ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΔΙΟΙΚΗΣΗ 6ης Υ.ΠΕ.
ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ – Κ.Υ. ΦΙΛΙΑΤΩΝ

ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Γενικό Νοσοκομείο - Κ.Υ. Φιλιατών
Ημερομηνία: 12/06/2026
Αρ. Πρωτ.: 9306

Τμήμα : Διοικητικό Οικονομικό
Ταχ. Διευθ. : Π. Μπέμπη 10
Ταχ. Κώδ. : 46300 Φιλιάτες
Πληροφορίες : Α.Τσούπη
Τηλέφωνο : 26643 60375
E-mail : tsoupia@gnfiliaton.gr

ΠΡΟΣ: ΥΠΟΨΗΦΙΟΥΣ ΑΝΑΔΟΧΟΥΣ

ΠΡΟΣΚΛΗΣΗ ΕΚΔΗΛΩΣΗΣ ΕΝΔΙΑΦΕΡΟΝΤΟΣ

ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ 25.000,00€ ΜΕ Φ.Π.Α

ΘΕΜΑ : Κατάθεση Προσφοράς, για την προμήθεια υπηρεσιών για :
(α) Διενέργεια Ελέγχου Ευπαθειών Δικτύου (Penetration Test),
(β) Αξιολόγηση Ευπαθειών Δικτύου (Vulnerability Assessment),
(γ) Σύνταξη Σχέδιου Συμμόρφωσης (Compliance Plan),
(δ) Σύνταξη Αναφορά Συνολικού Κινδύνου (Cybersecurity Risk Report),
(ε) Σύνταξη Σχέδιου Συμμόρφωσης (Compliance Plan),
(στ) Σύνταξη Πολιτικής Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών από απειλές όπως: κυβερνοεπιθέσεις, παραβιάσεις συστημάτων, διαρροές δεδομένων και κλοπή, συμμορφούμενες κατά NIS 2 για το Γεν. Νοσοκομείο – Κ.Υ Φιλιατών.

ΣΧΕΤ. : **α)** Ο Ν. 3329/2005 «Εθνικό Σύστημα Υγείας και Κοινωνικής Αλληλεγγύης και λοιπές διατάξεις» (Φ.Ε.Κ. Α’ 81 /4-4-2005), όπως ισχύει σήμερα.
β) Ο Ν. 3580/2007 «Προμήθειες Φορέων εποπτευόμενων από το Υπουργείο Υγείας και Κοινωνικής Αλληλεγγύης και άλλες διατάξεις» (Φ.Ε.Κ. Α’ 134 /18-6-2007) όπως ισχύει σήμερα.
γ) Ο Ν. 4412/2016 «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών (προσαρμογή στις Οδηγίες 2014/24/ ΕΕ και 2014/25/ΕΕ)», (Φ.Ε.Κ. 147/Α/8-08-2016).
δ) **Ο** Ν. 4782/2021 «Εκσυγχρονισμός, απλοποίηση και αναμόρφωση του ρυθμιστικού πλαισίου των δημοσίων συμβάσεων, ειδικότερες ρυθμίσεις προμηθειών στους τομείς της άμυνας και της ασφάλειας και άλλες διατάξεις για την ανάπτυξη, τις υποδομές και την υγεία.», (Φ.Ε.Κ. 36/Α/9-03-2021).
ε)Την 17η/14-05-2026 Απόφαση του Διοικητικού Συμβουλίου για έγκριση Τεχνικών Προδιαγραφών και έγκριση Προκήρυξης του Διαγωνισμού.

Καλούνται οι ενδιαφερόμενοι, να καταθέσουν **Κλειστή προσφορά** για την προμήθεια υπηρεσιών για :
(α) Διενέργεια Ελέγχου Ευπαθειών Δικτύου (Penetration Test),
(β) Αξιολόγηση Ευπαθειών Δικτύου (Vulnerability Assessment),
(γ) Σύνταξη Σχέδιου Συμμόρφωσης (Compliance Plan),
(δ) Σύνταξη Αναφορά Συνολικού Κινδύνου (Cybersecurity Risk Report),
(ε) Σύνταξη Σχέδιου Συμμόρφωσης (Compliance Plan),

(στ) Σύνταξη Πολιτικής Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών από απειλές όπως: κυβερνοεπιθέσεις, παραβιάσεις συστημάτων, διαρροές δεδομένων και κλοπή, συμμορφούμενες κατά NIS 2 για το Γεν. Νοσοκομείο – Κ.Υ Φιλιατών, σύμφωνα με τις επισυναπτόμενες τεχνικές προδιαγραφές, με κριτήριο κατακύρωσης την πλέον συμφέρουσα από οικονομική άποψη προσφορά μόνο βάσει της τιμής

Η παρών εκδήλωση αφορά την «Εναρμόνιση του Γενικού Νοσοκομείου ΚΥ Φιλιατών στις απαιτήσεις του ν. 4961/2022 και ν. 5160/2024 – Σχέδιο Ανάλυσης Κινδύνου και Ενιαία Πολιτική ασφάλειας Συστημάτων Πληροφορικής και Υπηρεσίες Υπεύθυνου Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (ΥΑΣΠΕ)»

1. ΔΙΚΑΙΟΛΟΓΗΤΙΚΑ ΣΥΜΜΕΤΟΧΗΣ

Α. Ο υποψήφιος ανάδοχος υποχρεούται να καταθέσει με την προσφορά του υπεύθυνη δήλωση που θα δηλώνει ότι:

1) Αποδέχεται πλήρως και ανεπιφύλακτα τους όρους της διακήρυξης.

Κριτήριο κατακύρωσης η πλέον συμφέρουσα από οικονομική άποψη προσφορά βάσει τιμής.

Οι προσφορές πρέπει να είναι καθαρογραμμένες χωρίς σβησίματα, προσθήκες, διορθώσεις. Εάν υπάρχει στην προσφορά οποιαδήποτε διόρθωση αυτή πρέπει να είναι καθαρογραμμένη και μονογραμμένη από τον προσφέροντα. Θα φέρουν τον τίτλο της εταιρείας ή του ιδιώτη και θα απευθύνονται προς την υπηρεσία που διενεργεί την Πρόσκληση Ενδιαφέροντος. Θα φέρουν σαν τίτλο την προμήθεια που αφορά και τον αριθμό της Πρόσκλησης Ενδιαφέροντος, στοιχεία που θα πρέπει να αναφέρονται και στο εξωτερικό του φακέλου που τις περιέχει.

Οι προσφορές υποβάλλονται μέσα σε φάκελο σφραγισμένο που θα περιέχει: **Υποφάκελλο δικαιολογητικών συμμετοχής, υποφάκελλο τεχνικής προσφοράς και υποφάκελλο οικονομικής προσφορά**ς.

1. Ο υποφάκελος των δικαιολογητικών θα περιέχει :

Α) Απόσπασμα του σχετικού μητρώου, όπως του ποινικού μητρώου ή, ελλείψει αυτού, ισοδύναμο έγγραφο που εκδίδεται από αρμόδια δικαστική ή διοικητική αρχή του κράτους-μέλους ή της χώρας καταγωγής ή της χώρας όπου είναι εγκατεστημένος ο οικονομικός φορέας, από το οποίο προκύπτει ότι πληρούνται αυτές οι προϋποθέσεις, που να έχει εκδοθεί έως τρεις (3) μήνες πριν από την υποβολή του . Η υποχρέωση προσκόμισης του ως άνω αποσπάσματος αφορά και στα μέλη του διοικητικού, διευθυντικού ή εποπτικού οργάνου του εν λόγω οικονομικού φορέα ή στα πρόσωπα που έχουν εξουσία εκπροσώπησης, λήψης αποφάσεων ή ελέγχου σε αυτό κατά τα ειδικότερα αναφερόμενα στην ως παράγραφο 1 του άρθρου 73 του Ν.4412/2016.

Εναλλακτικά μπορεί να προσκομιστεί υπεύθυνη δήλωση εκ μέρους του οικονομικού φορέα, σε περίπτωση φυσικού προσώπου ότι δεν συντρέχουν οι λόγοι αποκλεισμού της παραγράφου 1 του άρθρου 73 του Ν.4412/2016. Σε περίπτωση νομικού προσώπου η προαναφερόμενη υπεύθυνη δήλωση υποβάλλεται εκ μέρους του νομίμου εκπροσώπου του, όπως αυτός ορίζεται στην περίπτωση 79Α του Ν.4412/2016 και αφορά ιδίως: αα) στις περιπτώσεις εταιρειών περιορισμένης ευθύνης (Ε.Π.Ε.) και προσωπικών εταιρειών (Ο.Ε. και Ε.Ε.), τους διαχειριστές, β) στις περιπτώσεις ανωνύμων εταιρειών (Α.Ε.), τον Διευθύνοντα Σύμβουλο, καθώς και όλα τα μέλη του Διοικητικού Συμβουλίου. (άρθρο 80 παρ. 9 του Ν.4412/2016, όπως συμπληρώθηκε με την παρ. 7αγ του άρθρου 43 του Ν.4506/2019)

Η υπεύθυνη δήλωση γίνεται αποδεκτή εφόσον έχει συνταχθεί μετά την κοινοποίηση της παρούσας πρόσκλησης. (άρθρο 80 παρ.12 του Ν.4412/2016, όπως προστέθηκε με την παρ.7αδ του άρθρου 43 του Ν.4605/2019)

Βάσει του άρθρου 73, παρ: 11, για δημόσιες συμβάσεις σε δημόσιες συμβάσεις με εκτιμώμενη αξία ίση ή κατώτερη των δύο χιλιάδων πεντακοσίων (2.500) ευρώ χωρίς Φ.Π.Α. δεν απαιτείται το παρόν δικαιολογητικό συμμετοχής με την υποβολή της προσφοράς.

Β) Φορολογική ενημερότητα εν ισχύ κατά το χρόνο υποβολής της, άλλως, στην περίπτωση που δεν αναφέρεται σε αυτό χρόνος ισχύος, που να έχει εκδοθεί έως τρεις (3) μήνες πριν από την υποβολή της.

Βάσει του άρθρου 73, παρ: 11, για δημόσιες συμβάσεις σε δημόσιες συμβάσεις με εκτιμώμενη αξία ίση ή κατώτερη των δύο χιλιάδων πεντακοσίων (2.500) ευρώ χωρίς Φ.Π.Α. δεν απαιτείται το παρόν δικαιολογητικό συμμετοχής με την υποβολή της προσφοράς.

Γ) Ασφαλιστική ενημερότητα εν ισχύ κατά το χρόνο υποβολής της, άλλως, στην περίπτωση που δεν αναφέρεται σε αυτό χρόνος ισχύος, που να έχει εκδοθεί έως τρεις (3) μήνες πριν από την υποβολή της.

Βάσει του άρθρου 73, παρ: 11, για δημόσιες συμβάσεις σε δημόσιες συμβάσεις με εκτιμώμενη αξία ίση ή κατώτερη των δύο χιλιάδων πεντακοσίων (2.500) ευρώ χωρίς Φ.Π.Α. δεν απαιτείται το παρόν δικαιολογητικό συμμετοχής με την υποβολή της προσφοράς.

Δ) Για την απόδειξη της νόμιμης εκπροσώπησης, στις περιπτώσεις που ο οικονομικός φορέας είναι νομικό πρόσωπο και υποχρεούται, κατά την κείμενη νομοθεσία, να δηλώνει την εκπροσώπηση και τις μεταβολές της σε αρμόδια αρχή (πχ ΓΕΜΗ), προσκομίζει σχετικό **πιστοποιητικό ισχύουσας εκπροσώπησης,** το οποίο πρέπει να έχει εκδοθεί έως τριάντα (30) εργάσιμες ημέρες πριν από την υποβολή του. Στις λοιπές περιπτώσεις τα κατά περίπτωση νομιμοποιητικά έγγραφα νόμιμης εκπροσώπησης (όπως καταστατικά, αντίστοιχα ΦΕΚ, συγκρότηση Δ.Σ. σε σώμα, σε περίπτωση Α.Ε., κλπ., ανάλογα με τη νομική μορφή του οικονομικού φορέα), συνοδευόμενα από υπεύθυνη δήλωση του νόμιμου εκπροσώπου ότι εξακολουθούν να ισχύουν κατά την υποβολή τους.

Ε) Για την απόδειξη της νόμιμης σύστασης και των μεταβολών του νομικού προσώπου, εφόσον αυτή προκύπτει από πιστοποιητικό αρμόδιας αρχής (πχ γενικό πιστοποιητικό του ΓΕΜΗ), αρκεί η υποβολή αυτού, εφόσον έχει εκδοθεί έως τρεις (3) μήνες πριν από την υποβολή του. Στις λοιπές περιπτώσεις τα κατά περίπτωση νομιμοποιητικά έγγραφα νόμιμης σύστασης και μεταβολών (όπως καταστατικά, πιστοποιητικά μεταβολών, αντίστοιχα ΦΕΚ, κλπ., ανάλογα με τη νομική μορφή του οικονομικού φορέα), συνοδευόμενα από υπεύθυνη δήλωση του νόμιμου εκπροσώπου ότι εξακολουθούν να ισχύουν κατά την υποβολή τους.

Οι αλλοδαποί οικονομικοί φορείς προσκομίζουν τα προβλεπόμενα, κατά τη νομοθεσία της χώρας εγκατάστασης, αποδεικτικά έγγραφα, και εφόσον δεν προβλέπονται, υπεύθυνη δήλωση του νόμιμου εκπροσώπου, από την οποία αποδεικνύονται τα ανωτέρω ως προς τη νόμιμη σύσταση, μεταβολές και εκπροσώπηση του οικονομικού φορέα.

Οι ως άνω υπεύθυνες δηλώσεις γίνονται αποδεκτές, εφόσον έχουν συνταχθεί μετά την κοινοποίηση της πρόσκλησης για την υποβολή των δικαιολογητικών.

Από τα ανωτέρω έγγραφα πρέπει να προκύπτουν η νόμιμη σύσταση του οικονομικού φορέα, όλες οι σχετικές τροποποιήσεις των καταστατικών, το/τα πρόσωπο/α που δεσμεύει/ουν νόμιμα την εταιρία κατά την ημερομηνία διενέργειας του διαγωνισμού (νόμιμος εκπρόσωπος, δικαίωμα υπογραφής κλπ.), τυχόν τρίτοι, στους οποίους έχει χορηγηθεί εξουσία εκπροσώπησης, καθώς και η θητεία του/των ή/και των μελών του οργάνου διοίκησης/ νόμιμου εκπροσώπου.

ΣΤ) Υπεύθυνη Δήλωση του προσφέροντος οικονομικού φορέα ότι δεν έχει εκδοθεί σε βάρος του απόφαση αποκλεισμού, σύμφωνα με το άρθρο 74 του ν. 4412/2016.

2. <u>Ο υποφάκελος της τεχνικής προσφοράς θα περιέχει:</u>

Η προσφορά πρέπει να περιλαμβάνει όλα τα έγγραφα και δικαιολογητικά, βάσει των οποίων θα αξιολογηθεί η καταλληλότητα των προσφερόμενων ειδών, σύμφωνα με τις τεχνικές προδιαγραφές της Πρόσκλησης .

3. <u>Ο υποφάκελος της οικονομικής προσφοράς θα περιέχει:</u>

Την οικονομική προσφορά όπου θα αναφέρεται η τιμή μονάδος του είδους και απαραίτητα ο αύξοντας αριθμός της κατάστασης. Στην τιμή περιλαμβάνονται οι κρατήσεις υπέρ τρίτων και κάθε άλλη επιβάρυνση, εκτός από το ΦΠΑ.

<u>Καταληκτική ημερομηνία υποβολής προσφοράς ορίζεται η 06/07/2026 ημέρα Δευτέρα και ώρα 13:00 μμ στο Γραφείο Πρωτοκόλλου του Νοσοκομείου Φιλιατών.</u>

ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

Τεχνική Περιγραφή που αφορά την «Εναρμόνιση του ΓΝ – ΚΥ Φιλιατών με τις διατάξεις των Νόμων 4961/2022 και 5160/2024 για την κυβερνοασφάλεια»:

Αντικείμενο Έργου

Το παρόν έργο αφορά την επιλογή αναδόχου για την «Εναρμόνιση του Γενικού Νοσοκομείου ΚΥ Φιλιατών στις απαιτήσεις του ν. 4961/2022 και ν. 5160/2024 – Σχέδιο Ανάλυσης Κινδύνου και Ενιαία Πολιτική ασφάλειας Συστημάτων Πληροφορικής και Υπηρεσίες Υπεύθυνου Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (ΥΑΣΠΕ)» σε Ανάδοχο.

Σκοπός του έργου είναι:

- Η κάλυψη των απαιτήσεων των νόμων 4961/2022 και 5160/2024.
- Η υλοποίηση των απαραίτητων ενεργειών βάσει του άρθρου 20 του ν. 4961/2022.
- Η εναρμόνιση του Νοσοκομείου με τις απαιτήσεις της νομοθεσίας για την ενίσχυση της ανθεκτικότητας σε κυβερνοαπειλές.
- Η υλοποίηση των απαραίτητων ενεργειών βάσει των άρθρων 15 και 16 του νόμου 5160/2024.
- Η συμμόρφωση με την Οδηγία 2022/2555 (NIS2) της Ευρωπαϊκής Ένωσης.
- Η παροχή συμβουλευτικών υπηρεσιών στον Υπεύθυνο Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (ΥΑΣΠΕ) για ένα (1) έτος.

Γενική Όροι

Ισχύουσες Διατάξεις

Η υλοποίηση της υπηρεσίας διέπεται από τις ακόλουθες διατάξεις:

- Νόμος 4270/2014 (Αρχές δημοσιονομικής διαχείρισης και εποπτείας).
- Κανονισμός (ΕΕ) 2016/679 (Γενικός Κανονισμός Προστασίας Δεδομένων - GDPR).
- Κανονισμός (ΕΕ) 2019/881 (για τον ENISA – Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια).
- Κανονισμός (ΕΕ) 2021/887 (για τη σύσταση του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας).
- Νόμος 4624/2019 (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του GDPR).
- Νόμος 4577/2018 (Ενσωμάτωση της Οδηγίας 2016/1148/ΕΕ – για μέτρα υψηλού κοινού επιπέδου ασφάλειας συστημάτων δικτύου και πληροφοριών).
- Νόμος 4961/2022 (Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις)
- Ευρωπαϊκή Οδηγία 2022/2555 (NIS2).
- Νόμος 5160/2024 (Ενσωμάτωση της Οδηγίας (ΕΕ) 2022/2555 – Οδηγία NIS2).
- ΦΕΚ 2186/Β/2025 - Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας.

Χρόνος Εκτέλεσης Υπηρεσίας

Η συνολική διάρκεια της υπηρεσίας ορίζεται σε δώδεκα (12) μήνες από την ημερομηνία υπογραφής της Σύμβασης.

Προϋποθέσεις Επαγγελματικής και Τεχνικής Ικανότητας και Εμπειρογνωμοσύνης

Ο υποψήφιος ανάδοχος πρέπει:

- Να είναι πιστοποιημένος με ISO 27001, ISO 90001, ISO 20000-1, ISO 37001, ISO 22301, ISO 27701.
- Να έχει υλοποιήσει τουλάχιστον πέντε (5) έργα συμμόρφωσης με το ν. 5160/2024 σε δημόσια νοσοκομεία.
- Να διαθέτει κατάλληλη ομάδα έργου με τουλάχιστον έξι (6) μέλη για την ολοκλήρωση του έργου.

Η ομάδα έργου πρέπει να διαθέτει τουλάχιστον μέλη με τους εξής ρόλους και προσόντα:

- Υπεύθυνος Έργου / Project Manager:
    - Πανεπιστημιακό δίπλωμα ή πτυχίο (ΑΕΙ) ημεδαπής ή αλλοδαπής.
    - Εικοσαετή (20 έτη) επαγγελματική εμπειρία σε υλοποίηση ή/και διοίκηση έργων πληροφορικής.
    - Θα είναι υπεύθυνος για τη συνολική ευθύνη των εργασιών, τη διοίκηση, την πρόοδο, τον συντονισμό της ομάδας, τη διασφάλιση ποιότητας και την τήρηση προδιαγραφών.
    - Θα αναλάβει την λειτουργική εκπροσώπηση του Αναδόχου έναντι της Αναθέτουσας Αρχής και της Επιτροπής Παραλαβής του Έργου.
- Υπεύθυνος Νομικός Σύμβουλος:
    - Πανεπιστημιακό Πτυχίο (ΑΕΙ) Νομικής, ημεδαπής ή αλλοδαπής.
    - Μεταπτυχιακό Τίτλο σπουδών (ημεδαπής ή αλλοδαπής) σε αντικείμενο σχετικό με το Δίκαιο της Πληροφορικής.
    - Πιστοποίηση ISO/IEC 17024 για Υπεύθυνους Προστασίας Δεδομένων (DPO Executives).
    - Πιστοποίηση Certified Information Privacy Manager (CIPM).
    - Μέλος της Επιτροπής Εμπειρογνωμόνων του Ευρωπαϊκού Συμβουλίου για την προστασία των προσωπικών δεδομένων.
- Υπεύθυνος Ασφάλειας Πληροφοριακών Συστημάτων και Κυβερνοασφάλειας:
    - Πανεπιστημιακό Δίπλωμα (ΑΕΙ) Πληροφορικής, ημεδαπής ή αλλοδαπής.
    - Μεταπτυχιακό Δίπλωμα (ΑΕΙ) Πληροφορικής, ημεδαπής ή αλλοδαπής.
    - Διδακτορικό Δίπλωμα (ημεδαπής ή αλλοδαπής) σε αντικείμενο σχετικό με την προστασία δεδομένων σε ψηφιακά περιβάλλοντα.
    - Συμμετοχή σε δραστηριότητες προτυποποίησης με δημοσιευμένο επιστημονικό έργο.
    - Απαιτείται εμπειρία τουλάχιστον πέντε (5) ετών στην ασφάλεια πληροφοριακών συστημάτων, ειδικότερα των δεδομένων που κυκλοφορούν σε αυτά.

Τόπος παρεχόμενων υπηρεσιών

Ο Ανάδοχος θα παρέχει τις υπηρεσίες από την έδρα του και στους χώρους των αρμόδιων υπηρεσιών του ΓΝ – ΚΥ Φιλιατών.

Εμπιστευτικότητα – Εχεμύθεια

Ο Ανάδοχος υποχρεούται να υπογράψει Συμφωνητικό Εχεμύθειας – Εμπιστευτικότητας με την έναρξη της υπηρεσίας, διασφαλίζοντας την εχεμύθεια των αποτελεσμάτων και των συλλεχθέντων δεδομένων. Το συμφωνητικό καλύπτει όλα τα αποτελέσματα και τις πληροφορίες που θα ανακτηθούν κατά τη διάρκεια του έργου. Ο Ανάδοχος φέρει την ευθύνη για τη διασφάλιση της εμπιστευτικότητας των εμπλεκόμενων συμβούλων, μηχανικών και τεχνικών, όσον αφορά τη μη διαρροή πληροφοριών, του βαθμού διεκπεραίωσης και των λεπτομερειών του έργου.
Όλες οι εκθέσεις, διαγράμματα, σχέδια, πλάνα, στατιστικά στοιχεία και άλλα σχετικά έγγραφα που αποκτώνται ή καταρτίζονται από τον συμβαλλόμενο κατά την εκτέλεση του έργου είναι εμπιστευτικά και ανήκουν στην απόλυτη κυριότητα του Φορέα. Ο συμβαλλόμενος δεν επιτρέπεται να αποκαλύψει πληροφορίες ή να κοινοποιήσει στοιχεία χωρίς την προηγούμενη γραπτή συναίνεση του Φορέα. Σε περίπτωση αθέτησης, ο Φορέας δικαιούται να απαιτήσει αποκατάσταση ζημίας και άμεση παύση της κοινοποίησης. Ο συμβαλλόμενος δεν θα προβαίνει σε δημόσιες δηλώσεις σχετικές με την κατάσταση του Φορέα χωρίς γραπτή άδεια. Δεσμεύεται από την τήρηση του απορρήτου και της εμπιστευτικότητας, φέροντας ευθύνη και για παραβάσεις των μελών της ομάδας του, υπογράφοντας σχετική υπεύθυνη δήλωση αμέσως μετά την υπογραφή της Σύμβασης.

Υποχρεώσεις Αναθέτουσας Αρχής

Ο Φορέας υποχρεούται να διευκολύνει την εργασία του Αναδόχου, παρέχοντας συνεργασία με τη διοίκηση και τους υπηρεσιακούς παράγοντες, καθώς και πρόσβαση σε δεδομένα και πράξεις. Επίσης, πρέπει να διασφαλίσει στον ανάδοχο την πρόσβαση σε εγκαταστάσεις για την άσκηση των καθηκόντων του.

Τεχνική Περιγραφή

Το έργο αφορά την παροχή συμβουλευτικών υπηρεσιών, καθώς και την προσαρμογή και εναρμόνιση του Γενικού Νοσοκομείου ΚΥ Φιλιατών με τις απαιτήσεις του Νόμου 4961/2022 και της Ευρωπαϊκής Οδηγίας NIS2. Στόχος είναι η ενίσχυση της ανθεκτικότητας του Νοσοκομείου έναντι των κινδύνων του Κυβερνοχώρου.
Βάσει της οδηγίας NIS2 (2022/2555), πρέπει να ληφθούν κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων ασφάλειας των συστημάτων δικτύου και πληροφοριών, καθώς και για την πρόληψη ή ελαχιστοποίηση των επιπτώσεων των περιστατικών. Τα μέτρα αυτά, λαμβάνοντας υπόψη τα σύγχρονα πρότυπα και το κόστος εφαρμογής, εξασφαλίζουν επίπεδο ασφάλειας ανάλογο του κινδύνου. Κατά την αξιολόγηση της αναλογικότητας, λαμβάνονται υπόψη η έκθεση σε κινδύνους, η πιθανότητα και η σοβαρότητα των περιστατικών, συμπεριλαμβανομένων των κοινωνικών και οικονομικών επιπτώσεων.
Το έργο θα περιλαμβάνει υπηρεσίες για τη διενέργεια μελέτης εναρμόνισης του Φορέα έναντι του ν. 5160/2024, του προγενέστερου ν. 4961/2022 και της Οδηγίας 2022/2555 (NIS2).
Στο αντικείμενο του έργου συμπεριλαμβάνονται:

- Εγκατάσταση λογισμικού για την κατάρτιση καταλόγου με τις υποδομές πληροφορικής του Φορέα (IT Assets Catalog).
- Report Συνολικού Κινδύνου του Φορέα.
- Disaster Recovery Plan.
- Πλάνο Διαχείρισης Περιστατικών Ασφαλείας.
- Vulnerability Assessment στα συστήματα του Φορέα.

- Πλάνο για την υλοποίηση διορθωτικών ενεργειών.
- Δημιουργία Πολιτικών για την ασφάλεια των συστημάτων πληροφορικής.
- Προσαρμογή στα άρθρα 15 και 16 του Ν. 5160/2024.
- Παροχή Συμβουλευτικών υπηρεσιών στον ΥΑΣΠΕ για ένα (1) έτος.

Αναλυτικά, το αρχικό έργο που θα υλοποιήσει ο Ανάδοχος περιλαμβάνει κατ' ελάχιστο:

- Ανάλυση της τρέχουσας κατάστασης των πληροφοριακών συστημάτων, δικτυακών υποδομών, λογισμικών, εφαρμογών και κάθε στοιχείου που επηρεάζει την επιχειρησιακή συνέχεια του Φορέα.
- Δημιουργία Καταλόγου με όλες τις εκτιμώμενες απειλές που ενδέχεται να εκδηλωθούν στους καταγεγραμμένους πόρους Πληροφορικής.
- Διενέργεια Vulnerability Assessment για την εκτίμηση κινδύνων και την καταγραφή ευπαθειών των συστημάτων πληροφορικής και επικοινωνιών.
- Σύνταξη προτάσεων για βελτίωση του επιπέδου ασφάλειας του Φορέα σε σχέση με την Κυβερνοασφάλεια και τα πληροφοριακά συστήματα.
- Σύνταξη των απαραίτητων προτάσεων για Πολιτικές Ασφάλειας Πληροφοριών και Ασφάλειας συστημάτων Πληροφορικής.
- Σύνταξη διαδικασίας για την επικοινωνία με την Εθνική Αρχή Κυβερνοασφάλειας σε περίπτωση περιστατικών.
- Σύνταξη Disaster Recovery Plan.
- Εκτίμηση του ρίσκου που λαμβάνει ο Φορέας βάσει των υποδομών του.

Η ανωτέρω αξιολόγηση θα περιλαμβάνει τουλάχιστον τα εξής:

- Αξιολόγηση δυνατότητας ικανοποίησης των δικαιωμάτων των φυσικών προσώπων.
- Αξιολόγηση ικανοποιητικού επιπέδου ασφαλείας και επιχειρησιακής συνέχειας.
- Αξιολόγηση επαρκούς οργανωτικής δομής.
- Αξιολόγηση πληροφορικών συστημάτων και πολιτικών που επιβάλλονται από την πληροφορική.
- Αξιολόγηση σχετικών γραπτών πολιτικών και διαδικασιών.
- Αξιολόγηση των υποδομών πληροφορικής και επικοινωνιών του Φορέα.
- Αξιολόγηση των ευπαθειών και των κινδύνων που θα προκύψουν από τη Μελέτη.

Στα πλαίσια του έργου ο Ανάδοχος υποχρεούται να :

- Συμπεριλάβει ανάλυση της τρέχουσας κατάστασης των πληροφοριακών συστημάτων, δικτυακών υποδομών, υφιστάμενων πολιτικών, διαδικασιών και πρακτικών σχετικών με την ασφάλεια πληροφοριών, επιχειρησιακή συνέχεια και προστασία δεδομένων.
- Διενεργήσει Έλεγχο Ευπαθειών Δικτύου (Penetration Test)
- Διεξάγει συνεντεύξεις και ερωτηματολόγια με τα αρμόδια στελέχη του τμήματος Μηχανογράφησης για καταγραφή εξοπλισμού και πολιτικών.
- Δημιουργήσει λεπτομερές πλάνο ενεργειών αντιμετώπισης και διαχείρισης ευρημάτων.

- Πραγματοποιήσει αξιολόγηση όλων των πρακτικών σχετικών με την επεξεργασία προσωπικών δεδομένων και θα παρέχει συγκεκριμένες προτάσεις συμμόρφωσης.
- Διενεργήσει Vulnerability Assessment για εκτίμηση ευπαθειών των συστημάτων του Φορέα.
- Προσδιορίσει τον κίνδυνο και τον τρόπο αντιμετώπισής του με τεχνικά και οργανωτικά μέτρα.

Υπηρεσίες Υποστήριξης ΥΑΣΠΕ του ΓΝ - ΚΥ Φιλιατών
Βάσει του άρθρου 18 του ν. 4961, κάθε Δημόσιος Οργανισμός είναι υποχρεωμένος να ορίσει έναν Υπεύθυνο Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (ΥΑΣΠΕ) για τη λήψη οργανωτικών μέτρων βελτίωσης της ανθεκτικότητας σε κυβερνοεπιθέσεις.
Οι αρμοδιότητες της Αναδόχου Εταιρείας για την υποστήριξη του ΥΑΣΠΕ θα είναι οι εξής:

α) Διαρκής μέριμνα για την ασφάλεια των συστημάτων δικτύου και πληροφοριών.
β) Συνεργασία με τους αρμόδιους φορείς κυβερνοασφάλειας και εφαρμογή κατευθυντήριων οδηγιών και μέτρων.
γ) Τήρηση μητρώου του φορέα με υποδομές πληροφορικής και επικοινωνιών, λογισμικό και πληροφοριακά αγαθά.
δ) Συμμετοχή στη διενέργεια ελέγχων για διακρίβωση του υφιστάμενου επιπέδου ασφάλειας.
ε) Εποπτεία της τήρησης της πολιτικής ασφάλειας συστημάτων πληροφορικής και επικοινωνιών.
στ) Παρακολούθηση και αξιοποίηση νέων τεχνολογιών και εργαλείων ασφάλειας για ενίσχυση του επιπέδου κυβερνοασφάλειας.
ζ) Διενέργεια αξιολογήσεων του επιπέδου κυβερνοασφάλειας σε συνεργασία με τις αρμόδιες αρχές.
η) Εγκατάσταση και επικαιροποίηση λογισμικού προστασίας από κυβερνοεπιθέσεις, παρέχοντας:

* Threat Detection και Παρακολούθηση σε Πραγματικό Χρόνο.
* Ανάλυση Δεδομένων Καταγραφής και Integrity Monitoring.
* Compliance Management και Vulnerability Detection.
* Security Configuration Assessment.
* Email Alerts για αντιμετώπιση Συμβάντων.

- Ο ανάδοχος θα παρέχει επικαιροποιήσεις και ανανεώσεις του λογισμικού καθ' όλη τη διάρκεια της Σύμβασης.

Η συνολική διάρκεια των υπηρεσιών του αναδόχου θα είναι δώδεκα (12) μήνες από την υπογραφή της Σύμβασης.
Παραδοτέα:

- 3μηνιαία Reports με τις δράσεις της Εταιρείας.
- Συνολικό Report για τον κίνδυνο που αντιμετωπίζει ο Οργανισμός και προτεινόμενες ενέργειες αντιμετώπισης.
- Παροχή Συντήρησης και ενημέρωσης Λογισμικού Cyber Security για προστασία από τις κυβερνοεπιθέσεις.

Φάσεις του Έργου - Παραδοτέα

1η : Έναρξη Έργου – Οργάνωση Δράσεων

- Δράσεις: Καταγραφή εργασιών, καθορισμός παραδοτέων και χρονικών οροσήμων, συστηματική παρακολούθηση προόδου, εκτίμηση απαιτούμενων ανθρωποημερών, οργάνωση και προγραμματισμός συναντήσεων.
- Παραδοτέα: Πλάνο Υλοποίησης Έργου – Εγχειρίδιο Παράδοσης του Έργου.

2η : Συλλογή Δεδομένων / Καταγραφή Πληροφοριακών Assets

- Δράσεις: Συγκέντρωση πληροφοριών για καταγραφή εξοπλισμού (σταθμοί εργασίας, διακομιστές, δικτυακές συσκευές, εκτυπωτές, λογισμικά, πληροφοριακά αγαθά ανά κτιριακή υποδομή),

καταγραφή εκτιμώμενων απειλών, ορισμός κρίσιμων υποδομών βάσει του άρθρου 15 του ν. 5160/2024. Εγκατάσταση λογισμικού για την δημιουργία Καταλόγου Πληροφοριακού Υλικού και Λογισμικού (IT Assets Catalog). Διενέργεια Ελέγχου Ευπαθειών Δικτύου (Penetration Test).

- Παραδοτέα: Κατάλογος Πληροφοριακών Assets του Φορέα (περιλαμβάνει Κατάλογο Πληροφοριακών Assets και Ορισμό Κρίσιμων Υποδομών).

3η : Vulnerability Assessment

- Δράσεις: Προσδιορισμός περιουσιακών στοιχείων για αξιολόγηση ευπάθειας, προτεραιοποίηση βασικών επιχειρησιακών εργαλείων, σάρωση ευπάθειας, ανάλυση αποτελεσμάτων και προτάσεις άμεσης αποκατάστασης, προσδιορισμός συνολικού κινδύνου.
- Παραδοτέα: Vulnerability Assessment, Report Συνολικού Κινδύνου.

4η : Ανάπτυξη Σχεδίου Διορθωτικών Ενεργειών

- Δράσεις: Σύνταξη αναλυτικού σχεδίου με προτάσεις βελτίωσης για αντιμετώπιση ελλείψεων/αποκλίσεων από το κανονιστικό πλαίσιο, προσδιορισμός συγκεκριμένων ενεργειών για βελτίωση του επιπέδου εναρμόνισης και ανθεκτικότητας, προτάσεις συμμόρφωσης μέσω τροποποίησης περιβάλλοντος λειτουργίας, διατήρησης ικανοποιητικού επιπέδου συμμόρφωσης και συστηματικής βελτίωσης ανθεκτικότητας.
- Παραδοτέα: Compliance Plan για βελτίωση της ανθεκτικότητας, Disaster Recovery Plan (Σχέδιο Έκτακτων Συνθηκών).

5η : Δημιουργία Πολιτικής Ασφάλειας

- Δράσεις: Κατάρτιση ενιαίας πολιτικής ασφάλειας συστημάτων πληροφορικής και επικοινωνιών, περιλαμβάνοντας:
    - Στόχους ασφάλειας και προσέγγιση διαχείρισης.
    - Τρόπο διαχείρισης απαιτήσεων από επιχειρησιακή στρατηγική, νομοθετικές/κανονιστικές/συμβατικές υποχρεώσεις και διεθνές περιβάλλον κυβερνοαπειλών.
    - Ανάθεση ρόλων και ευθυνών για τη διαχείριση της ασφάλειας πληροφοριακών συστημάτων.
    - Διαδικασίες για χειρισμό αποκλίσεων και εξαιρέσεων.
- Επιμέρους Πολιτικές: Πολιτική Ασφάλειας Δικτύων, Πολιτική Ορθής Χρήσης, Πολιτική Διαχείρισης ταυτότητας και ελέγχου πρόσβασης, Πολιτική Αντιγράφων Ασφαλείας, Πολιτική Διαχείρισης Περιστατικών και Επιχειρησιακής Συνέχειας, Πολιτική Φυσικής Ασφάλειας, Πολιτική Αξιολόγησης Αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον τομέα της Κυβερνοασφάλειας (αρ. 15 Ν. 5160/2024).
- Παραδοτέα: Πολιτική Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών.

6η : Εγκατάσταση Λογισμικού Cyber Security

- Γενικές αρχές: Ανθεκτικότητα και βιωσιμότητα του Νοσοκομείου, προστασία υποδομών και υπηρεσιών, εμπιστοσύνη των πολιτών.
- Προστασία: Το έργο θα αποτελείται από συστήματα προστασίας των υποδομών πληροφορικής. Για τους σταθμούς εργασίας προβλέπεται προστασία ενσωματωμένη στα λειτουργικά συστήματα, παρέχοντας υψηλό επίπεδο ασφάλειας και πρόληψης μολύνσεων από κακόβουλο λογισμικό μηδενικού χρόνου (0-day).

- Δυνατότητες Λογισμικού: Live response σε επιλεγμένους χρήστες σε περίπτωση κακόβουλης ενέργειας, threat intelligence για βελτιστοποίηση της ανταπόκρισης σε επιθέσεις.
- Το Λογισμικό θα πρέπει να καλύπτει επίσης και να περιλαμβάνει:
    - Κεντρική Διαχείριση και Ενοποίηση: Ενιαία κονσόλα διαχείρισης, αυτόματη ανακάλυψη και εγγραφή νέων συστημάτων, ομαδοποίηση παραγόντων για ευκολότερη διαχείριση και εφαρμογή πολιτικών.
    - Ειδοποιήσεις και Απόκριση: Δημιουργία ειδοποιήσεων και ενεργοποίηση αυτοματοποιημένων ενεργειών απόκρισης σε απειλές.
    - Anomaly Detection: Εντοπισμός μοτίβων που αποκλίνουν από το κανονικό για προληπτικό εντοπισμό απειλών.
        - Μέθοδοι: Καθιέρωση βασικής γραμμής κανονικής συμπεριφοράς, ανίχνευση απόκλισης, μηχανική μάθηση για αναγνώριση πολύπλοκων μοτίβων και προσαρμοστική μάθηση, ανίχνευση βασισμένη σε κανόνες με προσαρμόσιμους κανόνες.

7η : Παρουσίαση των αποτελεσμάτων και εκπαίδευση

- Παραδοτέα Φάσης 7: Στο τέλος του έργου ακολουθεί η παρουσίαση των αποτελεσμάτων στην Ομάδα Παραλαβής και στη Διοίκηση του Γενικού Νοσοκομείου ΚΥ Φιλιατών καθώς και οι εκπαίδευση του ΥΑΣΠΕ και του προσωπικού του Τμήματος Οργάνωση και Πληροφορικής στις αρχές και στα εγκατεστημένα συστήματα κυβερνοασφάλειας .

8η : Συμβουλευτικές Υπηρεσίες ΥΑΣΠΕ

- Παραδοτέα Φάσης 8: Παροχή Συμβουλευτικών Υπηρεσιών στον Υπεύθυνο Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών του Φορέα και συντήρηση/αναβάθμιση του παρεχόμενου λογισμικού για 12 μήνες από την υπογραφή της σύμβασης

Η ΔΙΟΙΚΗΤΡΙΑ

ILIANA KAINTASI
Διοικήτρια
12.06.2026 10:36