



Υπουργείο Ψηφιακής
Διακυβέρνησης



ΕΘΝΙΚΟ
ΠΡΟΓΡΑΜΜΑ
ΑΝΑΠΤΥΞΗΣ
2021-2025



ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

ΕΘΝΙΚΟ ΔΙΚΤΥΟ ΥΠΟΔΟΜΩΝ ΤΕΧΝΟΛΟΓΙΑΣ & ΕΡΕΥΝΑΣ ΑΕ – ΕΔΥΤΕ ΑΕ

Αθήνα, 11/03/2026

Αρ. Πρωτ. 4737/ΑΣ

Προκήρυξη Ανοικτού Ηλεκτρονικού Διαγωνισμού άνω των ορίων για Σύναψη Συμφωνίας Πλαίσιο για το Υπόεργο 1 «Ενίσχυση της κυβερνοασφάλειας των ΟΤΑ Α' βαθμού» του Έργου «Προμήθεια εξοπλισμού και υπηρεσιών Κυβερνοασφάλειας για τους ΟΤΑ» της Πράξης «Προμήθεια εξοπλισμού και υπηρεσιών Κυβερνοασφάλειας για τους ΟΤΑ» με κωδικό ΟΠΣ (MIS) 5225494

Υπηρεσίες

Τμήμα Ι: Αναθέτουσα αρχή

I.1) Επωνυμία και διευθύνσεις

Εθνικό Δίκτυο Υποδομών Τεχνολογίας & Έρευνας ΑΕ - ΕΔΥΤΕ ΑΕ, ΛΕΩΦΟΡΟΣ ΚΗΦΙΣΙΑΣ 7, ΑΘΗΝΑ, 11523, ΕΛΛΑΔΑ, Αρμόδιος για πληροφορίες: Κωνσταντίνος Γραμματικός Τηλέφωνο: +30 2107474274, Ηλεκτρονικό ταχυδρομείο: info@grnet.gr

Διεύθυνση(-εις) στο διαδίκτυο: Γενική διεύθυνση: <https://grnet.gr>

I.2) Πληροφορίες σχετικά με τις από κοινού προμήθειες

I.3) **Επικοινωνία:** Τα έγγραφα της Σύμβασης είναι διαθέσιμα για απεριόριστη, πλήρη, άμεση και δωρεάν πρόσβαση στη διεύθυνση: www.promitheus.gov.gr.

Περαιτέρω πληροφορίες είναι διαθέσιμες από: προαναφερθείσα διεύθυνση.

Οι προσφορές ή οι αιτήσεις συμμετοχής πρέπει να υποβάλλονται ηλεκτρονικά στη διεύθυνση: www.promitheus.gov.gr.

Οι προσφορές ή οι αιτήσεις συμμετοχής πρέπει να υποβάλλονται στην προαναφερθείσα διεύθυνση.

I.4) Είδος της Αναθέτουσας Αρχής

Άλλο είδος: Ανώνυμη Εταιρία του Δημοσίου, τεχνολογικός φορέας του Υπουργείου Ψηφιακής Διακυβέρνησης και ανήκει στη Γενική Κυβέρνηση

I.5) Κύρια δραστηριότητα

Άλλες δραστηριότητες: Παροχή δικτυακών και υπολογιστικών υπηρεσιών

Τμήμα II: Αντικείμενο

II.1) Εύρος της σύμβασης

II.1.1) **Τίτλος:** Σύναψη Συμφωνίας Πλαίσιο για το Υποέργο 1 «Ενίσχυση της κυβερνοασφάλειας των ΟΤΑ Α' βαθμού» του Έργου «Προμήθεια εξοπλισμού και υπηρεσιών Κυβερνοασφάλειας για τους ΟΤΑ»

Αριθμός αναφοράς: **4736/ΑΣ/11.03.2026**

II.1.2) **Κωδικός κύριου λεξιλογίου CPV:** 72000000-5 - Υπηρεσίες τεχνολογίας των πληροφοριών: παροχή συμβουλών, ανάπτυξη λογισμικού, Διαδίκτυο και υποστήριξη

II.1.3) **Είδος σύμβασης:** Υπηρεσίες

II.1.4) **Σύντομη περιγραφή:** Το έργο αφορά την προμήθεια εξοπλισμού και την παροχή υπηρεσιών κυβερνοασφάλειας για την υποστήριξη των Οργανισμών Τοπικής Αυτοδιοίκησης (ΟΤΑ), με στόχο την επίτευξη υψηλού επιπέδου ασφάλειας πληροφοριών και την προστασία των πληροφοριακών τους συστημάτων από κυβερνοαπειλές.

II.1.5) **Εκτιμώμενη συνολική αξία:** Αξία χωρίς ΦΠΑ: € 8.246.830,65 (συμπεριλαμβανομένου του δικαιώματος Προαίρεσης)

II.1.6) Πληροφορίες σχετικά με τα τμήματα

Η παρούσα σύμβαση υποδιαιρείται σε τμήματα: όχι

II.2) Περιγραφή

II.2.1) **Τίτλος:** «Προμήθεια εξοπλισμού και υπηρεσιών Κυβερνοασφάλειας για τους ΟΤΑ»

II.2.2) **Επιπλέον κωδικός(-οί) CPV:**

- 79417000-0 - Υπηρεσίες παροχής συμβουλών σε θέματα ασφάλειας
- 80550000-4 - Υπηρεσίες εκπαίδευσης σε θέματα ασφάλειας
- 48730000-4 - Πακέτα λογισμικού ασφαλείας
- 30200000-1 - Εξοπλισμός ηλεκτρονικών υπολογιστών και προμήθειες

II.2.3) **Τόπος εκτέλεσης:** Κύριος τόπος ή τοποθεσία εκτέλεσης: ΕΛΛΗΝΙΚΗ ΕΠΙΚΡΑΤΕΙΑ

II.2.4) **Περιγραφή της σύμβασης:**

Το έργο αφορά την προμήθεια εξοπλισμού και την παροχή υπηρεσιών κυβερνοασφάλειας για την υποστήριξη των Οργανισμών Τοπικής Αυτοδιοίκησης (ΟΤΑ), με στόχο την επίτευξη υψηλού επιπέδου ασφάλειας πληροφοριών και την προστασία των πληροφοριακών τους συστημάτων από κυβερνοαπειλές. Οι βασικοί τομείς παρέμβασης περιλαμβάνουν:

- Πρόληψη: Ανάπτυξη ικανοτήτων για την αποτροπή κυβερνοεπιθέσεων.
- Αναγνώριση και αποτροπή απειλών: Ανίχνευση και αποτροπή κακόβουλων ενεργειών.

- Αντιμετώπιση και αποκατάσταση: Διαχείριση περιστατικών και αποκατάσταση των λειτουργιών. Αναφορικά με τις λύσεις που προτείνεται να αποτελέσουν το φυσικό αντικείμενο, αυτές καλύπτουν ευρύ φάσμα δράσεων, οι οποίες αναφέρονται στα εξής:
 1. Εκπόνηση Μελέτη Ανάλυσης και Αξιολόγησης Κινδύνων: Σχεδιασμός στρατηγικών για την ανίχνευση και εκτίμηση κινδύνων.
 2. Διαμόρφωση πλάνου ανάκαμψης από καταστροφές: Ανάπτυξη στρατηγικής για την αποκατάσταση της λειτουργίας σε περίπτωση καταστροφής.
 3. Διενέργεια ελέγχων διείσδυσης εξωτερικών δικτύων, εφαρμογών Ιστού, φυσικής ασφάλειας και διαρροής δεδομένων: Ανάλυση των δικτύων και εφαρμογών για τρωτά σημεία.
 4. Διαμόρφωση Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ) με βάση το πρότυπο ISO 27001 ΚΑΙ Εκπόνηση Μελέτης Ανάλυσης και Αξιολόγησης Κινδύνων: Σύστημα ISO 27001 για την ασφάλεια των πληροφοριών.
 5. Διενέργεια δράσεων ενημέρωσης για τη μεταφορά τεχνογνωσίας και τη διαμόρφωση κουλτούρας ενεργούς ευαισθητοποίησης για τους κινδύνους κυβερνοασφάλειας: Δράσεις για την ανάπτυξη κουλτούρας ευαισθητοποίησης σε θέματα κυβερνοασφάλειας.
 6. Υπηρεσίες SOC (Security Operations Center): Παροχή υπηρεσιών παρακολούθησης και ανίχνευσης επιθέσεων.
 7. Υπηρεσίες Ransomware readiness assessment: Ανάλυση ετοιμότητας για την αντιμετώπιση ransomware.
 8. Άσκηση Προσομοίωσης Phishing: Άσκηση για την εκπαίδευση στην ανίχνευση επιθέσεων τύπου phishing.
 9. Τείχος προστασίας επόμενης γενιάς: Εφαρμογή προηγμένων συστημάτων firewall.
 10. Προστασία Τελικού Σημείου: Στρατηγικές ασφάλειας για τα τερματικά συστήματα.
 11. Πλατφόρμα κυβερνοασφάλειας: Εργαλεία για την κεντρική διαχείριση της ασφάλειας.
 12. Έλεγχος Ταυτότητας Πολλαπλών Παραγόντων (MFA): Εφαρμογή MFA για ενισχυμένη ασφάλεια.
 13. Προστασία Ηλεκτρονικού Ταχυδρομείου / Secure Mail Gateway: Προστασία των επικοινωνιών μέσω ηλεκτρονικού ταχυδρομείου.
 14. Υπηρεσία Ασφαλούς Πρόσβασης Άκρου / Secure Access Service Edge (SASE): Ενίσχυση της ασφαλούς πρόσβασης στα δίκτυα.
 15. Υπηρεσία Διαχείρισης Ψηφιακού Κινδύνου: Ανάπτυξη στρατηγικών για τη διαχείριση και την προστασία από ψηφιακούς κινδύνους.

II.2.5) Κριτήρια ανάθεσης

Η συμφωνία - πλαίσιο θα ανατεθεί με το κριτήριο την πλέον συμφέρουσα από οικονομική άποψη προσφοράς, βάσει της βέλτιστης σχέσης ποιότητας – τιμής, όπως αναλυτικά αναφέρεται στο άρθρο 2.3.1 της παρούσας.

II.2.6) **Εκτιμώμενη αξία:** Αξία χωρίς ΦΠΑ € 8.246.830,65 (συμπεριλαμβανομένου του δικαιώματος Προαίρεσης)

II.2.7) **Διάρκεια σύμβασης, συμφωνίας-πλαίσιο ή δυναμικού συστήματος αγορών**

Η διάρκεια της συμφωνίας - πλαίσιο ορίζεται σε δώδεκα (12) μήνες από την ημερομηνία υπογραφής της.

Οι εκτελεστικές συμβάσεις μπορούν να συνάπτονται έως και τη συμπλήρωση του χρόνου διάρκειας της συμφωνίας-πλαίσιο. Η διάρκεια των εκτελεστικών συμβάσεων μπορεί να υπερβαίνει τον χρόνο λήξης της συμφωνίας-πλαίσιο.

II.2.10) **Πληροφορίες σχετικά με εναλλακτικές προσφορές**

Θα γίνουν δεκτές εναλλακτικές προσφορές: όχι

II.2.11) **Πληροφορίες σχετικά με δικαιώματα προαίρεσης**

Δικαιώματα προαίρεσης: ναι (Η αναθέτουσα αρχή διατηρεί, ως δικαίωμα προαίρεσης (σύμφωνα προαίρεσης Αστικού Κώδικα) τη δυνατότητα, με μονομερή δήλωση της κατά τη διάρκεια εκτέλεσης της συμφωνίας-πλαίσιο, να αναθέσει στους συμβαλλόμενους στη συμφωνία-πλαίσιο, πρόσθετα πακέτα υπηρεσιών, πρόσθετες άδειες χρήσης λογισμικού ή/και επέκταση χρονικής ισχύος αδειών χρήσης λογισμικού, πρόσθετο εξοπλισμό με αντικείμενο όμοιο με αυτές της παρούσας, συνολικής εκτιμώμενης αξίας δύο εκατομμυρίων επτακοσίων σαράντα οχτώ χιλιάδων εννιακοσίων σαράντα τριών ευρώ και πενήντα πέντε λεπτών (2.748.943,55 €) πλέον ΦΠΑ, με βάση τις τιμές μονάδας της Συμφωνίας Πλαίσιο που θα συναφθεί βάσει των οικονομικών προσφορών των Αντισυμβαλλομένων αυτής και με χρονοδιάγραμμα υλοποίησης έως δώδεκα (12) μήνες από την άσκησή του.)

II.2.12) **Πληροφορίες σχετικά με ηλεκτρονικούς καταλόγους**

II.2.13) **Πληροφορίες σχετικά με τα Ταμεία της Ευρωπαϊκής Ένωσης**

Η σύμβαση σχετίζεται με έργο ή/και πρόγραμμα χρηματοδοτούμενο από τα Ταμεία της Ευρωπαϊκής Ένωσης: όχι

Φορέας χρηματοδότησης της παρούσας Συμφωνίας Πλαίσιο και των συμβάσεων που βασίζονται σε αυτή (εκτελεστικές συμβάσεις) είναι το Υπουργείο Ψηφιακής Διακυβέρνησης. Η παρούσα συμφωνία-πλαίσιο υλοποιείται στο πλαίσιο του Υποέργου 1 «Ενίσχυση της κυβερνοασφάλειας των ΟΤΑ Α Βαθμού» της πράξης «Προμήθεια εξοπλισμού και υπηρεσιών κυβερνοασφάλειας για τους ΟΤΑ» που

έχει ενταχθεί στο ΤΠΑ «Ψηφιακής Διακυβέρνησης 2021-2025» με την υπ. αριθμ. πρωτ: ΓΔΟΔΥ/523/2025-28/8/2025 Απόφαση Ένταξης με κωδικό ΟΠΣ 5225494 και ΣΑΕ 2025NA16300013.

Το δικαίωμα προαίρεσης δύναται να χρηματοδοτηθεί από οποιαδήποτε πηγή χρηματοδότησης.

II.2.14) Συμπληρωματικές πληροφορίες

Όπως Τεύχος Διακήρυξης

Τμήμα III: Νομικές, οικονομικές, χρηματοοικονομικές και τεχνικές πληροφορίες

III.1) Προϋποθέσεις συμμετοχής

III.1.1) Άδεια άσκησης επαγγελματικής δραστηριότητας, συμπεριλαμβανομένων των απαιτήσεων για την εγγραφή σε επαγγελματικό ή εμπορικό μητρώο

Οι οικονομικοί φορείς που συμμετέχουν στη διαδικασία σύναψης της παρούσας συμφωνίας-πλαίσιο απαιτείται να ασκούν δραστηριότητα συναφή με το αντικείμενο των προς παροχή υπηρεσιών, ήτοι να δραστηριοποιούνται επαγγελματικά με την παροχή υπηρεσιών πληροφορικής.

Οι οικονομικοί φορείς που είναι εγκατεστημένοι σε κράτος μέλος της Ευρωπαϊκής Ένωσης απαιτείται να είναι εγγεγραμμένοι σε ένα από τα επαγγελματικά μητρώα που τηρούνται στο κράτος εγκατάστασής τους ή να ικανοποιούν οποιαδήποτε άλλη απαίτηση ορίζεται στο Παράρτημα XI του Προσαρτήματος Α' του ν. 4412/2016. Εφόσον οι οικονομικοί φορείς απαιτείται να διαθέτουν ειδική έγκριση ή να είναι μέλη συγκεκριμένου οργανισμού για να μπορούν να παράσχουν τη σχετική υπηρεσία στη χώρα καταγωγής τους, η αναθέτουσα αρχή μπορεί να τους ζητεί να αποδείξουν ότι διαθέτουν την έγκριση αυτή ή ότι είναι μέλη του εν λόγω οργανισμού ή να τους καλέσει να προβούν σε ένορκη δήλωση ενώπιον συμβολαιογράφου σχετικά με την άσκηση του συγκεκριμένου επαγγέλματος.

Στην περίπτωση οικονομικών φορέων εγκατεστημένων σε κράτος μέλους του Ευρωπαϊκού Οικονομικού Χώρου (Ε.Ο.Χ) ή σε τρίτες χώρες που προσχωρήσει στη ΣΔΣ, ή σε τρίτες χώρες που δεν εμπίπτουν στην προηγούμενη περίπτωση και έχουν συνάψει διμερείς ή πολυμερείς συμφωνίες με την Ένωση σε θέματα διαδικασιών ανάθεσης δημοσίων συμβάσεων, απαιτείται να είναι εγγεγραμμένοι σε αντίστοιχα επαγγελματικά μητρώα.

Οι εγκατεστημένοι στην Ελλάδα οικονομικοί φορείς να είναι εγγεγραμμένοι στο οικείο επαγγελματικό μητρώο, εφόσον κατά την κείμενη νομοθεσία, απαιτείται η εγγραφή του για την υπό ανάθεση υπηρεσία.

Στην περίπτωση ένωσης οικονομικών φορέων η καταλληλότητα άσκησης επαγγελματικής δραστηριότητας απαιτείται να καλύπτεται από τουλάχιστον ένα μέλος της ένωσης.

III.1.2) Οικονομική και χρηματοοικονομική επάρκεια

Όσον αφορά την οικονομική και χρηματοοικονομική επάρκεια για την παρούσα διαδικασία σύναψης συμφωνίας - πλαίσιο, οι υποψήφιοι απαιτείται να διαθέτουν μέσο γενικό ετήσιο κύκλο εργασιών για τις τρεις (3) προηγούμενες του έτους του διαγωνισμού χρήσεις (2022, 2023 και 2024) τουλάχιστον ίσο με το 200% της εκτιμώμενης αξίας της παρούσας συμφωνίας πλαίσιο, χωρίς ΦΠΑ και χωρίς το δικαίωμα προαίρεσης. Σε περίπτωση που ο υποψήφιος δραστηριοποιείται για χρονικό διάστημα μικρότερο των ως άνω τριών (3) διαχειριστικών χρήσεων, θα πρέπει να πληροί το ελάχιστο ως άνω επίπεδο χρηματοοικονομικής επάρκειας για όσες διαχειριστικές χρήσεις δραστηριοποιείται συναρτήσει της έναρξης των δραστηριοτήτων του.

Σε περίπτωση ένωσης οικονομικών φορέων, οι παραπάνω απαιτήσεις μπορούν να καλύπτονται αθροιστικά από τα μέλη της ένωσης.

III.1.3) Τεχνική και επαγγελματική ικανότητα

Όσον αφορά στην τεχνική και επαγγελματική ικανότητα για την παρούσα διαδικασία σύναψης της συμφωνίας - πλαίσιο, οι οικονομικοί φορείς (ή σε περίπτωση ένωσης/κοινοπραξίας εταιρειών αθροιστικά τα μέλη της ένωσης/ κοινοπραξίας) απαιτείται:

A) Να έχουν ολοκληρώσει επιτυχώς κατά τη διάρκεια της τελευταίας πενταετίας πριν από την καταληκτική ημερομηνία υποβολής προσφορών του παρόντος διαγωνισμού:

1. Δύο (2) ή περισσότερα έργα που αθροιστικά να περιλαμβάνουν και υλοποίηση Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών ή/και παροχής συμβουλευτικών/ μελετητικών υπηρεσιών για την εκπόνηση μελετών, πολιτικών, διαδικασιών και προτύπων ασφάλειας, ή/και Υπηρεσίες Υποστήριξης για Πιστοποίηση κατά ISO 27001:2013
2. Ένα (1) ή περισσότερα έργα που να περιλαμβάνει την παροχή υπηρεσιών, σχετικά με την αποτύπωση τρέχουσας στρατηγικής και υφιστάμενης κατάστασης πληροφοριακών συστημάτων, την ανάλυση θεσμικού περιβάλλοντος, με εστίαση στη συμμόρφωση με όλες τις προβλέψεις του θεσμικού ή/και κανονιστικού πλαισίου την πρόταση και ανάλυση αλλαγών σε οργανωτικό και επιχειρησιακό επίπεδο και την εκπόνηση προτάσεων για την ασφάλεια συστημάτων.
3. Δύο ή περισσότερα (2) έργα που να αφορούν εκπαίδευση - ευαισθητοποίηση προσωπικού στην ασφάλεια πληροφοριών, μέσω ηλεκτρονικών υπηρεσιών.
4. Δύο ή περισσότερα (2) έργα που να περιλαμβάνουν πιστοποιημένες εκπαιδεύσεις.
5. Δύο ή περισσότερα (2) έργα που να περιλαμβάνουν τη διενέργεια ελέγχων διείσδυσης (Penetration test).
6. Ένα ή περισσότερα (1) έργα που να περιλαμβάνει την προμήθεια εξοπλισμού ασφάλειας (τείχη προστασίας - firewalls) και την εγκατάσταση του εν λόγω εξοπλισμού.

7. Έως οχτώ (8) έργα που έχουν συνολικό προϋπολογισμό τουλάχιστον ενός εκατομμυρίου ευρώ (1.000.000 €) και περιλαμβάνουν αθροιστικά τα κάτωθι αντικείμενα:

- ο Σχεδιασμό ή/και συντήρηση (υποστήριξη) Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
- ο Σχεδιασμό ή/και συντήρηση (υποστήριξη) πλάνου ανάκαμψης από καταστροφή ή/και Συστήματος διαχείρισης επιχειρησιακής συνέχειας
- ο Διενέργεια ελέγχων παρείσδυσης (penetration test)
- ο Εκπόνηση μελέτης αξιολόγησης κινδύνων
- ο Εκπόνηση προτάσεων για την ασφάλεια συστημάτων
- ο Παροχή υπηρεσιών εκπαίδευσης ή/και ευαισθητοποίησης για την κυβερνοσφάλεια με χρήση πλατφόρμας εκπαίδευσης
- ο Πιστοποιημένες εκπαιδεύσεις στην ασφάλεια πληροφοριών ή/και την επιχειρησιακή συνέχεια
- ο Προμήθεια εξοπλισμού ασφάλειας (τείχη προστασίας - firewalls) και εγκατάσταση του εν λόγω εξοπλισμού σε τουλάχιστον τριάντα (30) σημεία με γεωγραφική διασπορά σε τουλάχιστον έξι (6) περιφέρειες.
- ο Υλοποίηση τουλάχιστον τριών (3) από τις παρακάτω λύσεις κυβερνοασφάλειας:
 - ☐ Υποσύστημα SIEM με αξιοποίηση AI αλγόριθμων.
 - ☐ Υποσύστημα δημιουργίας για honeypots.
 - ☐ Υποσύστημα στατική ανάλυση κώδικα.
 - ☐ Προστασία Ηλεκτρονικού Ταχυδρομείου / Secure Mail Gateway
 - ☐ Προστασία Τελικού Σημείου

Επισημαίνεται ότι (α) δεν λαμβάνονται υπόψη εν εξελίξει συμβάσεις, δηλαδή συμβάσεις που δεν ολοκληρώθηκαν εντός της περιόδου αναφοράς και (β) εάν κάποιος/κάποια από τα έργα που τεκμηριώνουν την κάλυψη των ανωτέρω απαιτήσεων έχει/έχουν υλοποιηθεί από τον υποψήφιο ως μέλος ένωσης, προσμετράται μόνο η συμβατική αξία που αντιστοιχεί στο ποσοστό συμμετοχής του σε εκείνη την ένωση.

Δύναται ένα έργο να καλύπτει περισσότερες από μία από τις ανωτέρω απαιτήσεις.

2.2.6.2 Επαγγελματική Ικανότητα – Ομάδα Έργου

Β) Να διαθέτουν προσωπικό επαρκές σε πλήθος και δεξιότητες για την υλοποίηση της Συμφωνίας-Πλαίσιο. Συγκεκριμένα απαιτείται να διαθέτουν κατ' ελάχιστον τα παρακάτω στελέχη στις κάτωθι βασικές κατηγορίες προφίλ (key experts):

1. Ένα (1) στέλεχος σε ρόλο Υπεύθυνο Έργου το οποίο να διαθέτει τουλάχιστον τα ακόλουθα προσόντα:

- ο Πανεπιστημιακό και μεταπτυχιακό τίτλο σπουδών
 - ο τουλάχιστον δεκαετή (10) αποδεδειγμένη εργασιακή εμπειρία σε Διαχείριση Έργων
- Να είναι κάτοχος πιστοποίησης στη διαχείριση έργων (PMI ή PM2 ή PRINCE2 ή αντίστοιχη ή ισοδύναμη).
2. Ένα (1) στέλεχος σε ρόλο Αναπληρωτή Υπεύθυνου Έργου το οποίο να διαθέτει τουλάχιστον τα ακόλουθα προσόντα:
- ο Πανεπιστημιακό τίτλο σπουδών
 - ο Τουλάχιστον πενταετή (5) αποδεδειγμένη εργασιακή εμπειρία σε Διαχείριση Έργων
 - ο πιστοποίηση στη διαχείριση έργων (PMI ή PM2 ή PRINCE2 ή αντίστοιχη ή ισοδύναμη).
3. Ένα (1) στέλεχος σε ρόλο υπεύθυνου ομάδας υπηρεσιών ασφάλειας, το οποίο να διαθέτει:
- ο Πανεπιστημιακό και μεταπτυχιακό τίτλο σπουδών.
 - ο Τουλάχιστον 10ετή εμπειρία σε έργα ανάπτυξης, εγκατάστασης και εφαρμογής Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών και Συστημάτων Διαχείρισης Επιχειρησιακής Συνέχειας ή/και σε έργα ανάλυσης, αξιολόγησης κινδύνων (risk analysis & assessment), ή/και στον λειτουργικό /οργανωτικό ανασχεδιασμό δημόσιων ή/και ιδιωτικών Φορέων.
 - ο Επιπλέον, ο Υπεύθυνος ομάδας υπηρεσιών ασφάλειας και ο Αναπληρωτής Υπεύθυνος ομάδας υπηρεσιών ασφάλειας αθροιστικά πρέπει να κατέχουν τις ακόλουθες ή ισοδύναμες πιστοποιήσεις:
 - ☐ ISO 27001 Lead Auditor
 - ☐ Certified Information Security Manager (CISM)
 - ☐ Business Continuity Certified Lead Auditor
 - ☐ Data Protection Officer (DPO)
 - ☐ ITIL® Foundation in IT Service Management.
 - ☐ Certified Information Privacy Professional /Europe (CIPP/E)
4. ένα (1) στέλεχος σε ρόλο αναπληρωτή υπεύθυνου ομάδας υπηρεσιών ασφάλειας, το οποίο να διαθέτει:
- ο Πανεπιστημιακό και μεταπτυχιακό τίτλο σπουδών
 - ο τουλάχιστον 5ετή επαγγελματική εμπειρία στην υλοποίηση έργων παροχής συμβουλευτικών υπηρεσιών καθώς και σε έργα σχεδιασμού και εφαρμογής Συστημάτων Ασφάλειας Πληροφοριών και Συστημάτων Διαχείρισης Επιχειρησιακής Συνέχειας και σε έργα ανάλυσης και αξιολόγησης κινδύνων (risk analysis & assessment).
 - ο Επιπλέον, ο Υπεύθυνος ομάδας υπηρεσιών ασφάλειας και ο Αναπληρωτής Υπεύθυνος ομάδας υπηρεσιών ασφάλειας αθροιστικά πρέπει να κατέχουν τις ακόλουθες ή ισοδύναμες πιστοποιήσεις:

- ISO 27001 Lead Auditor
 - Certified Information Security Manager (CISM)
 - Business Continuity Certified Lead Auditor
 - Data Protection Officer (DPO)
 - ITIL® Foundation in IT Service Management.
 - Certified Information Privacy Professional /Europe (CIPP/E)
5. Ένα (1) στέλεχος σε ρόλο εμπειρογνώμονα κυβερνοασφάλειας, το οποίο να διαθέτει:
- ο Πανεπιστημιακό σπουδών στην πληροφορική
 - ο Τουλάχιστον 10ετή εμπειρία στην κυβερνοασφάλεια.
 - ο Να έχει συμμετάσχει σε έργα που να καλύπτουν σωρευτικά τα κάτωθι αντικείμενα:
 - Σχεδιασμό αντιμετώπισης κινδύνων κυβερνοασφάλειας για ομάδα επιχειρήσεων ή οργανισμών.
 - Υποστήριξη δημιουργίας δικτύου για την κοινή αντιμετώπιση απειλών κυβερνοασφάλειας και την ενημέρωση των πολιτών για τους κινδύνους κυβερνοασφάλειας.
 - Σχεδιασμό πλαισίου αντιμετώπισης καινοτόμων απειλών για εφαρμογές τεχνολογίας αιχμής
 - Ανάπτυξη λύσης ασφάλειας για εφαρμογές τεχνολογίας αιχμής (π.χ. AI, IOT κλπ)
6. Δύο (2) στελέχη σε ρόλο συμβούλων ασφάλειας το καθένα εκ των οποίων να διαθέτει:
- ο Πανεπιστημιακό τίτλο σπουδών ή/και Μεταπτυχιακό τίτλο σπουδών
 - ο Τουλάχιστον 3ετή εμπειρία σε έργα συμβουλευτικών υπηρεσιών ή/και ανάπτυξης, εγκατάστασης και εφαρμογής Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών ή/και σε έργα ανάλυσης, αξιολόγησης κινδύνων (risk analysis & assessment).
- Επιπλέον, αθροιστικά πρέπει να κατέχουν τις εξής πιστοποιήσεις ή ισοδύναμες:
- ο ISO 27001:2013
 - ο CompTIA security+ ή ISC² Certified in Cybersecurity (CC)
7. Τρία (3) στελέχη σε ρόλο έμπειρου στελέχους διενέργειας ελέγχων παρείσδυσης (penetration test), το οποίο να διαθέτει:
- ο Πανεπιστημιακό τίτλο σπουδών
 - ο τουλάχιστον 4ετή επαγγελματική εμπειρία στη διενέργεια ελέγχων παρείσδυσης (penetration test).
 - ο Επιπλέον, αθροιστικά πρέπει να κατέχουν τις εξής πιστοποιήσεις ή ισοδύναμες:
 - ☒ Certified Ethical Hacker (CEH - Practical)
 - ☒ Licensed Penetration Tester (LPT)

- Offensive Security Certified Professional (OSCP)
- Offensive Security Wireless Professional (OSWP)
- Certified Red Team Expert (CRTE)
- NCSC CHECK Team Leader - Infrastructure (CTL - INF) ή CREST Certified Infrastructure Tester (CCT - INF)
- NCSC CHECK Team Leader - Web Applications (CTL - APP) ή CREST Certified Web Applications Tester (CCT - APP) ή Certified Penetration Testing Professional (C|PENT)
- CREST Practitioner Security Analyst (CPSA)

8. Τρία (3) στελέχη σε ρόλο στελέχους διενέργειας ελέγχων παρεϊσδυσης (penetration test), τα οποία να διαθέτουν:

- ο Πανεπιστημιακό τίτλο σπουδών
- ο Τουλάχιστον 2ετή επαγγελματική εμπειρία στη διενέργεια ελέγχων παρεϊσδυσης (penetration test).
- ο Επιπλέον, αθροιστικά πρέπει να κατέχουν τις εξής πιστοποιήσεις ή ισοδύναμες:
 - Certified Ethical Hacker (CEH - Practical)
 - Licensed Penetration Tester (LPT)
 - Offensive Security Certified Professional (OSCP)
 - Offensive Security Wireless Professional (OSWP)
 - GIAC Reverse Engineering Malware
 - API Penetration Testing
 - Certified Red Team Operator

9. Δύο (2) στελέχη σε ρόλο στελέχους ηλεκτρονικής εκπαίδευσης, το καθένα εκ των οποίων να διαθέτει:

- ο Πανεπιστημιακό τίτλο σπουδών
- ο Συμμετοχή σε πέντε (5) ή περισσότερα έργα που να αφορούν εκπαίδευση - ευαισθητοποίηση προσωπικού στην ασφάλεια πληροφοριών, μέσω ηλεκτρονικών υπηρεσιών.

10. Δύο (2) στελέχη σε ρόλο στελεχών εγκατάστασης εξοπλισμού ασφάλειας, το καθένα εκ των οποίων να διαθέτει διετή εμπειρία στην εγκατάσταση εξοπλισμού ασφάλειας

11. Δύο (2) στελέχη σε ρόλο στελεχών υλοποίησης λύσεων κυβερνοασφάλειας, το καθένα εκ των οποίων να διαθέτει διετή εμπειρία στην υλοποίηση λύσεων κυβερνοασφάλειας

Τα φυσικά πρόσωπα που δηλώνονται από τον προσφέροντα στην Ομάδα Έργου δύνανται να απασχολούνται με εξαρτημένη σχέση εργασίας ή σύμβαση ανεξαρτήτων υπηρεσιών, η οποία είναι σε

ισχύ ήδη κατά τον χρόνο υποβολής της προσφοράς. Στην τελευταία αυτή περίπτωση θεωρούνται ίδιοι πόροι του οικονομικού φορέα και όχι τρίτοι δανείζοντες και δεν απαιτείται εκ μέρους τους η υποβολή ΕΕΕΣ και των σχετικών αποδεικτικών μέσων.

Διευκρινίζεται ότι σε περίπτωση που ο υποψήφιος ανάδοχος είναι ένωση, οι παραπάνω απαιτήσεις μπορούν να καλύπτονται αθροιστικά από τα μέλη της ένωσης.

III. 1.4) Πρότυπα διασφάλισης ποιότητας και πρότυπα περιβαλλοντικής διαχείρισης

Οι οικονομικοί φορείς που συμμετέχουν στη διαδικασία σύναψης της παρούσας απαιτείται να εξασφαλίζουν την ποιότητα των παρεχόμενων υπηρεσιών και να διαθέτουν οργανωμένο σύστημα διαχείρισης Ποιότητας ή ισοδύναμο με τα παρακάτω Πρότυπα Διασφάλισης ποιότητας:

- ISO 9001:2015 για τη Διαχείριση της Ποιότητας ή ισοδύναμο, εν ισχύ, από διαπιστευμένο οργανισμό.
- ISO 27001:2013 για την Ασφάλεια των Πληροφοριών ή ισοδύναμο, εν ισχύ, από διαπιστευμένο οργανισμό.
- ISO 20000:2018 για την παροχή υπηρεσιών πληροφορικής ή ισοδύναμο, εν ισχύ, από διαπιστευμένο οργανισμό.
- ISO 27701:2013 για τη Διαχείριση Προσωπικών Δεδομένων ή ισοδύναμο, εν ισχύ, από διαπιστευμένο οργανισμό.
- ISO 22301:2013 για την Επιχειρησιακή Συνέχεια ή ισοδύναμο, εν ισχύ, από διαπιστευμένο οργανισμό.
- ISO 45001:2018 για την Υγεία και Ασφάλεια στην Εργασία ή ισοδύναμο, εν ισχύ, από διαπιστευμένο οργανισμό.
- ISO 29993:2017 ή άλλο ισοδύναμο εν ισχύ για την παροχή υπηρεσιών εκπαίδευσης.

Η αναθέτουσα αρχή αναγνωρίζει ισοδύναμα πιστοποιητικά που έχουν εκδοθεί από φορείς διαπιστευμένους από ισοδύναμους Οργανισμούς διαπίστευσης, οι οποίοι εδρεύουν και σε άλλα κράτη – μέλη σύμφωνα με τον Κανονισμό 765/2008. Επίσης, κάνει δεκτά άλλα αποδεικτικά στοιχεία για ισοδύναμα μέτρα διασφάλισης ποιότητας, εφόσον ο ενδιαφερόμενος οικονομικός φορέας δεν είχε τη δυνατότητα να αποκτήσει τα εν λόγω πιστοποιητικά εντός των σχετικών προθεσμιών για λόγους για τους οποίους δεν ευθύνεται ο ίδιος, υπό την προϋπόθεση ότι ο οικονομικός φορέας αποδεικνύει ότι τα προτεινόμενα μέτρα διασφάλισης ποιότητας πληρούν τα απαιτούμενα πρότυπα διασφάλισης ποιότητας.

Διευκρινίζεται ότι σε περίπτωση που ο υποψήφιος ανάδοχος είναι ένωση ή κοινοπραξία, οι ανωτέρω απαιτήσεις μπορούν να πληρούνται αθροιστικά από τα μέλη της ένωσης ή κοινοπραξίας.

III.1.5) Πληροφορίες για ανατιθέμενες κατ' αποκλειστικότητα συμβάσεις

III.2) Όροι που αφορούν τη σύμβαση

III.2.1) Πληροφορίες σχετικά με συγκεκριμένη επαγγελματική κατηγορία

III.2.2) Όροι εκτέλεσης της σύμβασης: Όπως Τεύχος Διακήρυξης

III.2.3) Πληροφορίες σχετικά με το προσωπικό που αναλαμβάνει την εκτέλεση της σύμβασης: δεν αφορά

Τμήμα IV: Διαδικασία

IV.1) Περιγραφή

IV.1.1) Είδος διαδικασίας: Ανοιχτός Διαγωνισμός άνω των ορίων

IV.1.3) Πληροφορίες σχετικά με συμφωνία-πλαίσιο ή δυναμικό σύστημα αγορών Αριθμός συμβαλλομένων οικονομικών φορέων: Η ολοκλήρωση αυτής της διαγωνιστικής διαδικασίας θα οδηγήσει στη σύναψη συμφωνίας – πλαίσιο με έναν (1) οικονομικό φορέα.

IV.1.4) Πληροφορίες σχετικά με τη μείωση του αριθμού των λύσεων ή των προσφορών κατά τη διάρκεια της διαπραγμάτευσης ή του διαλόγου

IV.1.6) Πληροφορίες σχετικά με τον ηλεκτρονικό πλειστηριασμό

IV.1.8) Πληροφορίες για τη Συμφωνία περί Δημοσίων Προμηθειών (GPA)

Η σύμβαση καλύπτεται από τη Συμφωνία περί Δημοσίων Προμηθειών: ναι

IV.2) Διοικητικές πληροφορίες

IV.2.1) Προηγούμενη δημοσίευση σχετικά με την εν λόγω διαδικασία

IV.2.2) Προθεσμία παραλαβής των προσφορών ή των αιτήσεων συμμετοχής

Ημερομηνία: **24/04/2026**, Τοπική ώρα: **12:00μ.μ.**

IV.2.3) Εκτιμώμενη ημερομηνία αποστολής των προσκλήσεων υποβολής προσφορών ή συμμετοχής στους επιλεγέντες υποψηφίους

IV.2.4) Γλώσσες στις οποίες μπορούν να υποβληθούν οι προσφορές ή οι αιτήσεις συμμετοχής: Ελληνικά

IV.2.6) Ελάχιστη απαιτούμενη χρονική διάρκεια ισχύος της προσφοράς

Διάρκεια σε μήνες: 12 από την επόμενη της της καταληκτικής ημερομηνίας υποβολής προσφορών

IV.2.7) Όροι για την αποσφράγιση των προσφορών

Ημερομηνία: **24/04/2026**, Τοπική ώρα: **12:30μ.μ.**

Τόπος: Αθήνα, Γραφεία ΕΔΥΤΕ ΑΕ, Λεωφόρος Κηφισίας 7, 2ος όροφος.

Πληροφορίες για τα εξουσιοδοτημένα άτομα και τη διαδικασία αποσφράγισης προσφορών: Μόνο εξουσιοδοτημένοι εκπρόσωποι της Αναθέτουσας Αρχής.

Τμήμα VI: Πρόσθετες πληροφορίες

VI.1) Πληροφορίες σχετικά με επαναλαμβανόμενες συμβάσεις

Πρόκειται για επαναλαμβανομένη δημόσια σύμβαση: όχι

VI.2) Πληροφορίες σχετικά με τις ηλεκτρονικές ροές εργασίας

VI.3) Συμπληρωματικές πληροφορίες: Όπως Τεύχος Διακήρυξης.

VI.4) Διαδικασίες προσφυγής

VI.4.1) Φορέας αρμόδιος για τις διαδικασίες προσφυγής

ΕΑΔΗΣΥ, Δώρου 7-9, Αθήνα 10432, ΕΛΛΑΔΑ, Τηλέφωνο: +30 2132141216, Ηλεκτρονικό ταχυδρομείο:
aep@aepp-procurement.gr, Διεύθυνση στο διαδίκτυο: <http://www.aep-procurement.gr/>

VI.4.2) Φορέας αρμόδιος για τις διαδικασίες διαμεσολάβησης

VI.4.3) Υποβολή προσφυγών

Ακριβείς πληροφορίες σχετικά με την (τις) προθεσμία(-ες) για την υποβολή προσφυγών: Βλ. Ν. 4412/2016, όπως κάθε φορά ισχύει.

VI.4.4) Ημερομηνία αποστολής της παρούσας προκήρυξης: 11/03/2026

Αριστείδης Σωτηρόπουλος

Διευθύνων Σύμβουλος ΕΔΥΤΕ Α.Ε.