

## 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

## 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 20<sup>ης</sup> Μαΐου 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 21<sup>η</sup> 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).



Με τη συγχρηματοδότηση  
της Ευρωπαϊκής Ένωσης



Κυπριακή Δημοκρατία

## 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<sup>1</sup> να αποκτήσουν Πιστοποίηση σε θέματα Κυβερνοασφάλειας. Η Πιστοποίηση εκδίδεται από

<sup>1</sup> 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.



Με τη συγχρηματοδότηση  
της Ευρωπαϊκής Ένωσης



Κυπριακή Δημοκρατία

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 πληροφοριών 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,



Με τη συγχρηματοδότηση  
της Ευρωπαϊκής Ένωσης



Κυπριακή Δημοκρατία

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 κακόβουλο 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 B.1, B.2)



Με τη συγχρηματοδότηση  
της Ευρωπαϊκής Ένωσης



Κυπριακή Δημοκρατία



## 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



Με τη συγχρηματοδότηση  
της Ευρωπαϊκής Ένωσης



Κυπριακή Δημοκρατία

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:



Με τη συγχρηματοδότηση  
της Ευρωπαϊκής Ένωσης



Κυπριακή Δημοκρατία





- 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(I)/2007)». Το ΙΔΕΚ διατηρεί το δικαίωμα να διενεργήσει ελέγχους στα αρμόδια



Με τη συγχρηματοδότηση  
της Ευρωπαϊκής Ένωσης



Κυπριακή Δημοκρατία

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).



Με τη συγχρηματοδότηση  
της Ευρωπαϊκής Ένωσης



Κυπριακή Δημοκρατία

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).



Με τη συγχρηματοδότηση  
της Ευρωπαϊκής Ένωσης



Κυπριακή Δημοκρατία

## 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.



Με τη συγχρηματοδότηση  
της Ευρωπαϊκής Ένωσης



Κυπριακή Δημοκρατία

## 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.



Με τη συγχρηματοδότηση  
της Ευρωπαϊκής Ένωσης



Κυπριακή Δημοκρατία



## 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](mailto: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.*



Με τη συγχρηματοδότηση  
της Ευρωπαϊκής Ένωσης



Κυπριακή Δημοκρατία