

FUNDING SCHEME

Programme Announcement of the National Cybersecurity Coordination Centre (NCC-CY) of the Republic of Cyprus

PROGRAMME

«Enhancing Cybersecurity for Cypriot Small and Medium Enterprises 2023»

CALL FOR PROPOSALS

NCC-CY-ENTERPRISES/1223



Co-funded by
the European Union



Republic of Cyprus

The Programme is co-financed by the Republic of Cyprus
and the Digital Europe Programme of the European Union

INTRODUCTION

The Research and Innovation Foundation (RIF) in collaboration with the Digital Security Authority (DSA) as the National Cybersecurity Coordination Centre (NCC-CY), announce the Call for Proposals for the Programme "Enhancing Cybersecurity for Small and Medium Enterprises in the Republic of Cyprus 2023" and invites beneficiaries to submit relevant Project Proposals (Proposals).

The present Call is announced as part of a series of actions of the NCC-CY. With the introduction of European Regulation (EU) 2021/887 by the European Parliament and the Council on May 20, 2021, the European Competence Centre (ECCC) for Industrial, Technological, and Research Issues in Cybersecurity was established, consisting of the National Coordination Centres (NCCs) in each EU member state, with the goal of developing technological and industrial capabilities for cybersecurity issues in the European Union.

By a decision of the Council of Ministers on December 21, 2021, DSA, as an entity of the broader Public Sector, was appointed as the NCC-CY for cybersecurity matters in the Republic of Cyprus. At the same time, the Research and Innovation Foundation (RIF) was appointed as a member of the NCC-CY consortium, with responsibilities for managing funds secured by NCC-CY through European Programmes, with the aim of providing financial support to small and medium-sized enterprises (SMEs) within the Republic of Cyprus.

The "N4CY-Development of the National Cybersecurity Coordination Center of the Republic of Cyprus" (Grant Agreement 101101331) project is co-financed by the Republic of Cyprus and the "Digital Europe" Programme of the European Union.



GENERAL CALL INFORMATION

Programme	ENHANCING CYBERSECURITY IN SMALL AND MEDIUM ENTERPRISES IN THE REPUBLIC OF CYPRUS 2023
Call Code	NCC-CY-ENTERPRISES/1223
Call Budget	1.000.000 Euro
Minimum funding per proposal	20.000 Euro
Maximum Funding per proposal	60.000 Euro
Intensity of Funding	60%
Date of Publication	08 December 2023
Closing Date	31 January 2024, 13:00

Objectives

The Programme aims to ensure that SMEs reach a basic level of cybersecurity in order to protect their infrastructures, systems and information. This will be achieved through the purchase of solutions and services to maintain and strengthen the level of security and resilience of small and medium enterprises (SMEs), as well as through the evaluation and identification of challenges and weaknesses. Additionally, the Programme seeks to achieve their compliance of SMES with European and internationally accepted measures and standards through a certification scheme, the Cyber-Hygiene Framework for Small and Medium Enterprises (SME) of the NCC-CY.

Description

Through the Programme, SMEs¹ will have the opportunity to obtain a Cybersecurity Certification. The Certification is issued by Certification Bodies, which have been accredited

¹ *The category of each enterprise will be checked by the RIF as part of the legal status check during the proposal submission stage and validated at the time of contract preparation and before the final decision for funding.*
Small Enterprises: An enterprise which employs fewer than fifty (50) employees and has an annual turnover or



according to ISO 17021 and ISO 27006, hence are competent to carry out inspections and certifications for information security management systems according to ISO/IEC 27001:2013 and/or ISO/IEC 27001:2022.

Following acquisition of the Certification, enterprises will be able to assess their current level of maturity, identify vulnerabilities and mitigate risk, while strengthening their cybersecurity practices. It will also allow them to invest in the protection of information and data, based on specific specifications and minimum requirements set out in the NCC-CY Cyber-Hygiene Framework for SMEs.

The Programme has a simple procedure for submitting proposals, short time for the evaluation and announcement of results and ensures timely implementation of projects in the pre-defined maximum implementation period for resolving problems faced by enterprises in cybersecurity matters.

For the purposes of participating in the Programme and submitting a Proposal, a gap analysis is required. The gap analysis will determine an SMEs' current cybersecurity situation in real time, at a technical, operational and strategic level in relation to the set of rules, control measures and procedures set out for establishing a basic level of cybersecurity as defined in the NCC-CY Cyber-Hygiene for SMEs framework and which are summarized as follows:

1. Security Policy

Control Measure 1.1: The organisation's senior management has created, approved and communicated its cybersecurity policy internally and externally. The cybersecurity policy shall be reviewed at least once a year and updated as required.

2. Awareness and Training

Control Measure 2.1: Staff employed by the organisation and users who have access to its information (regardless of their employment relationship) must be aware of information security and in particular how they contribute to it through their role. Appropriate cybersecurity awareness activities shall be carried out on a regular basis and at least once a year.

an annual balance sheet total not exceeding ten (10) million Euros. Start-ups are also included in this category.

Medium Enterprise: An enterprise which employs fifty (50) to up to two hundred forty-nine (249) employees and has an annual turnover of up to fifty (50) million Euro or an annual balance sheet total not exceeding forty-three (43) million Euro.

4



Co-funded by
the European Union



Republic of Cyprus

The Programme is co-financed by the Republic of Cyprus
and the Digital Europe Programme of the European Union

Control Measure 2.2: Staff employed by the organisation and users who have access to its information (regardless of their employment relationship) receive education, training and information on the policies, procedures, security measures implemented by the organisation as well as relevant technological or organisational issues. The training provided shall be tailored to the security requirements of the different roles within the organisation.

3. *Software Update*

Control Measure 3.1: The organisation's IT and communications systems must have the latest, stable security updates installed from trusted sources only (e.g. the manufacturer).

Control Measure 3.2: Automated vulnerability scanning and penetration tests are implemented once a year.

Control Measure 3.3: Information and communication systems that are no longer supported by their manufacturers with (at least) end-of-life security updates shall not be used by the organisation.

4. *Protection from Malicious Software*

Control Measure 4.1: Malicious software protection programmes and functions are installed on all of the organisation's IT and communication systems and are updated on a regular basis.

5. *Network Security*

Control Measure 5.1: The organisation has installed and configured firewalls at appropriate points in its network, in order to effectively protect its systems and information from relevant threats.

Control Measure 5.2: If the organisation provides the capability for wireless access to the organisation's network, this should be done with appropriate routing and protection through the installed firewall(s).

6. *Backups*

Control Measure 6.1: The organisation identifies its critical information and backs it up on a regular basis in alignment with the relevant backup policy.

7. *Access Control*

Control Measure 7.1: The organisation identifies where important information is located. For each information type and based on its use and criticality, the organisation has created a structure in an appropriate storage area, which allows it to grant access rights to authorised and authenticated users following the need-to-know principle.

Control Measure 7.2: The organisation has created an appropriate password policy, which is implemented in all its systems.

Control Measure 7.3: Administrative rights or privileged rights (admin/privileged rights) are granted to a minimum necessary number of authorised staff.



8. Security Incidents

Control Measure 8.1: The organisation has established structures and process for responding to security incidents. The staff involved in the respective procedures are appropriately trained.

9. Physical Security Measures

Control Measure 9.1: The organisation has adopted physical security measures to protect systems and facilities from natural and environmental threats.

10. Data Protection

Control Measure 10.1: The organisation designs, implements, approves and publishes a Personal Data Protection Policy based on the general [GDPR regulation](#).

11. Operational Impact Analysis

Control Measure 11.1: The organization has designed and implemented an appropriate methodology for operational impact analysis. The results and key figures resulting from the application of the methodology are recorded, maintained and utilized accordingly to design relevant measures and implementations.

Depending on the analysis of the current situation of the company in relation to the above analysis, interested enterprises will prepare their proposal, which will include the list of solutions and services they intend to use in order to gain the “Cyber-Hygiene Framework for SME of NCC-CY” certification.

BENEFICIARIES

Small and Medium Enterprises (Categories B.1, B.2)

SPECIFIC RESTRICTIONS AND CONDITIONS FOR PARTICIPATION

The Host Organisation (HO) of the Project must be a small or a medium-sized enterprise.

Each organization can only receive funding as a Host Organization once.

Participation of entities engaged in an economic activity in a proposal shall be deemed valid, if they are legally established and are active in territories under the control of the Republic of Cyprus. The activity of the entities is documented by the existence of facilities and staff in territories under the control of the Republic of Cyprus and, indicatively and not restrictively, by audited financial statements, the tax return of the entity in the Republic of Cyprus, etc.

6



Co-funded by
the European Union



Republic of Cyprus

The Programme is co-financed by the Republic of Cyprus
and the Digital Europe Programme of the European Union

These conditions should be met to the satisfaction of RIF and without prejudice to the Foundation to request further data and information from the entities.

Upon completion of the projects, each SME will be required to undertake at least one publicity activity (media/social media publication, video, event, etc.) highlighting the achievement of the Certification following the implementation of the funded project, with references to the benefit derived from the funding. For publicity actions, the obligations for promotion and publicity for projects funded by the Digital Europe Programme should be applied, including the logos of the NCC-CY, the Research and Innovation Foundation (RIF), the Commissioner of Communications and the Digital Security Authority, as well as reference to the co-funding by the Republic of Cyprus.

PROJECT ACTIVITIES

The projects include activities related to the process of obtaining the NCC-CY's Cyber-Hygiene Certification for SMEs, aiming at the adoption of solutions and the purchase of services to achieve a basic level of cybersecurity and preparedness to protect infrastructures, systems and data of enterprises.

Specifically, eligible costs must be in line with the measures to be taken to enable certification by the Certification Bodies accredited to ISO 17021 and ISO 27006 to conduct information security management system audits and certifications in accordance with ISO/IEC 27001:2013 or ISO/IEC 27001:2022, as defined in the Annex of this Call for Proposals.

DURATION OF PROJECT IMPLEMENTATION

Six (6) months

Extensions to the project implementation period cannot be granted in the frame of this Call for Proposals.

Upon completion of the projects, a "Final Activity Report" and "Funding Payment Request" must be submitted within one (1) month for the purposes of securing the final instalment, subject to securing the Certification of the NCC-CY Cyber-Hygiene Framework for SMEs.

BUDGET

€ 1.000.000

7



Co-funded by
the European Union



Republic of Cyprus

The Programme is co-financed by the Republic of Cyprus
and the Digital Europe Programme of the European Union

MINIMUM - MAXIMUM FUNDING PER PROJECT

€20.000 – €60.000

The aid intensity is 60% of eligible costs.

If, upon completion of the projects, the total eligible expenses based on approved costs (total amount of eligible expenses taking into account the aid intensity – 60%) are less than the minimum project funding, the funding will not be granted to the beneficiary.

ELIGIBLE EXPENSES

All expenditures necessary for the purposes of securing the Cybersecurity Certification, in accordance with the requirements of the NCC-CY through the Cyber-Hygiene Framework for SMEs, which will fall under the categories "Costs for external services" and/or "Costs for Instruments and Equipment".

Eligible costs may include the purchase and implementation of the following:

- Design and implementation services related to Group Policies and other security features of domain controllers and other related equipment.
- Services obtained from consultants for training and educating staff on cybersecurity
- Installation of two-factor authentication.
- Cybersecurity incident management systems, consulting and incident response services and products
- Privileged Access Management
- Sandbox technology solutions
- Email filtering solutions
- Security information and incident management services (SOC)
- Implementation of physical security and access control measures
- Development of a Business Continuity Plan
- Web Application Firewall Solutions (WAF)
- Tools / services for electronic fraud (phishing)
- Firewall with or without integrated threat management
- Software solutions and backup equipment (Storage, Tapes, Licensed Software)
- Intrusion detection/prevention systems (IDS and IPS)
- Antivirus software

8



**Co-funded by
the European Union**



Republic of Cyprus

**The Programme is co-financed by the Republic of Cyprus
and the Digital Europe Programme of the European Union**



- Systems to detect and respond to network attacks
- Penetration Testing
- Planning and implementation services of policies and procedures
- Consulting Services related to the Business Impact Analysis
- Design and implementation services of a data privacy policy
- Network equipment that enables/improves/supports cybersecurity (eg firewall, switch, concentrators, load balancers, access points)
- Protection Services DoS/DDoS
- Servers used for security related purposes (proxy servers, web application servers etc)
- Equipment to achieve increased durability (hard drives, etc.)
- Hardware/software SIEM
- Consulting services for purposes of analysis and conclusions on the current situation of businesses in cybersecurity matters.
- Cost of NCC-CY Cybersecurity Certification audit (the cost of a single audit may be covered)
- Any other service, software/hardware or tools deemed necessary by the Host Organisation in order to meet the requirements of the Certification Scheme, provided that these are deemed reasonable during the evaluation process.

Beneficiaries must receive and evaluate at least three (3) independent tenders for each purchase exceeding Euro 15,000 (excluding VAT) resulting in the selection of the most economical solution that meets their needs.

VAT is not considered an eligible cost. Beneficiaries are responsible for VAT payments to all consultants and solution providers and certification bodies.

The total amount of funding is committed at the time of Project Contract preparation and the funding is made as a lump sum payment as de minimis aid (EU Regulation No 1407/2013 of 18 December 2013) in two instalments.

The first instalment of 40% is paid upon signing of the Project Contract and the second instalment is paid upon approval of the "Activity Report" and the "Funding Payment Request" which are submitted within one (1) month from the completion of the works by the Host Organization.

Failure to secure the Certification within the duration of the funded project will result in the funding not being granted and a refund of the pre-financing will be requested.

9



Co-funded by
the European Union



Republic of Cyprus

The Programme is co-financed by the Republic of Cyprus
and the Digital Europe Programme of the European Union

It is clarified that, according to the EU Regulation No. 1407/2013 on de minimis funding, enterprises active in the fisheries and aquaculture sectors and in the primary production of agricultural products cannot be funded.

SPECIFIC CONDITIONS

All private sector entities (Host Organisation) are required to register the updated data regarding its ultimate beneficial owners in the Competent National Registry / Archive, as per «The prevention and suppression of money laundering and terrorist financing Law of 2007 (188(I)/2007)». The RIF maintains the right to proceed with the appropriate checks in the competent Registries to verify the registration of the data and it is possible to request for the submission of official proof.

Funded Projects should comply with the «Do No Significant Harm» principle, according to which they must not include or support activities that could cause significant harm to any of the six environmental objectives, as per Article 17 of Regulation (EU) No 2020/852, on the establishment of a framework to facilitate sustainable investment.

SUBMISSION

Proposals are submitted through the Research and Innovation Foundation's IRIS Portal (<https://iris.research.org.cy/#/>).

It is noted that, the Project Coordinator and all local participating organizations of the Cypriot Consortium, should register in advance on the IRIS Portal.

Potential applicants are advised to read the general «**Guide for Applicants**» and «**IRIS Portal User Manual**» which can be found on the IRIS Portal (<https://iris.research.org.cy/#/documentlibrary>).

The Research and Innovation Foundation encourages in all its Calls for Proposals:

- *the participation of women as Project Coordinators, and*
- *a gender-balanced participation in Projects.*





STRUCTURE OF PROPOSALS

The Project Proposal consists of the following parts:

1. Part A – General Information & Budget (electronic form (fields) to be completed online through the IRIS Portal).
2. Part B – Technical Annex (document to be uploaded as an Annex on the IRIS Portal in PDF format) – **Mandatory Submission**
Note: *The template provided for this Call must be submitted **without any alterations**. The Part B template for this Call can be found on the IRIS Portal, under the relevant Call for Proposals (Call Documents).*
3. Annex II - Call Specific Information (files which are posted as Annexes on the IRIS Portal in pdf format) - **Mandatory Submission:**
(a) Gap Analysis
4. Annex III - Call Specific Information (files which are posted as Annexes on the IRIS Portal in pdf format) - **Mandatory Submission:**
(a) Written Declaration (Form K.E.2) issued under Regulation 3(2) of the State Aid (Control of State Aid (De Minimis Aid) Regulations 2009 and 2012, completed and signed,
(b) Single Undertaking Declaration
(c) Declaration of the Host Organization

PROJECT SELECTION

Evaluation Procedure

For the evaluation of the Proposals in this Call, a process of Preliminary Check and Evaluation by an Independent Evaluation Committee (IEC) will be followed. The committee will include experts with a background in business and specialization in cybersecurity issues. Proposals that meet all the criteria will be forwarded for evaluation by the members of the IEC. During the IEC session, the members rank the Proposals in order of priority (ranking list) and document the rationale for their decision in a relevant Evaluation Report. Upon completion of the process, the Evaluation Report from the IEC regarding each proposal will be communicated to the Project Coordinator.

It should be noted that the work of the IEC will be supported by RIF staff.





The final decision regarding the selection of a proposal for funding by the RIF, is at the discretion of the Committee. The Committee's decision is final and cannot be appealed against.

Evaluation Criteria

1. *Relevance – Weight 30%*

- Alignment of the Proposal and the expected project results with the objectives and activities described in this Call
- Degree of cybersecurity upgrading/development in the company in relation to the current state/operation of the company (holistic approach based on gap analysis and obtaining the Cybersecurity certification).

2. *Added Value and Benefit – Weight 40%*

- Degree to which the proposed project can ensure the expected results and deliverables stated in this Call.
- Effectiveness of the proposed actions in terms of visibility to demonstrate the benefits of the funding.
- Degree of enhancement of the competitiveness of the enterprise and effectiveness of the funding in terms of increasing the level of cyber security of the enterprise itself and thereby providing increased security to its customers and recipients of its services.
- Degree of positive impact on the overall operations of the business as a result of the increased level of cybersecurity (resilience, increased efficiency, reduced costs, exploitation of new capabilities/opportunities).

3. *Implementation – Weight 30%*

- Maturity of the proposed project and adequacy of the needs analysis based on the existing infrastructure in the Host Organization.
- Completeness and appropriateness of the action plan, timeline and budget for securing the products and services based on the gap analysis and certification.
- Completeness, quality and capacity of the Host Organization to carry out the project and implement the proposed objectives and action plan.
- Plan to ensure that the increased level of cybersecurity resulting from the funding is preserved over time.



Selection

Proposals deemed as eligible following proposal evaluation will be selected for funding according to their ranking. It is clarified that the total requested funding of selected projects will not exceed the total Call budget.

The Host Organizations whose Proposals will be selected for funding will become beneficiaries by the 30th of May 2024.

FUNDING PAYMENT

Within one (1) month of the completion of the projects, the Host Organization will submit an "Activity Report" and the 'Funding Payment Request' form to the RIF, available on the IRIS Portal.

In addition, monitoring visits may be carried out by RIF for on-site verifications whenever deemed necessary.

The method of payment of the RIF funding shall be as follows:

- Pre-financing: pre-financing corresponds to 40% of the Requested Funding and will be paid upon Contract signature.
- Final Payment: the Final Payment, may correspond to up to the balance of the Requested Funding, taking into consideration the eligible costs of the project and the Final Aid Intensity.

It is noted that the Final Instalment will be paid on the condition that the Host Organization has secured certification from Certification Bodies accredited under ISO 17021 and ISO 27006 to carry out audits and certification of information security management systems in accordance with ISO/IEC 27001: 2013 or ISO/IEC 27001:2022, certifying that the company is able to protect its infrastructure, systems and information against specific specifications and minimum requirements defined in the Cybersecurity Certification Scheme for SMEs.

The invoices for the provision of services and products/solutions and the cost of the certification body must be attached to the "Funding Payment Request".



If the cost of the eligible expenses, based on the supporting documents, is less than the amount of the total requested funding for the proposal, then the final, actual cost will be provided.

In addition, if the Host Organization has not secured certification and/or the total eligible expenses based on approved costs (total amount of eligible expenses taking into account the aid intensity – 60%) are less than the minimum project funding, the funding will not be granted to the beneficiary and the entire funding given will be returned to RIF.

RESTART 2016-2020 WORK PROGRAMME

In the context of this Call, all general rules and procedures for the participation of organizations and persons, the eligible activities and costs as well as the required details are applicable, as included in the RESTART 2016-2020 Work Programme - Period 05/2022 - 12/2023 which is a key reference document and an important information tool for stakeholders and is available on the IRIS portal. (<https://iris.research.org.cy/#/documentlibrary>).

INFORMATION – CONTACT DETAILS

RIF Support Service

E-mail

support@research.org.cy

Telephone

+35722205000

The Research and Innovation Foundation may at its discretion, proceed to the extension or revocation of the present Call by applying the same publication procedure.

