analysis of the threat landscape for the offshore wind energy sector
- the set-up of the Federated Digital Twin-based Cyber Range Platform
- the development of an Interactive Cyber Range Training Programme
- the customisation of cybersecurity preparedness support services
- the execution of internal and external pilot operations
- the evaluation, benchmarking and demonstration of the AENAON approach
- knowledge sharing, mentoring, capacity building, dissemination, exploitation, sustainability and market uptake.

The project is organised into six Work Packages. These cover project management and coordination; requirements specification, cyber range platform set-up and training programme development; customisation of cybersecurity preparedness support services and consultancy; Open Call execution, demonstration and validation activities; pilot operation execution, evaluation, mutual assistance and capacity building; and dissemination, exploitation, sustainability and market take-up.

Within AENAON, WP4 governs the full Open Call lifecycle. This includes Open Call design, definition of scope, eligibility and award criteria, templates and applicant guidance, communication and outreach, evaluation and selection of applications, and the onboarding, contracting, monitoring and closure of supported third-party projects. WP4 also ensures that the Open Calls remain aligned with the AENAON technical direction and that lessons learned from the first Open Call are used to refine the second Open Call.

The AENAON consortium brings together complementary expertise required for the implementation of the project, including cybersecurity, risk and threat assessment, penetration and security testing, cyber ranges, digital twin and virtualisation technologies, cybersecurity training and mentoring, regulatory, legal and ethical aspects, standardisation and policy development, offshore wind sector knowledge, stakeholder engagement, pilot validation, dissemination, exploitation and sustainability. The consortium is composed of SMEs, non-profit organisations and associations, industrial partners and a national standardisation body, collectively covering the technical, administrative, validation, evaluation, dissemination and exploitation activities of the project.

The project is strategically positioned to contribute to the cybersecurity preparedness and resilience of the offshore wind energy sector by supporting real-life validation, cross-sector collaboration, stakeholder engagement and the development of reusable and scalable solutions. Through its Open Calls for Financial Support to Third Parties, AENAON will extend its impact beyond the consortium by enabling external stakeholders to validate, customise and scale cybersecurity solutions in operationally relevant offshore wind environments.

In this context, the AENAON Open Calls constitute a central mechanism for broadening participation, accelerating uptake and anchoring the project's outcomes in real offshore wind farm environments and across the wider offshore wind ecosystem.

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

1.3.Source-of-truth rule

The final Open Call Notice and the documents published on the official AENAON Open Call website for each round are the source of truth for deadlines, eligible countries, award amounts, exact funding conditions, templates, contact points and contractual clauses. If a conflict exists between draft materials and the final published Open Call package, the final published package prevails, subject to the Grant Agreement.

These Guidelines are intended to provide the general framework applicable to both AENAON Open Call rounds. Where round-specific conditions differ, including implementation duration, eligible activities, budget allocation, reporting deadlines, payment triggers or portfolio rules, the relevant Open Call Notice and Sub-Grant Agreement will specify the applicable conditions for that round.

2.AENAON Innovation Calls for Cybersecurity Preparedness

The AENAON Innovation Calls for Cybersecurity Preparedness form part of the project's Financial Support to Third Parties (FSTP) activities and will be implemented through the two competitive Open Call rounds: i. Open Call 1 – Cybersecurity Technology Enhancement for Offshore Wind Energy Operators, and ii. Open Call 2 – Scaling Cybersecurity Resilience across the Offshore Wind Ecosystem, as mentioned in the previous section.

The AENAON Open Call process covers the full lifecycle from call preparation and publication to proposal submission, admissibility and eligibility checks, independent evaluation, ranking and selection, contracting, implementation, monitoring and closure. The same overall lifecycle applies to both Open Call rounds, while allowing refinements in the second round based on lessons learned from the first.

Following the key elements and the context of the project, this section presents the main framework of the AENAON Open Calls, including their objectives, key characteristics, proposal requirements, eligible activities, funding conditions and indicative implementation arrangements.

The Open Calls are intended to support selected third parties in contributing to the validation, customisation, integration and scaling of AENAON cybersecurity preparedness solutions in operationally relevant offshore wind environments and across the wider offshore wind ecosystem.

2.1.Objectives

The AENAON Open Calls are designed to:

- a) broaden participation and ensure uptake of AENAON assets by relevant stakeholders in the offshore wind and energy cybersecurity ecosystem
- b) support validation of AENAON services in realistic operational contexts and
- c) generate replicable results that strengthen cybersecurity preparedness and resilience across the sector.

The objectives of the AENAON Innovation Calls are aligned with the overall goals of the AENAON project and with the Financial Support to Third Parties framework described in the Grant Agreement. In particular, the Open Calls aim to support the following objectives:

1. **Adoption and customisation of AENAON cybersecurity preparedness services:** The Open Calls aim to support the adoption, customisation and integration of advanced cybersecurity solutions into AENAON's Federated Digital Twin-based Cyber Range Platform. Selected applicants will contribute to the enhancement of cybersecurity preparedness and defence capabilities for offshore wind farm operators by developing, adapting or validating cybersecurity tools, methods, scenarios or services that respond to the specific needs of offshore wind environments.

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

2. **Validation and scaling of solutions for offshore wind cyber threats:** The Open Calls will support the validation and scaling of cybersecurity solutions addressing the unique cyber threats, operational constraints and digital infrastructure requirements of the offshore wind sector. Funded sub-projects should demonstrate practical relevance and applicability in real-life or operationally relevant settings, contributing to improved threat detection, incident response and overall digital resilience.
3. **Enhancement of cybersecurity technology for offshore wind energy operators:** Open Call 1 focuses on strengthening cybersecurity preparedness for offshore wind farm operators. It will support activities that expand the capabilities of the AENAON Cyber Range Platform through more targeted content and the integration of new solutions. This may include the development of sector-specific vulnerabilities, testing scenarios, digital twin simulations, penetration-testing validation, OT/IT security validation, risk scenarios and related cybersecurity preparedness services.
4. **Scaling cybersecurity resilience across the offshore wind ecosystem:** Open Call 2 builds on the outcomes of Open Call 1 and aims to extend the scope of participation beyond offshore wind farm operators. It will support the validation, scaling and wider adoption of cybersecurity technologies across the broader offshore wind ecosystem, including supply chain actors, grid service providers, cybersecurity authorities, regulatory bodies, National Coordination Centres, and other relevant stakeholders involved in offshore wind and critical energy infrastructure resilience.
5. **Collaboration and knowledge sharing across key stakeholders:** The Open Calls aim to promote collaboration and knowledge sharing among offshore wind farm operators, grid operators, Transmission System Operators, regulators, supply chain vendors, cybersecurity providers, research organisations and other relevant actors. This collaboration is intended to support coordinated cybersecurity threat intelligence, response capabilities, mutual assistance, mentoring, technology transfer and the development of shared preparedness practices across the sector.
6. **Supply chain and critical infrastructure resilience:** AENAON seeks to expand cybersecurity preparedness beyond individual offshore wind operators by involving interconnected stakeholders across the offshore wind supply chain and supporting infrastructure. The Open Calls are expected to contribute to a stronger cybersecurity landscape for offshore wind energy by promoting engagement among operators, manufacturers, service providers, grid-related actors, oversight entities and other organisations involved in the security and continuity of offshore renewable energy systems.
7. **Innovation in OT/IT cybersecurity methods and tools:** The Open Calls will encourage the development and deployment of innovative cybersecurity methods and tools for offshore wind energy operations, including advanced approaches for identifying, assessing and mitigating cyber threats. Particular emphasis will be placed on solutions that improve automation, user experience, interoperability and security validation across operational technology (OT) and information technology (IT) environments.
8. **Support for regulatory alignment and cybersecurity maturity:** Funded sub-projects are expected to contribute, where relevant, to improved cybersecurity maturity and alignment with applicable EU cybersecurity and critical infrastructure policy objectives, including NIS2 and CER-related preparedness and resilience considerations. Selected participants may benefit from tailored consultancy, real-world validation and regulatory alignment support in order to strengthen the practical relevance and adoption potential of their solutions.
9. **Demonstration, uptake and exploitation of project outcomes:** The Open Calls are designed to broaden the testing and demonstration environment of AENAON solutions, support uptake beyond the consortium and generate evidence for the project's validation, exploitation and sustainability activities. By engaging external innovators and operational stakeholders, AENAON aims to promote the practical deployment of reusable and scalable cybersecurity preparedness solutions for offshore wind energy infrastructure and its wider ecosystem.

Supported third-party projects are expected to contribute to one or more of AENAON's core capability areas, including cyber range training and scenario-based exercises aligned with offshore wind operational realities; cybersecurity preparedness support services such as vulnerability discovery, penetration testing, threat and risk assessment, and risk monitoring or cyberattack management; and the practical validation and enhancement of the Federated Digital Twin-based Cyber Range Platform through integration, testing, feedback and improvements.

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

2.2.Main Characteristics

The AENAON Innovation Calls for Cybersecurity Preparedness exhibit several key characteristics that distinguish them as a strategic initiative within the broader AENAON project.

Item	Details
Eligible Applicants	Open Call 1: Offshore wind energy operators, supply chain stakeholders, National Coordination Centres (NCCs), cybersecurity and technology providers, SMEs and research and innovation organisations. Detailed eligibility conditions are set out in Section 3.1. Open Call 2: SMEs, large enterprises, research and innovation organisations, cybersecurity and technology providers, offshore wind farm operators, supply chain actors and critical infrastructure service providers. Applicants under Open Call 2 must demonstrate their capacity to scale cybersecurity solutions across diverse offshore wind operational environments and stakeholder groups. Detailed eligibility conditions are set out in Section 3.1.
Open Call Time Frame	The AENAON FSTP scheme will be implemented through two Open Call rounds: Open Call 1 – Cybersecurity Technology Enhancement for Offshore Wind Energy Operators and Open Call 2 – Scaling Cybersecurity Resilience across the Offshore Wind Ecosystem. OC1 focuses on content enrichment, integration and testing of the AENAON Cyber Range Platform and associated services. OC2 builds on the results of OC1 and focuses on scaling, validation and broader ecosystem deployment across multiple operational environments and stakeholder groups. The exact opening date, submission deadline and evaluation period for each round will be specified in the respective Open Call Notice.
Activities to be Funded	Activities supporting the validation, customisation, integration, testing, demonstration and scaling of cybersecurity preparedness solutions for offshore wind farms and the broader offshore wind ecosystem. Funded activities may include, as applicable, the use or enhancement of AENAON's Federated Digital Twin-based Cyber Range Platform, cyber range exercises, threat and risk assessment, OT/IT cybersecurity validation, incident response, digital twin simulations, penetration-testing scenarios, supply-chain resilience testing, and other cybersecurity preparedness services relevant to offshore wind operations.
Duration of Activities	The duration of funded activities depends on the relevant Open Call round. For Open Call 1, selected sub-projects will be implemented during M13-M20 (January-August 2027), with an active funded implementation duration of 8 months. Open Call 1 assessment and lessons learned take place in M21 (September 2027). For Open Call 2, implementation runs from M24-M33 (December 2027-September 2028), with an active funded implementation duration of 10 months. The exact phase structure, deliverables, reporting deadlines and payment triggers will be specified in the relevant Open Call Notice and Sub-Grant Agreement.

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Item	Details
Budget per Project	The total FSTP envelope for the AENAON Open Calls is EUR 4,100,000 , to be indicatively allocated as EUR 2,100,000 for Open Call 1 and EUR 2,000,000 for Open Call 2. Financial support will be provided through lump-sum sub-grants. AENAON applies a justified derogation from the standard EUR 60,000 threshold, allowing financial support of up to EUR 100,000 per participating third-party beneficiary/legal entity . Where proposals are submitted by small consortia, the maximum support applies per beneficiary/legal entity and not automatically per consortium as a whole. This ceiling applies cumulatively across both Open Call rounds. Where the same legal entity has received AENAON FSTP funding under a previous Open Call round, the maximum amount that may be awarded in any subsequent round is reduced accordingly, so that the aggregate total does not exceed EUR 100,000. Any amount not committed under Open Call 1 may be reallocated to Open Call 2, subject to the applicable Open Call rules, budget availability and the principles of transparency, equal treatment and sound financial management.
Funding rate	Financial support will cover 50% of the eligible budget of each supported sub-project. Applicants must therefore provide the remaining share through own resources or other eligible co-funding.
Evaluation of Proposals	Proposals will be evaluated through a transparent process, including admissibility and eligibility checks followed by quality evaluation by independent experts, according to the evaluation criteria published in the Open Call documentation.
Number of Proposals to be Selected	The number of proposals to be selected will be determined for each Open Call round on the basis of the available budget, the requested and approved financial support per proposal, the evaluation results, and the quality of the proposals received. The Open Call Notice may define an indicative or minimum number of projects to be funded per round.
Milestones / Payments	Payments follow a staged 30%-40%-30% model. The initial 30% (pre-financing) is released upon signature of the Sub-Grant Agreement and completion of onboarding requirements. The second 40% is released following successful completion of the mid-term review and acceptance of the corresponding interim report, deliverables and milestone evidence. The final 30% is released following acceptance of the final report, final deliverables and performance evidence.

2.3.Proposal Requirements and Services

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Applicants are required to submit proposals that comprehensively address the objectives of the AENAON Innovation Calls for Cybersecurity Preparedness, with a specific focus on enhancing cybersecurity preparedness, resilience and digital infrastructure protection in offshore wind farms and the wider offshore wind ecosystem.

Proposals should demonstrate how the proposed activities will contribute to the validation, customisation, integration, testing, demonstration or scaling of cybersecurity solutions relevant to offshore wind operations. This may include, as applicable, solutions related to threat detection, incident response, risk and vulnerability assessment, OT/IT cybersecurity validation, cyber range exercises, digital twin-based simulations, penetration-testing scenarios, supply-chain resilience, regulatory alignment, and other cybersecurity preparedness services relevant to the AENAON project.

Proposals should also clearly indicate how the proposed action contributes to one or more AENAON capability areas, including cyber range training and scenario-based exercises, vulnerability discovery, penetration testing, threat and risk assessment, risk monitoring, cyberattack management, and the integration, testing or enhancement of the Federated Digital Twin-based Cyber Range Platform.

Selected applicants will be expected to make use of, interact with, customise, validate or contribute to AENAON's Federated Digital Twin-based Cyber Range Platform and associated cybersecurity preparedness support services, in accordance with the scope and requirements of the relevant Open Call round. The AENAON consortium will provide the necessary guidance, technical support, documentation and access arrangements required for the implementation of the selected sub-projects, as further specified in the Open Call documentation and the Sub-Grant Agreement.

2.4.Funding Scheme

The AENAON Innovation Calls for Cybersecurity Preparedness allocate a total FSTP budget of **EUR 4,100,000**, indicatively allocated as EUR 2,100,000 for Open Call 1 and EUR 2,000,000 for Open Call 2, to support external third parties through two competitive Open Call rounds. Financial support will be provided exclusively in the form of lump-sum sub-grants, in accordance with the applicable provisions governing Financial Support to Third Parties under the DIGITAL framework and Article 207 of the EU Financial Regulation (Regulation (EU, Euratom) 2024/2509), together with Articles 6.2.D.1 and 9.4 of the DIGITAL Europe Programme Model Grant Agreement. Any amount not committed under Open Call 1 may be reallocated to Open Call 2, subject to the applicable Open Call rules, budget availability and the principles of transparency, equal treatment and sound financial management.

- Maximum funding per participating third-party beneficiary/legal entity: up to EUR 100,000**
 AENAON applies a justified derogation from the standard EUR 60,000 threshold for financial support to third parties, allowing financial support of up to **EUR 100,000** per individual third-party beneficiary / recipient / participating legal entity. This ceiling applies cumulatively across both Open Call rounds. Where the same legal entity participates in both Open Call 1 and Open Call 2, whether as a single applicant or as a member of a small consortium, the total amount of AENAON FSTP funding awarded to that entity across both rounds may not exceed EUR 100,000 in aggregate. Where a legal entity has already received AENAON FSTP funding under a previous Open Call round, the maximum amount that may be awarded in any subsequent round will be reduced accordingly so that the cumulative total does not exceed EUR 100,000. For proposals submitted by small consortia, the ceiling applies per participating legal entity and not to the proposal, consortium or action as a whole. No individual consortium member may receive more than EUR 100,000 in aggregate across both Open Call rounds, regardless of whether that entity participates as coordinator, consortium member or single applicant. The exact lump-sum amount awarded to each selected beneficiary is fixed at contracting stage through a needs-based and auditable right-sizing process, within the applicable ceiling and in relation to the scope, complexity and implementation requirements of the proposed action.
- Funding rate and co-funding:** The funding rate for supported actions is set at **50% of the eligible budget** of each sub-project. Financial support therefore operates as a co-funding mechanism and applicants must demonstrate their capacity to cover the remaining share of the project budget.

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

- **Funding model:** AENAON applies a lump-sum sub-grant model in order to simplify financial management, reduce administrative burden and facilitate participation by eligible entities, including SMEs and specialised actors. The lump-sum model is combined with predefined milestones, deliverables and acceptance criteria.
- **Number of selected projects:** The exact number of selected projects will depend on the available FSTP budget per Open Call round, the requested and approved financial support per selected beneficiary, the quality of the applications received, the evaluation ranking and any portfolio considerations published in the relevant Open Call Notice. The relevant Open Call Notice may specify an indicative or minimum number of projects to be funded under each Open Call round.
- **Travel Costs:** No separate fixed travel allowance is foreseen unless expressly stated in the relevant Open Call Notice. Where participation in AENAON meetings, reviews, demonstrations, training, showcase or dissemination activities is required, related travel and subsistence costs may be eligible only if they are necessary for the approved sub-project, included in the approved budget, compliant with the applicable eligibility rules, and within the maximum financial support awarded to the recipient.
- **Participation in final assessment / demonstration activities:** Selected projects may be required to participate in AENAON demonstration, validation, assessment, dissemination or final reporting activities, as specified in the relevant Open Call Notice and Sub-Grant Agreement. Such participation may include presenting results, contributing to lessons learned, supporting the final Open Call assessment, and providing evidence of impact, scalability and readiness for wider adoption.
- **Participation rule:** Legal entities may participate in both Open Call rounds, whether as single applicants or as consortium members. Participation in both rounds is subject to the cumulative maximum support ceiling of EUR 100,000 per legal entity across both rounds. Applicants must not receive double funding for the same activities.

Funding will be distributed in the following stages, subject to acceptance of the corresponding reports, milestones and supporting evidence:

- **Stage 1 – Planning and onboarding** :30% pre-financing is released upon signature of the Sub-Grant Agreement and completion of the onboarding requirements. The Project Plan / first onboarding deliverable (confirming the detailed work plan, KPI targets, implementation schedule, risk register, budget and co-funding confirmation, and data/security arrangements) is due at the end of Month 1; the subsequent (40%) and final (30%) payments are released only after acceptance of the corresponding reports and deliverables.
- **Stage 2 – Mid-term implementation review:** 40% of the allocated funding will be released following successful completion of the mid-term review and acceptance of the corresponding progress report, technical evidence and milestone verification (deliverable).
- **Stage 3 – Final completion and acceptance:** The final 30% will be released following acceptance of the final report, final deliverables, KPI achievement evidence, validation results, security-cleared public summary and any required contribution to AENAON assessment or dissemination activities.

Where the right-sizing process results in a proposed financial support amount materially lower than the amount requested by the applicant, AENAON will notify the applicant during the contracting phase and provide an opportunity to adjust the scope or withdraw. AENAON will document the right-sizing outcome and its justification in the contracting record.

Where the financial support requested by the next-ranked proposal exceeds the remaining budget available under the relevant Open Call, AENAON may offer financial support limited to the remaining available amount. The applicant will be informed in writing of the maximum amount available and may either accept the reduced amount and submit a proportionately revised scope, work plan, budget, milestones and deliverables, subject to AENAON

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

approval, or withdraw from the contracting process. If the applicant declines the reduced amount, or if the revised action is not considered technically and financially viable, AENAON may invite the next eligible proposal from the reserve list. The procedure shall respect the published ranking, equal treatment, transparency and sound financial management principles.

The exact timing of each stage will be adapted to the implementation duration of the relevant Open Call round. Open Call 1 may apply an implementation duration of 8 months, while Open Call 2 is expected to apply an implementation duration of 10 months.

The exact amount of financial support awarded to each selected project will be fixed at the contracting stage through a needs-based and auditable right-sizing process. This process will take into account the scope, complexity, implementation requirements, use-case scenario, infrastructure scale, compliance dimension, delivery profile and exploitation potential of the proposed action.

The funding process will be implemented in accordance with the rules on Financial Support to Third Parties, ensuring objective, transparent and non-discriminatory procedures, equal treatment of applicants, and a complete audit trail. All payments will be contingent upon the successful completion of predefined milestones, acceptance of deliverables and submission of the necessary documentation.

2.5. Timeline

The following timeline outlines the indicative phases and deadlines for the AENAON Open Calls. The exact dates will be specified in the relevant Open Call Notice for each round.

Phase	Indicative Timeline	Calendar period
OC1 - Design and preparation	M1-M6	January-June 2026
OC1 - Publication and applicant support	M7-M8	July-August 2026
OC1 - Submission Period	M9-M10	1 September- 31 October 2026
OC1 - Evaluation and selection	M11-M12	November-December 2026
OC1 – Admissibility and eligibility checks	After submission deadline	Preliminary administrative checks may take place during the submission period; final admissibility and eligibility checks will begin after the submission deadline
OC1 - Implementation and monitoring	M13-M20	January-August 2027 (8 months)
OC1 - Assessment and lessons learned	M21	September 2027
OC2 - Preparation and refinement	M18-M19	June-July 2027
OC2 - Publication and applicant support	M20-M21	August-September 2027

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Phase	Indicative Timeline	Calendar period
OC2 - Submission and eligibility checks	M21	September 2027
OC2 - Evaluation and selection	M22-M23	October-November 2027
OC2 - Implementation and monitoring	M24-M33	December 2027-September 2028 (10 months)
Final assessment and reporting	M34-M35	October-November 2028

The AENAON Grant Agreement foresees a structured Open Call process covering design, preparation, announcement, submission, evaluation, implementation, assessment and final reporting activities. Open Call 1 is expected to focus on technology enhancement, vulnerability assessments and testing of the AENAON Cyber Range Platform. Open Call 2 is expected to focus on scaling, broader validation and ecosystem-level deployment, supporting actions aimed at extending the use of AENAON services across multiple operational environments, enabling cross-entity collaboration, and validating advanced threat scenarios and coordinated resilience approaches across interconnected systems and supply chains.

Call Launch: The launch date of each Open Call will be announced through the official AENAON communication channels and Open Call documentation. The Open Call Notice will specify the opening date, submission deadline, submission platform, templates and all relevant applicant instructions.

Proposal Submission Deadline: All proposals must be submitted electronically through the official AENAON submission system by the deadline specified in the relevant Open Call Notice. The Open Call 1 submission period will run from **1 September to 31 October 2026**, subject to the exact closing time specified in the Open Call Notice. Late submissions will not be accepted, except in cases of documented system-wide technical failure or other circumstances expressly communicated by AENAON.

Evaluation and Selection: Following the closure of each Open Call, AENAON will initiate the eligibility, evaluation and selection process. The Open Call Coordination Committee will verify compliance with admissibility and eligibility criteria, including legal status, geographical eligibility and completeness of the submission. Eligible proposals will then proceed to evaluation by independent experts, according to the published evaluation criteria.

Notification of Selected Projects: All applicants will be informed in writing of the outcome of the evaluation. Selected applicants will be invited to enter the contracting phase. Applicants whose proposals are found inadmissible or ineligible will receive a rejection notification stating the grounds, without proceeding to evaluation. Applicants whose proposals are evaluated but do not meet the thresholds, or which meet the thresholds but are placed on the reserve list, will receive a notification of their status together with the corresponding Evaluation Summary Report. All notifications include information on the redress procedure. The content of each notification and the applicable timelines are set out in Section 5 (Notification, Feedback and Redress).

Project Implementation Period: After completion of the contract preparation and signature process, selected projects will begin implementation. The implementation duration will depend on the relevant Open Call round. Open Call 1 sub-projects will have an implementation duration of 8 months, while Open Call 2 sub-projects are expected to have an implementation duration of 10 months. The exact start date, end date, reporting deadlines, deliverables, payment milestones and acceptance criteria will be specified in the relevant Open Call Notice and Sub-Grant Agreement.

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Implementation Stages: Following the completion of the evaluation, selection and contracting process, selected projects will enter the implementation phase. The implementation stages will be adapted to the relevant Open Call round. Given that an 8-month implementation structure is applied for Open Call 1 and a 10-month implementation structure is applied for Open Call 2, funded projects will be divided into three stages covering planning/onboarding, deployment/implementation, and evaluation/reporting.

For Open Call 1, where an 8-month implementation structure is applied, funded sub-projects may be structured as follows:

1. **Planning and Onboarding – Month 1:** Strategy definition, project set-up, detailed planning, integration approach, KPI plan, risk register, data/security plan and access/onboarding arrangements.
2. **Deployment and Implementation – Months 2–5:** Technology integration, cybersecurity testing, cyber range scenario development, digital twin-based simulations, validation activities, OT/IT security testing, penetration-testing scenarios and implementation of the approved use case.
3. **Evaluation, Refinement and Reporting – Months 6–8:** Performance assessment, KPI evidence, validation results, refinement of outputs, lessons learned, security-cleared public summary and contribution to AENAON assessment and dissemination activities.

For Open Call 2, where a 10-month implementation structure is applied, funded sub-projects may be structured as follows:

1. **Planning and Onboarding – Month 1:** Strategy definition, project set-up, detailed planning, integration approach, KPI plan, risk register, data/security plan and access/onboarding arrangements.
2. **Deployment and Implementation – Months 2–6:** Technology integration, cybersecurity testing, simulations, validation activities, multi-site or cross-stakeholder deployment, supply-chain resilience testing, training or exercise activities and implementation of the approved use case.
3. **Evaluation, Refinement and Reporting – Months 7–10:** Performance assessment, scalability assessment, KPI evidence, validation results, regulatory alignment evidence, final reporting, lessons learned and contribution to AENAON final assessment activities.

The exact phase structure, deliverables, reporting deadlines and acceptance criteria will be specified in the relevant Open Call Notice and Sub-Grant Agreement.

Final Assessment: At the end of the Open Call implementation cycle, AENAON will assess the impact of the funded projects, document best practices, evaluate scalability and readiness for wider adoption and consolidate the lessons learned and results of the Open Call actions. These findings will contribute to the final assessment and reporting of the AENAON Open Call scheme.

2.6.Applicant KPI Framework

Each funded sub-project must contribute to the AENAON project-level KPIs. Applicants must propose, in Section 2 of their technical proposal (Annex 3), specific and measurable target values for the KPIs relevant to their action. Final KPI targets are fixed proportionately in the Sub-Grant Agreement at contracting stage, taking into account the scope, scale and complexity of the approved action. Achievement of the agreed KPI targets is verified at reporting stage and forms part of the acceptance criteria for the mid-term and final payments (Sections 7.1 and 7.3).

3. Eligibility Criteria

All applications will first undergo an admissibility check. This check will verify whether the proposal has been submitted before the published deadline, whether the official application form and required templates have been used, whether all mandatory sections have been completed and whether all requested declarations and supporting documents have been duly provided.

Applications that pass the admissibility stage will undergo an eligibility check. This check will confirm that the applicant belongs to one of the categories of eligible recipients defined for the relevant Open Call, is established in an eligible country, proposes activities within the thematic scope of the Open Call and within the closed list of eligible actions, and complies with the applicable legal, ethical, regulatory and security requirements.

All applicants must comply with the general requirements set out in this section in order to be considered eligible to participate in the AENAON- Open Calls. The eligibility check will verify that:

- submissions are made only through the official AENAON Open Call submission system and by the deadline defined in the relevant Open Call Notice;
- applicants are legal entities established in an eligible country, in accordance with the applicable [DIGITAL Europe / EU funding rules](#) and the specific conditions of the AENAON Open Call;
- applicants fall within the defined categories of eligible recipients for the relevant Open Call round;
- applicants submit all requested documents exclusively in the English language;
- the proposal is submitted in accordance with the official Guidelines for Applicants, the relevant Open Call Notice and the mandatory templates;
- a complete proposal is submitted, including all requested administrative data, declarations and supporting documents;
- the proposal is aligned with the objectives, scope and expected outcomes of the relevant AENAON Open Call round;
- applicants demonstrate the capacity to implement the proposed action and to co-fund the required share of costs;
- applicants comply with the applicable ethics, security, data protection, ownership/control, regulatory, double-funding and exclusion requirements, and disclose any relationship or circumstance that could affect the impartiality of the Open Call process;
- applicants comply with any multiple-submission rule specified in the relevant Open Call Notice;
- A proposal will be considered eligible only if its content specifically aligns with the objectives of the AENAON Innovation Calls, including the eligibility conditions set out in the relevant sections of these Guidelines and in the Open Call Notice.

The eligibility check enables the establishment of a shortlist of proposals to be submitted for quality evaluation. Only eligible proposals will proceed to the evaluation phase.

To participate in the AENAON Open Calls, applicants must meet the eligibility criteria set out below. The Grant Agreement provides that AENAON financial support is intended for external legal entities that can contribute to offshore wind cybersecurity preparedness, including offshore wind operators, supply chain actors, cybersecurity providers, SMEs, research institutions, NCCs and other critical infrastructure stakeholders.

3.1. Applicants and Consortium Eligibility

Eligible Participants: Eligible applicants must be legally established in one of the 27 Member States of the European Union, Iceland, Liechtenstein or Norway. Any additional third country may participate only where it is expressly confirmed as fully associated with the Digital Europe Programme for Specific Objective 3 –

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Cybersecurity and Trust and is included in the definitive '**AENAON Open Call 1 – List of Eligible Countries.**' Eligible applicants may include SMEs, large enterprises, research organisations, cybersecurity providers, offshore wind operators, supply-chain actors and other eligible legal entities identified in the relevant Open Call Notice eligible under the applicable Digital Europe Programme conditions (see Section 3.2), including SMEs, large enterprises, research organisations, cybersecurity providers, offshore wind operators and supply chain actors. Small consortia combining complementary expertise may also be supported where this enhances the quality and impact of the proposed action.

For **Open Call 1 – Cybersecurity Technology Enhancement for Offshore Wind Energy Operators**, eligible applicants include offshore wind operators, supply chain stakeholders, NCCs, cybersecurity providers, SMEs and research institutions.

For **Open Call 2 – Scaling Cybersecurity Resilience across the Offshore Wind Ecosystem**, eligible applicants include SMEs, large enterprises, research institutions, cybersecurity providers, offshore wind farm operators, supply chain actors and critical infrastructure service providers. Applicants under Open Call 2 must demonstrate their capacity to scale platform solutions across diverse offshore wind operational environments.

Country eligibility of consortium members: For consortium applications, every participating legal entity must independently satisfy the applicable country-eligibility requirements described in Section 3.3. If any consortium member is established in an ineligible country, the entire proposal will be declared ineligible at the eligibility-check stage and will not proceed to quality evaluation. The lead applicant is responsible for verifying the country eligibility of every consortium member before submission.

Involvement of External Stakeholders: The AENAON Open Calls encourage the involvement of external stakeholders able to contribute to real-life validation, technology integration, cybersecurity simulations, risk and vulnerability assessment, threat detection, incident response, regulatory alignment, supply-chain resilience, mutual assistance, training and wider adoption of AENAON cybersecurity preparedness services.

AENAON consortium beneficiaries under Grant Agreement No. 101249723 and their affiliated entities are **not** eligible to receive financial support under the AENAON Open Calls under any circumstances. This prohibition is absolute and applies regardless of the nature of the proposed activities, the role of the entity in the consortium, or any other consideration. For the purposes of this rule, an affiliated entity means any legal entity that is under the direct or indirect control of an AENAON beneficiary, under the same direct or indirect control as an AENAON beneficiary, or that directly or indirectly controls an AENAON beneficiary, within the meaning of the applicable EU financial rules. In addition, evaluators, members of the OCCC, OCTT or OCEP, and any other person or organisation with an actual or potential conflict of interest in the Open Call process may not receive funding under the Open Calls where such participation would compromise impartiality, equal treatment or the integrity of the evaluation process. Applications submitted in breach of this rule will be declared ineligible at the admissibility and eligibility check stage and will not proceed to evaluation. Any financial support awarded in breach of this rule will be subject to recovery in full.

3.2.Role and Responsibilities of the Lead Beneficiary (Small Consortia)

Where a proposal is submitted by a small consortium of more than one legal entity, one entity must be designated as the lead beneficiary. The lead beneficiary is the single point of contact between the consortium and AENAON and carries the following responsibilities throughout the Open Call and implementation lifecycle:

- **Submission:** submitting the proposal on behalf of all consortium members and ensuring the consortium declaration or commitment letter is included in the proposal package
- **Contracting:** signing the Sub-Grant Agreement on behalf of the consortium and, where applicable, ensuring each member adheres to the applicable flow-down obligations;
- **Financial administration:** receiving the lump-sum payments from AENAON and distributing the corresponding shares to consortium members in accordance with the agreed internal budget
- **Reporting:** consolidating and submitting the Project Plan, Mid-term Progress Report and Final Report, and consolidating KPI evidence from all members

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

- **Compliance:** ensuring that all consortium members comply with the Sub-Grant Agreement, including confidentiality, security, ethics, data protection, IPR and visibility obligations;
- **Coordination:** acting as the primary contact for monitoring, review meetings, technical support and any corrective-action or escalation procedure
- **Notification:** informing AENAON without undue delay of any change in the consortium composition, any withdrawal of a member, or any circumstance affecting delivery.

The lead beneficiary is responsible to AENAON for the coordination and overall delivery of the sub-project, including the consolidated submission of reports, deliverables and KPI evidence. Each consortium member remains liable for its own obligations, as set out in the Sub-Grant Agreement. The cumulative EUR 100,000 ceiling applies per participating legal entity and not to the consortium as a whole (Section 2.4). Internal arrangements between consortium members (roles, budget shares, IPR) should be set out in a simple internal agreement, which AENAON may request to see at contracting stage.

3.3. Eligible Countries

Financial support under the AENAON Open Calls is limited to legal entities established in countries eligible under the applicable Digital Europe Programme rules, the AENAON Grant Agreement and the conditions of the relevant Open Call.

For Open Call 1, eligible applicants must be legally established in:

- one of the 27 Member States of the European Union
- Iceland
- Liechtenstein or
- Norway.

Any additional third country may participate only where it is expressly confirmed as fully associated with the Digital Europe Programme for **Specific Objective 3 – Cybersecurity and Trust** and is included in the definitive ‘**AENAON Open Call 1 – List of Eligible Countries.**’

Applicants established in countries associated with the Digital Europe Programme only for Specific Objectives 1, 2, 4 or 5 are not eligible under Open Call 1.

For consortium applications, every participating legal entity must independently satisfy the applicable country-eligibility requirements. If any consortium member is established in an ineligible country, the entire proposal will be declared ineligible and will not proceed to quality evaluation.

The definitive list of eligible countries is provided in the document “**AENAON Open Call 1 – List of Eligible Countries**”, published as part of the official Open Call package. Applicants are responsible for verifying their country eligibility before submission and throughout implementation.

Country-of-establishment eligibility is assessed separately from ownership-and-control requirements. Each participating legal entity must also comply with the applicable ownership-and-control, security, sanctions and strategic-autonomy conditions.

Entities subject to applicable EU restrictive measures are not eligible to participate in any capacity where such participation is prohibited by EU law or the applicable Open Call conditions.

This replacement removes the overly broad current reference to all associated countries.

3.4. Proposal Eligibility

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

To be eligible for evaluation, proposals must:

- be submitted electronically through the official AENAON Open Call submission system before the deadline specified in the relevant Open Call Notice
- be complete and include all required forms, annexes, declarations and supporting documents;
- be submitted in English
- use the official templates provided for the relevant Open Call round
- address the specific scope, objectives and expected outcomes of the relevant Open Call round
- propose innovative cybersecurity use cases relevant to offshore wind farms and/or the wider offshore wind ecosystem
- demonstrate a clear link to AENAON cybersecurity preparedness support services and, where applicable, to the Federated Digital Twin-based Cyber Range Platform
- describe the proposed technical approach, implementation plan, milestones, expected outputs, risks and mitigation measures
- explain the operational relevance of the proposed use case and its expected contribution to cybersecurity preparedness, threat detection, incident response, OT/IT security, resilience, scalability or regulatory alignment
- demonstrate feasibility within the expected duration, budget and available resources
- comply with applicable legal, ethical, security, data protection, dual-use and export-control requirements, where relevant
- not exceed the page limits specified in the relevant Open Call Notice and mandatory templates. Unless otherwise stated in the Open Call Notice, the technical proposal narrative must not exceed 10 pages
- declare whether they, or any member of their proposed consortium, have applied for or received AENAON FSTP funding under a previous Open Call round, for the purposes of verifying compliance with the cumulative maximum support ceiling
- not be in a situation of exclusion under the applicable EU financial rules (e.g., bankruptcy, serious professional misconduct, conviction for fraud or corruption, sanctions).

A proposal will be considered eligible only if it is clearly aligned with the objectives of the relevant AENAON Open Call round. The proposed activities must fall within the thematic scope of the relevant Open Call and within the closed list of eligible actions defined in the Open Call documentation. Open Call 1 focuses on enhancing cybersecurity preparedness for offshore wind farms through advanced threat detection, risk assessment, response technologies, risk scenarios, digital twin simulations and penetration testing. Open Call 2 focuses on scaling and validating the AENAON Cyber Range Platform across a broader range of stakeholders, including supply chain actors, cybersecurity authorities and NCCs.

3.5.Financial Eligibility

Applicants must demonstrate that they have the financial and operational capacity to implement the proposed action and to cover the required co-funding share.

The AENAON FSTP scheme has a total budget of **EUR 4,100,000**, indicatively allocated as EUR 2,100,000 for Open Call 1 and EUR 2,000,000 for Open Call 2, and is implemented through lump-sum sub-grants. The funding rate is 50% of the eligible budget of each supported sub-project. AENAON applies a justified derogation from the standard EUR 60,000 threshold, allowing support of up to **EUR 100,000 per individual third-party beneficiary / recipient / participating legal entity**. The exact amount awarded to each selected project will be determined at contracting stage through a needs-based and auditable right-sizing process, within the applicable ceilings and in relation to the scope, complexity and implementation requirements of the proposed action. This ceiling applies cumulatively across both Open Call rounds. Where the same legal entity has received AENAON FSTP funding under a previous Open Call round, the maximum amount that may be awarded in any subsequent round is

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

reduced accordingly, so that the aggregate total does not exceed EUR 100,000. Any amount not committed under Open Call 1 may be reallocated to Open Call 2, subject to the applicable Open Call rules, budget availability and the principles of transparency, equal treatment and sound financial management.

During the contract preparation phase, selected applicants must provide all required administrative, legal and financial documentation, which may include legal entity identification, VAT number where applicable, bank account information, declaration of honour, co-funding evidence, financial capacity information and any other documentation required by AENAON. Failure to provide the required documentation within the specified deadline may result in exclusion from contracting and replacement by a proposal from the reserve list.

Under the lump-sum model, financial support is not paid on the basis of individual cost verification. Recipients must nonetheless retain records sufficient to demonstrate that the approved action was properly implemented, that the financial support was not used for ineligible activities, and that no double funding occurred, in accordance with Section 8.1 and Section 14 of these Guidelines.

3.6.Language

English is the official language of the AENAON Open Calls. All proposals, declarations, annexes, supporting documents, correspondence, reports, deliverables and other documentation required during the application, evaluation, contracting and implementation phases must be submitted in English, unless otherwise expressly stated in the relevant Open Call Notice. Submissions in any language other than English may be deemed ineligible and may not be evaluated.

3.7.Impartiality, Applicant Declarations and Process-Side Conflicts of Interest

All persons involved in the AENAON Open Call process, including eligibility checks, evaluation, consensus, ranking, redress, contracting and monitoring, must act independently and impartially. Before accessing proposal information, evaluators, OCCC/OCTT/OCEP members, CEF Open Call management staff and any other persons involved in the process must declare the absence of any actual, potential or perceived conflict of interest. Where a conflict is identified, the person concerned must abstain from the relevant assessment, review, monitoring or decision-making process, and the recusal must be documented.

Applicants must disclose any personal, financial, commercial, institutional or organisational relationship with AENAON beneficiaries, affiliated entities, evaluators, OCCC/OCTT/OCEP members, CEF Open Call management staff or other persons involved in the Open Call process, where such relationship could reasonably affect, or appear to affect, the impartiality, equal treatment or integrity of the Open Call procedure.

AENAON will assess any disclosed relationship on a case-by-case basis. Where the relationship can be managed without compromising impartiality or equal treatment, appropriate mitigation measures may be applied, such as excluding the conflicted person from access, evaluation, monitoring or decision-making concerning the relevant proposal. Where the conflict cannot be effectively managed, the proposal may be declared ineligible or the recipient may be excluded from contracting or implementation.

AENAON beneficiaries under Grant Agreement and their affiliated entities are not eligible to receive financial support under the AENAON Open Calls. Evaluators, OCCC/OCTT/OCEP members and other persons involved in the preparation, management, evaluation, selection, redress, monitoring or decision-making of the Open Calls may not participate as funded applicants where such participation would compromise impartiality, equal treatment or the integrity of the process.

3.8.Documentation Format

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

All documentation required for any phase of the AENAON Open Calls must be submitted electronically through the official submission system, using the formats and templates specified in the relevant Open Call Notice. Unless otherwise stated in the Open Call Notice:

- proposal documents and annexes must be submitted in PDF format
- documents must be complete, legible and printable without restrictions
- mandatory templates must not be altered except where explicitly permitted
- page limits, file-size limits, naming conventions and formatting requirements must be respected
- supporting documents must be provided in the requested format and within the specified deadline.

Failure to comply with the required documentation format, templates, page limits, submission method or deadline may result in the proposal being declared inadmissible or ineligible.

4. Proposals – Process for Submission, Evaluation and Selection

4.1. Proposal Preparation and Submission

The AENAON Open Call process is designed to be straightforward, transparent and fully auditable. Applicants must read these Guidelines carefully before preparing their proposals. All proposals must be submitted electronically through the official AENAON Open Call portal, the address of which will be published in the relevant Open Call Notice. Submissions by email, post or any other means will not be accepted.

Proposals must be prepared using the mandatory templates provided with the relevant Open Call Notice and must include all required sections, declarations and supporting documents. Incomplete proposals may be declared inadmissible.

Applicants are strongly encouraged to submit their proposals well in advance of the deadline to avoid any last-minute technical difficulties. AENAON cannot be held responsible for delays caused by individual technical problems at the applicant's end.

4.1.1 Proposal package

A complete proposal package must include all of the following:

- the online application form, completed in full, with all required administrative information and declarations;
- the technical proposal, prepared using the official Technical Proposal Template (**Annex 3**), describing the proposed action, its relevance to the Open Call objectives, the methodology, work plan, milestones, expected outputs and risks, and respecting the 10-page limit and structure of that template;
- the budget and co-funding justification: the requested lump-sum amount, brief justification of the proportionality of the requested amount and confirmation of the 50% co-funding are provided in the online application form, and the justification of resources, cost-efficiency and financial realism is completed in Section 3.3 (Resource allocation and budgeting) of the Technical Proposal Template (**Annex 3**). Under the lumpsum model a detailed cost breakdown is not required;
- legal entity information, including legal entity identification number (PIC or equivalent), VAT number where applicable, and official registration extract or equivalent where requested;
- a **Declaration of Honour (Annex 5)**, signed by the applicant's authorised legal representative, confirming that the applicant is not in any of the exclusion situations under the applicable EU financial rules (e.g. bankruptcy, serious professional misconduct, fraud, corruption, sanctions);

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

- a **Consortium / Partner Declaration or commitment letter (Annex 6)**, where the proposal involves more than one legal entity;
- a confidentiality designation, identifying any elements of the proposal that the applicant designates as confidential, with a brief justification for each, completed in the designated confidentiality section of the Technical Proposal Template (**Annex 3**), in accordance with Section 18 of these Guidelines;
- an **IPR and Background Declaration (Annex 9)**, disclosing any relevant pre-existing intellectual property, third-party rights or licensing arrangements
- information on any planned subcontractors or external providers, where relevant;
- a **No Double Funding Declaration (Annex 8)**, completed by each participating legal entity, confirming that the same activities, costs, outputs or deliverables are not funded through another EU, national, regional or public source. Any prior AENAON FSTP funding must also be disclosed for verification of the cumulative EUR 100,000 ceiling.
- an **Ownership and Control Declaration (Annex 7)**, completed and signed by the applicant and, where applicable, by each participating legal entity in a small consortium, confirming that the applicant is established in an eligible country and is owned or controlled by natural or legal persons from eligible countries, within the meaning of the applicable Digital Europe Programme call conditions. The declaration must be completed using the standard template provided (**Annex 7**), adapted from the OCA declaration template available in the [Guidance on participation in DEP, Horizon Europe, EDF and CEF-DIG restricted calls](#). Failure to submit a completed and signed Ownership and Control Declaration will result in the proposal being declared inadmissible;
- any additional documents required by the relevant Open Call Notice.

4.2.Submission Rules

All proposals must be submitted electronically through the official AENAON submission portal before the deadline specified in the relevant Open Call Notice. The system-recorded timestamp at the time of submission is definitive. No extensions will be granted for individual technical problems, network delays, browser issues or last-minute file preparation difficulties.

Open calls will be kept open for a minimum of two months from the date of publication, in accordance with the applicable rules on financial support to third parties. The relevant Open Call Notice will specify the exact submission window for each round.

Applicants bear full responsibility for ensuring timely and complete submission. The AENAON helpdesk cannot guarantee a response to support requests submitted within 48 hours of the deadline.

4.3.Resubmission and Correction before the Deadline

Applicants may resubmit updated versions of their proposal through the official portal at any time before the deadline. Only the final version submitted before the deadline will be considered for evaluation. Earlier versions will be disregarded.

It is the applicant's responsibility to ensure that the final submitted version is complete, correct and using the required templates.

4.4.Late Submissions and Portal Failure

Late submissions will not be accepted. An exception may be considered only in the case of a documented, portal-wide technical failure officially acknowledged by AENAON and affecting multiple applicants. Any such decision will be communicated publicly through the official AENAON communication channels and will apply equally to all affected applicants.

4.5.Proposal Evaluation and Selection

The evaluation of proposals is carried out by the AENAON Open Call Evaluation Panel (OCEP) with the oversight of the Open Call Coordination Committee (OCCC). The process is designed to be fair, transparent, independent and fully auditable. All evaluators act independently and not as representatives of their employers, countries or any other organisation. The AENAON Open Call evaluation process is organised into the following stages:

4.5.1.Stage 1 – Admissibility and Eligibility Check

Following the closure of the submission window, the Open Call Coordination Committee (OCCC) secretariat or authorised Open Call management team will conduct an admissibility and eligibility check on all submitted proposals. This check will verify:

- that the proposal was submitted through the official portal and before the deadline
- that the proposal uses the mandatory templates and includes all required documents and declarations
- that the proposal is written in English
- that the applicant is a legal entity established in an eligible country, as described in Section 3.3. For consortium applications, this condition applies separately to every participating legal entity. Failure by any consortium member to satisfy the country-eligibility requirement renders the proposal ineligible as a whole. For consortium applications, this condition applies separately to every participating legal entity. Failure by any consortium member to satisfy the country-eligibility requirement renders the proposal ineligible as a whole.
- that each participating legal entity has submitted the required Ownership and Control Declaration and satisfies the applicable ownership-and-control conditions, where required.
- that the applicant falls within the categories of eligible recipients for the relevant Open Call round, as described in section 3.1;
- that the proposal's content is aligned with the thematic scope and objectives of the relevant Open Call round, as described in Section 2;
- that the applicant has submitted the required declarations, including the declaration of honour (Annex 5), no-double-funding declaration (Annex 8), prior AENAON FSTP funding declaration where applicable, and any required disclosure of relationships that could affect the impartiality of the Open Call process;
- that any applicable multiple-submission rules have been respected;
- that the applicant, and each consortium member, has declared any prior AENAON FSTP funding received, and that the proposed award would not result in any individual legal entity exceeding the cumulative EUR 100,000 ceiling across both Open Call rounds.

Proposals found to be inadmissible, or ineligible will receive a rejection letter with a brief justification. No technical evaluation feedback will be provided at this stage.

4.5.2.Stage 2 – Quality Evaluation by Independent Experts

Proposals that pass the admissibility and eligibility check will proceed to quality evaluation by the Open Call Evaluation Panel (OCEP). Each proposal will be assessed by at least two independent experts with relevant expertise in cybersecurity, offshore wind operations, OT/IT security, digital twin technologies, risk assessment, regulatory frameworks or related fields, as appropriate.

Each proposal will be evaluated against the following criteria:

5.

Evaluation Criterion	Assessment Focus
----------------------	------------------

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Evaluation Criterion	Assessment Focus
Excellence	Clarity, relevance and technical soundness of the proposed approach; relevance to offshore wind cybersecurity; maturity of the proposed solution; quality of the use case; and interaction with or contribution to AENAON cybersecurity preparedness services and the Federated Digital Twin-based Cyber Range Platform.
Impact	Expected contribution to cybersecurity preparedness and resilience for offshore wind operations and/or the wider offshore wind ecosystem; relevance to AENAON KPIs; scalability, replicability and ecosystem value; contribution to uptake, stakeholder engagement, regulatory alignment, supply-chain resilience and wider sector impact.
Implementation	Quality and feasibility of the work plan; adequacy of milestones, deliverables, timing and resources; team capacity and operational readiness; risk management; co-funding credibility; readiness to implement within the applicable Open Call duration; and ability to meet reporting, monitoring, security and contractual requirements.

Each criterion is assessed through sub-criteria. Each sub-criterion is scored on a scale from 0 to 5. The score for each main evaluation category is calculated as the normalised average of the sub-criteria scores under that category (i.e. the sum of sub-criteria scores divided by the number of sub-criteria), producing a category score on a scale from 0 to 5. The normalisation is calculated as follows: the Excellence category score is the sum of the 3 Excellence sub-criteria scores divided by 3 (maximum raw score: 15 points); the Impact category score is the sum of the 4 Impact sub-criteria scores divided by 4 (maximum raw score: 20 points); and the Implementation category score is the sum of the 6 Implementation sub-criteria scores divided by 6 (maximum raw score: 30 points). The normalised category score for each of the three criteria is then used for the calculation of the final weighted score, applying the Open Call-specific weights set out in the table below. The weights shown in the table apply to the normalised category score after averaging the sub-criteria scores, and not separately to each individual sub-criterion.

Evaluation Category	Sub-Criterion	Description / Focus Area	Score Range	OC1 Weight	OC2 Weight
Excellence	Technical and methodological quality	Clarity, relevance and rigour of the proposed concept, objectives and methodology, including the technical approach for using, integrating, validating or extending relevant AENAON tools, services and platform assets	0–5	30%	30%

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Evaluation Category	Sub-Criterion	Description / Focus Area	Score Range	OC1 Weight	OC2 Weight
	Innovation potential	Novelty of the approach, technological advancement or originality of the idea			
	Alignment with AENAON objectives	Degree to which the proposal contributes to AENAON's objectives, Open Call scope, expected use cases and the uptake or validation of AENAON tools, services and platform capabilities			
Impact	Expected outcomes and benefits	Contribution to target communities, sectors and measurable results	0–5	30%	40%
	Dissemination and exploitation strategy	Effectiveness of plans for knowledge sharing, adoption and sustainability			
	Contribution to AENAON ecosystem	Strategic value, stakeholder engagement and potential for real-world uptake, including contribution to the validation improvement, replication or wider adoption of AENAON assets and services			
Implementation	Work plan and methodological coherence	Logical structure and clarity of activities, consistency between objectives, tasks and deliverables, adequacy of described methods and timelines, including planned onboarding, integration, testing or validation activities involving AENAON tools/services	0–5	40%	30%
	Management structure and governance	Suitability of management setup, division of roles and responsibilities, coordination mechanisms, decision-making workflows, and financial accountability			
	Resource allocation and budgeting	Justification of costs, cost-efficiency, adequacy of human and technical resources, and financial realism, including the proportionality of the requested support to the proposed use of AENAON tools/services, integration effort, validation activities and expected contribution to AENAON objectives			

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Evaluation Category	Sub-Criterion	Description / Focus Area	Score Range	OC1 Weight	OC2 Weight
	Risk identification and mitigation	Completeness and credibility of risk analysis, contingency planning and mitigation measures			
	Team experience and capacity	Expertise, track record, and complementarity of consortium members in relevant fields			
	Monitoring and quality assurance	Clear progress tracking, performance indicators, and internal evaluation mechanisms ensuring delivery quality and compliance			
	Gender equality, diversity and inclusive participation	Credible and proportionate measures supporting gender equality, diversity and inclusive participation in the sub-project, including where relevant team composition, governance, stakeholder engagement, training or dissemination activities. Assessment is based only on information explicitly provided in the proposal.			

The three criteria are weighted differently for each Open Call round. For Open Call 1, the weights are: Excellence 30%, Impact 30%, Implementation 40%. For Open Call 2, the weights are: Excellence 30%, Impact 40%, Implementation 30%. These weights will be published in the relevant Open Call documentation and applied consistently to all eligible proposals submitted under the respective round.

4.5.3 Scoring Scale

Each criterion is scored on the following scale:

Score	Description
0 – Fail	Criterion not addressed or cannot be assessed due to missing or incomplete information.
1 – Poor	Criterion addressed inadequately; serious weaknesses that would impede success
2 – Fair	Criterion broadly addressed but with significant weaknesses that would hinder implementation
3 – Good	Criterion addressed adequately, with some room for improvement and certain details missing

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Score	Description
4 – Very Good	Criterion addressed very well; only minor improvements possible; minor details missing
5 – Excellent	Criterion fully and convincingly addressed; any shortcomings are negligible

Thresholds: Proposals must score at least 3 out of 5 on each individual criterion (Excellence, Impact and Implementation). Proposals failing to meet the minimum score on any individual criterion will be rejected and will not be included in the final ranking list. In addition, proposals must obtain a minimum overall weighted score of at least 3.33 out of 5, corresponding to the standard overall quality threshold of 10 out of 15 on the unweighted scale. Proposals failing either the individual criterion threshold or the overall weighted threshold will not be eligible for funding and will be notified accordingly.

4.5.4 Individual Evaluation, Consensus and Evaluation Summary Report (ESR)

Each eligible proposal will normally be assessed independently by two external evaluators. Each evaluator completes an Individual Evaluation Report (IER), assigning scores and comments for each criterion. Evaluators then participate, where required, in a consensus process to reconcile significant scoring differences and produce a single Evaluation Summary Report (ESR) per proposal.

The ESR is the basis for applicant feedback and ranking. It must not disclose confidential information about other applicants, evaluators or AENAON internal deliberations.

A significant divergence shall be deemed to exist where: (i) the difference between the scores awarded for any individual evaluation criterion is greater than 2.5 points; or (ii) the difference between the overall scores awarded to a proposal is greater than or equal to 4.5 points. In either case, the proposal enters a consensus process. The consensus process should be concluded within five working days. If the evaluators do not reach agreement within that period, a third independent evaluator is automatically appointed. The final evaluation outcome is then established through the prescribed consensus procedure and documented in the Evaluation Summary Report.

4.5.5 Ranking, Tie-Breaks and Reserve List

All proposals that pass all thresholds are ranked from highest to lowest overall weighted average score. In the event of proposals occupying the same position in the ranking, tie-breaks will be resolved by applying the following order of priority, unless otherwise specified in the relevant Open Call Notice:

For **Open Call 1**, where proposals obtain the same final weighted score, priority shall be given first to the proposal with the highest score under Implementation (the highest-weighted criterion in OC1); if the tie persists, to the proposal with the highest score under Excellence; and then Impact.

For **Open Call 2**, priority shall be given first to the proposal with the highest score under Impact (the highest-weighted criterion in OC2); if the tie persists, to the proposal with the highest score under Excellence; and then Implementation.

If the tie still persists, the final decision shall be taken by the OCCC on the basis of overall strategic fit with the objectives of the relevant Open Call, ensuring equal treatment, transparency and full documentation of the decision in the Open Call audit trail.

Proposals above the threshold but not immediately funded due to budget constraints will be placed on a reserve list in rank order. The reserve list will remain valid for the period specified in the Open Call Notice and may be used if selected applicants withdraw, fail the contracting checks or additional budget becomes available.

4.5.6 Evaluator Recruitment and Selection

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

To ensure independent and expert evaluation of submitted proposals, AENAON will conduct a public call for external evaluators. The call for evaluators will collect information on each candidate's area of expertise, previous experience in proposal evaluation or similar assessment activities, availability during the evaluation period, and declarations of independence, confidentiality and absence of conflict of interest. Only experts meeting the required independence and competence criteria will be selected. The evaluator call will be published on the AENAON website and will specify the target expertise profile, mandatory independence and availability requirements, and the application package required.

Target expertise includes: critical infrastructure cybersecurity, OT/ICS/SCADA security, offshore wind energy operations, cyber ranges and red/blue team exercises, risk and vulnerability assessment, and experience with EU-funded evaluation processes.

Mandatory requirements for all evaluators include: full independence from all AENAON consortium members and applicants; absence of conflict of interest; commitment to confidentiality; compliance with GDPR; and availability during the applicable evaluation window.

Evaluators assess proposals independently and do not take part in contracting, payment or monitoring decisions.

6. Notification, Feedback and Redress

6.1. Notifications

All applicants will be informed of the outcome of the evaluation process. The following table summarises the notification content for each possible outcome:

Outcome	Notification Content
Inadmissible / Ineligible	Rejection letter with a brief statement of the grounds for inadmissibility or ineligibility. No technical evaluation feedback is provided at this stage
Below threshold	ESR summary with final scores and a brief statement that the proposal did not meet the minimum score requirements
Above threshold but not funded	ESR summary with final scores and notification of non-funded status due to budget constraints or portfolio rules. Reserve list status, where applicable, will be specified
Reserve list	ESR summary, reserve list position, validity period and the conditions under which the applicant may be invited to enter contracting
Selected	Invitation to the contract preparation phase, with a list of required documents and checks and the relevant deadlines

6.2. Redress Procedure

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Applicants may request clarification on the evaluation outcome and may submit a request for redress where they consider that a procedural error may have occurred during the admissibility, eligibility, evaluation, ranking or selection process.

The redress procedure is strictly limited to verifying whether the evaluation and selection process was conducted in accordance with the published rules, criteria and procedures. It does not entail a re-evaluation of the proposal, a revision of the evaluators' scientific, technical or commercial judgement, or the introduction of new information by the applicant after the submission deadline.

Grounds for redress may include, for example:

- misapplication of the published admissibility or eligibility criteria;
- failure to apply the published evaluation criteria, thresholds, weighting or tie-break rules;
- arithmetic or clerical errors affecting the final score or ranking;
- a proven conflict of interest affecting the procedure;
- material administrative mishandling that may have affected the outcome.

Redress requests must be:

- submitted within the timeframe specified in the relevant Open Call documentation;
- submitted by the legal representative of the applicant or lead applicant;
- submitted using the official redress request form;
- accompanied by a clear description of the alleged procedural error and the grounds on which the request is based;
- limited to information already submitted before the applicable proposal deadline.

Requests for redress will be reviewed by the **Open Call Coordination Committee (OCCC)**. The OCCC will examine whether the applicable procedures were correctly and consistently applied. Where necessary, the OCCC may seek factual clarifications regarding the conduct of the procedure, including from the Open Call management team, evaluators or other persons involved in the process, without reopening the evaluation of the proposal itself.

If the OCCC confirms that a procedural error occurred and that the error may have affected the outcome, AENAON may take appropriate corrective measures in accordance with the published Open Call rules. Such measures shall be limited to correcting the procedural deficiency and restoring compliance with the applicable procedure. The redress procedure shall not be used to replace the independent evaluators' scientific or technical assessment.

Any member of the OCCC with an actual, potential or perceived conflict of interest in relation to the applicant concerned shall abstain from the redress review and decision-making process.

Applicants will be informed of the outcome of the redress procedure. All redress requests, reviews, decisions and related justifications will be documented and retained in the Open Call audit trail to ensure traceability, accountability and full auditability of the process.

The outcome of the redress procedure is final within the AENAON Open Call process.

7.Contract Preparation and Sub-Grant Agreement

7.1.Contract Preparation Phase

Selected applicants will be invited to enter the contract preparation phase. This phase involves a series of administrative, financial, technical and, where relevant, ethics and security checks. AENAON will communicate the specific documentation requirements and deadlines to each selected applicant.

Contract preparation checks include:

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

- legal entity validation and confirmation of representative authority;
- bank account and payment documentation;
- co-funding capacity and financial viability confirmation;
- ethics, security and data protection clarifications where needed;
- technical work plan refinement, including KPI targets, milestones, deliverables and acceptance criteria;
- IPR and background declarations and any access rights clarifications;
- subcontractor and third-party involvement verification
- confirmation of compliance with eligibility conditions, absence of double funding, and disclosure of any relationship or circumstance that could affect the impartiality or integrity of the Open Call process;
- Gender Equality Plan confirmation where required (for public bodies, higher education institutions and research organisations)

7.2.Failure to Complete Contracting

If a selected applicant fails to provide the required documentation within the specified deadlines, fails any of the contracting checks, requests modifications that are incompatible with the Open Call rules, or does not sign the Sub-Grant Agreement by the published deadline, AENAON reserves the right to withdraw the award decision and invite the next proposal from the reserve list.

7.3.Sub-Grant Agreement

The Sub-Grant Agreement will be signed, according to the relevant consortium authorisation, between the Circular Economy Foundation (CEF), acting as WP4 Lead and Open Call Manager, on behalf of the AENAON consortium for the purposes of FSTP management, and the selected recipient or lead beneficiary -acting on behalf of any consortium partners where applicable- of the selected sub-project (Annex 4).

The Sub-Grant Agreement will include, as a minimum:

- the parties, the role of the lead beneficiary and, where applicable, consortium partners;
- the approved work plan, deliverables, KPIs, milestones, acceptance criteria and implementation timetable;
- the maximum financial support, funding rate, co-funding obligation, milestone-linked payment instalments and supporting evidence requirements;
- flow-down obligations covering confidentiality and security, ethics and EU values, EU visibility, applicable DIGITAL-specific rules, information obligations, record-keeping, and audit access rights;
- data protection and processing roles, including controller/processor arrangements where personal data are involved;
- rules for the responsible handling of cybersecurity vulnerabilities, sensitive operational data, OT/IT information and incident-related data;
- IPR, background, results, access rights and publication review rules;
- communication, dissemination and EU visibility obligations;
- monitoring, reporting, review meetings, corrective action procedures, suspension and termination provisions;
- liability, indemnity, applicable law and dispute resolution provisions;
- verification of whether the selected applicant or any consortium member has previously received AENAON FSTP funding under another Open Call round, and adjustment of the final sub-grant amount where necessary to ensure the cumulative EUR 100,000 ceiling per legal entity is not exceeded.

8.AENAON Funding Programme: Implementation, Technical Support and Reporting

The AENAON FSTP funding programme is structured to support selected projects through implementation phases with defined objectives, deliverables, reporting obligations and payment triggers. The implementation duration depends on the relevant Open Call round. Open Call 1 sub-projects may have an implementation duration of up to 8 months, while Open Call 2 sub-projects are expected to have an implementation duration of up to 10 months. The exact start date, end date, phase structure, deliverables, reporting deadlines and payment triggers for each selected sub-project will be confirmed in the Sub-Grant Agreement following contract preparation and signature.

8.1.Implementation Phases

The implementation phases and deliverables will be adapted to the duration and scope of the relevant Open Call round. For Open Call 1, where an implementation duration of 8 months is applied, funded sub-projects may be structured as follows:

Phase 1 – Planning and Onboarding, Month 1

- Purpose: detailed project set-up, technical planning and integration readiness.
- Activities: strategy definition; detailed work plan finalisation; integration approach with AENAON services and platform; access and onboarding arrangements; risk register; KPI plan; data and security plan.
- Deliverable: first report/planning and onboarding deliverable, including milestones, budget breakdown, KPI targets, risk assessment and data/security plan.
- Payment trigger: 30% pre-financing of the total lump-sum support is released upon signature of the Sub-Grant Agreement and completion of the onboarding requirements.

Phase 2 – Deployment and Implementation, Months 2–5

- Purpose: integration, testing, cyber range scenario development and operational validation.
- Activities: technology integration and configuration; cybersecurity testing and validation; digital twin simulations; penetration-testing scenarios; OT/IT security validation; supply-chain resilience testing where applicable; training and exercise activities; mid-term progress documentation.
- Deliverable: mid-term progress report covering work completed, technical evidence, KPI progress, challenges encountered and risk updates.
- Payment trigger: 40% of the total lump-sum support is released upon acceptance of the mid-term report and corresponding milestone evidence.

Phase 3 – Evaluation, Refinement and Reporting, Months 6–8

- Purpose: performance assessment, results consolidation, final reporting and contribution to AENAON ecosystem activities.
- Activities: evaluation of results against KPI targets; platform and service refinement based on validation findings; regulatory alignment assessment; preparation of final technical and financial outputs; lessons learned documentation; contribution to AENAON dissemination, exploitation and assessment activities.
- Deliverable: final report, including project outcomes, KPI achievement evidence, validation results, lessons learned, a security-cleared public summary and contribution to AENAON's Open Call assessment activities.
- Payment trigger: 30% of the total lump-sum support is released upon acceptance of the final report, final deliverables and any required participation in AENAON showcase or dissemination activities.

For Open Call 2, where an implementation duration of 10 months is applied, funded sub-projects may be structured as follows:

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Phase 1 – Planning and Onboarding, Month 1

- Purpose: detailed project set-up, technical planning and integration readiness.
- Activities: strategy definition; detailed work plan finalisation; integration approach with AENAON services and platform; access and onboarding arrangements; risk register; KPI plan; data and security plan.
- Deliverable: first report/planning and onboarding deliverable.
- Payment trigger: 30% pre-financing of the total lump-sum support is released upon signature of the Sub-Grant Agreement and completion of the onboarding requirements.

Phase 2 – Deployment and Implementation, Months 2–6

- Purpose: integration, testing, cyber range scenario development, operational validation and scaling activities.
- Activities: technology integration and configuration; cybersecurity testing and validation; digital twin simulations; penetration-testing scenarios; OT/IT security validation; supply-chain resilience testing; multi-site or cross-stakeholder validation; training and exercise activities; mid-term progress documentation.
- Deliverable: mid-term progress report covering work completed, technical evidence, KPI progress, challenges encountered and risk updates.
- Payment trigger: 40% of the total lump-sum support is released upon acceptance of the mid-term report and corresponding milestone evidence.

Phase 3 – Evaluation, Refinement and Reporting, Months 7–10

- Purpose: performance assessment, scalability assessment, results consolidation, final reporting and contribution to AENAON ecosystem activities.
- Activities: evaluation of results against KPI targets; platform and service refinement based on validation findings; regulatory alignment assessment; scalability and replication assessment; preparation of final technical and financial outputs; lessons learned documentation; contribution to AENAON dissemination, exploitation and final assessment activities.
- Deliverable: final report, including project outcomes, KPI achievement evidence, validation results, lessons learned, a security-cleared public summary and contribution to AENAON's Final Open Call Assessment Report.
- Payment trigger: 30% of the total lump-sum support is released upon acceptance of the final report, final deliverables and any required participation in AENAON showcase or dissemination activities.

The exact phase structure, deliverables, deadlines and acceptance criteria will be specified in the relevant Open Call Notice and Sub-Grant Agreement.

8.2.Deliverables, Milestones and Linked Payments — Summary

The table below consolidates, in one place, the deliverables each funded sub-project must submit, the phase and indicative month, the payment tranche each deliverable unlocks, and the body responsible for acceptance. Indicative months correspond to the 8-month structure of Open Call 1; for Open Call 2 the same three-phase logic applies over 10 months (see Section 7.1). Exact dates and acceptance criteria are fixed in the Sub-Grant Agreement.

Deliverable	Month (OC1)	Precondition to unlock payment	Payment tranche	Acceptance body
Project Plan / Onboarding deliverable	M1	SGA signed and onboarding completed (the Project Plan / onboarding deliverable, covering	30%	OCTT verification → OCCC confirmation

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

		work plan, KPI targets, risk register, budget, co-funding confirmation and data/security plan, is due at M1)		
Mid-term Progress Report	M5 (OC1) / M6 (OC2)	Mid-term review passed; progress, technical evidence, KPI progress and milestone evidence accepted	40%	OCTT verification → OCCC confirmation
Final Report + security-cleared public summary	M8 (OC1) / M10 (OC2)	Final report, final deliverables, KPI achievement evidence, validation results and required participation in AENAON assessment/dissemination accepted	30%	OCTT verification → OCCC confirmation

No payment tranche is released until the corresponding deliverable has been technically verified by the OCTT and acceptance has been confirmed by the OCCC (Section 7.3). Where a deliverable is not accepted, the payment is withheld until the deliverable is corrected and accepted, in accordance with the non-performance escalation procedure in Section 8.6.

8.3. Technical Support and Guidance

Throughout the implementation period, selected sub-projects will receive ongoing technical support and guidance from the AENAON consortium. This includes:

- access to AENAON's Federated Digital Twin-based Cyber Range Platform and associated cybersecurity preparedness support services, in accordance with the scope agreed in the Sub-Grant Agreement;
- technical guidance from AENAON consortium members, including domain experts in OT/IT security, digital twin technologies, cyber range operations, threat and risk assessment, regulatory frameworks and cybersecurity preparedness;
- mentoring and capacity-building support, where applicable and subject to the scope and availability of WP5 activities; the specific scope of any mentoring support will be confirmed in the Sub-Grant Agreement;
- dedicated onboarding process, including guidance on platform access, integration requirements and reporting obligations;
- participation in at least two coordination meetings or review sessions during the implementation period, as well as ad hoc support as needed.

8.4. Reporting Requirements

All funded sub-projects must submit the reports defined in the relevant Open Call Notice and Sub-Grant Agreement. Indicatively, the reporting structure will include the following reports, adapted to the implementation duration of the relevant Open Call round:

- **Project Plan (end of Phase 1):** a detailed plan covering scope, milestones, KPI targets, risk register, integration approach, budget breakdown and data/security arrangements.
- **Mid-term Progress Report (end of Phase 2):** a report on progress made during implementation, KPI status, technical evidence, any deviations from the original plan, challenges encountered and solutions applied.
- **Final Report (end of Phase 3):** a comprehensive final report documenting outcomes, KPI achievement, validation evidence, lessons learned, exploitation and dissemination contributions, and a security-cleared public summary of the sub-project results.
- **Financial Reporting:** where relevant, financial information demonstrating proper use of the lump-sum support and absence of double funding.

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Additional incident, data breach, security, ethics, double-funding, eligibility or integrity-related notifications must be submitted without undue delay if such circumstances arise during the implementation period.

All reports will be reviewed and assessed by AENAON. Reports that do not meet the required quality standard may be returned for revision within a specified period. Repeated failure to submit acceptable reports may result in suspension or termination of the Sub-Grant Agreement and non-payment or recovery of support.

Deliverables and milestone evidence submitted by sub-grantees will be technically verified by the OCTT against the acceptance criteria defined in the Sub-Grant Agreement. On the basis of the OCTT verification record, the OCCC will confirm acceptance or non-acceptance for the purpose of payment authorisation. Payment will not be released without both OCTT verification and OCCC confirmation.

8.5. Monitoring and KPI Framework

AENAON will actively monitor the progress of each funded sub-project throughout the implementation period. Monitoring activities include:

- a kick-off meeting at the start of Phase 1 to confirm the detailed work plan and onboarding arrangements
- periodic progress check-ins (at least every two months) conducted by the assigned AENAON technical contact
- mid-term review at the end of Phase 2, assessing milestone completion, KPI progress, technical risks and deliverable quality
- final review at the end of Phase 3, assessing overall KPI achievement, output quality, compliance and readiness of results for wider adoption
- integration with AENAON's dedicated KPI dashboard, which will track performance across all funded sub-projects in real time.

Open Call Technical Team (OCTT) technical review activities are limited to monitoring, milestone verification and technical support. The OCTT does not modify evaluator scores, ranking decisions or redress outcomes at any stage of the Open Call process.

Each sub-project will be expected to contribute to one or more of the following AENAON project KPIs:

- development of risk scenarios for offshore wind operations (AENAON KPI: more than 20 risk scenarios across all Open Call projects)
- penetration testing activities (AENAON KPI: more than 10 penetration tests)
- engagement of industry stakeholders, contributing to the AENAON KPI of more than five industry stakeholders engaged across relevant Open Call testing, validation and pilot activities, with specific targets per sub-project to be defined proportionately in the Sub-Grant Agreement
- large-scale cybersecurity simulations, supply-chain resilience tests and cross-border threat response exercises (primarily Open Call 2)
- training and capacity-building activities for offshore wind sector personnel.

△ Final KPI targets per sub-project will be defined and confirmed in the Sub-Grant Agreement at contracting stage, proportionate to the scope, scale and complexity of the approved action.

9. Financial, Cost and Audit Rules

9.1. Funding Model and Payment Basis

AENAON provides financial support to third parties exclusively in the form of lump-sum sub-grants. Payments are linked to the verified completion and acceptance of predefined milestones and deliverables, as specified in the

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Sub-Grant Agreement. The lump-sum model is intended to simplify financial management, reduce administrative burden and facilitate participation by SMEs and other eligible actors.

Under the lump-sum model, payment is not based on reimbursement of actual costs incurred. Instead, recipients must demonstrate proper implementation and achievement of the agreed milestones and outputs. Recipients must retain sufficient records and evidence to demonstrate that the approved action has been properly implemented and that the financial support has not been used for ineligible activities or for activities funded by another EU grant.

9.2. Eligible Activities and Cost Principles

Activities funded under AENAON Open Calls must be directly linked to and necessary for the implementation of the approved sub-project, fall within the closed list of eligible activity types for the relevant Open Call round, and occur within the approved implementation period.

Expenditure must be reasonable, justified and consistent with sound financial management principles. Where sub-projects involve purchases, sub-contracts or use of external resources, recipients must ensure best value for money, avoid conflicts of interest and comply with applicable procurement rules.

The eligible activities for each Open Call round are defined by a closed and exhaustive list. Any activities outside this scope are not eligible. The closed lists for Open Call 1 and Open Call 2 are as follows:

Open Call 1 – Eligible Activity Types

Activity Code	Description and Scope
A1.1: Integration of cybersecurity technologies	Definition of cybersecurity requirements for the offshore wind sector; integration of AI-driven threat detection; analysis of OT security challenges and tools; predictive analytics. Scope limited to technologies relevant to offshore wind operational environments.
A1.2: Testing in real-world pilots	Performance evaluation and assessment of digital twin simulations; SCADA system security assessments; validation of penetration-testing mechanisms. Must demonstrate operational relevance to offshore wind installations.
A1.3: Compliance and resilience	Strategy and best practices validation; content delivery through the AENAON Federated Digital Twin-based Cyber Range Platform for strengthening alignment with NIS2 and CER mandates. Must include demonstrable regulatory alignment evidence.
A1.4: Dissemination and communication	Design and execution of targeted dissemination and communication plans; activities for increasing the visibility of the AENAON project and funded action impact, including website references, newsletters, technical blogs, videos, presentations and participation in AENAON or relevant sector events. Marketing activities unrelated to scientific, industrial or societal impact are not eligible.

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Activity Code	Description and Scope
A1.5: Collaboration and impact	Activities demonstrating contribution to AENAON KPIs, specifically: Activities demonstrating a proportionate contribution to the collective AENAON Open Call 1 KPIs, including the development of offshore-wind cybersecurity risk scenarios, penetration-testing or validation activities, and engagement of relevant industry stakeholders. The overall AENAON targets are more than 20 risk scenarios, more than 10 penetration tests and more than five industry stakeholders across the relevant funded Open Call projects. Individual sub-project targets will be agreed proportionately during contracting.

Open Call 2 – Eligible Activity Types

Activity Code	Description and Scope
A2.1: Scalability testing	Defining scaling strategies for offshore wind farms and supply chain actors; validation of multi-site cybersecurity deployments in offshore wind infrastructures. Must address multiple operational contexts or stakeholder groups.
A2.2: Complex threat simulation	Cybersecurity simulations addressing zero-day, DDoS and supply chain attack resilience; large-scale cross-border threat response exercises. Must demonstrate technical credibility and operational relevance.
A2.3: Industry collaboration and compliance	Demonstrating how applied solutions strengthen coordination between wind operators, suppliers and cybersecurity bodies; validation of coordinated resilience plans; regulatory alignment and NIS2/CER evidence across multiple stakeholders.
A2.4: Dissemination and communication	As per A1.4, with an emphasis on scaling and cross-stakeholder outreach. Same eligibility boundaries apply.
A2.5: Collaboration and impact at scale	Activities demonstrating contribution to large-scale AENAON KPIs, including multi-site cybersecurity exercises, cross-border threat response, trained professionals and supply-chain resilience metrics.

⚠ The eligible activity lists are closed and exhaustive. Any activities outside these types, including generic marketing, unrelated R&D, or capital investments not directly necessary for sub-project implementation, are not eligible for AENAON financial support.

9.3. Ineligible Costs and Activities

The following are not eligible under the AENAON FSTP scheme:

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

- activities not linked to the approved sub-project or not necessary for its implementation
- activities or costs already funded by another EU grant, EU Member State grant or other public funding in a way that constitutes double funding
- activities outside the closed list of eligible activity types for the relevant Open Call round
- debt, interest owed, exchange losses, excessive or reckless expenditure, provisions for losses or debts, return on capital or dividends
- deductible or refundable VAT where applicable
- costs incurred during periods of suspension or outside the approved implementation period
- activities involving entities established in or controlled by non-eligible countries where this is prohibited under the applicable call conditions or security and strategic autonomy rules
- activities that breach applicable ethics, data protection, security, confidentiality, export-control, sanctions or EU strategic autonomy rules
- generic marketing activities or other activities unrelated to the scientific, industrial or societal impact of the funded action.

9.4.Audit, Record-Keeping and Access Rights

Recipients must retain records and supporting documents demonstrating proper implementation of the approved action, achievement of agreed milestones, compliance with the Sub-Grant Agreement and absence of double funding. Records must be kept for at least five years after the final payment from AENAON, in accordance with the AENAON Grant Agreement and the applicable Open Call documentation. If any audit, review, investigation, recovery, litigation or dispute is ongoing at the end of the retention period, records must be retained until the relevant procedure is fully closed.

Recipients must allow access to their records, premises and relevant personnel for checks, reviews, audits, investigations and impact evaluations conducted by AENAON, the granting authority (ECCC), the European Commission, OLAF, EPPO, the European Court of Auditors and other competent bodies, for the same retention period.

9.5.Recoveries, Suspension and Termination

AENAON may suspend payments, reject deliverables, reduce support, terminate the Sub-Grant Agreement or recover amounts already paid in cases including: false or misleading declarations; ineligibility discovered after award; double funding; serious delay or non-implementation; breach of confidentiality, security, data protection or ethics obligations; unmanaged conflict of interest affecting the Open Call process, procurement, subcontracting, implementation or monitoring of the funded action;; audit refusal; failure to retain records; or breach of strategic autonomy or export-control rules.

Termination of the Sub-Grant Agreement does not affect surviving obligations, including confidentiality, security, record-keeping, audit access, data protection, IPR restrictions, publication rules and recovery obligations.

9.6.Non-Performance Escalation Procedure

Where a recipient fails to submit an acceptable deliverable, misses a milestone, or otherwise fails to comply with the Sub-Grant Agreement, AENAON will follow the escalation procedure below:

Step 1 — Early warning and clarification. The OCTT will record the issue (non-compliance note) and notify the sub-grantee in writing, requesting corrective actions and setting a cure deadline of typically 10–15 calendar days, unless the breach requires immediate action.

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Step 2 — If corrective actions are not provided within the cure period, or if progress evidence is insufficient, the OCCC may suspend the next payment tranche and/or accept deliverables conditionally, with a corrective action plan, revised timeline and revised verification points.

Step 3 — OCCC decision. If non-performance persists or cannot be remedied, the OCCC will decide on the appropriate course of action, which may include suspension of payments, reduction of financial support, termination of the Sub-Grant Agreement, or recovery of amounts already paid. The decision will be documented and communicated to the recipient in writing.

Step 4 — Coordinator and Programme Officer notification. Where the non-performance creates a material contractual or financial risk for the AENAON project, the OCCC will inform the Coordinator (ASFALYS SRL) and, where required by the AENAON Grant Agreement, the ECCC Programme Officer.

All escalation steps, decisions and communications will be retained in the AENAON audit record. Timeframes for each step will be confirmed in the Sub-Grant Agreement.

10. Ethics, Security, Confidentiality and Data Protection

10.1. Ethics and EU Values

All funded sub-projects must comply with applicable ethical principles, EU values and relevant EU, international and national law, in accordance with Annex 5 of the AENAON Grant Agreement (Specific Rules). Applicants must identify and manage ethical risks linked to their proposed activities, including cybersecurity testing in operational environments, human participation in training and exercises, dual-use potential of developed tools, responsible vulnerability disclosure, and any use or generation of sensitive or personal data.

Where required, recipients must obtain all necessary approvals from relevant ethics committees, data protection authorities or other competent bodies before commencing the relevant activities. Documentation must be retained and provided to AENAON upon request.

AENAON may require additional ethics and security safeguards or the exclusion of specific activities before contracting or during implementation if ethical or security risks are identified.

10.2. Cybersecurity, Sensitive Information and Responsible Disclosure

Given the nature of the AENAON project and the sensitive operational environments involved, recipients must apply robust cybersecurity safeguards throughout the implementation of their sub-projects. In particular:

- sensitive information, including vulnerabilities, incident data, threat intelligence, digital twin configurations, SCADA/OT/IT architecture, credentials, operational data and non-public AENAON technical information, must be protected and used only for the purposes of the approved sub-project
- sensitive information may be disclosed only to persons with a genuine need to know and who are bound by equivalent confidentiality obligations
- responsible disclosure procedures must be followed for any vulnerabilities identified during the sub-project: exploit details, weaknesses, operational configurations and security-sensitive findings must not be publicly disclosed without prior review and written clearance from AENAON. AENAON will complete its security and confidentiality review within 30 calendar days of receiving a submission. Where additional time is required due to the sensitivity or complexity of the material, AENAON may extend this period by a further 30 calendar days with written notice to the recipient. If AENAON does not respond within the applicable review period, the recipient must contact AENAON in writing to request a decision before proceeding with any disclosure. AENAON will treat such a request as urgent and respond within five working days. Publication without an explicit written clearance from AENAON remains prohibited regardless of elapsed time

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

- where EU classified information or information subject to specific security recommendations is involved, it must be handled in strict accordance with applicable EU, international and national classified information rules and any specific requirements communicated by AENAON or the granting authority
- recipients must immediately notify AENAON of any security incident, unauthorised access, data breach or other event that could affect the security of AENAON-related information or systems.

10.3.Data Protection

Applicants and recipients must comply with the General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) and applicable national data protection law in all activities involving the processing of personal data.

Proposals must describe, where relevant: the lawful basis for processing; data minimisation measures; access controls and security safeguards; data retention periods; cross-border transfer mechanisms; data subject information procedures; processor and sub-processor arrangements; and data breach notification procedures.

Where operational or cybersecurity data generated or processed during the sub-project contain personal data, recipients must apply appropriate pseudonymisation, anonymisation, minimisation and technical security measures. The determination of data controllership between AENAON and each recipient shall be analysed on a case-by-case basis, taking into account the specific nature, purpose and means of the personal data processing activities involved in each supported sub-project. For all processing activities undertaken as part of the Open Call process itself — including proposal submission, eligibility and admissibility checks, evaluation procedures, contracting and monitoring — Circular Economy Foundation (CEF), as Open Call manager, is the sole data controller. With respect to personal data processing carried out by recipients in the context of their funded sub-project activities, the applicable controllership arrangement — whether independent controllership, joint controllership or a controller/processor relationship — will be determined on a case-by-case basis and will form part of the contractual arrangements established between AENAON and each recipient through the Sub-Grant Agreement. Where joint controllership or a controller/processor arrangement is identified, the Sub-Grant Agreement will include the appropriate data protection provisions reflecting the respective roles and responsibilities of each party, in accordance with Articles 26 and 28 of Regulation (EU) 2016/679 (GDPR) as applicable. No personal data shall be shared between the parties until the applicable data protection arrangement has been documented and, where required, a Data Processing Agreement has been signed.

10.4.Confidentiality Duration

Confidentiality obligations under the Sub-Grant Agreement will apply for a period of five years after the final payment received by the recipient from AENAON, in accordance with the AENAON Grant Agreement.

11.IPR, Background, Results and Access Rights

The intellectual property provisions applicable to AENAON sub-grantees are governed by the relevant clauses of the Sub-Grant Agreement and are consistent with the AENAON Grant Agreement (Annex 5 – Specific Rules on IPR) and the applicable EU Financial Regulation rules on financial support to third parties.

11.1.Background

Applicants must identify, in their proposal and in the Sub-Grant Agreement, all pre-existing background knowledge, data, software, tools, standards materials and third-party rights that they intend to use during the sub-project. This includes any open-source software components, commercially licensed tools and datasets, the use of which must be consistent with applicable licence terms, confidentiality obligations and the security requirements of the AENAON project.

Background that is subject to control or restrictions by a non-eligible country or entity must not be used in the sub-project, in accordance with the EU strategic autonomy requirements applicable to the AENAON call.

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

11.2.Ownership of Results

Unless otherwise agreed in the Sub-Grant Agreement, results generated by the recipient during the implementation of the approved sub-project are owned by the recipient. The granting authority does not acquire ownership of sub-project results.

However, recipients must grant AENAON the access and use rights over sub-project results necessary for monitoring, validation, reporting to the granting authority, audit, impact assessment, contribution to AENAON dissemination, exploitation and sustainability activities, policy reporting, and ensuring continuity or interoperability of AENAON platform components, where required under the Sub-Grant Agreement and subject to confidentiality, security, data protection and IPR safeguards

11.3.Use of AENAON Background

Use of AENAON consortium members' background, including platform components, APIs, digital twin models, cyber range tools, cybersecurity service documentation and standards materials, is subject to the terms and conditions set out in the Sub-Grant Agreement or in any separate licence or access arrangement provided by the relevant AENAON partner.

Recipients must not reverse engineer, redistribute, sublicense, publicly disclose or commercially exploit AENAON consortium background except as expressly authorised in writing.

11.4.Open-Source Software and Third-Party Rights

Recipients are responsible for ensuring that all third-party software, data, content, standards, models and other materials used in the sub-project are properly licensed and that their use is compatible with the Sub-Grant Agreement terms, confidentiality obligations and applicable security requirements. Open-source software may be used only where the applicable licence terms are compatible with AENAON's requirements.

11.5.Exploitation Obligation

Recipients must use their best efforts to exploit their sub-project results, directly or through third parties, within four years of the end of the sub-project, in accordance with the applicable provisions of the AENAON Grant Agreement. Where EU strategic autonomy restrictions apply, exploitation must take place within the eligible countries or target countries set out in the call conditions, unless otherwise agreed with the granting authority.

11.6.Publication Review

Prior to any public disclosure of sub-project results, findings, tools or other outputs, recipients must notify AENAON to allow for a security and confidentiality review. Cybersecurity-sensitive information, including vulnerability details, exploit descriptions, operational configurations and non-public platform specifics, may not be publicly disclosed without prior written clearance from AENAON.

AENAON will complete its review within 30 calendar days of receipt, extendable by a further 30 calendar days with written notice. If no response is received within the applicable period, the recipient must submit a written request for a decision to AENAON before proceeding. AENAON will respond within five working days of such a request. Explicit written clearance from AENAON is required in all cases before any publication; silence does not constitute clearance.

12.Governance, Roles and Procedural Principles

The governance of the AENAON Open Calls is structured to ensure equal treatment, transparency, independence and full auditability throughout the Open Call lifecycle.

Body / Role	Main Responsibilities
-------------	-----------------------

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Body / Role	Main Responsibilities
Open Call Coordination Committee (OCCC)	Oversees and approves all Open Call documentation, FAQ updates, evaluator appointments, final ranking, award and reserve list decisions, and redress outcomes. Ensures compliance with equal treatment, transparency and auditability principles throughout the Open Call lifecycle.
Open Call Technical Team (OCTT)	Provides technical input for call topics; supports applicants through publicly available clarifications; supports selected recipients during implementation; reviews technical deliverables, verifies milestone evidence, monitors KPIs, identifies technical risks and supports integration with the AENAON platform. The OCTT does not modify evaluator scores or ranking outcomes. Where technical verification is necessary in relation to implementation feasibility, onboarding readiness or integration with the AENAON ecosystem, the OCTT may provide support to the OCCC. Such support is strictly limited to implementation-related verification and does not affect evaluator independence, the consensus outcome, the final scores or the ranking established by the external evaluators.
Open Call Evaluation Panel (OCEP)	Composed of independent experts. Evaluates eligible proposals against published criteria; prepares Individual Evaluation Reports; participates in consensus meetings; produces Evaluation Summary Reports.
CEF (Open Call Manager)	Circular Economy Foundation acts as WP4 Lead and Open Call Manager. Subject to the relevant consortium authorisation and applicable internal governance decision, CEF may act as FSTP manager and signatory/payment administrator for the Sub-Grant Agreements on behalf of the AENAON consortium, in coordination with the Coordinator and in accordance with the AENAON Grant Agreement, Consortium Agreement and Open Call documentation. CEF is responsible for Open Call management, contracting support, payment administration and FSTP audit-trail maintenance. In its payment administration capacity, CEF acts as the FSTP payment agent (referred to operationally as the 'Treasurer' in internal AENAON governance). Payments are released by CEF only after confirmed acceptance of the relevant milestone deliverable by the OCCC/OCTT.
Coordinator (ASFALYS SRL)	Acts as the overall project coordinator; ensures coherence of Open Call governance with AENAON Grant Agreement obligations; supports reporting to the granting authority.

12.1.Core Principles

The following principles govern all stages of the AENAON Open Call process:

- **Equal treatment:** all applicants receive the same published information and are assessed against the same criteria.
- **Transparency:** eligibility rules, evaluation criteria, scoring scales, thresholds, tie-break rules, payment triggers and redress procedures are published before the submission deadline.
- **Independence and impartiality:** evaluators act independently and sign conflict-of-interest and confidentiality declarations before accessing any proposals.

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

- **Traceability:** all eligibility decisions, scores, rankings, tie-breaks, redress outcomes, award decisions and payments are documented and retained.
- **Proportionality:** requirements on applicants are proportionate to the size and risk profile of the proposed action.
- **Security-by-design:** information handling, disclosure controls and cybersecurity safeguards are embedded throughout the process.
- **Auditability:** all records are retained and made available for checks, reviews, audits, investigations and impact evaluations.

12.2. Conflict of Interest and Confidentiality for Open Call Process Actors

All persons involved in eligibility checks, evaluation, consensus, ranking, redress, contracting and monitoring must sign declarations of confidentiality and absence of conflict of interest before accessing any proposal information.

Any actual, potential or perceived conflict of interest must be declared immediately. A conflicted person must be excluded from all access, scoring, consensus, redress or decision-making for the affected proposal. All recusals must be documented.

Proposals, evaluation records, applicant data, technical information and security-sensitive material must be treated as confidential and used only for the purposes of the AENAON Open Call process and project implementation.

The AENAON Open Calls must be published widely, including on the EU Funding and Tenders Portal and the AENAON project website, in accordance with the applicable specific rules for financial support to third parties.

13. Communication, Dissemination and Visibility

13.1. Acknowledgement of EU Funding

All funded sub-projects must acknowledge EU funding and AENAON support in all approved communication and dissemination materials, presentations, publications, websites and public outputs related to their sub-project. The following standard statement must be included:

"Funded by the European Union under Grant Agreement No. 101249723 (AENAON)."

Where required by AENAON communication guidance, recipients may also refer to the Digital Europe Programme.

The European Union emblem and the logo of the European Cybersecurity Competence Centre (ECCC) must both be displayed prominently in all public communications, publications, presentations, websites and other outputs relating to the funded sub-project. Both logos must remain visually distinct, separate and at least as prominent as other logos when displayed together. Logo files and branding guidelines will be provided by AENAON during onboarding. Recipients must not alter, distort or modify either logo in any way. Failure to comply with this obligation may be treated as a breach of the visibility requirements under the Sub-Grant Agreement and may result in corrective measures in accordance with Section 8.5 of these Guidelines.

13.2. Visibility of AENAON

Recipients must clearly reference AENAON in all sub-project communication outputs and use the AENAON project logo and branding as specified in the communication guidelines provided during onboarding. Recipients should also present the project on their websites and/or social media accounts, including a project summary, the AENAON reference, the European flag and the EU funding statement.

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

13.3.Disclaimer

All public communications related to the funded sub-project must include the following disclaimer:

"Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them."

13.4.Publication of Results and Security Clearance

Public dissemination of sub-project results is encouraged, subject to security and confidentiality review. Prior to any public disclosure, recipients must submit the proposed output to AENAON for review. Cybersecurity-sensitive information must not be publicly disclosed without prior written clearance. AENAON reserves the right to require modifications or embargo periods to protect security-sensitive findings.

Recipients must provide AENAON with the non-confidential summaries, outputs and supporting information reasonably required for AENAON to comply with its reporting, dissemination, visibility and results-platform obligations under the AENAON Grant Agreement. Direct upload by recipients to any EU platform will be required only where expressly stated in the Sub-Grant Agreement or requested by AENAON.

13.5.Participation in AENAON Dissemination Activities

Recipients may be required or invited to participate in AENAON dissemination activities, showcase events, webinars, training demonstrations, case studies and impact reporting activities. Participation in the final AENAON Open Call Assessment event or equivalent closing activity may be specified as a mandatory deliverable in the Sub-Grant Agreement.

13.6.Publication of Call Outcome on Recipient's Own Website

In addition to AENAON's own publication obligations, selected recipients are required to publish the outcome of the relevant AENAON Open Call on their own organisational website within 30 calendar days of the signature of the Sub-Grant Agreement. The published information must include: a description of the funded sub-project and its objectives; the award date; the duration of the supported action; and the legal name and country of the recipient or, where the sub-project is implemented by a small consortium, of each participating legal entity. The published information must remain accessible on the recipient's website for the duration of the implementation period and for at least one year following the final payment under the Sub-Grant Agreement. Recipients must provide AENAON with the URL of the relevant webpage upon publication and must notify AENAON of any subsequent changes to or removal of the published information. This obligation will be formalised in the Sub-Grant Agreement and constitutes a mandatory visibility requirement. It is without prejudice to the confidentiality requirements set out in Section 17 of these Guidelines. Information designated as confidential or falling within the categories of operationally sensitive information listed in Section 17.3 must not be included in the published outcome notice.

13.7. Minimum Communication and Dissemination Requirements

In addition to the acknowledgement, visibility and publication obligations set out above, each funded sub-project must deliver, as a minimum, the following measurable communication and dissemination actions. These form part of the sub-project KPIs (Section 2.6) and are verified at final reporting:

- **Own-website publication:** publish the outcome of the Open Call on the recipient's own website within 30 calendar days of Sub-Grant Agreement signature, and keep it online for at least one year after final payment (Section 12.6);
- **Public summary:** prepare at least one security-cleared public summary of the sub-project results suitable for public dissemination (Section 7.3);
- **Dissemination action:** carry out at least one dissemination action referencing AENAON and EU funding (e.g. a blog post, article, webinar contribution, presentation or case study);

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

- **Online presence:** present the project on the recipient's website and/or social media, including the AENAON reference, the EU emblem and the EU funding statement (Section 12.2);
- **Participation in AENAON events:** participate in at least one AENAON dissemination or showcase activity, and in the final AENAON Open Call Assessment event where specified as a mandatory deliverable in the Sub-Grant Agreement (Section 12.5).

14. Records Management, Audits and Retention

AENAON will maintain an auditable record set covering the complete Open Call lifecycle, including all published documentation, FAQ/clarification records, eligibility check records, evaluator declarations and conflict-of-interest records, individual evaluation reports, ESRs, rankings, tie-break decisions, redress records, award decisions, Sub-Grant Agreements, monitoring records, payment evidence and correspondence.

Recipients must retain all records for five years after the final payment received from AENAON, and until the conclusion of any ongoing audit, review, investigation or legal proceedings, whichever is later.

These access rights do not transfer ownership of recipients' confidential information, trade secrets, personal data or security-sensitive information. Such information will be handled in accordance with the confidentiality, security and data protection safeguards set out in these Guidelines, the Sub-Grant Agreement and the applicable institutional rules of the relevant audit or control body.

15. Responsibilities of Beneficiaries

Selected applicants (sub-grantees/recipients) are expected to comply with the following obligations throughout the lifecycle of their funded sub-project:

15.1. Compliance with Sub-Grant Agreement Conditions

Recipients must comply with all contractual obligations set out in the Sub-Grant Agreement, including financial reporting, technical reporting, milestone achievement, KPI delivery and participation in scheduled AENAON activities such as review meetings and showcase events.

15.2. Timely Reporting

All required reports (project plan, mid-term progress report and final report) must be submitted by the deadlines specified in the Sub-Grant Agreement. Failure to submit reports on time may result in the suspension of payments or, in repeated or serious cases, termination of the Sub-Grant Agreement.

15.3. Gender Equality

Applicants that are public bodies, higher education institutions or research organisations must comply with the Gender Equality Plan (GEP) requirements in line with the applicable Digital Europe Programme and European Commission guidelines. Diversity will be pursued in the composition of project teams and in stakeholder engagement activities.

15.4. Ownership and Control Safeguards

Recipients must respect the EU strategic autonomy requirements applicable to the AENAON project. Entities must ensure that control of sub-project results and sensitive assets remains within EU Member States or eligible associated countries, in accordance with the call conditions and the AENAON Grant Agreement.

In order to verify compliance with these requirements, all applicants — and, in the case of small consortia, each participating legal entity — must complete and submit a signed ownership and control declaration as part of the mandatory proposal package, using the standard template provided in the Open Call documentation. This

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

template has been adapted from the ownership and control assessment (OCA) declaration template available in the Guidance on participation in DEP, Horizon Europe, EDF and CEF-DIG restricted calls. The ownership and control assessment will be conducted by AENAON as part of the eligibility check and, where necessary, will be repeated or updated prior to contracting. Where the assessment raises concerns that cannot be resolved on the basis of the submitted declaration, AENAON reserves the right to request additional supporting documentation or to declare the application ineligible. The outcome of each ownership and control assessment will be documented and retained as part of the Open Call audit trail.

15.5.Cooperation with AENAON

Recipients are expected to cooperate actively with AENAON in monitoring, evaluation, lessons-learned exercises and dissemination activities. This includes providing accurate and timely information for KPI monitoring, contributing to the AENAON Final Open Call Assessment Report and supporting the wider exploitation and market uptake of the project's outcomes.

16. Applicant Integrity and Relationship Disclosure

Applicants must act honestly and transparently throughout the AENAON Open Call process. Applicants must not attempt to influence evaluators, OCCC/OCTT/OCEP members, CEF Open Call management staff, AENAON consortium beneficiaries or any other persons involved in the Open Call process.

Applicants must disclose, at proposal submission (Annex 5) and without undue delay if circumstances change, any personal, financial, commercial, institutional or organisational relationship with AENAON beneficiaries, affiliated entities, evaluators, OCCC/OCTT/OCEP members, CEF Open Call management staff or other persons involved in the Open Call process, where such relationship could reasonably affect, or appear to affect, the impartiality, equal treatment or integrity of the procedure.

Disclosed relationships will be assessed by AENAON on a case-by-case basis. Where possible, AENAON may apply mitigation measures, including exclusion of the conflicted person from access, evaluation, review, monitoring or decision-making concerning the relevant proposal. Where the conflict cannot be effectively managed, the proposal may be declared ineligible, the applicant may be excluded from contracting or implementation, or financial support may be suspended, terminated or recovered in accordance with the Sub-Grant Agreement.

AENAON beneficiaries and their affiliated entities are not eligible to receive financial support under the AENAON Open Calls. Evaluators, OCCC/OCTT/OCEP members and other persons involved in the preparation, management, evaluation, selection, redress, monitoring or decision-making of the Open Calls may not participate as funded applicants where such participation would compromise impartiality, equal treatment or the integrity of the process.

17.Support, Contact and Clarifications

17.1.Applicant Support Resources

AENAON will provide the following support resources to applicants throughout the application process:

- **Official Open Call website:** the Open Call Notice, these Guidelines, mandatory templates, FAQ document, deadline information and all relevant applicant instructions will be published on the official AENAON project website and Open Call portal.
- **Helpdesk:** applicants may submit questions and requests for clarification through the official AENAON helpdesk channel published in the Open Call Notice. Responses of general relevance will be published in the FAQ without disclosing applicant identity or confidential information.

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

- **Information webinars:** AENAON may organise information webinars or online information sessions. Any material information provided during such events will also be made publicly available to ensure equal treatment of all applicants.

17.2. Clarification Requests

Questions from applicants must be submitted through the official helpdesk or portal channel published in the Open Call Notice. Clarifications of general relevance will be published publicly in the FAQ, ensuring equal access to information for all applicants. Questions should be submitted well in advance of the deadline; AENAON cannot guarantee a timely response to requests submitted within 48 hours of the submission deadline.

Any information provided through individual responses that is of general relevance will be incorporated into the publicly available FAQ.

17.3. Contact Information

Contact details for the AENAON Open Call helpdesk, submission portal URL, Open Call Notice publication channels and the official AENAON website will be provided in the relevant Open Call Notice.

18. Protection of Applicant and Participant Confidential Information

AENAON recognises that applicants and selected recipients may include offshore wind farm operators, critical energy infrastructure operators, supply chain actors, grid service providers and other organisations whose operational environments, technical architectures and business information are genuinely sensitive. Participation in the Open Call process requires applicants to share information that may relate to their cybersecurity posture, OT/IT infrastructure, operational vulnerabilities, risk exposure, business relationships and internal processes.

AENAON is committed to ensuring that this information is handled with the highest standards of confidentiality, security and proportionality at every stage of the Open Call process, from proposal submission through to implementation, closure and audit. This section sets out the rules, commitments and mechanisms that apply.

18.1. Why Confidentiality Matters in This Context

Applicants active in the offshore wind sector and related critical energy infrastructure operate in environments where the disclosure of sensitive operational or technical information can create concrete security risks. Unlike other EU funding programmes, the nature of AENAON means that proposals and project outputs may contain:

- descriptions of OT/IT infrastructure, network topology, SCADA/ICS configurations or digital twin parameters;
- details of known or suspected vulnerabilities, threat exposure or past incident experience;
- proprietary cybersecurity tools, methods, detection logic or threat intelligence;
- commercial, contractual or supply-chain information whose disclosure could damage competitive position or trigger third-party liability;
- operational data whose public disclosure could facilitate cyberattacks against offshore wind installations or interconnected energy infrastructure.

AENAON therefore applies a two-track confidentiality framework: one track for the formal requirements flowing from the Grant Agreement and applicable EU law, and one track of additional operational security safeguards specifically designed to address the cyber-risk dimension of critical infrastructure participation.

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

18.2. Legal Basis: Article 13 of the Grant Agreement

The confidentiality obligations applicable to AENAON and its beneficiaries are grounded in Article 13 of the AENAON Grant Agreement. Article 13 requires all parties to keep confidential any data, documents or other material that is identified as sensitive in writing, during the implementation of the action and for at least five years after the final payment (as specified in the Data Sheet). This obligation binds the AENAON consortium, CEF as Open Call manager, ASFALYS as coordinator, all consortium partners involved in the Open Call process, and all external evaluators and experts engaged in assessment activities.

Article 13 further provides that sensitive information may be used only to implement the Agreement, and may be disclosed only to persons who need to know it in order to do so and who are bound by an equivalent obligation of confidentiality. Any disclosure required by EU, international or national law is the only exception to this rule, and even in such cases the disclosing party must take all available measures to limit disclosure to the minimum necessary.

18.3. What Applicants Can Designate as Confidential

Applicants and recipients have the right to designate specific information in their submissions, reports and other project-related materials as confidential. AENAON will respect such designations and will not publish, disclose or otherwise communicate designated confidential information to any party outside the strictly necessary processing chain, except as required by law or the Grant Agreement.

Information eligible for confidential designation includes, but is not limited to:

- descriptions or diagrams of OT/IT infrastructure, network architectures, SCADA/ICS systems or digital twin configurations
- details of vulnerabilities, security weaknesses, threat exposure or past incidents affecting the applicant's or operator's infrastructure
- cybersecurity risk assessments, penetration test results, threat intelligence, detection logic and incident response procedures
- proprietary tools, methods, algorithms, source code and technical know-how
- commercial agreements, pricing, supplier relationships and contractual arrangements
- internal organisational information, staffing arrangements, or operational procedures whose disclosure could facilitate social engineering or targeted attacks
- personal data and any information protected under GDPR or applicable national law
- any other information whose public disclosure could create a security risk for the applicant or for connected critical infrastructure.

18.4. How to Designate Confidential Information

Applicants must actively designate confidential information. AENAON will not apply confidentiality protection automatically to all submitted material. The following rules apply:

- in written documents (proposals, reports, annexes, declarations), confidential sections or passages must be clearly marked with the label [CONFIDENTIAL] at the beginning of the relevant section, paragraph or passage and again at the end;
- in the application form, applicants must complete the confidentiality designation section of Technical Proposal Template (Annex 3), listing the specific elements they designate as confidential and providing a brief justification for each designation
- for information shared orally during review meetings, kick-off sessions or other interactions, the applicant must notify the AENAON contact in writing within five working days that specific information shared during the session is to be treated as confidential

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

- overly broad or blanket confidentiality claims (for example, designating an entire proposal as confidential without specifying the sensitive elements) may be discussed with the applicant to identify the genuinely sensitive parts; AENAON reserves the right to apply graduated protection proportionate to the nature and specificity of the information.

18.5.How AENAON Handles Designated Confidential Information

Once information is designated as confidential by an applicant or recipient, the following commitments and safeguards apply throughout the AENAON Open Call lifecycle:

18.5.1.Access restriction

Access to confidential information is strictly limited to those persons within the AENAON consortium, CEF Open Call management team and evaluation process who genuinely need to access it for the purposes of eligibility checking, evaluation, contracting, monitoring or audit. This includes:

- members of the OCCC and OCTT who are directly involved in the proposal's processing or the recipient's monitoring, bound by written confidentiality declarations
- OCEP evaluators assigned to assess the relevant proposal, bound by a signed confidentiality and conflict-of-interest declaration before accessing any proposal material
- Circular Economy Foundation (CEF) staff involved in contracting and payment administration
- AENAON consortium members with a direct monitoring or technical support role for the specific sub-project.

Confidential information will not be shared with AENAON consortium members, project partners or third parties who do not have a genuine need to know for eligibility checking, evaluation, contracting, monitoring, technical support, audit or legal compliance purposes, unless the applicant has given explicit written consent or disclosure is required by law, the Grant Agreement, the Sub-Grant Agreement or competent audit/control bodies.

18.5.2. Evaluator binding obligations

All OCEP evaluators must sign a confidentiality and non-disclosure declaration before accessing any proposal. This declaration covers all proposal content, including designated confidential information, and extends for the duration of the evaluation process and for five years thereafter. Evaluators who are found to have mishandled confidential information will be immediately excluded from the process and may face contractual and legal consequences.

Where a proposal contains particularly sensitive operational or infrastructure information, AENAON may provide access to that information only to evaluators who have been specifically security-screened and who have signed additional declarations appropriate to the sensitivity level.

18.5.3.Publication controls

AENAON is required to publish the list of selected projects, awarded amounts and the names of selected recipients following each Open Call round. This is a legal obligation under the applicable rules on financial support to third parties and EU transparency requirements. However:

- only the following will be published by default: the legal name and country of the selected recipient or, in the case of small consortia, of each participating legal entity; the funded sub-project title and a brief non-technical description of the sub-project; the award date; the duration of the supported action; and the amount of financial support awarded. This information will be published on the official AENAON project website and on the EU Funding and Tenders Portal following the conclusion of the contracting process for each round
- no operational, technical, infrastructural or commercially sensitive information will be included in any public disclosure without the recipient's prior written consent

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

- sub-project final reports must include a security-cleared public summary prepared by the recipient, covering outcomes and lessons learned in terms suitable for public dissemination; the full technical final report remains confidential unless the recipient explicitly agrees otherwise
- recipients may request that specific findings, results or data be withheld from public dissemination on security, confidentiality, data protection or commercial sensitivity grounds. AENAON will assess such requests in good faith and will not publish cybersecurity-sensitive, operational or confidential information without the required clearance, except where disclosure is required by law, the Grant Agreement or competent authorities.

18.5.4.Cybersecurity-specific safeguards

Given the nature of AENAON, AENAON applies the following additional safeguards beyond the standard confidentiality regime, specifically to address the cyber-risk dimension of critical infrastructure participation:

- vulnerability information, exploit details, SCADA/ICS configurations, penetration test results and incident data will not be disclosed, referenced in public documents or shared with third parties, even in anonymised or aggregated form, without prior security review and, where the information relates to an identifiable applicant, recipient or infrastructure, the explicit written consent of the relevant applicant or recipient, unless disclosure is required by law, the Grant Agreement or competent authorities.
- AENAON will not publish, reference or otherwise disclose information that, even in anonymised form, could allow a third party to identify a specific operator's infrastructure, vulnerability profile or security posture;
- where an applicant or recipient identifies a specific risk that public disclosure of any aspect of their sub-project (even the project title or scope) could facilitate a cyberattack or enable targeting of their infrastructure, they may request that AENAON apply enhanced publication controls; such requests will be assessed on a case-by-case basis and, where justified, AENAON will omit or generalise the relevant information in any public output;
- all project-related digital communications involving confidential or sensitive content must use secure channels as specified in the Sub-Grant Agreement; transmission of sensitive information via unencrypted email is prohibited.

18.5.5. Obligations during monitoring and audit

Where AENAON, CEF, the granting authority (ECCC), the European Commission, OLAF, EPPO, the European Court of Auditors or other competent bodies conduct checks, reviews, audits or investigations, sensitive and confidential information provided or accessed during these processes will be handled in accordance with Article 13 of the Grant Agreement and the applicable confidentiality and data protection rules of the relevant institution or body.

Applicants and recipients have the right, where outside experts are used by the granting authority for reviews or audits, to object to their involvement on grounds of commercial confidentiality or conflict of interest, in accordance with the Grant Agreement. Such objections must be submitted in writing to AENAON without undue delay upon notification of the intended use of outside experts.

18.6.Duration of Confidentiality Obligations

Confidentiality obligations applying to designated sensitive information shared during the AENAON Open Call process and sub-project implementation will remain in force for:

- at least five years after the final payment received by the recipient from AENAON (for information designated by recipients/sub-grantees)
- at least five years after the relevant evaluation process (for information contained in proposals submitted but not selected)
- until the information enters the public domain through means other than a breach of confidentiality obligations

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

- a longer period if specifically requested by the recipient and agreed by AENAON, consistent with the AENAON Grant Agreement.

At the end of the retention period, AENAON will securely destroy or return confidential information that is no longer required for audit or legal purposes, upon written request by the applicant or recipient.

18.7. What Applicants Should Know Before Submitting

Before preparing and submitting a proposal, applicants should note the following practical points:

Question	Answer
Do I have to share all operational details in the proposal?	No. Proposals should describe the proposed action at a level sufficient for evaluation. You do not need to disclose specific vulnerability details, infrastructure configurations or sensitive operational data at the proposal stage. These can be shared, if necessary, at contracting stage or during implementation under appropriate security arrangements.
What if sharing even a high-level description of my infrastructure poses a risk?	You may submit a proposal that describes the general operational context and the type of cybersecurity challenge without identifying specific systems, sites or configurations. AENAON evaluators have the expertise to assess relevance and feasibility from a sufficiently described operational context without requiring identifying details.
Will my proposal be shared beyond the evaluation team?	Proposals are shared only with authorised persons who need access for the Open Call process, including designated OCCC/OCEP members, CEF Open Call management staff and, where necessary, OCTT members or AENAON partners with a direct technical, contracting, monitoring or audit role. All such persons are bound by confidentiality obligations. Proposals are not circulated to the wider AENAON consortium or third parties without a need to know, unless disclosure is required by law, the Grant Agreement or competent audit/control bodies.
Can I request that my organisation's name not be published?	The name of selected recipients, the funded amount and a brief non-confidential description of the funded action may be subject to EU transparency and visibility obligations and may be published in accordance with the Open Call documentation, the Sub-Grant Agreement and applicable EU rules.
What happens if confidential information is accidentally disclosed?	Any accidental or unauthorised disclosure of confidential information must be immediately reported to AENAON by the person or party responsible. AENAON will take all available measures to contain and mitigate the incident, notify the affected applicant or recipient without undue delay, and document the event in the audit record.

Grant Agreement Number: 101249723, Project URL: <https://aenaon-project.eu/>, Funding Authority: European Cybersecurity Competence Centre (ECCC), Call Identifier: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Question	Answer
Are evaluators required to sign NDAs?	Yes. All evaluators sign a confidentiality and non-disclosure declaration covering all proposal content before accessing any submitted material. This obligation extends for five years after the evaluation.

18.8. Reporting Breaches and Escalation

Any actual or suspected breach of confidentiality relating to applicant or recipient information must be reported immediately to the CEF Open Call manager and escalated to the Open Call Coordination Committee (OCCC) in accordance with the Open Call governance and incident-handling procedure. AENAON will:

- acknowledge receipt within one working day
- notify the affected applicant or recipient without undue delay
- conduct an immediate investigation and take containment measures
- document the incident and the measures taken in the Open Call audit record
- where the breach involves personal data, comply with applicable GDPR notification obligations, including notification to the competent supervisory authority within 72 hours if required.

Deliberate or reckless breach of confidentiality obligations by AENAON consortium members, evaluators or open call management staff may result in exclusion from the process, termination of relevant arrangements and further contractual or legal action.

⚠ Applicants and recipients are strongly encouraged to designate genuinely sensitive information as confidential. AENAON will apply the confidentiality framework to information clearly designated as confidential and may also treat information as confidential or operationally sensitive where its nature clearly indicates that disclosure could create security, commercial, data protection or critical infrastructure risks. However, failure to designate information as confidential may limit AENAON's ability to identify and apply enhanced handling safeguards.

! AENAON's confidentiality commitments in this section are grounded in Article 13 of the Grant Agreement (GA No. 101249723) and the applicable EU Financial Regulation rules on financial support to third parties. They do not limit or override the legal access and audit rights of the European Commission, ECCC, OLAF, EPPO, the European Court of Auditors or other competent bodies, which are exercised under their own confidentiality frameworks.