0001324278

ΑΔΑ: 916Π4690Β5-Ν4Ξ

Γ.Ν. Κορίνθου 23/09/2026

Α. Π.: 21710

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙ0 ΥΓΕΙΑΣ & ΚΟΙΝΩΝΙΚΗΣ ΑΛΛΗΛΕΓΓΥΗΣ
ΔΙΟΙΚΗΣΗ 6ΗΣ ΥΓΕΙΟΝΟΜΙΚΗΣ ΠΕΡΙΦΕΡΕΙΑΣ
ΠΕΛΟΠΟΝΝΗΣΟΥ, ΙΟΝΙΩΝ ΝΗΣΩΝ, ΗΠΕΙΡΟΥ & ΔΥΤ. ΕΛΛΑΔΑΣ
ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΚΟΡΙΝΘΟΥ
Λ. ΑΘΗΝΩΝ 53, ΚΟΡΙΝΘΟΣ - Τ.Κ. 20131
Δ/νση Διοικητικού
Τμήμα Οικονομικό - Γραφείο Προμηθειών
Πληροφορίες : Παπαφίλη Γ.
ΤΗΛ.27413 61857 - FAX: 27410-20529
E-mail: prom@hospkorinthos.gr

ΠΡΟΣΚΛΗΣΗ

εκδήλωσης ενδιαφέροντος προς τις εταιρείες NIGICO ΑΕΒΕ, SIMA Security και Computer Studio ΑΕ, για υπηρεσίες κυβερνοασφάλειας και υποστήριξης ΥΑΣΠΕ, CPV 72246000-1, , με τη διαδικασία της απευθείας ανάθεσης (δυνάμει του άρθρου 118 του ν. 4412/2016), ΑΛΕ 2.4.2.09.89.001.0001, συνολικής προϋπολογιζόμενης δαπάνης 19.000,00 € πλέον Φ.Π.Α. 24%, ήτοι 23.560,00 € συμπεριλαμβανομένου Φ.Π.Α., με κριτήριο κατακύρωσης και επιλογής αναδόχου την χαμηλότερη τιμή, μέσω της πλατφόρμα διενέργειας ηλεκτρονικών προμηθειών iSupplies.

Το Γενικό Νοσοκομείο ΚΟΡΙΝΘΟΥ έχοντας υπόψη:

1. <u>Τις διατάξεις:</u>

1.1 Την υπό στοιχεία Γ4β/Γ.Π.οικ.33822/31.07.2025 Απόφαση του Υπουργού και Υφυπουργού Υγείας (ΦΕΚ.967/Υ.Ο.Δ.Δ./31.07.2025) περί «Λήξης της θητείας του Διοικητή του Γενικού Νοσοκομείου ΚΟΡΙΝΘΟΥ και εκ νέου διορισμού του.
1.2 Την υπο στοιχεία Υ4α/οικ.112159 Κοινή Απόφαση των Υπουργών Οικονομικών – Διοικητικής Μεταρρύθμισης-Ηλεκτρονικής Διακυβέρνησης – Υγείας Οργανισμός του Γενικού Νοσοκομείου Κορίνθου όπως έχουν τροποποιηθεί και ισχύουν. (Β΄3284/2012).
1.3 Την αρ.πρωτ.2/53407/ΔΠΓΚ/17.07.2025 (ΑΔΑ: ΡΘ5ΠΗ-ΥΟΖ) εγκύκλιο του Υπ.Οικ/κών «Κατάρτιση προϋπολογισμού Γενικής κυβέρνησης οικονομικού έτους 2026»
1.4 Τον Ν.5262/25(Α 235) κύρωσης του Κρατικού Π/Υ οικ. έτους 2026 και την Εισηγητική Έκθεση του Υπουργού Οικονομικών.
1.5 Την αρ.πρωτ.2/99170/ΔΠΓΚ (ΑΔΑ: ΨΥ37Η-9ΚΝ) Εγκύκλιο του Υφυπουργού Εθνικής Οικονομίας και Οικονομικών με θέμα *«Εκτέλεση Προϋπολογισμού Οικονομικού Έτους 2026»*
1.6 Την υπ' αριθμ.Πρωτ.Β2.α/Γ.Π.257/09.01.2026 (ΑΔΑ: 9ΑΛΞ465ΦΥΟ–5Η8) Απόφαση Υφυπουργού Υγείας Έγκριση προϋπολογισμού οικονομικού έτους 2026 του Γενικού Νοσοκομείου Κορίνθου.
1.7 Την υπό στοιχεία Γ4β/13649/09-12-2025 ΦΕΚ.1717/τ.ΥΟΔΔ/31-12-2025 (ΑΔΑ: Ψ9ΞΜ465ΦΥΟ-ΔΩΜ) Απόφαση του Υπουργού και του Υφυπουργού Υγείας με θέμα: *Συγκρότηση και ορισμός μελών στο Διοικητικό Συμβούλιο του ΓΝ ΚΟΡΙΝΘΟΥ, αρμοδιότητας 6ης Δ.Υ.ΠΕ. Πελοποννήσου, Ιονίων Νήσων, Ηπείρου και Δυτικής Ελλάδας.*
1.8 Την Αριθ.Πρωτ.:99864/ 15-12-2025 (ΑΔΑ 6Ξ2346ΝΛΣΞ-446) Εγκύκλιο προς τις αναθέτουσες αρχές σχετικά με τη διενέργεια της διαδικασίας της απευθείας ανάθεσης συμβάσεων προμηθειών και υπηρεσιών του άρθρου 118 ν. 4412_2016.
1.9 Τον ν. 5160/2024, όπως αναφέρεται στην υπ' αρ. πρωτ. 16665/08-09-2026 ορθή επανάληψη αναφορά του Τμήματος Πληροφορικής, σχετικά με την ενσωμάτωση της Οδηγίας NIS2 και τις υποχρεώσεις κυβερνοασφάλειας των βασικών οντοτήτων.
1.10 Τον ν. 4961/2022, όπως αναφέρεται στην ίδια ως άνω αναφορά του Τμήματος Πληροφορικής.

2. <u>Τις Αποφάσεις:</u>

2.1. Την υπό στοιχεία Γ4β/Γ.Π.οικ.33822/31.07.2025 Απόφαση του Υπουργού και Υφυπουργού Υγείας (ΦΕΚ.967/Υ.Ο.Δ.Δ./31.07.2025) περί «Λήξης της θητείας του Διοικητή του Γενικού Νοσοκομείου ΚΟΡΙΝΘΟΥ, ΚΑΡΠΟΥΖΗ ΓΡΗΓΟΡΙΟΥ και εκ νέου διορισμού του.
2.2.Την υπό στοιχεία Υ4α/οικ.112159 Κοινή Απόφαση των Υπουργών Οικονομικών – Διοικητικής Μεταρρύθμισης-Ηλεκτρονικής Διακυβέρνησης – Υγείας Οργανισμός του Γενικού Νοσοκομείου Κορίνθου όπως έχουν τροποποιηθεί και ισχύουν. (Β΄3284/2012).
2.3.Την αρ.πρωτ.2/53407/ΔΠΓΚ/17.07.2025(ΑΔΑ:ΡΘ5ΠΗ-ΥΟΖ) Εγκύκλιο του Υπ.Οικ/κών «Κατάρτιση προϋπολογισμού Γενικής κυβέρνησης οικονομικού έτους 2026»
2.4. Τον Ν.5262/25(Α 235)κύρωσης του Κρατικού Π/Υ οικ. έτους 2026 και την Εισηγητική Έκθεση του Υπουργού Οικονομικών.
2.5. Την αρ. πρωτ.:2/99170/ΔΠΓΚ (ΑΔΑ: ΨΥ37Η-9ΚΝ) Εγκύκλιο του Υφυπουργού Εθνικής Οικονομία και Οικονομικών « Εκτέλεση Προϋπολογισμού Οικονομικού Έτους 2026»
2.6. Την υπ' αριθμ.Πρωτ.Β2.α/Γ.Π.257/09.01.2026 (ΑΔΑ: 9ΑΛΞ465ΦΥΟ–5Η8) Απόφαση Υφυπουργού Υγείας Έγκριση προϋπολογισμού οικονομικού έτους 2026 του Γενικού Νοσοκομείου Κορίνθου.
2.7. Την υπ' αριθμ.Πρωτ.Β2.α/Γ.Π.21999/04.06.2026 (ΑΔΑ: 9ΣΛΨ465ΦΥΟ-ΤΘ8) Απόφαση Υφυπουργού Υγείας Έγκριση 1ης τροποποίησης προϋπολογισμού οικονομικού έτους 2026 του Γενικού Νοσοκομείου Κορίνθου.
2.8. Την υπ' αριθμ.Πρωτ.Β2.α/Γ.Π.34793/04.08.2026 (ΑΔΑ: 9ΕΤ0465ΦΥΟ-1ΣΗ) Απόφαση Υφυπουργού Υγείας Έγκριση 2ης τροποποίησης προϋπολογισμού οικονομικού έτους 2026 του Γενικού Νοσοκομείου Κορίνθου.

3. Τα σχετικά

3.1Η αριθμ.πρωτ.16665/08-09-2026 ορθή επανάληψη αναφορά του τμήματος πληροφορικής του Γενικού Νοσοκομείου Κορίνθου.

3.2Η υπ. αριθ.: 25η/11-09-2026 θ.4ο απόφαση του Δ.Σ.

3.3Τις αρ.πρ.21336, 21337, 21342/21-09-2026 αποφάσεις Δέσμευσης Πίστωσης με ΑΔΑ: 9ΙΜ24690Β5-ΛΜΦ, ΡΒ2Τ4690Β5-ΒΚ9, ΨΝ8Φ4690Β5-Π1Ν, ΑΛΕ **2.4.2.09.89.001.0001**.

3.4Την αρ.πρ.21384/21-09-2026 με ΑΔΑ: 9Π6Ε4690Β5-Υ7ΥΒεβαίωση Πολυετούς Υποχρέωσης.

3.5Την αρ.πρ.21387/21-09-2026 με ΑΔΑ: 94ΖΤ4690Β5-ΝΓ0 Απόφαση Έγκρισης Ανάληψης Πολυετούς Υποχρέωσης.

ΑΝΑΚΟΙΝΩΝΕΙ

Πρόσκληση εκδήλωσης ενδιαφέροντος προς τις εταιρείες NIGICO AEBE, SIMA Security και Computer Studio AE, για υπηρεσίες κυβερνοασφάλειας και υποστήριξης ΥΑΣΠΕ, CPV 72246000-1, , με τη διαδικασία της απευθείας ανάθεσης (δυνάμει του άρθρου 118 του ν. 4412/2016), ΑΛΕ 2.4.2.09.89.001.0001, συνολικής προϋπολογιζόμενης δαπάνης 19.000,00 € πλέον Φ.Π.Α. 24%, ήτοι 23.560,00 € συμπεριλαμβανομένου Φ.Π.Α., με κριτήριο κατακύρωσης και επιλογής αναδόχου την χαμηλότερη τιμή, μέσω της πλατφόρμα διενέργειας ηλεκτρονικών προμηθειών iSupplies και συγκεκριμένα:

ΠΑΡΑΡΤΗΜΑ Α

ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ - ΑΠΑΙΤΗΣΕΙΣ ΠΡΟΣ ΥΛΟΠΟΙΗΣΗ

ΓΕΝΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΓΙΑ ΤΟ ΕΡΓΟ

1. Πραγματοποίηση ελέγχου/ων δοκιμής/ων παρείσδυσης, εσωτερικά και εξωτερικά και ανάλυσης κινδύνων του Νοσοκομείου, με στόχο την ανάδειξη ευπαθειών ασφαλείας στις υποδομές πληροφορικής, την περιγραφή των επιπτώσεών τους στην εύρυθμη και ασφαλή λειτουργία του Νοσοκομείου, την πρόταση αντιμέτρων για την μείωση του κινδύνου, ώστε να διατηρείται και συμμόρφωση με το NIS 2. Κατά το παρόν έργο ο ανάδοχος θα πρέπει να αναγνωρίσει και αποτιμήσει τις ευπάθειες των υποδομών πληροφορικής.
2. Risk Assessment για την εκτίμηση των κινδύνων στην περίπτωση συμβάντος ασφάλειας. Αξιολόγηση των απειλών με βάση την πιθανότητα να εμφανιστεί και του αντικτύπου που θα έχει μια πιθανή εμφάνισή της. Το αποτέλεσμα της διαδικασίας αυτής θα αναδείξει τα σημεία του δικτύου τα οποία χρήζουν πρόσθετων αντιμέτρων ώστε να μειωθεί το ρίσκο.
3. Υπηρεσία CISO (Chief Information Security Officer) για δεκαοκτώ (18) μήνες.

Σημείωση 1: Όλες οι αναφορές και τα παραδοτέα (reports) θα συντάσσονται στην ελληνική γλώσσα.

Σημείωση 2: Ο ανάδοχος θα υποβάλλει ανά σαράντα πέντε (45) ημέρες αναφορά (report) για τις ενέργειες που πραγματοποιήθηκαν και τα αποτελέσματα των ελέγχων.

1. EXTERNAL-INTERNAL PENETRATION TEST

Σκοπός του έργου είναι η πραγματοποίηση ελέγχου/ων δοκιμής/ων παρείσδυσης και ανάλυσης κινδύνων του Γενικού Νοσοκομείου Κορίνθου, με στόχο την ανάδειξη ευπαθειών ασφαλείας στις υποδομές πληροφορικής, την περιγραφή των επιπτώσεών τους στην εύρυθμη και ασφαλή λειτουργία του Νοσοκομείου και την πρόταση αντιμέτρων για την μείωση του κινδύνου.Ο ανάδοχος θα πρέπει να αναγνωρίσει και να αποτιμήσει τις ευπάθειες των υποδομών πληροφορικής και στη συνέχεια να διενεργήσει δοκιμές παρείσδυσης (Penetration Testing).

Για την υλοποίηση του παρόντος έργου ο ανάδοχος θα πρέπει να διενεργήσει τα ακόλουθα βήματα:

1. Αναγνώριση και αποτίμηση ευπαθειών.

Χρησιμοποιώντας κατάλληλα, καταξιωμένα διεθνή πρότυπα και δημοφιλή εργαλεία ανίχνευσης ευπαθειών, ο ανάδοχος θα διενεργήσει διαδικασία αναγνώρισής τους. Η διαδικασία αυτή θα αναλυθεί στα ακόλουθα επίπεδα:
i. Σε επίπεδο εφαρμογής χωρίς γνώση (Black Box) (μόνο στη δικτυακή διεύθυνση της εφαρμογής)
ii. Σε επίπεδο εφαρμογής με γνώση (White Box) (έχοντας συγκεκριμένα test accounts).

2. Διενέργεια Αρχικών Δοκιμών Παρείσδυσης.

Χρησιμοποιώντας κατάλληλα, καταξιωμένα διεθνή πρότυπα και δημοφιλή εργαλεία καθώς και όπου απαιτείται δικό του κώδικα, ο ανάδοχος θα διενεργήσει δοκιμές παρείσδυσης σε πληροφοριακά συστήματα που θα του υποδείξει ο φορέας. Η διαδικασία αυτή θα αναλυθεί στα ακόλουθα επίπεδα:
i. Σε επίπεδο εφαρμογής χωρίς γνώση (Black Box) (μόνο στη δικτυακή διεύθυνση της εφαρμογής)
ii. Σε επίπεδο εφαρμογής με γνώση (White Box) (έχοντας συγκεκριμένα test accounts).

Στην παρούσα φάση υλοποίησης του έργου οι δοκιμές θα πραγματοποιηθούν με συγκεκριμένα δικαιώματα χρήστη και με χρήση διαβαθμισμένων ρόλων, όπως αυτοί θα ορισθούν από τον φορέα. Συγκεκριμένα θα δημιουργηθούν δοκιμαστικοί λογαριασμοί (test accounts), που θα αντιπροσωπεύουν έναν απλό χρήστη των εφαρμογών καθώς και έναν χρήστη με δικαιώματα διαχειριστή.
Οι δοκιμές αυτές σκοπό έχουν να εξασφαλίσουν στον φορέα καλύτερη κατανόηση των αδυναμιών των κρίσιμων υποδομών του, με κύριο στόχο την προστασία του από ενδεχόμενες επιθέσεις που μπορεί να εκτελεσθούν από το διαδίκτυο.
Οι δοκιμές παρείσδυσης θα γίνουν τόσο εξωτερικά (external systems & network penetration tests), όσο και εσωτερικά (internal systems& network penetration tests).

Κατά τη διάρκεια των δοκιμών, ο ανάδοχος θα καλύψει κατ’ ελάχιστον:

i. Τα OWASP TOP 10 Vulnerabilities
ii. Επιθέσεις στο κανάλι σύνδεσης δεδομένων
iii. Επιθέσεις σε επίπεδο λειτουργικού συστήματος
iv. Επιθέσεις σε επίπεδο βάσης δεδομένων

v. Επιθέσεις άρνησης υπηρεσιών (DoS attacks).
vi. Έλεγχοι ασφάλειας σε 2 κρίσιμες εφαρμογές. Ενδεικτικά αναφέρονται:
- Πραγματοποίηση δοσοληψίων χωρίς εξουσιοδότηση
- Απόκτηση δικαιωμάτων πρόσβασης σε ευαίσθητα δεδομένα χωρίς την κατάλληλη εξουσιοδότηση
- Μη εξουσιοδοτημένη αλλαγή ή καταστροφή δεδομένων
- Μη εξουσιοδοτημένη τροποποίηση λογισμικού ή η παρείσφρηση κακόβουλου λογισμικού.

Για την περίπτωση που επιτευχθεί μη εξουσιοδοτημένη αλλαγή ή καταστροφή δεδομένων χωρίς πρόσβαση στη βάση δεδομένων (μέσω ευπάθειας λογισμικών συστημάτων/υποδομών ή εφαρμογής), θα πρέπει να έχει τηρηθεί καταγραφή των δεδομένων πριν την αλλαγή και στη συνέχεια να γίνει αναίρεση των αλλαγών που επιτεύχθηκαν.
Για την εξέταση της δυνατότητας μη-εξουσιοδοτημένης αλλαγής ή καταστροφής δεδομένων με απευθείας πρόσβαση στη βάση δεδομένων ζητείται ο έλεγχος της δυνατότητας δημιουργίας χρήστη στη βάση δεδομένων με προνόμια διαχειριστή, χωρίς να πραγματοποιηθεί η αυτή καθαυτή αλλαγή στη βάση δεδομένων.
Σε ό,τι αφορά μη-εξουσιοδοτημένη τροποποίηση λογισμικού ή παρείσφρηση κακόβουλου λογισμικού στο λογισμικό συστημάτων/υποδομών και στο λογισμικό της βάσης δεδομένων, ζητείται ο έλεγχος της δυνατότητας να γίνει τροποποίηση, χωρίς να επιτευχθεί η τροποποίηση αυτή καθαυτή.
Ο ανάδοχος έχοντας ολοκληρώσει τους ελέγχους που προβλέπονται στο έργο, θα συντάξει εκθέσεις, στην Ελληνική γλώσσα, από τον έλεγχο ασφαλείας που θα περιλαμβάνει τα πιθανά ευρήματα ασφάλειας, τις επιπτώσεις αυτών καθώς και προτεινόμενες ενέργειες αντιμετώπισής τους, όπως περιγράφεται παρακάτω. Όλες οι εκθέσεις θα πρέπει να ομαδοποιούν το σύνολο των ευρημάτων, ανάλογα με το ρίσκο, στις ακόλουθες κατηγορίες:

1. Κρίσιμο (Critical) - #αρ. ευρημάτων
2. Υψηλού ρίσκου (High) - #αρ. ευρημάτων
3. Μεσαίου ρίσκου (Medium) - #αρ. ευρημάτων
4. Χαμηλού ρίσκου (Low) - #αρ. ευρημάτων
5. Συστάσεις (Recommendations) - #αρ. ευρημάτων

Παραδοτέα PENETRATION TEST:

i. Μεθοδολογία Αναγνώρισης & αποτίμησης ευπαθειών, Διενέργειας Δοκιμών Παρείσδυσης. Στο πλαίσιο αυτού του παραδοτέου, θα περιγραφούν τα βήματα υλοποίησης των συγκεκριμένων ενεργειών, περιλαμβανομένων των εργαλείων που θα χρησιμοποιηθούν, των ενεργειών για την διασφάλιση της εμπιστευτικότητας του συνόλου των στοιχείων του έργου κ.α.
ii. Έκθεση αποτελεσμάτων της Ανάλυσης και αποτίμησης Ευπαθειών.
iii. Έκθεση αποτελεσμάτων των δοκιμών παρείσδυσης ανά δοκιμή και συστάσεις για την αντιμετώπιση των ευπαθειών. Οι εκθέσεις αποτελεσμάτων των δοκιμών παρείσδυσης θα περιλαμβάνουν κατ' ελάχιστον τις ακόλουθες πληροφορίες:

• Περίληψη κυριότερων σημείων.

• Πεδίο εφαρμογής των υπηρεσιών.
• Μεθοδολογίες και εργαλεία που χρησιμοποιήθηκαν για τη διεξαγωγή των ελέγχων.
• Προσδιορισμός των κρίσιμων στοιχείων ελέγχου και επεξήγηση γιατί δοκιμάστηκαν αυτά τα στοιχεία.
• Περιγραφή της εξέλιξης του κύκλου ελέγχων και των προβλημάτων που παρουσιάστηκαν κατά τη διάρκεια εκτέλεσής τους (χρονοδιάγραμμα).
• Για κάθε ευπάθεια/αδυναμία θα δίνονται οι ακόλουθες πληροφορίες:

1. χρόνος και τεχνογνωσία που θα χρειαζόταν ένας επιτιθέμενος για να εντοπίσει την ευπάθεια/αδυναμία.
2. τα ενδεχόμενα σενάρια επίθεσης στα οποία μπορεί να χρησιμοποιηθεί η εν λόγω ευπάθεια/αδυναμία.
3. κρισιμότητα (π.χ. Κρίσιμη, Υψηλή, Μεσαία, Χαμηλή, σύσταση).
4. το επίπεδο έκθεσης σε κίνδυνο, σύμφωνα με τα παρακάτω κριτήρια: η ύπαρξη αυτής της ευπάθειας/αδυναμίας επιτρέπει άμεση διακύβευση της ασφάλειας ή σε συνεργασία με άλλες ευρεθείσες ευπάθειες/αδυναμίες μπορεί να χρησιμοποιηθεί για την πραγματοποίηση επίθεσης.
5. διορθωτικές ενέργειες έκτακτης ανάγκης.

• Καταγραφή των επιτυχημένων ευπαθειών που εκτελέστηκαν στο πλαίσιο των ελέγχων παρείσδυσης.
• Αναλυτική περιγραφή των σεναρίων επιθέσεων που υλοποιήθηκαν. Θα περιλαμβάνονται τα σενάρια επίθεσης που σχεδιάστηκαν και ελέγχθηκαν και το κατά πόσο είναι δυνατή η πραγματοποίησή τους. Για κάθε επιτυχές σενάριο επίθεσης θα δίνονται τα παρακάτω:

1. αποδείξεις των επιτυχημένων δοκιμών παρείσδυσης (π.χ. σχετικά screenshots, video).
2. ο χρόνος, η τεχνογνωσία και οι πόροι που θα χρειαζόταν ο επιτιθέμενος για να το φέρει επιτυχώς εις πέρας.
3. η επίπτωση που θα είχε στην ασφάλεια της υπό έλεγχο πληροφοριακής υποδομής
4. ο κίνδυνος στον οποίο είναι εκτεθειμένη η υπό έλεγχο πληροφοριακή υποδομή (το επίπεδο κινδύνου ορίζεται ως το γινόμενο της “ευκολίας εκμετάλλευσης μιας ευπάθειας/αδυναμίας” επί την “επίπτωση”).
5. οι εναλλακτικές διορθωτικές ενέργειες για τη μείωση/εξάλειψη του κινδύνου.

• Συγκεκριμένες πρακτικές συστάσεις για την αποκατάσταση των εντοπισμένων ευπαθειών.

2. RISK ASSESSMENT

Το Risk Assessment αποσκοπεί στην εκτίμηση των κινδύνων στην περίπτωση συμβάντος ασφάλειας . Εδώ αξιολογείται η κάθε απειλή που μπορεί να συμβεί στο πληροφοριακό σύστημα του νοσοκομείου, βάσει της πιθανότητας να εμφανιστεί και του αντικτύπου που θα έχει μια πιθανή εμφάνισή της. Το αποτέλεσμα της διαδικασίας αυτής, θα αναδείξει τα σημεία του δικτύου τα οποία χρήζουν πρόσθετων αντιμέτρων, ώστε να μειωθεί το ρίσκο. Τα αντίμετρα είναι τόσο τεχνικής φύσεως, όσο και σε επίπεδο πολιτικών και διαδικασιών.

Θα πραγματοποιηθεί Διενέργεια Άσκησης Αξιολόγησης Κινδύνων Ασφάλειας Πληροφοριών και Κυβερνοασφάλειας, σε όλο το εύρος του νοσοκομείου (Top-down Risk Assessment) και σύμφωνα με τις διεθνείς καλές πρακτικές όπως NIS 2. Στο πλαίσιο αυτό, θα πρέπει να πραγματοποιηθούν από τον ανάδοχο, κατ' ελάχιστον τα παρακάτω:

- Αναγνώριση και καταγραφή απειλών και κινδύνων κυβερνοασφάλειας και ασφάλειας πληροφοριών του νοσοκομείου (Risk Registry).
- Διενέργεια άσκησης Εκτίμησης Επιχειρησιακού Αντικτύπου (Business Impact Analysis).
- Υπολογισμός πρωταρχικών κινδύνων (Inherent Risk Rating).
- Διενέργεια άσκησης αξιολόγησης των δικλείδων ασφάλειας του νοσοκομείου (Maturity Assessment).
- Υπολογισμός υπολειπόμενου κινδύνου (Residual Risk Rating).
- Ανάπτυξη πλάνου μετριασμού των εντοπισμένων κινδύνων από την άσκηση αξιολόγησης (Risk Treatment Plan).

Το πλάνο θα περιέχει τα ακόλουθα:

- Τις προτεινόμενες δικλείδες ασφάλειας και δράσεις για τον μετριασμό των κινδύνων.
- Τους εκάστοτε ιδιοκτήτες κινδύνων.
- Τον προτεινόμενο χρόνο υλοποίησης των δράσεων.
- Δημιουργία λεπτομερούς αναφοράς για τα αποτελέσματα της άσκησης (Detailed Risk Assessment Report).
- Δημιουργία αναφοράς στην Ανώτερη Διοίκηση για τα αποτελέσματα της άσκησης (Executive Risk Assessment Report).
- Δημιουργία πίνακα ελέγχου για την παρακολούθηση του προφίλ αναγνωρισμένων κινδύνων, της έκθεσης σε απειλές και της ωριμότητας των δικλίδων ασφαλείας.

3. ΥΠΗΡΕΣΙΑ CISO

Οι υπηρεσίες CISO θα περιλαμβάνουν:

- Σχεδιασμό πολιτικής ασφάλειας και ελέγχων για τη μείωση του κινδύνου.
- Αξιολόγηση κινδύνου: Αξιολόγηση των δυνητικών απειλών στα πληροφοριακά συστήματα.
- Λεπτομερείς έλεγχοι.
- Συμμόρφωση: Προσαρμογή στους εξελισσόμενους κανονισμούς συμμόρφωσης.
- Ανάκτηση από καταστροφές: Ανάπτυξη διαδικασιών για την εξασφάλιση της ανθεκτικότητας της επιχείρησης σε περίπτωση επιθέσεων, συμπεριλαμβανομένων περιοδικών δοκιμών.
- Πρόληψη απώλειας δεδομένων και απάτης: Διασφάλιση ότι το προσωπικό έχει πρόσβαση μόνο στα δεδομένα που είναι απαραίτητα για την εργασία του.
- Έρευνες και εγκληματολογία: Εντοπισμός αδυναμιών και σχεδιασμός στρατηγικών, για την πρόληψη της επανεμφάνισής τους.
- Στενή συνεργασία με το τμήμα πληροφορικής.
- Συμβουλευτική διαχείριση σχετικά με την ενσωμάτωση πρακτικών ασφαλείας, στις λειτουργικές διαδικασίες.
- Ανάπτυξη προγραμμάτων εκπαίδευσης και ευαισθητοποίησης.
- Διεξαγωγή και αξιολόγηση εξωτερικών/εσωτερικών δοκιμών διείσδυσης.

Οφέλη για τον οργανισμό:

• Ανάπτυξη κατάλληλων πολιτικών και διαδικασιών, για την προστασία και τη διαχείριση των πληροφοριών.

• Διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των ψηφιακών πληροφοριών.

• Προστασία Δεδομένων: Διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των δεδομένων του οργανισμού.

• Μείωση Κινδύνου: Μείωση των κινδύνων από κυβερνοεπιθέσεις και παραβιάσεις δεδομένων.

• Επαγγελματισμός: Διατήρηση της φήμης του οργανισμού και της εμπιστοσύνης των πολιτών.

• Συμμόρφωση: Αποφυγή νομικών συνεπειών λόγω μη συμμόρφωσης με κανονισμούς.

• Ετοιμότητα: Γρήγορη και αποτελεσματική ανταπόκριση σε περιστατικά ασφαλείας.

• Η θέση του CISO είναι κρίσιμη για την προστασία των πληροφοριακών πόρων του οργανισμού και τη διασφάλιση της αδιάλειπτης λειτουργίας του στον σύγχρονο τεχνολογικό κόσμο.

ΠΡΟΫΠΟΘΕΣΕΙΣ ΓΙΑ ΤΟΝ ΑΝΑΔΟΧΟ ΤΟΥ ΕΡΓΟΥ

Οι παρακάτω εργασίες απαιτείται να ολοκληρωθούν σε περίοδο 2 μηνών, εφόσον υπάρχει η σχετική διαθεσιμότητα του τμήματος πληροφορικής του νοσοκομείου.

- External Pen Test
- Internal Pen Test
- IT Audit
- NIS2 GAP Analysis
- NIS 2 Πολιτικές
- Risk Assessment

ΠΡΟΫΠΟΘΕΣΕΙΣ ΕΠΑΓΓΕΛΜΑΤΙΚΗΣ ΚΑΙ ΤΕΧΝΙΚΗΣ ΙΚΑΝΟΤΗΤΑΣ ΑΝΑΔΟΧΟΥ

Ο Ανάδοχος θα πρέπει να είναι πιστοποιημένος κατά ISO 27001.

Η ομάδα έργου θα πρέπει να διαθέτει τουλάχιστον 7 από τις παρακάτω πιστοποιήσεις:

ISO 27001 Lead Auditor
OSCP - Offensive Security Certified Professional
CISSP - Certified Information Systems Security Professional
CRTO – Certified Red Team Operator
OSWE - Offensive Security Web Expert
CIH - Certified Incident Handler
CPTS - Hackthebox Certified Penetration Testing Specialist
CCT INF - CREST Certified Tester – Infrastructure

OSEP – Offensive Security Experienced penetration tester

ISC2 CCSP - Certified Cloud Security Professional certification from ISC2

Ο Ανάδοχος θα πρέπει να έχει πραγματοποιήσει δοκιμές παρείσδυσης (penetration tests) την τελευταία τριετία σε τουλάχιστον 3 δημόσιους φορείς/οργανισμούς εκ των οποίων οι 2 να είναι φορείς υγείας και να έχει αναλάβει έργο υποστήριξης ΥΑΣΠΕ / CISO σε τουλάχιστο ένα δημόσιο φορέα υγείας. Η προϋπηρεσία θα πιστοποιείται με προσκόμιση δημοσιευμένης σύμβασης στο ΚΗΜΔΗΣ και βεβαίωση καλής εκτέλεσης. Η ομάδα έργου θα πρέπει να αποτελείται από εργαζόμενους του Αναδόχου με μόνιμη σχέση εργασίας. Θα πρέπει να προσκομισθούν τα βιογραφικά της ομάδας έργου και οι ανωτέρω τουλάχιστον 7 πιστοποιήσεις. Όλα τα μέλη της ομάδας έργου θα πρέπει να πραγματοποιήσουν μία τουλάχιστον φυσική παρουσία στους χώρους του Νοσοκομείου.

ΠΑΡΑΡΤΗΜΑ Β – ΠΙΝΑΚΑΣ ΣΥΜΜΟΡΦΩΣΗΣ ΥΠΟΨΗΦΙΩΝ ΑΝΑΔΟΧΩΝ

Α/Α	**Απαίτηση**	**Περιγραφή Συμμόρφωσης**	**Συμμόρφωση**
1	Εμπειρία PenTest	3 δημόσιοι φορείς/οργανισμοί, εκ των οποίων 2 φορείς υγείας	
2	Εμπειρία ΥΑΣΠΕ/CISO	1 δημόσιος φορέας υγείας	
3	ISO 27001	Πιστοποίηση αναδόχου	
4	Πιστοποιήσεις ομάδας έργου	≥ 7 πιστοποιήσεις (OSCP, CISSP, OSWE, OSEP κ.λπ.)	
5	Μόνιμη σχέση εργασίας	Όλα τα μέλη	
6	Φυσική παρουσία	Τουλάχιστον μία επίσκεψη	
7	External PenTest	Black Box & White Box	
8	Internal PenTest	Black Box & White Box	
9	OWASP Top 10	Πλήρης κάλυψη	
10	Έλεγχοι σε κρίσιμες εφαρμογές	≥2 εφαρμογές	
11	DoS, OS, DB attacks	Πλήρης κάλυψη	
12	Αναλυτικά reports	Πλήρης τεκμηρίωση	
13	Risk Assessment	NIS2, Risk Registry, BIA, Maturity	
14	Risk Treatment Plan	Δράσεις, ιδιοκτήτες, χρονοδιάγραμμα	
15	Detailed & Executive Reports	Πλήρης κάλυψη	
16	CISO υπηρεσίες	18 μήνες	
17	NIS2 GAP Analysis	Πλήρης κάλυψη	
18	NIS2 Πολιτικές	Πλήρης κάλυψη	

Α/Α	Απαίτηση	Περιγραφή Συμμόρφωσης	Συμμόρφωση
19	IT Audit	Πλήρης κάλυψη	
20	Χρονοδιάγραμμα 2 μηνών	Δυνατότητα υλοποίησης	
21	Reports στα Ελληνικά	Πλήρης κάλυψη	
22	Εμπιστευτικότητα	GDPR compliance	
23	Ασφάλιση επαγγελματικής ευθύνης	Υποχρεωτική	

Ημερομηνία Λήξης Υποβολής Προσφορών : 28-09-2026 ημέρα Δευτέρα και ώρα 11:00 π.μ.

Ημερομηνία Αποσφράγισης Προσφορών 28-09-2026 ημέρα Δευτέρα και ώρα 12:00 π.μ.

Για την επιτάχυνση των διαδικασιών και για τη διευκόλυνση των ενδιαφερόμενων αναδόχων, το Νοσοκομείο διεξάγει έρευνα αγοράς μέσω της υπηρεσίας ηλεκτρονικής διαχείρισης αιτημάτων / προσφορών **iSupplies** (http://isupplies.gr) της εταιρείας iSmart P.C.

Προκειμένου να μπορέστε να συμμετέχετε και να υποβάλετε απαντήσεις σχετικά με τις προσκλήσεις ενδιαφέροντος ή/και υποβολής προσφοράς, θα πρέπει να αποκτήσετε κωδικούς πρόσβασης για την εφαρμογή.
Η εγγραφή στην πλατφόρμα iSupplies είναι δωρεάν και γίνεται είτε μέσω τηλεφώνου στην iSmart P.C. στο 2103601671 είτε συμπληρώνοντας τη σχετική φόρμα εγγραφής στη διεύθυνση: http://isupplies.gr/auth/register.

Για κάθε έρευνα που καλείστε να συμμετάσχετε, θα ενημερώνεστε μέσω email στη διεύθυνση ηλεκτρονικής αλληλογραφίας που θα δηλώσετε κατά την εγγραφή σας.
Για οποιαδήποτε περαιτέρω πληροφορία σχετικά με την πλατφόρμα iSupplies μπορείτε να απευθύνεστε στα ακόλουθα στοιχεία επικοινωνίας: email: info@isupplies.gr, τηλ: 2103601671.

ΑΠΑΡΑΙΤΗΤΗ ΠΡΟΫΠΟΘΕΣΗ ΓΙΑ ΤΗ ΣΥΜΜΕΤΟΧΗ ΣΤΟ ΔΙΑΓΩΝΙΣΜΟ ΝΑ ΚΑΤΑΤΕΘΟΥΝ ΤΑ ΠΑΡΑΚΑΤΩ ΔΙΚΑΙΟΛΟΓΗΤΙΚΑ:

Α/Α	ΠΕΡΙΓΡΑΦΗ ΔΙΚΑΙΟΛΟΓΗΤΙΚΩΝ
1.	Υπεύθυνη δήλωση ν. 1599/1986 του/των νόμιμου/-ων εκπροσώπου/ων, στην οποία θα δηλώνεται ότι: • ο προσφέρων αποδέχεται πλήρως τους όρους της παρούσας πρόσκλησης και των παρατημάτων αυτής, • δεν υφίσταται αμετάκλητη καταδικαστική απόφαση για τους λόγους που αναφέρονται στην παρ. 1 του άρθρου 73 του ν. 4412/2016 εις βάρος του οικονομικού φορέα, όσο και εις βάρος: - στις περιπτώσεις εταιρειών περιορισμένης ευθύνης (Ε.Π.Ε.), ιδιωτικών κεφαλαιουχικών εταιρειών (Ι.Κ.Ε.) και προσωπικών εταιρειών (Ο.Ε. και Ε.Ε.), των διαχειριστών, - στις περιπτώσεις ανωνύμων εταιρειών (Α.Ε.) από τον νόμιμο εκπρόσωπο της Α.Ε., - στις περιπτώσεις των συνεταιρισμών, των μελών του Διοικητικού Συμβουλίου, - στις υπόλοιπες περιπτώσεις νομικών προσώπων, του κατά περίπτωση νόμιμου εκπροσώπου. • δεν βρίσκεται σε κατάσταση σύγκρουσης συμφερόντων του άρθρου 24 του Ν. 4412/2016 σύμφωνα με τα οριζόμενα στο άρθρο αυτό, όπως τροποποιήθηκε και ισχύει, • περί μη επιβολής σε βάρος του, της κύρωσης του οριζόντιου αποκλεισμού του άρθρου 74, παρ.4 του ν. 4412/2016. Η υπεύθυνη δήλωση θα πρέπει να έχει συνταχθεί μετά την δημοσίευση της παρούσας.
2.	Πιστοποιητικό εγγραφής στο Μητρώο του Εμπορικού και Βιομηχανικού ή Βιοτεχνικού Επιμελητηρίου

	της έδρας της εταιρείας, με εγγεγραμμένη δραστηριότητα αυτήν του αντικειμένου της παρούσας.
3.	Πιστοποιητικό ΓΕΜΗ (μεταβολών/εκπροσώπησης), έκδοσης εντός του τελευταίου τριμήνου, από το οποίο να προκύπτει ποιος ή ποιοι εκπροσωπούν και δεσμεύουν την εταιρεία.
4.	Εκτύπωση της καρτέλας "Στοιχεία Μητρώου/Επιχείρησης" από την ηλεκτρονική πλατφόρμα της Ανεξάρτητης Αρχής Δημοσίων Εσόδων, από την οποία να προκύπτει η μη αναστολή της επιχειρηματικής της δραστηριότητας.
5.	Τεχνική προσφορά σύμφωνα με τα οριζόμενα στο σώμα της πρόσκλησης.
6.	Συμπληρωμένο έντυπο οικονομικής προσφοράς.
7.	ΦΥΛΛΟ ΣΥΜΜΟΡΦΩΣΗΣ ΥΠΟΨΗΦΙΩΝ ΑΝΑΔΟΧΩΝ

Η υποβαλλόμενη προσφορά ισχύει και δεσμεύει τους οικονομικούς φορείς για διάστημα δώδεκα (12) μηνών από την επόμενη της καταληκτικής ημερομηνίας υποβολής προσφορών.

ΠΑΡΑΚΑΛΟΥΜΕ ΟΠΩΣ ΣΤΗΝ ΠΡΟΣΦΟΡΑ ΣΑΣ ΝΑ ΑΝΑΦΕΡΕΤΑΙ Ο ΧΡΟΝΟΣ ΙΣΧΥΟΣ

ΕΝΑΛΛΑΚΤΙΚΕΣ ΠΡΟΣΦΟΡΕΣ ΔΕΝ ΓΙΝΟΝΤΑΙ ΔΕΚΤΕΣ ΚΑΙ ΑΠΟΡΡΙΠΤΟΝΤΑΙ

Ο ανάδοχος υπόκειται στις νόμιμες κρατήσεις. Ο ΦΠΑ βαρύνει το νοσοκομείο.

Τρόπος πληρωμής:

Η πληρωμή του συμβατικού τιμήματος της ανάθεσης υπηρεσιών θα υποβάλλεται ανά δίμηνο. Η πληρωμή του συμβατικού τιμήματος θα γίνεται με την προσκόμιση των νομίμων παραστατικών και δικαιολογητικών που προβλέπονται από τις διατάξεις του άρθρου 200 παρ. 4 του Ν. 4412/2016, καθώς και κάθε άλλου δικαιολογητικού που τυχόν ήθελε ζητηθεί από τις αρμόδιες υπηρεσίες που διενεργούν τον έλεγχο και την πληρωμή (αποδεικτικά φορολογικής και ασφαλιστικής ενημερότητας κ.λ.π.).

Ειδικοί Όροι συμμετοχής:

Ο ανάδοχος με την συμμετοχή του δηλώνει ότι φέρει εις το ολόκληρον αλληλεγγύως και απεριορίστως την ευθύνη για την επίτευξη του σκοπού μετά των παρεπομένων αυτού υποχρεώσεων. Κατά τον αυτό τρόπο εγγυάται την εκτέλεση της υπό ανάθεση υπηρεσίας και επιβαρύνεται με τις ενδεχόμενες κυρώσεις ή εκπτώσεις σε περίπτωση μη παράδοσης των υπηρεσιών.

Ο ΔΙΟΙΚΗΤΗΣ

ΚΑΡΠΟΥΖΗΣ ΓΡΗΓΟΡΙΟΣ

ΠΙΝΑΚΑΣ ΑΠΟΔΕΚΤΩΝ (μέσω DocuTracks)

Μέλη Επιτροπής διενέργειας της διαγωνιστικής διαδικασίας

1. Οικονομόπουλο Νίκο, (ΠΕ) Πληροφορικής
2. Παπασταματίου Γεωργία, (ΔΕ) Πληροφορικής
3. Τσίλη Γεωργία, (ΤΕ) Δ/κού Λογ/κού & γραμματέας

ΕΣΩΤΕΡΙΚΗ ΔΙΑΝΟΜΗ : (μέσω DocuTracks)

1. κ. Διοικητή
2. Δ/ντή – Υπ/ντρια Διοικητικής – Οικονομικής Υπηρεσίας
3. Προϊσταμένη Οικονομικού Τμήματος
4. Γραφείο Υλικού
5. Γραφείο Προμηθειών