



ΟΡΓΑΝΙΣΜΟΣ ΠΛΗΡΩΜΩΝ ΚΑΙ ΕΛΕΓΧΟΥ  
ΚΟΙΝΟΤΙΚΩΝ ΕΝΙΣΧΥΣΕΩΝ ΠΡΟΣΑΝΑΤΟΛΙΣΜΟΥ ΚΑΙ ΕΓΓΥΗΣΕΩΝ  
(Ο.Π.Ε.Κ.Ε.Π.Ε.)

**ΚΑΤΑΧΩΡΙΣΤΕΟ ΣΤΟ ΚΗΜΑΗΣ**

**ΔΙΑΒΑΘΜΙΣΗ ΕΓΓΡΑΦΟΥ: ΔΗΜΟΣΙΟ**

**ΓΡΑΦΕΙΟ ΔΙΟΙΚΗΣΗΣ & ΓΡΑΜΜΑΤΕΙΑΣ Δ. Σ.**

**Αθήνα, 24/03/2025**

**Δ/ΝΣΗ ΔΙΟΙΚΗΤΙΚΗΣ & ΟΙΚΟΝΟΜΙΚΗΣ ΥΠΟΣΤΗΡΙΞΗΣ**

**Αρ. πρωτ.: 21843**

**ΤΜΗΜΑ ΠΡΟΜΗΘΕΙΩΝ**

Πληροφορίες: Βασίλης Σιαμέτης

Τηλ.: 210-8802661

**ΠΡΟΣ: Priority Ε.Π.Ε.**

Σοφοκλή Βενιζέλου 49-51, Λυκόβρυση, Τ.Κ. 141 23

Τηλέφωνο: +30 210 2509900

Ηλεκτρονική διεύθυνση: [info@priority.com.gr](mailto:info@priority.com.gr)

**ΠΡΟΣΚΛΗΣΗ**

**ΘΕΜΑ:** «Έγκριση παροχής υπηρεσιών μετάβασης στην ανανεωμένη έκδοση του προτύπου ISO 27001:2022 για το έτος 2025, με τη διαδικασία της απευθείας ανάθεσης, σύμφωνα με το Νόμο 4412/2016, όπως αυτός έχει τροποποιηθεί και ισχύει, συνολικού προϋπολογισμού έως 30.000 ευρώ πλέον ΦΠΑ».

**Κριτήριο Αξιολόγησης :**

Η πλέον συμφέρουσα από οικονομική άποψη προσφορά βάσει ποιότητας-τιμής.

**Αντικείμενο του έργου**

Η παροχή υπηρεσιών ασφάλειας με σκοπό τη μετάβαση στο ανανεωμένη έκδοση του προτύπου ISO 27001:2022, και συγκεκριμένα:

## 1. Υπηρεσίες

### 1.1 Διαθεσιμότητα τεχνικών

Ο Ανάδοχος υποχρεούται να παρέχει καθ' όλη τη διάρκεια της σύμβασης, ομάδα εξειδικευμένων στελεχών, που θα συνδράμουν στην παροχή των απαιτούμενων υπηρεσιών ασφαλείας, ενώ θα είναι επαρκώς ενημερωμένοι για την τεχνολογική και οργανωτική υποδομή του Ο.Π.Ε.Κ.Ε.Π.Ε., ώστε να μπορούν να υποστηρίξουν άμεσα τις ανάγκες ασφαλείας του Ο.Π.Ε.Κ.Ε.Π.Ε.

Ο Ανάδοχος υποχρεούται καθ' όλη τη διάρκεια της σύμβασης, να έχει ορίσει:

1. Έναν ή περισσότερους Έμπειρους Συμβούλους Ασφάλειας Πληροφοριών (Senior Information Security Consultants).
2. Έναν ή περισσότερους Συμβούλους Ασφάλειας Πληροφοριών (Information Security Consultants).

Ο Ανάδοχος οφείλει κατά την υποβολή της προσφοράς του να προσκομίσει τα βιογραφικά των στελεχών που θα διαθέσει στον ΟΠΕΚΕΠΕ. Ο Ανάδοχος δύναται να αντικαταστήσει τα στελέχη του, κατά τη διάρκεια εκτέλεσης της σύμβασης, μόνο κατόπιν σχετικού αιτήματος προς τον ΟΠΕΚΕΠΕ. Αφού αξιολογηθεί το αίτημα και γίνει αποδεκτό από τον ΟΠΕΚΕΠΕ, ο Ανάδοχος μπορεί να αποσύρει το στέλεχος μετά από πέντε (5) εργάσιμες ημέρες και αφού κατά την εκτίμηση της αρμόδιας Δ/νσης του ΟΠΕΚΕΠΕ (Δ/νσης Πληροφορικής) έχει ενημερώσει επαρκώς τον αντικαταστάτη του.

## 2. Απαιτούμενα Προσόντα

Τα στελέχη του Αναδόχου που θα απαρτίζουν την ομάδα έργου θα πρέπει να διαθέτουν τα ακόλουθα προσόντα, αποδεικνυόμενα με την προσκόμιση του βιογραφικού:

### **Έμπειροι Σύμβουλοι Ασφάλειας Πληροφοριών (Senior Information Security Consultants)**

- Πανεπιστημιακό Τίτλο Σπουδών στην Πληροφορική.
- Δεκαετή (10) επαγγελματική εμπειρία σε Διαχείριση και Διοίκηση Έργων στην Ανάπτυξη, Υλοποίηση και Εφαρμογή Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών, σύμφωνα με τις απαιτήσεις του προτύπου ISO 27001 ή/και στην Ανάλυση και Αξιολόγηση Κινδύνων Ασφάλειας Πληροφοριών (Information Security Risk Assessment).

## 25PROC016521795 2025-03-24

- Πιστοποιημένη γνώση στη διαχείριση Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών κατά ISO 27001 (π.χ. πιστοποίηση επικεφαλής επιθεωρητή για το πρότυπο ISO 27001, ISO 27001 Lead Auditor).
- Αποδεδειγμένη εμπειρία στο αντικείμενο της προστασίας δεδομένων προσωπικού χαρακτήρα (π.χ. Πιστοποιημένος Υπεύθυνος Προστασίας Δεδομένων, Data Protection Officer – DPO).

Επιπροσθέτως, θα πρέπει να διαθέτουν τουλάχιστον δύο από τις ακόλουθες επαγγελματικές πιστοποιήσεις σε θέματα Ασφάλειας Πληροφοριών:

- CISSP (Certified Information Systems Security Professional)
- ISSMP (Information Systems Security Management Professional)
- CCSP (Certified Cloud Security Professional)
- CISM (Certified Information Security Manager)
- ISO/IEC 27005 Risk Manager
- Certified Data Protection Officer
- Business Continuity Manager

### **Σύμβουλοι Ασφάλειας Πληροφοριών (Information Security Consultants)**

- Πανεπιστημιακό Τίτλο Σπουδών στην Πληροφορική.
- Διετή (2) επαγγελματική εμπειρία στην Ανάπτυξη, Υλοποίηση και Εφαρμογή Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών, σύμφωνα με τις απαιτήσεις του προτύπου ISO 27001 ή/και στην Ανάλυση και Αξιολόγηση Κινδύνων Ασφάλειας Πληροφοριών (Information Security Risk Assessment).
- Πιστοποιημένη γνώση στη διαχείριση Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών κατά ISO 27001 (π.χ. πιστοποίηση επιθεωρητή για το πρότυπο ISO 27001, ISO 27001 Lead Auditor).

**Οι πιστοποιήσεις θα προσκομιστούν με την τεχνική προσφορά του Αναδόχου.**

### **3. Αρμοδιότητες**

Το αντικείμενο των εργασιών που θα αναλάβουν τα στελέχη της ομάδας υποστήριξης του Αναδόχου σχετικά με το Σ.Δ.Α.Π. του οργανισμού είναι:

#### **3.1 Αξιολόγηση του υπάρχοντος Σ.Δ.Α.Π.**

Αναθεώρηση / επικαιροποίηση των υφιστάμενων πολιτικών, διαδικασιών, οδηγιών και γενικότερα όλων των εγγράφων του υπάρχοντος Συστήματος Διαχείρισης Ασφάλειας

Πληροφοριών (ΣΔΑΠ) και αναπροσαρμογή των υφιστάμενων ελέγχων σύμφωνα με τις νέες προδιαγραφές.

Για τη συμμόρφωση του οργανισμού με το νέο πρότυπο ISO 27001:2022, είναι σημαντικό οι πολιτικές και οι διαδικασίες να προσαρμοστούν ώστε να υποστηρίξουν τη μετάβαση του οργανισμού σε περιβάλλον cloud. Παράλληλα, θα πρέπει να καλύπτουν τις αυξημένες απαιτήσεις για ασφαλή ανάπτυξη λογισμικού, όπως ορίζει το νέο πρότυπο. Τέλος, απαιτείται η τεκμηρίωση όλων των διαδικασιών του οργανισμού.

Επιπλέον, απαιτείται μελέτη της σχετικής νομοθεσίας που αφορά το Σ.Δ.Α.Π. του οργανισμού, ανασκόπηση και επικαιροποίηση του εγγράφου "Κατάλογος Νομοθεσίας", καθώς και εντοπισμός τυχόν αναγκαίων αλλαγών. Στο πλαίσιο αυτό, θα πρέπει επίσης να εξεταστεί η οδηγία NIS2 και ο πιθανός αντίκτυπός της στο Σ.Δ.Α.Π.

## **Παραδοτέα:**

- **Gap Analysis (Ανάλυση Κενών)** που θα παρουσιάζει τις πιθανές αλλαγές που θα πρέπει να γίνουν στο Σ.Δ.Α.Π.
- **Ενημέρωση των αρχείων του Σ.Δ.Α.Π. του οργανισμού σύμφωνα με το νέο πρότυπο ISO 27001:2022 και πιθανές αλλαγές που προκύπτουν από την αναθεώρηση της ισχύουσας νομοθεσίας (π.χ. NIS2 οδηγία).**

## **3.2. Εκτίμησης Κινδύνων Ασφάλειας Πληροφοριών**

Διενέργεια Μελέτης Εκτίμησης Κινδύνων Ασφάλειας Πληροφοριών (Risk Assessment) για το σύνολο των πόρων του οργανισμού, καταγραφή στο εργαλείο Αξιολόγησης Κινδύνων Monarc και εξαγωγή του Πλάνου Διαχείρισης των Κινδύνων (Risk Treatment Plan)

## **Παραδοτέα:**

- **Μελέτη Εκτίμησης Κινδύνων Ασφάλειας Πληροφοριών (Risk Assessment)**
- **Πλάνο Διαχείρισης των Κινδύνων (Risk Treatment Plan)**

## **3.3. Επιχειρησιακή Συνέχεια**

Επικαιροποίηση της υπάρχουσας Εκτίμησης Επιχειρησιακών Επιπτώσεων (BIA) και ενημέρωση Σχεδίου Επιχειρησιακής Συνέχειας (BCP)

**Παραδοτέα:**

- Σχέδιο Επιχειρησιακής Συνέχειας (BCP)
- Εκτίμηση Επιχειρησιακών Επιπτώσεων (BIA)
- Σενάρια ελέγχου Επιχειρησιακής Συνέχειας
- Εκπαίδευση συμβαλλόμενων στο σχέδιο Επιχειρησιακής Συνέχειας

**3.4. Σχέδιο Ανάκαμψης από Καταστροφή**

Επικαιροποίηση του Σχεδίου Ανάκαμψης από Καταστροφή (DRP)

**Παραδοτέα:**

- Σχέδιο Ανάκαμψης από Καταστροφή (DRP)

**3.5. Εσωτερικές Επιθεωρήσεις**

Σχετικά με τις Εσωτερικές Επιθεωρήσεις του οργανισμού ο ανάδοχος θα πρέπει να επιθεωρήσει την Κεντρική Υπηρεσία (ΚΥ) καθώς και το Data Center του Ο.Π.Ε.Κ.Ε.Π.Ε και να καταχωρήσει πιθανά ευρήματα στο περιβάλλον καταχώρησης του οργανισμού (eQual Suite ή σε νέα πλατφόρμα εφόσον υπάρχει η σύμφωνη γνώμη του οργανισμού).

**Παραδοτέα:**

- Αναφορά εσωτερικών επιθεωρήσεων ΚΥ και Data Center του Ο.Π.Ε.Κ.Ε.Π.Ε και καταχώριση σχετικών ευρημάτων σε ειδική εφαρμογή του οργανισμού.

**3.6. Μέτρηση και Στοχοθεσία**

Θέσπιση ενδεδειγμένου Προγράμματος Μέτρησης του Επιπέδου Ασφάλειας, βάσει του οποίου θα αξιολογείται το επίπεδο ασφάλειας στο οποίο βρίσκεται ανά πάσα στιγμή ο οργανισμός, μέσω του καθορισμού συγκεκριμένων, μετρήσιμων και αντικειμενικών δεικτών.

**Παραδοτέα:**

- Επικαιροποιημένο έντυπο Δείκτες Στόχοι
- Επικαιροποιημένο έντυπο Πλάνο Επίτευξης Στόχων

**3.7. Εξωτερική επιθεώρηση**

- Παροχή καθοδήγησης και υποστήριξης κατά τη διάρκεια της επιθεώρησης από τον εξωτερικό φορέα πιστοποίησης για την επαναπιστοποίηση κατά ISO 27001:2022.

- Διασφάλιση ότι το σύστημα συμμορφώνεται πλήρως με τις απαιτήσεις του προτύπου, διευκολύνοντας τη διαδικασία πιστοποίησης.

### 3.8. Συνεχής υποστήριξη

Παροχή συνεχούς υποστήριξης για την επίλυση ζητημάτων και την προσαρμογή του ΣΔΑΠ σε ενδεχόμενες αλλαγές, ώστε να διατηρείται η αποτελεσματικότητα και η συμμόρφωση του συστήματος.

## 4. Διοίκηση έργου

Η ομάδα έργου και ιδιαίτερα τα στελέχη που θα απασχολούνται στο κτίριο της Κεντρικής Υπηρεσίας θα συνεργάζονται με τους υπαλλήλους του Ο.Π.Ε.Κ.Ε.Π.Ε. και θα ακολουθούν τις υποδείξεις και τις οδηγίες του Προϊστάμενου της Δ/σης Πληροφορικής και των Προϊσταμένων του Τμήματος Ανάπτυξης Εφαρμογών και Ασφάλειας Συστημάτων και του Τμήματος Υποστήριξης Συστημάτων και Εφαρμογών του Ο.Π.Ε.Κ.Ε.Π.Ε.

Μετά την κατακύρωση της προμήθειας υπηρεσιών η ομάδα του Αναδόχου, σε συνεργασία με τα στελέχη του ΟΠΕΚΕΠΕ θα καταρτίσουν πλάνο εργασιών με τον καθορισμό ημερομηνιών παράδοσης των προς μελέτη αντικειμένων.

### 4.1 Χρονοπρογραμματισμός έργου

Το πλάνο είναι ενδεικτικό και μπορεί να τροποποιηθεί ανάλογα με τις ανάγκες του έργου κάθε φορά. Ακολουθώς παρατίθεται περιγραφή του έργου ανά φάση.

## Φάση 1: Ανασχεδιασμός και Προσαρμογή

### Αντικείμενο Φάσης:

Επισκόπηση των τρεχόντων πολιτικών και διαδικασιών για τον εντοπισμό κενών με βάση το ISO 27001:2022 και αναθεώρηση ΣΔΑΠ.

### Στόχοι:

- Μελέτη υπάρχοντος ΣΔΑΠ σύμφωνα με το ανανεωμένο πρότυπο **ISO 27001:2013**  
Και της οδηγίας **NIS2**
- Αναθεώρηση / επικαιροποίηση των υφιστάμενων πολιτικών, διαδικασιών, οδηγιών, προτύπων ασφαλείας και γενικότερα όλων των εγγράφων του υπάρχοντος Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών και ανάπτυξη νέων εγγράφων, εφόσον κριθεί αναγκαίο.

ΚΩΔ.	Τίτλος Παραδοτέου
------	-------------------

Π1.1	Gap Analysis που θα παρουσιάζει τις πιθανές αλλαγές που θα πρέπει να γίνουν στο Σ.Δ.Α.Π.
------	--

Π1.2	Αναθεώρηση του συνόλου των εγγράφων του υπάρχοντος Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών σύμφωνα με το ανανεωμένο πρότυπο ISO 27001:2022
------	---

## Φάση 2: Πλαίσιο Διαχείρισης Κινδύνων

### Αντικείμενο Φάσης:

Παρακολούθηση και υλοποίηση εργασιών σχετικών με το Σ.Δ.Α.Π. του οργανισμού όπως αυτές ανατίθενται από τα στελέχη του οργανισμού και ολοκληρώνονται από τα στελέχη του αναδόχου.

### Αναλυτικά:

- **Εκτίμηση Κινδύνων Ασφάλειας Πληροφοριών:** Διενέργεια Μελέτης Εκτίμησης Κινδύνων Ασφάλειας Πληροφοριών (Risk Assessment) για το σύνολο των πόρων του οργανισμού, καταγραφή στο αντίστοιχο εργαλείο και εξαγωγή του Πλάνου Διαχείρισης των Κινδύνων (Risk Treatment Plan)
- **Επιχειρησιακή Συνέχεια:** Επικαιροποίηση της υπάρχουσας Εκτίμησης Επιχειρησιακών Επιπτώσεων (BIA) και ενημέρωση Σχεδίου Επιχειρησιακής Συνέχειας (BCP). Έλεγχος Σχεδίου Επιχειρησιακής Συνέχειας και καταχώρηση σχετικών ευρημάτων. Εκπαίδευση συμβαλλόμενων στο νέο σχέδιο Επιχειρησιακής Συνέχειας.
- **Σχέδιο Ανάκαμψης από Καταστροφή:** Επικαιροποίηση του Σχεδίου Ανάκαμψης από Καταστροφή (DRP)

ΚΩΔ.	Τίτλος Παραδοτέου
------	-------------------

Π2.1	Risk Assessment
------	-----------------

Π2.2	Risk Treatment Plan
------	---------------------

Π2.3	BIA (Business Impact Analysis)
------	--------------------------------

Π2.4	BCP (Business Continuity Plan)
------	--------------------------------

Π2.5	DRP (Disaster Recovery Plan)
------	------------------------------

**Φάση 3: Προετοιμασία για Έλεγχο****Αντικείμενο Φάσης:**

Διενέργεια εσωτερικού ελέγχου πριν τον έλεγχο επαναπιστοποίησης από τον εξωτερικό επιθεωρητή.

## Αναλυτικά:

- **Εσωτερικές επιθεωρήσεις:** Επιθεώρηση Data Center και Κεντρικής Υπηρεσίας του οργανισμού σύμφωνα με το ανανεωμένο πρότυπο Σ.Δ.Α.Π. και καταχώρηση πιθανών ευρημάτων σε ειδική εφαρμογή του οργανισμού.
- **Μέτρηση και στοχοθεσία:** Θέσπιση ενδεδειγμένου Προγράμματος Μέτρησης του Επιπέδου Ασφάλειας, βάσει του οποίου θα αξιολογείται το επίπεδο ασφάλειας στο οποίο βρίσκεται ανά πάσα στιγμή ο οργανισμός, μέσω του καθορισμού συγκεκριμένων, μετρήσιμων και αντικειμενικών δεικτών. Ανασκόπηση Πλάνου Επίτευξης Στόχων και προετοιμασία νέου πλάνου για το νέο έτος.
- **Συμβουλευτική υποστήριξη** κατά τη διάρκεια ελέγχου από τον φορέα πιστοποίησης.

**ΚΩΔ.****Τίτλος Παραδοτέου****Π3.1**

Αναφορές εσωτερικών επιθεωρήσεων

**Π3.2**

Επικαιροποιημένο έντυπο Δείκτες Στόχοι (E10.4-01) και Επικαιροποιημένο έντυπο Πλάνου Επίτευξης Στόχων (E10.4-02)

**Προϋπολογισμός – Πληρωμή**

Ο προϋπολογισμός του έργου υπολογίζεται έως € **30.000,00 πλέον ΦΠΑ**.

Σε συνέχεια των ανωτέρω, καλείστε να υποβάλλετε στον Ο.Π.Ε.Κ.Ε.Π.Ε. (Τμήμα Πρωτοκόλλου, Δομοκού 5, Τ.Κ. 10445, Αθήνα) την τεχνικοοικονομική προσφορά σας, έως τις 31 / 03 /2025 και ώρα 11.00 π.μ.



Η επιστολή αυτή αποτελεί πρόσκληση για την υποβολή της προσφοράς και δεν δεσμεύει καθ' οιονδήποτε τρόπο τον Ο.Π.Ε.Κ.Ε.Π.Ε., ο οποίος θα αναλάβει υποχρέωση έναντι του αναδόχου, μόνον με την υπογραφή της σχετικής σύμβασης.

**Ο ΠΡΟΕΔΡΟΣ ΤΟΥ Ο.Π.Ε.Κ.Ε.Π.Ε.**

**ΝΙΚΟΛΑΟΣ ΣΑΛΑΤΑΣ**

**Εσωτερική διανομή :**

- ΓΡΑΦΕΙΟ ΔΙΟΙΚΗΣΗΣ & ΓΡΑΜΜΑΤΕΙΑΣ Δ.Σ.
- Δ/ΝΣΗ ΤΕΧΝΙΚΩΝ ΕΛΕΓΧΩΝ