Κυπριακό Εμπορικό & Βιομηχανικό Επιμελητήριο

ΕΓΚΥΚΛΙΟΣ

Λευκωσία, 14 Δεκεμβρίου 2023

Προς: Όλους τους ενδιαφερόμενους

Θέμα: ΕΝΙΣΧΥΣΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΤΙΣ ΚΥΠΡΙΑΚΕΣ ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ 2023

Αγαπητοί,

Θα θέλαμε να σας ενημερώσουμε ότι η Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ) ως το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας (NCC-CY) σε συνεργασία με το Ίδρυμα Έρευνας και Καινοτομίας (ΙδΕΚ), ανακοινώνουν την Πρόσκληση για Υποβολή Προτάσεων του Προγράμματος:

«Ενίσχυση Κυβερνοασφάλειας στις Κυπριακές Μικρομεσαίες Επιχειρήσεις 2023» και καλεί τους δικαιούχους να υποβάλουν σχετικές Προτάσεις Έργων.

Η Πρόσκληση συγχρηματοδοτείται από την Κυπριακή Δημοκρατία και το Πρόγραμμα «Ψηφιακή Ευρώπη» της Ευρωπαϊκής Ένωσης, στο πλαίσιο υλοποίησης του Ευρωπαϊκού Έργου **«N4CY-Development of the National Cybersecurity Coordination Centre of the Republic of Cyprus»** (Grant Agreement 101101331).

Η υποβολή προτάσεων γίνεται μέσω της πύλης IRIS του ΙδΕΚ και η καταληκτική ημερομηνία είναι η 31/01/24

Προϋπολογισμός Πρόσκλησης:	1.000.000 Ευρώ
Ελάχιστη Χρηματοδότηση ανά Έργο:	20.000 Ευρώ
Μέγιστη Χρηματοδότηση ανά Έργο:	60.000 Ευρώ
Ένταση Ενίσχυσης:	60%

Επισυνάπτεται σχετική πληροφόρηση για περαιτέρω ενέργειες.

Με εκτίμηση,

Χρίστος Πετσίδης
Διευθυντής
Τμήματος Εμπορίου, Υπηρεσιών και Ψηφιοποίησης

Λεωφ. Γρίβα Διγενή 38 & Δεληγιώργη 3, 1066, Τ.Θ 21455, 1509 Λευκωσία, Κύπρος
T: +357 22889890 **F:** +357 22667593 **E:** petsides@ccci.org.cy **W:** www.ccci.org.cy

Cyprus Chamber of Commerce & Industry

CIRCULAR

Nicosia, December 14, 2023

To: All interested parties

Re: ENHANCING CYBERSECURITY IN CYPRIOT SMALL AND MEDIUM-SIZED ENTERPRISES 2023

Dear all,

We would like to inform you that the Digital Security Authority (DSA) as the National Cybersecurity Coordination Center (NCC-CY) in collaboration with the Foundation for Research and Innovation Foundation (FRI) announced a Call for Proposals for the Program:

"Enhancement of Cybersecurity in Cypriot Small and Medium-sized Enterprises (SMEs) 2023" invites beneficiaries to submit relevant Project Proposals.

The Call is co-funded by the Republic of Cyprus and the "Digital Europe" Program of the European Union, in the framework of the implementation of the European Project "N4CY-Development of the National Cybersecurity Coordination Centre of the Republic of Cyprus" (Grant Agreement 101101331).).

Proposals are submitted through the IRIS portal of the FRI and the deadline is January 31, 2024.

Call Budget:	1.000.000 Euros
Minimum Funding per Project:	20.000 Euros
Maximum Funding per Project:	60.000 Euros
Aid intensity:	60%

Relevant information is attached for further action.

Yours faithfully,

Christos Petsides
Director
Department of Trade, Services and Digitization

38 Grivas Dhigenis Avenue & 3 Deligiorgis Street 1066, PO BOX 21455, 1509 Nicosia, Cyprus
T: +357 22889890 **F:** +357 22667593 **E** petsides@ccci.org.cy **W:** www.ccci.org.cy

ΣΧΕΔΙΟ ΧΟΡΗΓΙΩΝ

Προκήρυξη Προγράμματος Εθνικού Κέντρου Συντονισμού Κυβερνοασφάλειας (NCC-CY) στην Κυπριακή Δημοκρατία

ΠΡΟΓΡΑΜΜΑ

«Ενίσχυση Κυβερνοασφάλειας στις Κυπριακές Μικρομεσαίες Επιχειρήσεις 2023»

ΠΡΟΣΚΛΗΣΗ ΥΠΟΒΟΛΗΣ ΠΡΟΤΑΣΕΩΝ

NCC-CY-ENTERPRISES/1223

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Κυπριακή Δημοκρατία

Το Πρόγραμμα συγχρηματοδοτείται από την Κυπριακή Δημοκρατία και το Πρόγραμμα «Ψηφιακή Ευρώπη» της Ευρωπαϊκής Ένωσης

ΕΙΣΑΓΩΓΗ

Το Ίδρυμα Έρευνας και Καινοτομίας **(ΙδΕΚ)** σε συνεργασία με την Αρχή Ψηφιακής Ασφάλειας (**ΑΨΑ**) ως το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας (NCC-CY), ανακοινώνουν την Πρόσκληση για Υποβολή Προτάσεων του Προγράμματος «Ενίσχυση Κυβερνοασφάλειας στις Κυπριακές Μικρομεσαίες Επιχειρήσεις 2023» και καλεί τους δικαιούχους να υποβάλουν σχετικές Προτάσεις Έργων (Προτάσεις).

Η παρούσα Πρόσκληση ανακοινώνεται στο πλαίσιο σειράς δράσεων του Εθνικού Κέντρου Συντονισμού (National Coordination Centre–NCC-CY) Κυβερνοασφάλειας στην Κύπρο. Με τη θέσπιση του Ευρωπαϊκού Κανονισμού (ΕΕ) 2021/887 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ης Μάϊου 2021, ιδρύεται το Ευρωπαϊκό Κέντρο Αρμοδιότητας (ECCC) για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας και το Δίκτυο, το οποίο αποτελείται από τα Εθνικά Κέντρα Συντονισμού (NCCs) σε κάθε κράτος μέλος της ΕΕ, με απώτερο σκοπό την ανάπτυξη τεχνολογικών και βιομηχανικών ικανοτήτων για θέματα της κυβερνοασφάλειας στην Ευρωπαϊκή Ένωση. Με απόφαση του Υπουργικού Συμβουλίου την 21η Δεκεμβρίου 2021, η Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ) ως οντότητα του ευρύτερου Δημόσιου Τομέα, ορίστηκε ως το Εθνικό Κέντρο Συντονισμού (NCC-CY) για θέματα Κυβερνοασφάλειας στην Κυπριακή Δημοκρατία. Παράλληλα, ορίστηκε το Ίδρυμα Έρευνας και Καινοτομίας (ΙδΕΚ) ως μέλος της κοινοπραξίας του NCC-CY με καθήκοντα οικονομικού διαχειριστή των χρηματοδοτήσεων που θα εξασφαλίζει το NCC-CY μέσω των Ευρωπαϊκών προγραμμάτων, με σκοπό την οικονομική ενίσχυση των μικρομεσαίων επιχειρήσεων (ΜμΕ) εντός της Κυπριακής Δημοκρατίας.

Η Πρόσκληση συγχρηματοδοτείται από την Κυπριακή Δημοκρατία και το Πρόγραμμα «Ψηφιακή Ευρώπη» της Ευρωπαϊκής Ένωσης, στο πλαίσιο υλοποίησης του Ευρωπαϊκού Έργου «N4CY-Development of the National Cybersecurity Coordination Centre of the Republic of Cyprus» (Grant Agreement 101101331).

ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ ΠΡΟΣΚΛΗΣΗΣ ΥΠΟΒΟΛΗΣ ΠΡΟΤΑΣΕΩΝ

Πρόγραμμα	**ΕΝΙΣΧΥΣΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΤΙΣ ΚΥΠΡΙΑΚΕΣ ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ 2023**
Κωδικός Πρόσκλησης	**NCC-CY-ENTERPRISES/1223**
Προϋπολογισμός Πρόσκλησης	**1.000.000 Ευρώ**
Ελάχιστη Χρηματοδότηση ανά Έργο	**20.000 Ευρώ**
Μέγιστη Χρηματοδότηση ανά Έργο	**60.000 Ευρώ**
Ένταση Ενίσχυσης	**60%**
Ημερομηνία Δημοσίευσης	**08 Δεκεμβρίου 2023**
Καταληκτική Ημερομηνία	**31 Ιανουαρίου 2023, 13:00**

ΣΤΟΧΟΙ

Το Πρόγραμμα στοχεύει στην εξασφάλιση ενός βασικού επιπέδου κυβερνοασφάλειας με σκοπό την προστασία υποδομών, συστημάτων και πληροφοριών μέσα από την αγορά λύσεων και υπηρεσιών για τη διατήρηση και την ενίσχυση του επιπέδου ασφάλειας και της ανθεκτικότητας των μικρομεσαίων επιχειρήσεων (ΜμΕ), καθώς, επίσης και την αξιολόγηση και αντιμετώπιση προκλήσεων και αδυναμιών που εντοπίζονται. Επιπρόσθετα, το Πρόγραμμα επιδιώκει την πιστοποίηση των μικρομεσαίων επιχειρήσεων όσον αφορά στη συμμόρφωσή τους με ευρωπαϊκά και διεθνώς αποδεκτά μέτρα κυβερνοασφάλειας, τα οποία έχουν καθοριστεί μέσω του Πλαισίου Κυβερνο-Υγιεινής για Μικρομεσαίες Επιχειρήσεις (ΜμΕ) του Εθνικού Κέντρου Συντονισμού Κυβερνοασφάλειας (NCC-CY).

ΠΕΡΙΓΡΑΦΗ

Μέσα από το Πρόγραμμα δίνεται η ευκαιρία σε μικρές και μεσαίες επιχειρήσεις [1] να αποκτήσουν Πιστοποίηση σε θέματα Κυβερνοασφάλειας. Η Πιστοποίηση εκδίδεται από

[1] *Η κατηγοριοποίηση των επιχειρήσεων θα ελέγχεται από το ΙδΕΚ στο πλαίσιο νομοτυπικού ελέγχου κατά το στάδιο υποβολής της πρότασης και θα επανελέγχεται κατά τη στιγμή της ετοιμασίας του συμβολαίου και πριν την τελική απόφαση για χρηματοδότηση.*
Μικρή Επιχείρηση: Νοείται η επιχείρηση που έχει λιγότερους από πενήντα (50) εργαζόμενους και ετήσιο κύκλο εργασιών ή σύνολο ετήσιου ισολογισμού που να μην ξεπερνά τα δέκα (10) εκατ. Ευρώ. Στην κατηγορία αυτή εντάσσονται και οι Νεοσύστατες Επιχειρήσεις.
Μεσαία Επιχείρηση: Νοείται η επιχείρηση που έχει από πενήντα (50) έως και διακόσιους σαράντα εννέα (249) εργαζόμενους και ετήσιο κύκλο εργασιών έως και πενήντα (50) εκατ. Ευρώ ή συνολικό ετήσιο ισολογισμό έως και σαράντα τρία (43) εκατ. Ευρώ.

Φορείς Πιστοποίησης, οι οποίοι έχουν διαπιστευτεί σύμφωνα με τα πρότυπα ISO 17021 και ISO 27006 για τη διενέργεια επιθεωρήσεων και πιστοποιήσεων συστημάτων διαχείρισης ασφάλειας πληροφοριών σύμφωνα με το ISO/IEC 27001:2013 ή ISO/IEC 27001:2022. Με την πιστοποίηση η επιχείρηση θα είναι σε θέση να αξιολογήσει το τρέχον επίπεδο ωριμότητας, να προσδιορίσει τα τρωτά σημεία και να μετριάσει τον κίνδυνο, ενισχύοντας παράλληλα τις πρακτικές κυβερνοασφάλειας που εφαρμόζει, ώστε να επενδύσει σωστά στην προστασία των πληροφορίων και των δεδομένων τους, με βάση συγκεκριμένες προδιαγραφές και ελάχιστες απαιτήσεις που έχουν οριστεί στο Πλαίσιο Κυβερνο-Υγιεινής για ΜμΕ του NCC-CY.

Το Πρόγραμμα χαρακτηρίζεται από απλή διαδικασία υποβολής προτάσεων, σύντομο χρόνο στην εξέταση και ανακοίνωση των αποτελεσμάτων, ταχύτητα στην υλοποίηση των έργων με προκαθορισμένο μέγιστο χρόνο υλοποίησης για την επίλυση προβλημάτων που αντιμετωπίζουν οι επιχειρήσεις σε θέματα κυβερνοασφάλειας.

Για σκοπούς συμμετοχής στο Πρόγραμμα και υποβολής Πρότασης, οι επιχειρήσεις θα πρέπει να προχωρούν με ανάλυση χάσματος (gap analysis) και εξαγωγή συμπερασμάτων για την παρούσα κατάσταση κυβερνοασφάλειας τους σε πραγματικό χρόνο, σε τεχνικό, επιχειρησιακό και στρατηγικό επίπεδο σε σχέση με το σύνολο κανόνων, σημείων ελέγχου και διαδικασιών για ένα βασικό επίπεδο ασφάλειας στον κυβερνοχώρο, όπως ορίζονται στο πλαίσιο Κυβερνο-Υγιεινής για ΜμΕ του NCC-CY και τα οποία συνοψίζονται ως εξής:

1. *Πολιτική Ασφάλειας*

Σημείο Ελέγχου 1.1: Η ανώτατη διοίκηση του οργανισμού έχει δημιουργήσει, εγκρίνει και επικοινωνήσει εσωτερικά και εξωτερικά την πολιτική κυβερνοασφάλειας του. Η πολιτική κυβερνοασφάλειας ανασκοπείται κατ' ελάχιστον μια φορά το χρόνο και επικαιροποιείται όπως απαιτείται.

2. *Ενημέρωση και Εκπαίδευση*

Σημείο Ελέγχου 2.1: Το προσωπικό που απασχολείται στον οργανισμό, οι εξωτερικοί συνεργάτες και οι χρήστες που έχουν πρόσβαση στις πληροφορίες του (ανεξάρτητα από τη σχέση εργασίας), πρέπει να είναι ενήμεροι και να έχουν επίγνωση σχετικά με την ασφάλεια πληροφοριών και ειδικότερα με τον τρόπο με τον οποίο συνεισφέρουν μέσα από τον ρόλο τους. Κατάλληλες δράσεις ευαισθητοποίησης για την κυβερνοασφάλεια διενεργούνται σε τακτική βάση και τουλάχιστον μια φορά ανά έτος

Σημείο Ελέγχου 2.2: Το προσωπικό που απασχολείται από τον οργανισμό, οι εξωτερικοί συνεργάτες και οι χρήστες που έχουν πρόσβαση στις πληροφορίες του (ανεξάρτητα από την σχέση εργασίας), λαμβάνουν εκπαίδευση, κατάρτιση και ενημέρωση σχετικά με τις πολιτικές,

τις διαδικασίες, τα μέτρα ασφάλειας που εφαρμόζει ο οργανισμός καθώς και σχετικά τεχνολογικά ή οργανωτικά ζητήματα. Οι παρεχόμενες εκπαιδευτικές δράσεις είναι κατάλληλες και προσαρμοσμένες στις απαιτήσεις ασφαλείας των διαφόρων ρόλων εντός του οργανισμού.

3. *Ενημέρωση Λογισμικού*

Σημείο Ελέγχου 3.1: Τα συστήματα πληροφορικής και επικοινωνιών του οργανισμού πρέπει να έχουν εγκατεστημένες τις τελευταίες, σταθερές ενημερώσεις ασφαλείας από αξιόπιστες πηγές μόνο (π.χ. κατασκευαστή).

Σημείο Ελέγχου 3.2: Αυτοματοποιημένες ανιχνεύσεις ευπαθειών και δοκιμές παρείσδυσης υλοποιούνται μια φορά ανά έτος (vulnerability scanning and penetration tests).

Σημείο Ελέγχου 3.3: Συστήματα πληροφορικής και επικοινωνιών που δεν υποστηρίζονται πλέον από τους κατασκευαστές τους με ενημερώσεις (κατ' ελάχιστον) ασφαλείας (end of life), δεν πρέπει να χρησιμοποιούνται από τον οργανισμό.

4. *Προστασία από Κακόβουλο Λογισμικό*

Σημείο Ελέγχου 4.1: Προγράμματα και λειτουργίες προστασίας έναντι κακόβουλου λογισμικού είναι εγκατεστημένα στο σύνολο των συστημάτων πληροφορικής και επικοινωνιών του οργανισμού. Ενημερώσεις γίνονται σε τακτική βάση.

5. *Ασφάλεια Δικτύου*

Σημείο Ελέγχου 5.1: Ο οργανισμός έχει εγκαταστήσει και παραμετροποιήσει firewall σε κατάλληλα σημεία του δικτύου του, με σκοπό την αποτελεσματική προστασία των συστημάτων και των πληροφοριών του από τις σχετικές απειλές.

Σημείο Ελέγχου 5.2: Σε περίπτωση που ο οργανισμός παρέχει τη δυνατότητα ασύρματης πρόσβασης στο δίκτυο του οργανισμού, αυτό θα πρέπει να γίνεται με κατάλληλη δρομολόγηση και προστασία μέσω του (των) εγκατεστημένων firewall.

6. *Αντίγραφα Ασφαλείας (Backups)*

Σημείο Ελέγχου 6.1: Ο οργανισμός αναγνωρίζει την κρίσιμη πληροφορία του και λαμβάνει αντίγραφα ασφαλείας της σε τακτά χρονικά διαστήματα σύμφωνα με τη σχετική πολιτική αντιγράφων ασφαλείας.

7. *Έλεγχος Πρόσβασης*

Σημείο Ελέγχου 7.1: Ο οργανισμός αναγνωρίζει τα σημεία στα οποία βρίσκεται σημαντική πληροφορία για αυτόν. Για την πληροφορία και με βάση το είδος, τη χρήση και την κρισιμότητά της, ο οργανισμός έχει δημιουργήσει μια δομή σε κατάλληλο αποθηκευτικό

χώρο, η οποία του επιτρέπει να παρέχει δικαιώματα πρόσβασης σε εξουσιοδοτημένους και αυθεντικοποιημένους χρήστες ακολουθώντας την αρχή Need-to-know (ανάγκη γνώσης).
Σημείο Ελέγχου 7.2: Ο οργανισμός έχει δημιουργήσει, εφαρμόσει σε όλα τα συστήματά του και τηρεί κατάλληλη πολιτική κωδικών πρόσβασης.
Σημείο Ελέγχου 7.3: Διαχειριστικά δικαιώματα ή προνομιακά δικαιώματα (admin./privileged rights) δίνονται στο ελάχιστο απαραίτητο εξουσιοδοτημένο προσωπικό.

8. Περιστατικά Ασφάλειας

Σημείο Ελέγχου 8.1: Ο οργανισμός έχει δημιουργήσει μια δομή και διαδικασία ανταπόκρισης σε περιστατικά ασφαλείας. Το προσωπικό που θα συμμετέχει στις αντίστοιχες διαδικασίες είναι κατάλληλα εκπαιδευμένο.

9. Μέτρα Φυσικής Ασφάλειας

Σημείο Ελέγχου 9.1: Ο οργανισμός έχει υιοθετήσει μέτρα φυσικής ασφάλειας για την προστασία των συστημάτων και των εγκαταστάσεων από φυσικές και περιβαλλοντικές απειλές.

10. Προστασία Δεδομένων

Σημείο Ελέγχου 10.1: Ο οργανισμός σχεδιάζει, υλοποιεί, εγκρίνει και δημοσιοποιεί Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα με βάση το γενικό κανονισμό ΓΚΠΔ.

11. Ανάλυση Επιχειρησιακών Επιπτώσεων

Σημείο Ελέγχου 11.1: Ο οργανισμός έχει σχεδιάσει και υλοποιήσει κατάλληλη μεθοδολογία για την ανάλυση επιχειρησιακών επιπτώσεων. Τα αποτελέσματα και τα βασικά μεγέθη που προκύπτουν από την εφαρμογή της μεθοδολογίας καταγράφονται, διατηρούνται και τροφοδοτούν τον σχεδιασμό σχετικών μέτρων και υλοποιήσεων.

Αναλόγως της ανάλυσης της παρούσας κατάστασης της επιχείρησης τους σε σχέση με τα πιο πάνω, οι ενδιαφερόμενες επιχειρήσεις θα ετοιμάζουν την πρόταση τους η οποία θα περιλαμβάνει τη λίστα λύσεων και υπηρεσιών που προτίθενται να εξασφαλίσουν για σκοπούς εξασφάλισης της πιστοποίησης μέσω του Πλαισίου-Κυβερνο-Υγιεινής για ΜμΕ του NCC-CY.

ΔΙΚΑΙΟΥΧΟΙ

Μικρές και Μεσαίες Επιχειρήσεις (Κατηγορίες Β.1, Β.2)

ΕΙΔΙΚΟΙ ΠΕΡΙΟΡΙΣΜΟΙ ΚΑΙ ΠΡΟΫΠΟΘΕΣΕΙΣ ΣΥΜΜΕΤΟΧΗΣ

Ανάδοχος Φορέας ενός έργου μπορεί να είναι μικρή ή μεσαία επιχείρηση.

Κάθε Φορέας μπορεί να λάβει χρηματοδότηση ως Ανάδοχος Φορέας μόνο σε ένα Έργο.
Η συμμετοχή φορέων καθώς και φυσικών προσώπων τα οποία ασκούν τακτικά οικονομική δραστηριότητα σε πρόταση θεωρείται έγκυρη εφόσον είναι νόμιμα εγκαταστημένοι και δραστηριοποιούνται σε περιοχές που ελέγχει η Κυπριακή Δημοκρατία. Η δραστηριοποίηση των φορέων τεκμηριώνεται με την ύπαρξη εγκαταστάσεων και προσωπικού στις περιοχές που ελέγχει η Κυπριακή Δημοκρατία και ενδεικτικά και όχι περιοριστικά, από ελεγμένες οικονομικές καταστάσεις, τη φορολογική δήλωση του φορέα στην Κυπριακή Δημοκρατία, κοκ.

Οι εν λόγω προϋποθέσεις θα πρέπει να συντρέχουν προς ικανοποίηση του ΙδΕΚ και με την επιφύλαξη του Ιδρύματος να ζητήσει περαιτέρω στοιχεία και πληροφορίες από τους φορείς.

Κατά την ολοκλήρωση των Έργων, κάθε ΜμΕ θα πρέπει να προβεί υποχρεωτικά σε τουλάχιστον μία δράση δημοσιότητας (δημοσίευση στα ΜΜΕ/μέσα κοινωνικής δικτύωσης, βίντεο, εκδήλωση κλπ) στην οποία θα αναδεικνύεται η εξασφάλιση της Πιστοποίησης σε συνέχεια υλοποίησης του χρηματοδοτούμενου έργου, με αναφορές στο όφελος που προέκυψε από την χρηματοδότηση. Για τις δράσεις δημοσιότητας, θα πρέπει να εφαρμόζονται οι κανόνες προβολής και δημοσιότητας για τα προγράμματα που χρηματοδοτούνται από το Πρόγραμμα Digital Europe, με συμπερίληψη των λογότυπων του NCC-CY, του ΙδΕΚ, του Επιτρόπου Επικοινωνιών και της Αρχής Ψηφιακής Ασφάλειας καθώς και αναφορά στη συγχρηματοδότηση από την Κυπριακή Δημοκρατία.

ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ ΕΡΓΩΝ

Τα έργα αφορούν δραστηριότητες που σχετίζονται με τη διαδικασία εξασφάλισης πιστοποίησης στο πλαίσιο Κυβερνο-Υγιεινής για ΜμΕ του Εθνικού Κέντρου Συντονισμού NCC-CY, για την εφαρμογή λύσεων και την αγορά υπηρεσιών για την επίτευξη ενός βασικού επιπέδου κυβερνοασφάλειας και ετοιμότητας για την προστασία υποδομών, συστημάτων και πληροφοριών στις επιχειρήσεις.

Συγκεκριμένα, οι επιλέξιμες δαπάνες θα πρέπει να συνάδουν με τα μέτρα που θα πρέπει να ληφθούν, προκειμένου να καταστεί δυνατή η εξασφάλιση της πιστοποίησης από Φορείς Πιστοποίησης, οι οποίοι έχουν διαπιστευτεί σύμφωνα με το ISO 17021 και ISO 27006 για την διενέργεια επιθεωρήσεων και πιστοποιήσεων συστημάτων διαχείρισης ασφάλειας

πληροφοριών σύμφωνα με το ISO/IEC 27001:2013 ή ISO/IEC 27001:2022, όπως αυτά ορίζονται στο Συνημμένο Έγγραφο της παρούσας Πρόσκλησης.

ΔΙΑΡΚΕΙΑ ΥΛΟΠΟΙΗΣΗΣ ΕΡΓΩΝ

Έξι (6) μήνες

Στο πλαίσιο της παρούσας Πρόσκλησης, δεν είναι δυνατή η παροχή τυχόν παρατάσεων στην υλοποίηση έργων.

Κατά την ολοκλήρωση των έργων, εντός ενός (1) μήνα υποβάλλεται «Έκθεση Πεπραγμένων» και «Αίτηση Καταβολής Χορηγίας» για σκοπούς εξασφάλισης της τελικής δόσης, με προϋπόθεση την εξασφάλιση Πιστοποίησης στο Πλαίσιο Κυβερνο-Υγιεινής για Μικρομεσαίες Επιχειρήσεις του NCC-CY.

ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ

€ 1.000.000

ΕΛΑΧΙΣΤΗ - ΜΕΓΙΣΤΗ ΧΡΗΜΑΤΟΔΟΤΗΣΗ ΑΝΑ ΕΡΓΟ

€20.000 – €60.000

Η Ένταση Ενίσχυσης ανέρχεται σε 60% επί των επιλέξιμων δαπανών.

Σε περίπτωση που κατά την ολοκλήρωση των έργων, η τελική χρηματοδότηση βάση πιστοποιημένων δαπανών (συνολικό ποσό επιλέξιμων δαπανών μετά την εφαρμογή της έντασης ενίσχυσης ύψους 60%) είναι μικρότερη της ελάχιστης χρηματοδότησης ανά έργο, δεν θα είναι δυνατή η καταβολή της χορηγίας.

ΕΠΙΛΕΞΙΜΕΣ ΔΑΠΑΝΕΣ

Δαπάνες που είναι απαραίτητες για την εξασφάλιση της Πιστοποίησης Κυβερνοασφάλειας, σύμφωνα με τις απαιτήσεις του NCC-CY μέσω του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ, που θα εμπίπτουν στις κατηγορίες «Δαπάνες για Αγορά Υπηρεσιών» και/ή «Δαπάνες για Όργανα και Εξοπλισμό».

Οι επιλέξιμες δαπάνες μπορούν να περιλαμβάνουν αγορά και υλοποίηση των πιο κάτω:

- Υπηρεσίες σχεδιασμού και υλοποίησης που σχετίζονται με Πολιτικές Ομίλου και άλλα χαρακτηριστικά ασφαλείας ελεγκτών τομέα και άλλου σχετικού εξοπλισμού.
- Υπηρεσίες για εκπαίδευση και διαφώτιση προσωπικού για τα θέματα κυβερνοασφάλειας από συμβούλους.
- Εγκατάσταση ελέγχου ταυτότητας δύο παραγόντων (*two-factor authentication*).
- Συστήματα διαχείρισης περιστατικών κυβερνοασφάλειας, συμβουλευτικές υπηρεσίες και υπηρεσίες και προϊόντα απόκρισης σε περιστατικά.
- Συστήματα προνομιακής διαχείρισης πρόσβασης (Privileged Access Management).
- Λύσεις τεχνολογίας Sandbox.
- Λύσεις φιλτραρίσματος ηλεκτρονικού ταχυδρομείου (Email filtering)
- Υπηρεσίες διαχείρισης πληροφοριών ασφαλείας και συμβάντων (SOC).
- Εφαρμογή μέτρων φυσικής ασφάλειας και ελέγχου πρόσβασης.
- Ανάπτυξη Σχεδίου Επιχειρησιακής Συνέχειας.
- Λύσεις Web Application Firewall (WAF).
- Εργαλεία / υπηρεσίες για ηλεκτρονικές απάτες (phishing).
- Firewall με ή χωρίς ενοποιημένη διαχείριση απειλών.
- Λύσεις λογισμικού και εξοπλισμός για αντίγραφα ασφαλείας (Storage, Tapes, Licensed Software).
- Συστήματα ανίχνευσης/πρόληψης εισβολών (IDS και IPS).
- Λογισμικό προστασίας από ιούς.
- Συστήματα ανίχνευσης και απόκρισης επιθέσεων δικτύου.
- Δοκιμές διείσδυσης (Penetration Testing).
- Υπηρεσίες σχεδιασμού και εφαρμογής πολιτικών και διαδικασιών κυβερνοασφάλειας.
- Συμβουλευτικές Υπηρεσίες που σχετίζονται με Ανάλυση Επιχειρηματικού Αντικτύπου.
- Υπηρεσίες σχεδιασμού και εφαρμογής πολιτικής απορρήτου δεδομένων
- Εξοπλισμός δικτύου που ενεργοποιεί / βελτιώνει / υποστηρίζει την ασφάλεια στον κυβερνοχώρο (π.χ. firewall, switch, concentrators, load balancers, access points)
- Υπηρεσίες προστασίας DoS / DDoS
- Servers που χρησιμοποιούνται για σκοπό που σχετίζεται με την ασφάλεια (proxy servers, web application servers etc)
- Εξοπλισμός για την επίτευξη αυξημένης ανθεκτικότητας (σκληροί δίσκοι, κτλ.)
- Εξοπλισμός / λογισμικό SIEM
- Συμβουλευτικές υπηρεσίες για σκοπούς ανάλυσης και εξαγωγής συμπερασμάτων για την υφιστάμενη κατάσταση επιχειρήσεων σε θέματα κυβερνοασφάλειας.
- Κόστος ελέγχου Πιστοποίησης Κυβερνοασφάλειας ΑΨΑ (μπορεί να καλυφθεί το κόστος ενός ελέγχου)

- Οποιαδήποτε άλλη υπηρεσία, software/hardware ή εργαλεία που κρίνονται απαραίτητα από τον Ανάδοχο Φορέα για την επίτευξη των απαιτήσεων του Σχήματος Πιστοποίησης, νοουμένου ότι αυτά κριθούν ως εύλογα κατά τη διαδικασία αξιολόγησης.

Οι επιχειρήσεις θα πρέπει να λαμβάνουν και να αξιολογούν τουλάχιστον τρεις (3) ανεξάρτητες προσφορές για κάθε αγορά που ξεπερνά τις 15.000 Ευρώ (μη συμπεριλαμβανομένου του ΦΠΑ) με αποτέλεσμα την επιλογή της πιο οικονομικής λύσης που ικανοποιεί τις ανάγκες τους.

Ο ΦΠΑ δεν θεωρείται επιλέξιμη δαπάνη. Οι δικαιούχοι αναλαμβάνουν την ευθύνη εξόφλησης του ΦΠΑ σε όλες τις εταιρείες παροχής συμβουλευτικών υπηρεσιών και λύσεων και στους φορείς πιστοποίησης.

Το συνολικό ποσό χρηματοδότησης δεσμεύεται κατά την ετοιμασία του Συμβολαίου Έργου και η χρηματοδότηση γίνεται με την καταβολή εφάπαξ ποσού, ως Ενίσχυση Ήσσονος Σημασίας (Κανονισμός ΕΕ, Αρ. 1407/2013 της 18ης Δεκεμβρίου 2013) σε δύο δόσεις.

Η πρώτη δόση, ύψους 40% καταβάλλεται κατά την υπογραφή του Συμβολαίου Έργου και η δεύτερη δόση καταβάλλεται με την έγκριση της «Έκθεσης Πεπραγμένων» και της «Αίτησης Καταβολής Χορηγίας» οι οποίες υποβάλλονται εντός ενός (1) μήνα από την ολοκλήρωση των έργων από τον Ανάδοχο Φορέα.

Σε περίπτωση μη εξασφάλισης της Πιστοποίησης εντός της διάρκειας του χρηματοδοτούμενου έργου, δεν θα είναι δυνατή η καταβολή της χορηγίας και θα ζητείται η επιστροφή της προκαταβολής.

Διευκρινίζεται ότι, σύμφωνα με τον κανονισμό της ΕΕ Αρ. 1407/2013 για τις χρηματοδοτήσεις Ήσσονος Σημασίας, δεν μπορούν να χρηματοδοτηθούν επιχειρήσεις που δραστηριοποιούνται στους τομείς της αλιείας και της υδατοκαλλιέργειας και στην πρωτογενή παραγωγή γεωργικών προϊόντων.

ΕΙΔΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

- Όλοι οι φορείς Ιδιωτικού Δικαίου (Ανάδοχος Φορέας) έχουν υποχρέωση καταχώρησης των επικαιροποιημένων στοιχείων των πραγματικών τους δικαιούχων στα αρμόδια Εθνικά Μητρώα, βάσει του «Περί της Παρεμπόδισης και Καταπολέμησης της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες Νόμου του 2007 (188(Ι)/2007)». Το ΙδΕΚ διατηρεί το δικαίωμα να διενεργήσει ελέγχους στα αρμόδια

Μητρώα για επιβεβαίωση της καταχώρησης των στοιχείων και ενδέχεται να ζητήσει την υποβολή επίσημου αποδεικτικού της καταχώρησης.

- Τα χρηματοδοτούμενα έργα θα πρέπει να συμμορφώνονται με την αρχή της «μη πρόκλησης σημαντικής βλάβης», σύμφωνα με την οποία δεν πρέπει να περιλαμβάνουν δραστηριότητες που προκαλούν σημαντική επιβάρυνση σε οποιοδήποτε από τους έξι περιβαλλοντικούς στόχους, κατά την έννοια του Άρθρου 17 του Κανονισμού της ΕΕ 2020/852, σχετικά με τη θέσπιση πλαισίου για τη διευκόλυνση των βιώσιμων επενδύσεων.

ΥΠΟΒΟΛΗ

Η Υποβολή Προτάσεων γίνεται μέσω της **Πύλης Ηλεκτρονικών Υπηρεσιών IRIS** (https://iris.research.org.cy/#!/) του Ιδρύματος Έρευνας και Καινοτομίας (ΙδΕΚ).

Σημειώνεται ότι, ο/η Συντονιστής/τρια Έργου και ο Ανάδοχος Φορέας, θα πρέπει να εγγραφούν εκ των προτέρων στην Πύλη IRIS.

Οι ενδιαφερόμενοι/νες καλούνται να αξιοποιήσουν τον γενικό «Οδηγό Ετοιμασίας Προτάσεων» και το «**Εγχειρίδιο Χρήσης της Πύλης IRIS**» που είναι αναρτημένα στην Πύλη IRIS (**https://iris.research.org.cy/#/documentlibrary**).

Το Ίδρυμα Έρευνας και Καινοτομίας ενθαρρύνει σε όλες του τις Προσκλήσεις Υποβολής Προτάσεων:

- *τη συμμετοχή των γυναικών ως Συντονίστριες Έργου, και*
- *την ισόρροπη συμμετοχή γυναικών και ανδρών στα Έργα.*

ΔΟΜΗ ΠΡΟΤΑΣΕΩΝ

Η πρόταση αποτελείται από τα ακόλουθα μέρη:

1. Part A – General Information & Budget (ηλεκτρονικό έντυπο (πεδία) το οποίο συμπληρώνεται διαδικτυακά στην Πύλη IRIS).
2. Part B – Technical Annex (αρχείο το οποίο αναρτάται ως Παράρτημα στην Πύλη IRIS σε μορφή pdf) – ***Υποχρεωτική Υποβολή***
   Σημειώνεται ότι θα πρέπει να υποβάλλεται το προβλεπόμενο για την εν λόγω Πρόσκληση έντυπο, χωρίς οποιαδήποτε διαφοροποίηση. Το πρότυπο για το εν λόγω έγγραφο βρίσκεται αναρτημένο στην Πύλη IRIS, κάτω από την ανακοίνωση της σχετικής Πρόσκλησης Υποβολής Προτάσεων (Call Documents).

3. Annex II – Call Specific Information (αρχεία το οποία αναρτώνται ως Παράρτημα στην Πύλη IRIS σε μορφή pdf) - ***Υποχρεωτική Υποβολή***:
   (α) Ανάλυση Χάσματος (Gap Analysis)
4. Annex III – Call Specific Information (αρχεία το οποία αναρτώνται ως Παράρτημα στην Πύλη IRIS σε μορφή pdf) - ***Υποχρεωτική Υποβολή***:
   (α) Γραπτή Δήλωση (Έντυπο Κ.Ε.2) η οποία εκδίδεται δυνάμει του Κανονισμού 3(2) των Περί Ελέγχου των Κρατικών Ενισχύσεων (Ενισχύσεις Ήσσονος Σημασίας) Κανονισμών του 2009 και 2012, συμπληρωμένη και υπογεγραμμένη,
   (β) Δήλωση Ενιαίας Επιχείρησης
   (γ) Υπεύθυνη Δήλωση του Ανάδοχου Φορέα

ΕΠΙΛΟΓΗ ΕΡΓΩΝ

Διαδικασία Αξιολόγησης

Για την αξιολόγηση των Προτάσεων της παρούσας Πρόσκλησης θα ακολουθηθεί διαδικασία Προκαταρκτικού Ελέγχου και Αξιολόγησης από Ανεξάρτητη Επιτροπή Αξιολόγησης (ΑΕΑ). Στην επιτροπή θα συμμετέχουν εμπειρογνώμονες με επιχειρηματικό υπόβαθρο και εξειδίκευση στα θέματα κυβερνοασφάλειας. Οι προτάσεις που ικανοποιούν όλα τα προαπαιτούμενα κριτήρια προωθούνται για αξιολόγηση από τα μέλη της ΑΕΑ. Κατά τη συνεδρία της ΑΕΑ, τα μέλη της κατατάσσουν τις Προτάσεις προς χρηματοδότηση κατά σειρά προτεραιότητας (ranking list) και τεκμηριώνουν το σκεπτικό της απόφασής τους σε σχετική Έκθεση Αξιολόγησης. Με την ολοκλήρωση της διαδικασίας θα κοινοποιείται στον Συντονιστή Έργου η σχετική Έκθεση Αξιολόγησης της ΑΕΑ για την πρότασή τους.

Σημειώνεται ότι, στις εργασίες της ΑΕΑ συμμετέχουν με ρόλο υποστηρικτικό στελέχη του ΙδΕΚ.

Η τελική απόφαση για τη χρηματοδότηση μίας πρότασης από το ΙδΕΚ είναι στην κρίση της Επιτροπής, είναι τελεσίδικη και δεν υπάρχει δυνατότητα υποβολής ένστασης.

Κριτήρια Αξιολόγησης

1. Συνάφεια – Βαρύτητα – 30%

- Ευθυγράμμιση της Πρότασης και των αναμενόμενων αποτελεσμάτων έργου με τους στόχους και δραστηριότητες που περιγράφονται στην παρούσα Πρόσκληση
- Βαθμός αναβάθμισης/ανάπτυξης της κυβερνοασφάλειας στην επιχείρηση σε σχέση με την υφιστάμενη κατάσταση/λειτουργία της επιχείρησης (ολιστική προσέγγιση με βάση την ανάλυση χάσματος (gap analysis) και την απόκτηση της πιστοποίησης Κυβερνοασφάλειας).

2. Προστιθέμενη Αξία και Όφελος – Βαρύτητα – 40%

- Βαθμός στον οποίο το προτεινόμενο έργο δύναται να εξασφαλίσει τα αναμενόμενα αποτελέσματα και παραδοτέα που αναφέρονται στην παρούσα Πρόσκληση
- Αποτελεσματικότητα των προτεινόμενων δράσεων για προβολή για ανάδειξη του οφέλους της χρηματοδότησης.
- Βαθμός ενίσχυσης της ανταγωνιστικότητας της επιχείρησης και αποτελεσματικότητα της χρηματοδότησης ως προς την αύξηση του επιπέδου κυβερνοασφάλειας της ίδιας της επιχείρησης και κατ' επέκταση της παροχής αυξημένης ασφάλειας στους πελάτες της και αποδέκτες των υπηρεσιών της.
- Βαθμός επίτευξης θετικού αντικτύπου στις συνολικές εργασίες της επιχείρησης, ως αποτέλεσμα του αυξημένου επιπέδου κυβερνοασφάλειας (ανθεκτικότητα επιχείρησης, αυξημένη αποδοτικότητα, μείωση εξόδων, εκμετάλλευση νέων ικανοτήτων/ευκαιριών).

3. Υλοποίηση – Βαρύτητα – 30%

- Ωριμότητα του προτεινόμενου έργου και επάρκεια της ανάλυσης των αναγκών με βάση την υφιστάμενη κατάσταση υποδομών στον Ανάδοχο Φορέα.
- Πληρότητα και καταλληλότητα του πλάνου δράσης, χρονοδιαγράμματος και προϋπολογισμού για εξασφάλιση των προϊόντων και υπηρεσιών με βάση την ανάλυση χάσματος και της πιστοποίησης.
- Πληρότητα, ποιότητα και ικανότητα του Ανάδοχου Φορέα για τη διεκπεραίωση του έργου και την υλοποίηση των προτεινόμενων στόχων και πλάνου δράσης.
- Πλάνο διασφάλισης του αυξημένου επιπέδου κυβερνοασφάλειας ως αποτέλεσμα της χρηματοδότησης για διατήρηση των αποτελεσμάτων σε βάθος χρόνου.

Επιλογή

Επιλέγονται για χρηματοδότηση οι Προτάσεις που έχουν κριθεί, κατόπιν αξιολόγησης, επιλέξιμες για χρηματοδότηση. Νοείται ότι το σύνολο των εγκεκριμένων χρηματοδοτήσεων των έργων, δεν θα ξεπερνά το σύνολο του προϋπολογισμού της Πρόσκλησης.

Οι Ανάδοχοι Φορείς των οποίων οι Προτάσεις θα λάβουν χρηματοδότηση, θα καταστούν δικαιούχοι μέχρι τις 30 Μαΐου 2024.

ΚΑΤΑΒΟΛΗ ΧΟΡΗΓΙΑΣ

Εντός ενός (1) μήνα από την ολοκλήρωση των έργων, ο Ανάδοχος Φορέας υποβάλλει στο ΙδΕΚ «Έκθεση Πεπραγμένων» καθώς και το ειδικό έντυπο «Αίτηση Καταβολής Χορηγίας», το οποίο βρίσκεται διαθέσιμο στο Ηλεκτρονικό Σύστημα.

Επιπλέον, δύναται να διενεργούνται επισκέψεις ελέγχου από το ΙδΕΚ για επιτόπιες επαληθεύσεις όποτε κρίνεται απαραίτητο.

Ο τρόπος καταβολής της χρηματοδότησης του ΙδΕΚ καθορίζεται ως ακολούθως:
- Προκαταβολή Χρηματοδότησης, που ανέρχεται σε 40% της Αιτούμενης Χρηματοδότησης καταβάλλεται με την υπογραφή του Συμβολαίου.
- Τελική Δόση Χρηματοδότησης, που μπορεί να ανέλθει μέχρι το υπόλοιπο της Αιτούμενης Χρηματοδότησης, λαμβάνοντας υπόψη τις επιλέξιμες δαπάνες του έργου και την Τελική Ένταση Ενίσχυσης.

Σημειώνεται ότι η τελική δόση καταβάλλεται νοουμένου ότι ο Ανάδοχος Φορέας έχει εξασφαλίσει πιστοποίηση από Φορείς Πιστοποίησης, οι οποίοι έχουν διαπιστευτεί σύμφωνα με το ISO 17021 και ISO 27006 για τη διενέργεια επιθεωρήσεων και πιστοποιήσεων συστημάτων διαχείρισης ασφάλειας πληροφοριών σύμφωνα με το ISO/IEC 27001:2013 ή ISO/IEC 27001:2022, πιστοποιώντας ότι η επιχείρηση είναι σε θέση να προστατεύσει τις υποδομές, συστήματα και πληροφορίες της με βάση συγκεκριμένες προδιαγραφές και ελάχιστες απαιτήσεις που έχουν οριστεί στο Σχήμα Πιστοποίησης Κυβερνοασφάλειας για ΜμΕ.

Στην «Αίτηση Καταβολής Χορηγίας» επισυνάπτονται τα τιμολόγια για την εξασφάλιση υπηρεσιών και προϊόντων/λύσεων και το κόστος του φορέα πιστοποίησης.

Στην περίπτωση που το κόστος των επιλέξιμων δαπανών, βάσει των αποδεικτικών στοιχείων, είναι μικρότερο από το ποσό έγκρισης της καταρχήν επιλέξιμης πρότασης τότε κατά την καταβολή της χορηγίας θα λαμβάνεται υπόψη το τελικό, πραγματικό κόστος.

Επιπρόσθετα, σε περίπτωση που ο Ανάδοχος Φορέας δεν έχει εξασφαλίσει την πιστοποίηση και/ή το κόστος των δαπανών είναι μικρότερο από την ελάχιστη χρηματοδότηση (€20.000) τότε το σύνολο του ποσού που δόθηκε επιστρέφεται στο Ίδρυμα.

ΠΡΟΚΗΡΥΞΗ ΤΩΝ ΠΡΟΓΡΑΜΜΑΤΩΝ RESTART 2016-2020

Στο πλαίσιο της παρούσας Πρόσκλησης, ισχύουν όλοι οι γενικοί κανονισμοί και διαδικασίες συμμετοχής φορέων και προσώπων, οι επιλέξιμες δραστηριότητες και δαπάνες καθώς και οι απαιτούμενες λεπτομέρειες οι οποίες περιλαμβάνονται στην Προκήρυξη των Προγραμμάτων RESTART 2016-2020 - Προγράμματα Περιόδου 05/2022 – 12/2023 που αποτελεί βασικό έγγραφο αναφοράς και σημαντικό εργαλείο πληροφόρησης των ενδιαφερομένων φορέων και είναι αναρτημένη στην Πύλη Ηλεκτρονικών Υπηρεσιών IRIS του ΙδΕΚ (https://iris.research.org.cy/#/documentlibrary).

ΠΛΗΡΟΦΟΡΙΕΣ - ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ

Υπηρεσία Υποστήριξης του ΙδΕΚ

Ηλεκτρονικό Ταχυδρομείο
support@research.org.cy

Τηλέφωνο
+35722205000

Το Ίδρυμα Έρευνας και Καινοτομίας δύναται κατά την κρίση του να προβεί σε παράταση ή ανάκληση της ισχύος της παρούσας Πρόσκλησης εφαρμόζοντας τον ίδιο τρόπο δημοσίευσής της.

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.

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

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, SMEs [1] 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

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

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 acquirement 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.

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.

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

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.

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

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

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.

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.*

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

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.

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

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.

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

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".

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

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.

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