

**ΠΡΟΣΚΛΗΣΗ ΣΥΛΛΟΓΗΣ ΠΡΟΣΦΟΡΩΝ**

ΘΕΜΑ: Υπηρεσίες υποστήριξης προς τον υπεύθυνο ασφαλείας συστημάτων πληροφορικής και επικοινωνίας (Υ.Α.Σ.Π.Ε.) ΠΟΧ, ΚΥΑΑ Κ. Πρίφτης & ΓΝΘ και υπηρεσίες συμμόρφωσης με τον νομό 4961/2022 & 5160/2024

ΣΧΕΤΙΚΑ :

- α. Ν.4412/16 και τις λοιπές διατάξεις κείμενης νομοθεσίας
β. Υπ' αριθμ. 39(θέμα 03)/17-10-2025 απόφαση του Δ.Σ. της Α.Ε.Μ.Υ. Α.Ε. με ΑΔΑ:999ΘΟΡΡ3-6Τ1

Προϋπολογισμός : 30.000 ευρώ συμπεριλαμβανομένου ΦΠΑ 24%

ΧΡΟΝΟΣ ΔΙΕΝΕΡΓΕΙΑΣ ΔΙΑΓΩΝΙΣΜΟΥ

ΤΟΠΟΣ ΥΠΟΒΟΛΗΣ ΠΡΟΣΦΟΡΩΝ	ΤΕΛΙΚΗ ΗΜΕΡΟΜΗΝΙΑ ΥΠΟΒΟΛΗΣ ΠΡΟΣΦΟΡΩΝ	ΤΕΛΙΚΗ ΗΜΕΡΑ ΥΠΟΒΟΛΗΣ ΠΡΟΣΦΟΡΩΝ	ΤΕΛΙΚΗ ΩΡΑ ΥΠΟΒΟΛΗΣ ΠΡΟΣΦΟΡΩΝ
Γεωργίου Δαμάσκου 1, Πολυκλινική Ολυμπιακού Χωριού, τ.κ. 13677,) ή στο mail: kbaliousi@aemy.gr	05/12/2025	Παρασκευή	12:00

ΠΕΡΙΓΡΑΦΗ ΕΡΓΟΥ

Υπηρεσίες Υποστήριξης προς τον Υπεύθυνο Ασφαλείας Συστημάτων και Επικοινωνιών (Υ.Α.Σ.Π.Ε)

Οι υπηρεσίες του Συμβούλου θα αφορούν στην πλήρη υποστήριξη των καθηκόντων του Υ.Α.Σ.Π.Ε. που είναι:

- α) η διαρκής μέριμνα για την ασφάλεια των συστημάτων δικτύου και πληροφοριών του φορέα κατά την έννοια της περ. 2 του άρθρου 3 του ν. 4577/2018 (Α' 199),
- β) η συνεργασία με τους αρμόδιους φορείς στον τομέα της κυβερνοασφάλειας και η μέριμνα για την εφαρμογή των κατευθυντήριων οδηγιών, απαιτήσεων και μέτρων ασφαλείας που εκδίδουν,
- γ) η τήρηση μητρώου του φορέα με τις υποδομές πληροφορικής και επικοινωνιών, το λογισμικό και τα πληροφοριακά αγαθά,
- δ) η συμμετοχή στη διενέργεια ελέγχων σε συστήματα πληροφορικής και επικοινωνιών του φορέα για τη διακρίβωση του υφιστάμενου επιπέδου ασφαλείας,
- ε) η εποπτεία της τήρησης της πολιτικής ασφαλείας συστημάτων πληροφορικής και επικοινωνιών του φορέα,
- στ) η παρακολούθηση και αξιοποίηση νέων τεχνολογιών και εργαλείων ασφαλείας συστημάτων πληροφορικής και επικοινωνιών για την ενίσχυση του επιπέδου κυβερνοασφάλειας του φορέα και
- ζ) η διενέργεια αξιολογήσεων του επιπέδου κυβερνοασφάλειας του φορέα σε συνεργασία με τις κατά περίπτωση αρμόδιες αρχές.

Ο Υ.Α.Σ.Π.Ε. δεσμεύεται, κατά την εκτέλεση των καθηκόντων του, από την τήρηση της εμπιστευτικότητας και του απορρήτου που προβλέπεται από ειδικές διατάξεις της εθνικής και της ενωσιακής νομοθεσίας.

Οι υπηρεσίες του Συμβούλου αναλύονται ως εξής:

Φάση 1η: Έλεγχος – αξιολόγηση του τρέχοντος επιπέδου ασφαλείας

Αρχικά ο Σύμβουλος θα προβεί σε λεπτομερή έλεγχο - αξιολόγηση του τρέχοντος επιπέδου ασφαλείας για τα πληροφοριακά συστήματα, τις εφαρμογές, τα λογισμικά, τις δικτυακές υποδομές και τις διαδικασίες και πολιτικές που τηρούνται στον Οργανισμό με βάση δομημένο ερωτηματολόγιο που διαθέτει για το σκοπό αυτό. Ως αποτέλεσμα του ελέγχου θα παραδοθεί αναλυτική Αναφορά, η οποία θα περιέχει όχι μόνο τα ευρήματα – αποκλίσεις, αλλά και τις προτάσεις αποκατάστασής τους.

Φάση 2η: Διενέργεια Vulnerability Assessment & Penetration Testing

Ο Σύμβουλος με εξειδικευμένα εργαλεία που έχει στην κατοχή του θα διενεργήσει στα συστήματα και στις υποδομές, Vulnerability Assessment (σε τετραμηνιαία βάση & Penetration Testing (σε ετήσια βάση) προκειμένου να εντοπιστούν κενά ασφαλείας και να καταγραφούν οι πιθανές ευπάθειες των συστημάτων πληροφορικής και επικοινωνιών. Ο

Έλεγχος Διείσδυσης εκτελείται σε κατάσταση “White Box”, δηλαδή, εκ των έσω και με γνωστή την δομή του εσωτερικού δικτύου. Ως εργαλείο για τον Έλεγχο Διείσδυσης θα χρησιμοποιηθεί περιβάλλον LINUX, και ειδικότερα η πλατφόρμα NESSUS, σε διαμόρφωση KALI. Μετά την υλοποίηση κάθε ελέγχου θα παραδίδεται αναλυτική Αναφορά με τα ευρήματα ανά επίπεδο κινδύνου.

Φάση 3η: Αξιολόγηση Κινδύνων Ασφάλειας για τα Πληροφοριακά Στοιχεία

Με βάση τα αποτελέσματα του Ελέγχου Συμμόρφωσης και των Vulnerability Assessment & Penetration Testing ο Σύμβουλος θα υποστηρίξει τον Οργανισμό στην αξιολόγηση Κινδύνων Ασφάλειας για τα Πληροφοριακά Στοιχεία (πόρους), όπως σταθμούς εργασίας, εξυπηρετητές, δίκτυα, λογισμικά κλπ. Η αξιολόγηση θα δημιουργήσει ένα πλήρες μητρώο κινδύνων και θα αναδείξει τις περιοχές υψηλής επικινδυνότητας, για τις οποίες θα προταθούν μέτρα αντιμετώπισης, ενώ θα υπολογιστεί και ο υπολειπόμενος κίνδυνος μετά την υλοποίηση των μέτρων.

Φάση 4η: Σύνταξη Πολιτικών και Διαδικασιών Ασφαλείας

Ως αποτέλεσμα των προηγούμενων Φάσεων ο Σύμβουλος θα υποστηρίξει τον Οργανισμό στη Σύνταξη Πολιτικών και Διαδικασιών Ασφαλείας. Σχεδιασμός Πολιτικών και Διαδικασιών, οι οποίες καλύπτουν όλες τους τομείς κυβερνοασφάλειας, όπως ασφάλεια προσβάσεων, ορθή χρήση εξοπλισμού, ασφάλεια δικτύων, φυσική ασφάλεια, διαχείριση περιστατικών, επιχειρησιακή συνέχεια, κλπ. Το σύνολο των Πολιτικών και Διαδικασιών θα είναι πλήρως συμβατό με τις απαιτήσεις του Νόμου 5160/2024 και τα διεθνή πρότυπα Ασφάλειας, ούτως ώστε μελλοντικά, να υπάρχει η δυνατότητα άμεσης πιστοποίησης του Οργανισμού με το πρότυπο ISO 27001.

Ενδεικτικές επιμέρους πολιτικές:

Γενική πολιτική ασφάλειας πληροφοριών
Πολιτική ελέγχου πρόσβασης
Πολιτική διαχείρισης αγαθών
Πολιτική ορθής χρήσης αγαθών και δεδομένων
Πολιτική αφαιρούμενων μέσων αποθήκευσης
Πολιτική διαχείρισης περιστατικών κυβερνοασφάλειας
Πολιτική ασφάλειας εφοδιαστικής αλυσίδας
Πολιτική ασφάλειας δικτύων
Πολιτική διενέργειας ελέγχων κυβερνοασφάλειας
Πολιτική αντιγράφων ασφαλείας
Πολιτική κρυπτογράφησης δεδομένων και επικοινωνιών
Πολιτική φυσικής και περιβαλλοντικής ασφάλειας.

Ενδεικτικές Διαδικασίες Ασφάλειας Πληροφοριών:

Διαχείριση κινδύνων Ασφάλειας Πληροφοριών
Διαχείριση Προσωπικού (απόδοση, τροποποίηση και αφαίρεση δικαιωμάτων πρόσβασης)



Διαχείριση Ασφαλούς Ανάπτυξης Εφαρμογών
 Διαχείριση Αλλαγών σε Πληροφοριακά Συστήματα και Υποδομές
 Εκπαίδευση και Ευαισθητοποίηση σε θέματα κυβερνοασφάλειας
 Διαχείριση περιστατικών κυβερνοασφάλειας
 Επιχειρησιακή συνέχεια και διαχείριση κρίσεων

Φάση 5η: Ετήσια Υποστήριξη Υπευθύνου Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.)

Ο Σύμβουλος με τους εξειδικευμένους συνεργάτες του θα παρέχει συνεχή υποστήριξη στον ΥΑΣΠΕ της Εταιρείας που περιλαμβάνουν τις παρακάτω υπηρεσίες:

Υποστήριξη στην πληροφόρηση για το ευρύτερο περιβάλλον κυβερνοασφάλειας και τους νέους κινδύνους που απειλούν τους οργανισμούς και τους τρόπους προστασίας (threat intelligence).

Υποστήριξη στη διαχείριση Περιστατικών. Στην περίπτωση που εντοπιστεί Περιστατικό Ασφάλειας, ο Σύμβουλος θα συνδράμει τον ΥΑΣΠΕ στη διαχείρισή του με την εμπειρία και την τεχνογνωσία του.

Υποστήριξη στην επικαιροποίηση της Αξιολόγησης Κινδύνων Ασφάλειας. Ο Σύμβουλος θα παρέχει διαρκή υποστήριξη στον ΥΑΣΠΕ για την επικαιροποίηση της Αξιολόγησης Επικινδυνότητας και την ενσωμάτωση πιθανών νέων περιπτώσεων απειλών στη μελέτη.

Έλεγχος εφαρμογής Πολιτικών και Διαδικασιών Ασφάλειας. Ο Σύμβουλος θα εκτελεί σε ετήσια βάση έλεγχο επιπέδου εφαρμογής των εγκεκριμένων Πολιτικών και Διαδικασιών Ασφάλειας και υποστηρίζει τον ΥΑΣΠΕ στην επικαιροποίησή τους εφόσον απαιτείται.

Εκπαίδευση προσωπικού. Ο Σύμβουλος θα αναλάβει τη συνεχή εκπαίδευση του ΥΑΣΠΕ και του αρμόδιου προσωπικού πάνω στους βασικούς κανόνες ασφάλειας πληροφοριών και στην εφαρμογή των πολιτικών ασφαλείας που θα έχουν εγκριθεί από τη Διοίκηση του Οργανισμού.

Παραδοτέα:

Έλεγχος – αξιολόγηση του τρέχοντος επιπέδου ασφαλείας για τα πληροφοριακά συστήματα, τις εφαρμογές, τα λογισμικά, τις δικτυακές υποδομές και τις διαδικασίες και πολιτικές

Τρεις Αναφορές Vulnerability Assessment (σε ετήσια βάση)

Αναφορά Penetration Testing

Αξιολόγηση Κινδύνων Ασφάλειας για τα Πληροφοριακά Στοιχεία

Εγχειρίδιο Πολιτικών και Διαδικασιών Ασφαλείας

Αναφορές Ελέγχου Εφαρμογής Πολιτικών και Διαδικασιών Ασφάλειας (σε ετήσια βάση)

Αναφορές Threat Intelligence

Αναφορές διαχείρισης περιστατικών ασφαλείας (εφόσον υπάρξει περιστατικό)

Εκπαιδευτικό υλικό

ΓΕΝΙΚΟΙ ΟΡΟΙ :

- Ισχύς Προσφορών: 60 ημέρες κατ' ελάχιστο.



- Αποστολή προσφορών: Ανοιχτές προσφορές στο email: **kbaliousi@aemy.gr** έως **05/12/2025** ημέρα Παρασκευή και ώρα 12:00 μ.μ.
- Τρόπος Πληρωμής: Με δέσμευση του ποσού των ΚΑΕ 61.98.16.00 του προϋπολογισμού έτους χρήσης 2026 της ΑΕΜΥ Α.Ε. και εντός 60 ημερών από την έκδοση τιμολογίου και την οριστική παραλαβή του.
- Τα έξοδα αποστολής βαρύνουν τον ανάδοχο.
- Στην υποβληθείσα προσφορά θα πρέπει να υπάρχει ρητή αναφορά ότι συμμορφώνεται πλήρως με τις τεχνικές προδιαγραφές της παρούσας πρόσκλησης.
- Η προσφορά θα πρέπει να φέρει σφραγίδα και υπογραφή .
- Για ποσά πάνω από 1.500€ είναι απαραίτητη η προσκόμιση φορολογικής ενημερότητας και για ποσά πάνω από 3.000€ είναι απαραίτητη η προσκόμιση φορολογικής και ασφαλιστικής ενημερότητας.
- Ο ΑΝΑΔΟΧΟΣ υποχρεούται στην έκδοση ΗΛΕΚΤΡΟΝΙΚΩΝ ΤΙΜΟΛΟΓΙΩΝ σύμφωνα με τις διατάξεις της υπ' αριθμ. 52445 ΕΞ 2023 ΚΥΑ «Υποχρέωση υποβολής ηλεκτρονικών τιμολογίων από τους οικονομικούς φορείς» ΦΕΚ 2385/τ. Β'/12.04.2023.

Μαρία Θεοδοροπούλου

Διευθύνουσα Σύμβουλος ΑΕΜΥ Α.Ε.