



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ  
ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ  
1<sup>η</sup> Υ.ΠΕ. ΑΤΤΙΚΗΣ

ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ  
Α Θ Η Ν Ω Ν  
«ΚΟΡΓΙΑΛΕΝΕΙΟ – ΜΠΕΝΑΚΕΙΟ Ε.Ε.Σ.»

Αθήνα, 15 Ιουνίου 2026  
Αρ. πρωτ.:.....

Δ/ΝΣΗ: ΔΙΟΙΚΗΤΙΚΟΥ  
ΥΠΟΔ/ΝΣΗ: ΟΙΚΟΝΟΜΙΚΟΥ  
ΤΜΗΜΑ: ΠΡΟΜΗΘΕΙΩΝ  
ΔΙΕΥΘΥΝΣΗ: ΑΘΑΝΑΣΑΚΗ 2  
ΤΑΧ. ΚΩΔ.: 115 – 26  
ΠΛΗΡΟΦΟΡΙΕΣ: κ. Κωνσταντίνα Μπαλάσκα  
ΤΗΛΕΦΩΝΟ: 213 2068917  
e-mail: [prom@0310.syzefxis.gov.gr](mailto:prom@0310.syzefxis.gov.gr)

**ΠΡΟΣΚΛΗΣΗ ΥΠΟΒΟΛΗΣ ΠΡΟΣΦΟΡΩΝ ΓΙΑ ΤΗΝ ΑΝΑΔΕΙΞΗ ΑΝΑΔΟΧΟΥ ΜΕ ΑΠΕΥΘΕΙΑΣ ΑΝΑΘΕΣΗ (αρθ. 118 ν.4412/2016) ΓΙΑ ΤΗΝ «ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ & ΕΝΑΡΜΟΝΙΣΗΣ ΤΟΥ ΝΟΣΟΚΟΜΕΙΟΥ ΜΕ ΤΟΝ Ν.5160/2024 ΚΑΙ ΤΗΝ ΟΔΗΓΙΑ ΝΙΣ 2» (CPV:79417000-0 ΥΠΗΡΕΣΙΕΣ ΠΑΡΟΧΗΣ ΣΥΜΒΟΥΛΩΝ ΣΕ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ) ΓΙΑ ΔΙΑΣΤΗΜΑ ΕΞΙ (6) ΜΗΝΩΝ ΠΡΟΥΠΟΛΟΓΙΣΜΕΝΗΣ ΔΑΠΑΝΗΣ 24.190,00€ ΠΛΕΟΝ ΦΠΑ 24% (29.995,60€ ΣΥΜΠΕΡΙΛΑΜΒΑΝΟΜΕΝΟΥ ΦΠΑ 24%) (Α.Α. 20/2026).**

**ΑΝΤΙΚΕΙΜΕΝΟ ΤΟΥ ΔΙΑΓΩΝΙΣΜΟΥ-ΣΥΝΟΠΤΙΚΑ ΣΤΟΙΧΕΙΑ**

|                                      |                                                                                                         |
|--------------------------------------|---------------------------------------------------------------------------------------------------------|
| Είδος Διαγωνισμού                    | ΑΠΕΥΘΕΙΑΣ ΑΝΑΘΕΣΗ                                                                                       |
| Αναθέτουσα Αρχή                      | ΝΠΔΔ Γ.Ν.Α. «Κοργιαλένιο-Μπενάκειο Ε.Ε.Σ.»                                                              |
| Κριτήριο Κατακύρωσης                 | Πλέον συμφέρουσα από οικονομική άποψη βάσει τιμής προσφορά                                              |
| Τόπος Υποβολής Προσφορών             | Πρωτόκολλο<br>Γ.Ν.Α. «Κοργιαλένιο-Μπενάκειο Ε.Ε.Σ.»,<br>Αθανασάκη 2, Τ.Κ. 11526 Αθήνα                   |
| Ημερομηνία Λήξης Κατάθεσης Προσφορών | Ημερομηνία: 22/06/2026 Ημέρα: Δευτέρα<br>Ωρα:14:00                                                      |
| Χρόνος Διενέργειας                   | Ημερομηνία: 23/06/2026 Ημέρα: Τρίτη<br>Ωρα 10:00                                                        |
| Τόπος Διενέργειας                    | Τμήμα Προμηθειών                                                                                        |
| Περιγραφή Είδους / Υπηρεσίας         | Παροχή Υπηρεσιών Κυβερνοασφάλειας & εναρμόνισης του νοσοκομείου με τον Ν.5160/2024 και την οδηγία ΝΙΣ 2 |
| Προϋπολογισθείσα Δαπάνη              | 24.190,00€ πλέον ΦΠΑ 24%                                                                                |

|                            |                                        |
|----------------------------|----------------------------------------|
| Διάρκεια της σύμβασης      | ΕΞΙ (6) ΜΗΝΩΝ                          |
| Χρόνος και Τόπος Παράδοσης | Γ.Ν.Α. «Κοργιαλέναιο-Μπενάκειο Ε.Ε.Σ.» |

Έχοντας υπόψη τις διατάξεις:

Του 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»

Του Ν.4727/2020 Ψηφιακή Διακυβέρνηση – Ηλεκτρονικές Υπηρεσίες

Του Ν.4412/2016 (ΦΕΚ147/8-8-2016 τ.Α΄) «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών (προσαρμογή στις Οδηγίες 2014/24/ΕΕ και 2014/25/ΕΕ)»

Του Ν.4542/2016 (Α΄95) άρθρο 4° «Ρυθμίσεις για την Εθνική Κεντρική Αρχή Προμηθειών Υγείας»

Του Ν.4270/2014 (Α'143) «Αρχές δημοσιονομικής διαχείρισης και εποπτείας (ενσωμάτωση της Οδηγίας 2011/85/ΕΕ) – δημόσιο λογιστικό και άλλες διατάξεις»

Του Ν.4152/2013, υποπαρ.Ζ5 περί συναλλαγών μεταξύ επιχειρήσεων και δημοσίων αρχών

Του Ν.3918/11, άρ.13 «Διαρθρωτικές αλλαγές στο σύστημα υγείας και άλλες διατάξεις»

Του Ν.3329/05 (ΦΕΚ81Α΄/4-4-05) «Εθνικό Σύστημα Υγείας και Κοινωνικής Αλληλεγγύης και λοιπές διατάξεις»

Του Π.Δ.80/2016 «Ανάληψη Υποχρεώσεων από τους Διατάκτες»

Των σε εκτέλεση των ανωτέρω νόμων εκδοθεισών κανονιστικών πράξεων, των λοιπών διατάξεων που αναφέρονται ρητά ή απορρέουν από τα οριζόμενα της παρούσας διακήρυξης, καθώς και του συνόλου των διατάξεων του ασφαλιστικού, εργατικού, κοινωνικού, περιβαλλοντικού και φορολογικού δικαίου που διέπει την ανάθεση και εκτέλεση της παρούσας σύμβασης, έστω και αν δεν αναφέρονται ρητά παραπάνω.

Σύμφωνα με τις αποφάσεις:

1. Την υπ' αριθ. πρωτ. 18995/10-06-2026 απόφαση του Διοικητικού Συμβουλίου (Συν. 19<sup>η</sup>/Θ.7<sup>ο</sup>/09-06-2026) με την οποία εγκρίνεται η σκοπιμότητα, οι τεχνικές προδιαγραφές και η έναρξη διαγωνιστικής διαδικασίας με απευθείας ανάθεση για την ανάδειξη αναδόχου, για την παροχή υπηρεσιών κυβερνοασφάλειας & εναρμόνισης του Νοσοκομείου με το Ν.5160/2024 με την οδηγία NIS 2, για διάστημα έξι (6) μηνών προϋπολογισμένης δαπάνης 24.190, 00€ πλέον ΦΠΑ 24% (29.995,60€ συμ/νου ΦΠΑ 24%).
2. Την Απόφαση Ανάληψης Υποχρέωσης με ΑΔΑ: Π9ΒΤ46904Χ-4ΕΕ

## ΠΡΟΣΚΑΛΟΥΜΕ

Σε κατάθεση γραπτών και σφραγισμένων προσφορών, για την ανάθεση της υπηρεσίας «Παροχή Υπηρεσιών κυβερνοασφάλειας & εναρμόνισης του Νοσοκομείου με το Ν.5160/2024 με την οδηγία NIS 2» με (CPV: 79417000-0\_Υπηρεσίες Παροχής συμβουλών σε θέματα ασφάλειας) προϋπολογισθείσας δαπάνης 24.190,00€ πλέον ΦΠΑ 24% με κριτήριο

κατακύρωσης την πλέον συμφέρουσα από οικονομική άποψη προσφορά αποκλειστικά βάσει τιμής.

Η αποσφράγιση των προσφορών θα γίνει στο Νοσοκομείο (Τμήμα Προμηθειών), ενώπιον επιτροπής, στις 23/06/2026 ημέρα Τρίτη και ώρα 10:00.

Η ημερομηνία λήξης κατάθεσης των προσφορών είναι η προηγούμενη (εργάσιμη) ημέρα από την ημερομηνία διενέργειας του διαγωνισμού, δηλαδή στις 22/06/2026, ημέρα Δευτέρα και ώρα 14:00.

Η κατάθεση των προσφορών θα γίνεται στο Πρωτόκολλο του Νοσοκομείου. Προσφορές που κατατίθενται στην Υπηρεσία μετά την παραπάνω ημερομηνία και ώρα είναι εκπρόθεσμες και θα επιστρέφονται χωρίς να αποσφραγισθούν.

Η διάρκεια της σύμβασης ορίζεται σε έξι (6) μήνες.

#### **Διευκρινήσεις:**

Το πλήρες κείμενο της πρόσκλησης είναι αναρτημένο σε ηλεκτρονική μορφή στην ιστοσελίδα της αναθέτουσας αρχής: <http://www.korgialenio-benakio.gr> → Διαγωνισμοί Προκηρύξεις Προμήθειες → Τμήμα Προμηθειών → Διαγωνισμοί – Προμήθειες → Documents → Α.Α. 20/2026 για την ανάδειξη αναδόχου για την υπηρεσία «Παροχή Υπηρεσιών κυβερνοασφάλειας & εναρμόνισης του Νοσοκομείου με το Ν.5160/2024 με την οδηγία NIS 2».

Δικαίωμα συμμετοχής στο διαγωνισμό έχουν φυσικά ή νομικά πρόσωπα ή ενώσεις/κοινοπραξίες αυτών ή συνεταιρισμοί που πληρούν τους όρους της Πρόσκλησης.

1. Το πλήρες κείμενο της πρόσκλησης δημοσιεύτηκε στο Κ.Η.Μ.ΔΗ.Σ. σύμφωνα με τα οριζόμενα στο Ν.4412/16.

2. **Η προσφορά να κατατεθεί στην ελληνική γλώσσα μέσα σε κλειστό σφραγισμένο φάκελο (κυρίως φάκελος) ο οποίος θα περιλαμβάνει τέσσερις υποφακέλους: έναν υποφάκελο με τα δικαιολογητικά συμμετοχής, έναν υποφάκελο με την τεχνική προσφορά, έναν υποφάκελο με την οικονομική προσφορά και έναν υποφάκελο με τα δικαιολογητικά κατακύρωσης.**

3. Ο κυρίως φάκελος θα φέρει τα πλήρη στοιχεία του αποστολέα, καθώς και τα στοιχεία της πρόσκλησης (τον αριθμό και τον τίτλο/αντικείμενο της πρόσκλησης, την επωνυμία της διενεργούντος προσκλήσεως και την ημερομηνία διενέργειας).

4. Μέσα στον κυρίως φάκελο τοποθετούνται τα παρακάτω:

Α) Καλά σφραγισμένος υποφάκελος με τα αναφερόμενα στο (3) σχετικά στοιχεία και την ένδειξη **ΔΙΚΑΙΟΛΟΓΗΤΙΚΑ ΣΥΜΜΕΤΟΧΗΣ** στον οποίο περιλαμβάνονται:

**Α1) Υπεύθυνη δήλωση** (όπως εκάστοτε ισχύει σε εφαρμογή και των άρθρων 1 και 3 του Ν. 4250/26-03-2014 (ΦΕΚ 74/Α/26-03-2014), του Ν. 1599/1986 στην οποία να αναγράφονται τα στοιχεία του διαγωνισμού, στον οποίο συμμετέχει ο οικονομικός φορέας και σύμφωνα με την οποία θα δηλώνεται ότι:

- Μέχρι και την ημέρα υποβολής της προσφοράς του ο οικονομικός φορέας δεν βρίσκεται σε μία από τις καταστάσεις των παρ. 1, 2 και 4β του άρθρου 73 και των παρ. 1 και 2 του άρθρου 74 για τις οποίες οι οικονομικοί φορείς αποκλείονται ή μπορούν να αποκλεισθούν από την συμμετοχή τους σε διαγωνισμούς του Δημοσίου.
- Αποδέχεται ανεπιφύλακτα τους όρους της παρούσας πρόσκλησης.

- Η προσφορά συντάχθηκε σύμφωνα με τους όρους της παρούσας πρόσκλησης των οποίων οι προσφέροντες έλαβαν πλήρη και ανεπιφύλακτη γνώση.
- Τα στοιχεία που αναφέρονται στην προσφορά είναι αληθή και ακριβή.
- Παραιτείται από κάθε δικαίωμα αποζημίωσής του σχετικά με οποιαδήποτε απόφαση της Αναθέτουσας Αρχής για αναβολή ή ακύρωση – ματαίωση του διαγωνισμού.
- Στην περίπτωση νομικών προσώπων, η υπογραφή της ως άνω Υπεύθυνης Δήλωσης απαιτείται από τον κατά περίπτωση νόμιμο εκπρόσωπο του οικονομικού φορέα.

**A2) Παραστατικό εκπροσώπησης** εφόσον συμμετέχει με αντιπρόσωπο τους.

**B)** Καλά σφραγισμένος υποφάκελος με την ένδειξη **ΤΕΧΝΙΚΗ ΠΡΟΣΦΟΡΑ** στον οποίο τοποθετείται η τεχνική προσφορά με τα απαιτούμενα δικαιολογητικά σε έντυπη μορφή (και σε ηλεκτρονική, **σε μορφή word** προς διευκόλυνση της Υπηρεσίας για την σύνταξη των αναλόγων πρακτικών). Στην τεχνική προσφορά ο προσφέρων θα δηλώνει αναλυτικά τη συμμόρφωση ή μη των προσφερόμενων ειδών/υπηρεσιών σε σχέση με τις αντίστοιχες προδιαγραφές της Πρόσκλησης (ΠΑΡΑΡΤΗΜΑ Α').

Οι συμμετέχοντες υποχρεούνται να υποβάλουν κάθε στοιχείο σχετικό με την αναφερόμενη προμήθεια/υπηρεσία, (πιστοποιήσεις ISO, CE, Βεβαιώσεις, κ.λπ.), που περιγράφονται στο **ΠΑΡΑΡΤΗΜΑ Α' (Τεχνικές Προδιαγραφές)** και να δηλώνουν το όνομα ή την Εμπορική Επωνυμία και Διεύθυνση του παραγωγού συσκευαστή.

**Γ)** Καλά σφραγισμένος υποφάκελος με τα ανωτέρω στοιχεία και την ένδειξη **ΟΙΚΟΝΟΜΙΚΗ ΠΡΟΣΦΟΡΑ** στον οποίο τοποθετείται η οικονομική προσφορά σε έντυπη μορφή (και σε ηλεκτρονική, **σε μορφή word** προς διευκόλυνση της Υπηρεσίας για την σύνταξη των αναλόγων πρακτικών). Η οικονομική προσφορά πρέπει να συμπληρωθεί και να υποβληθεί σύμφωνα με το υπόδειγμα (**ΠΑΡΑΡΤΗΜΑ Β'**).

**Δ)** Καλά σφραγισμένος υποφάκελος με τα αναφερόμενα στο (3) σχετικά στοιχεία και την ένδειξη **ΔΙΚΑΙΟΛΟΓΗΤΙΚΑ ΚΑΤΑΚΥΡΩΣΗΣ** στον οποίο περιλαμβάνονται:

Ο ανάδοχος προς απόδειξη της μη συνδρομής των λόγων αποκλεισμού από διαδικασίες σύναψης δημοσίων συμβάσεων των παρ.1 και 2 του άρθρου 73 του Ν.4412/2016 θα πρέπει να προσκομίσει τα παρακάτω δικαιολογητικά κατακύρωσης σύμφωνα με το άρθρο 80 του Ν.4412/2016.

**α. Απόσπασμα ποινικού μητρώου.** Απόσπασμα σχετικού μητρώου, όπως του ποινικού ή ελλείπει αυτού, ισοδύναμου εγγράφου 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. Η υποχρέωση αυτή αφορά: α) στις περιπτώσεις ΕΠΕ, ΟΕ και ΕΕ, τους διαχειριστές, β) στις περιπτώσεις ανωνύμων εταιρειών Α.Ε, τον Διευθύνοντα Σύμβουλο και όλα τα μέλη του ΔΣ. Αναλόγως να υποβληθεί το ισχύον κωδικοποιημένο καταστατικό του Γ.Ε.ΜΗ. από το οποίο να προκύπτουν οι διαχειριστές ή ο Διευθύνων Σύμβουλος ή τα μέλη του ΔΣ. γ) στις περιπτώσεις των συνεταιρισμών τα μέλη του Διοικητικού Συμβουλίου. Εκδίδεται έως τρείς (3) μήνες πριν από την υποβολή τους.

**β. Φορολογική ενημερότητα.** (Το παρόν πιστοποιητικό θα πρέπει να ισχύει κατά τον χρόνο υποβολής του).

**γ. Ασφαλιστική ενημερότητα** (άρθρο 80 παρ.2 του Ν.4412/2016) (Το παρόν πιστοποιητικό θα πρέπει να ισχύει κατά τον χρόνο υποβολής του).

**δ. Πιστοποιητικό ΓΕΜΗ ή το ισχύον καταστατικό** της εταιρείας από όπου προκύπτουν τα μέλη και ο νόμιμος εκπρόσωπος της εταιρείας (Το παρόν πιστοποιητικό γίνεται αποδεκτό εφόσον έχει εκδοθεί έως τριάντα (30) εργάσιμες ημέρες πριν την υποβολή του).

**ε. Υπεύθυνη Δήλωση** ότι τηρεί τις υποχρεώσεις τους στους τομείς του περιβαλλοντικού, κοινωνικοασφαλιστικού και εργατικού δικαίου, που έχουν θεσπίσει με το δίκαιο της Ένωσης, το εθνικό δίκαιο, συλλογικές συμβάσεις ή διεθνείς διατάξεις περιβαλλοντικού, κοινωνικοασφαλιστικού και εργατικού δικαίου, οι οποίες απαριθμούνται στο Παράρτημα Χ του Προσαρτήματος Α του Ν. 4412/2016.

**στ. Υπεύθυνη δήλωση** της εταιρείας/οικονομικού φορέα περί Αφερεγγυότητας, Πτώχευσης ή το αντίστοιχο Πιστοποιητικό από το αρμόδιο Πρωτοδικείο.

5. Οι τιμές των προσφορών για τα προσφερόμενα είδη/υπηρεσίες θα εκφράζονται σε ευρώ (€). Στην προσφερόμενη τιμή θα περιλαμβάνονται οι τυχόν υπέρ τρίτων κρατήσεις, ως και κάθε άλλη επιβάρυνση εκτός ΦΠΑ. **Οι προσφερόμενες τιμές αναγράφονται αριθμητικώς και ολογράφως, είναι δεσμευτικές καθ' όλη τη διάρκεια της σύμβασης. Προσφορές στις οποίες δεν προκύπτει με σαφήνεια η τιμή, που υπερβαίνουν την προϋπολογισθείσα δαπάνη ή που θέτουν όρο αναπροσαρμογής, απορρίπτονται ως μη κανονικές.** Εναλλακτικές προσφορές ή αντιπροσφορές απορρίπτονται.

6. Η ΑΠΟΣΦΡΑΓΙΣΗ του φακέλου των δικαιολογητικών συμμετοχής, των τεχνικών προσφορών, των οικονομικών προσφορών, και έπειτα των δικαιολογητικών κατακύρωσης γίνεται σε μία δημόσια συνεδρίαση.

7. Κατά την αποσφράγιση της προσφοράς δικαιούνται να παρίστανται ο προσφέρων στο διαγωνισμό ή οι νόμιμοι εκπρόσωποι αυτών, που απαραίτητα θα πρέπει να έχουν νόμιμο παραστατικό εκπροσώπησης.

8. **Κατά την αξιολόγηση η Υπηρεσία διατηρεί το δικαίωμα να ζητήσει οποιαδήποτε διευκρίνιση ή στοιχείο κρίνει απαραίτητο.**

9. Οι προσφορές θα ισχύουν για χρονικό διάστημα τουλάχιστον εκατόν ογδόντα (180) ημερών και θα αναγράφουν την αποδοχή των όρων της Πρόσκλησης.

10. Τρόπος Πληρωμής: Όλες οι πληρωμές θα γίνονται σε ευρώ (€) μετά τη διαδικασία της παραλαβής των υπηρεσιών από την Επιτροπή Παραλαβής και την προσκόμιση των νομίμων δικαιολογητικών που προβλέπονται από τις ισχύουσες διατάξεις κατά το χρόνο πληρωμής και σε χρόνο προσδιοριζόμενο από την αναγκαία διοικητική διαδικασία για έκδοση των σχετικών χρηματικών ενταλμάτων, σύμφωνα με τα όσα ορίζονται στην υποπαρ.Ζ5 του Ν.4152/13 «περί συναλλαγών μεταξύ επιχειρήσεων και δημοσίων αρχών».

11. Τον Ανάδοχο βαρύνουν οι υπέρ τρίτων κρατήσεις, ως και κάθε άλλη επιβάρυνση, σύμφωνα με την κείμενη νομοθεσία, μη συμπεριλαμβανομένου Φ.Π.Α. Ιδίως βαρύνεται με τις ακόλουθες κρατήσεις:

α) ποσοστό 0,1% υπέρ της Ενιαίας Αρχής Δημοσίων Συμβάσεων (Ε.Α.ΔΗ.ΣΥ.) (άρθρο 7 του ν.4912/2022), η οποία υπολογίζεται επί της αξίας κάθε πληρωμής προ φόρων και κρατήσεων της αρχικής, καθώς και κάθε συμπληρωματικής σύμβασης.

β) ποσοστό 2% επί του τιμολογίου της σύμβασης μετά την αφαίρεση του Φ.Π.Α. και κάθε άλλου ποσού παρακρατούμενου υπέρ τρίτων, σύμφωνα με την αριθμ. ΔΥ6α/Γ.Π./οικ. 36932/17-3-2009 Κ.Υ.Α. σε εφαρμογή του άρθρου 3 του Ν. 3580/2007.

Με κάθε πληρωμή θα γίνεται η προβλεπόμενη από την κείμενη νομοθεσία παρακράτηση φόρου εισοδήματος αξίας 8%, για υπηρεσίες και 4% για προμήθειες/αγαθά επί του καθαρού ποσού.

**Σημειώνεται ότι οι κρατήσεις θα προσαρμίζονται αυτόματα στην εκάστοτε ισχύουσα νομοθεσία.**

12. Σε περίπτωση αθέτησης των όρων της Σύμβασης, ο ανάδοχος κηρύσσεται έκπτωτος (άρθρο 203 του Ν.4412/16).
13. Για κάθε θέμα που δεν αναφέρεται ρητώς στην πρόσκληση, ισχύει η κείμενη Νομοθεσία.
14. Σε περίπτωση κατακύρωσης αντίστοιχου διαγωνισμού από την ΕΚΑΠΥ, την ΥΠΕ, το Υπουργείο ή άλλο Φορέα, μονομερώς το Νοσοκομείο και χωρίς δικαίωμα για αποζημίωση του αναδόχου, θα διακόψει την σύμβαση.
15. Η αναθέτουσα αρχή ματαιώνει ή δύναται να ματαιώσει εν όλω ή εν μέρει αιτιολογημένα τη διαδικασία ανάθεσης. Επίσης, αν διαπιστωθούν σφάλματα ή παραλείψεις σε οποιοδήποτε στάδιο της διαδικασίας ανάθεσης, μπορεί, να ακυρώσει μερικώς τη διαδικασία ή να αναμορφώσει ανάλογα το αποτέλεσμα της ή να αποφασίσει την επανάληψή της από το σημείο που εμφολόγησε το σφάλμα ή η παράλειψη. Κατά τα λοιπά εφαρμόζονται οι διατάξεις του άρθρου 106 του Ν.4412/2016.

Ο ΔΙΟΙΚΗΤΗΣ  
ΤΟΥ ΝΟΣΟΚΟΜΕΙΟΥ

ANASTASIOS KARANDREAS  
15/06/2026 09:31

ΑΝΑΣΤΑΣΙΟΣ ΚΑΡΑΝΔΡΕΑΣ

#### ΠΑΡΑΡΤΗΜΑ Α'

#### **ΠΡΟΔΙΑΓΡΑΦΕΣ-ΤΕΧΝΙΚΗ ΠΕΡΙΓΡΑΦΗ-ΟΡΟΙ**

#### **ΕΝΔΕΙΚΤΙΚΕΣ ΤΕΧΝΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΤΟΥ ΕΡΓΟΥ**

##### **Αντικείμενο Έργου**

Το παρόν έργο αφορά την επιλογή αναδόχου για την «Εναρμόνιση του ΓΝΑ Κοργιαλένιο Μπενάκειο ΕΕΣ 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)».

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.

#### Γενικοί 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.

Συγκεκριμένα ο Ανάδοχος αναλαμβάνει να παράσχει τις ακόλουθες υπηρεσίες:

1. **Πραγματοποίηση ελέγχου/ων δοκιμής/ων παρείσδυσης**, εσωτερικά και εξωτερικά και ανάλυσης κινδύνων του ΓΝΑ Κοργιαλένιο Μπενάκειο ΕΕΣ, με στόχο την ανάδειξη ευπαθειών ασφαλείας στις υποδομές πληροφορικής, την περιγραφή των επιπτώσεών τους στην εύρυθμη και ασφαλή λειτουργία του Νοσοκομείου, την πρόταση αντίμετρων για την μείωση του κινδύνου, ώστε να γίνει και συμμόρφωση με το NIS 2.

Κατά το παρόν έργο ο ανάδοχος θα πρέπει να αναγνωρίσει και αποτιμήσει τις ευπάθειες των υποδομών πληροφορικής.

2. **Security Audit** με στόχο την ολοκληρωμένη προσέγγιση της ασφάλειας του δικτύου και με σκοπό να ελεγχθούν συνολικά οι μηχανογραφικές υποδομές, οι επικοινωνίες και οι διαδικασίες της μηχανογράφησης και να υπάρξει συμμόρφωση κατά NIS 2.

3. **NIS 2 Gap Analysis**. Αναλυτική περιγραφή των υποδομών, των πολιτικών και διαδικασιών που απαιτούνται στο ΓΝΑ Κοργιαλένιο Μπενάκειο ΕΕΣ ώστε να συμμορφώνεται με το NIS 2.

4. **Υπηρεσία ISMS Implementation (Ανάπτυξη Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών)** με στόχο τη διαχείριση και αντιμετώπιση των κινδύνων ασφαλείας που σχετίζονται με την ψηφιακή πληροφορία, ώστε το νοσοκομείο να συμμορφώνεται με την οδηγία NIS 2.

5. **Risk Assessment** για την εκτίμηση των κινδύνων στην περίπτωση συμβάντος ασφαλείας. 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 χρίζουν επιπλέον αντίμετρα ώστε να μειωθεί το ρίσκο.

**6. Υπηρεσία CISO (Chief Information Security Officer)** για ένα (1) έτος, με ημερομηνία έναρξης μετά από την παράδοση και αποδοχή της μελέτης.

Σημείωση: Όλα τα παραδοτέα reports θα είναι γραμμένα στα Ελληνικά.

### **EXTERNAL-INTERNAL PENETRATION TEST**

Σκοπός του έργου είναι η πραγματοποίηση ελέγχου/ων δοκιμής/ων παρείσδυσης και ανάλυσης κινδύνων του ΓΝΑ Κοργιαλένιο Μπενάκειο ΕΕΣ, με στόχο την ανάδειξη ευπαθειών ασφαλείας στις υποδομές πληροφορικής, την περιγραφή των επιπτώσεών τους στην εύρυθμη και ασφαλή λειτουργία του Νοσοκομείου και την πρόταση αντίμετρων για την μείωση του κινδύνου.

Ο ανάδοχος θα πρέπει να αναγνωρίσει και να αποτιμήσει τις ευπάθειες των υποδομών πληροφορικής, αξιοποιώντας μεταξύ άλλων τεχνολογιών και εξειδικευμένη πλατφόρμα External Attack Surface Management (EASM), η οποία επιτρέπει τη συνεχή αναγνώριση, αποτύπωση και παρακολούθηση των externally exposed assets (domain names, IP addresses, network services, web applications), και υποστηρίζει τη διαδικασία αξιολόγησης ευπαθειών και δοκιμών παρείσδυσης. 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 αναγνώρισης τους. Η διαδικασία αυτή θα αναλυθεί στα ακόλουθα επίπεδα:

- α. Σε επίπεδο εφαρμογής χωρίς γνώση (BlackBox) (μόνο στην δικτυακή διεύθυνση της εφαρμογής)
- β. Σε επίπεδο εφαρμογής με γνώση (WhiteBox) (έχοντας συγκεκριμένα testaccounts).

#### **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, βάσει των αποτελεσμάτων της αποτύπωσης της εξωτερικής επιφάνειας επίθεσης μέσω πλατφόρμας EASM, και με χρήση συνδυασμού αυτοματοποιημένων τεχνικών και χειροκίνητων δοκιμών παρείσδυσης (manual penetration testing), σύμφωνα με διεθνή πρότυπα όπως OWASP Testing Guide, PTES και NIST SP 800-115.

Η διαδικασία αυτή θα αναλυθεί στα ακόλουθα επίπεδα:

- α. Σε επίπεδο εφαρμογής χωρίς γνώση (BlackBox) (μόνο στην δικτυακή διεύθυνση της εφαρμογής)
- β. Σε επίπεδο εφαρμογής με γνώση (WhiteBox) (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 ένα 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:

- Τα OWASP TOP 10 Vulnerabilities
- Επιθέσεις στο κανάλι σύνδεσης δεδομένων
- Επιθέσεις σε επίπεδο λειτουργικού συστήματος
- Επιθέσεις σε επίπεδο βάσης δεδομένων
- Επιθέσεις άρνησης υπηρεσιών (DoS attacks).
- Έλεγχοι ασφάλειας σε 2 κρίσιμες εφαρμογές. Ενδεικτικά αναφέρονται:
  - ο Πραγματοποίηση δοσοληψιών χωρίς εξουσιοδότηση
  - ο Απόκτηση δικαιωμάτων πρόσβασης σε ευαίσθητα δεδομένα χωρίς την κατάλληλη εξουσιοδότηση
  - ο Μη εξουσιοδοτημένη αλλαγή ή καταστροφή δεδομένων
  - ο Μη εξουσιοδοτημένη τροποποίηση λογισμικού 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 ότι 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 ασφαλείας, 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:**

ι.Μεθοδολογία Αναγνώρισης & αποτίμησης ευπαθειών, Διενέργειας Δοκιμών Παρείσδυσης.

α.Στα πλαίσια 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 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.

## **SECURITY AUDIT**

Το Security Audit ελέγχει την αρχιτεκτονική του δικτύου, συμπεριλαμβανομένων των επιμέρους στοιχείων του, με σκοπό την αναλυτική αποτύπωση του επιπέδου ασφάλειας. Εκτός των ελέγχων επί της παραμετροποίησης των δικτυακών συσκευών, ο ανάδοχος θα

ελέγξει και τις διαδικασίες που ακολουθούνται, καθώς και αυτές που συμβάλουν στο υφιστάμενο επίπεδο ασφάλειας. Αφού ελεγχθεί κάθε στοιχείο και διαδικασία του πληροφοριακού συστήματος, τα αποτελέσματα θα αξιολογηθούν και συγκριθούν με διεθνώς αναγνωρισμένα μέτρα προστασίας και πρακτικές.

Καθώς οι ανάγκες ασφάλειας δεν είναι ίδιες για όλες τις επιχειρήσεις, το IT Security Audit θα κατηγοριοποιήσει τις απαιτήσεις, ώστε το νοσοκομείο να επιλέξει το επίπεδο προστασίας στο οποίο στοχεύει και παράλληλα να γνωρίζει το επίπεδο ασφάλειας που έχει.

### **Ολοκλήρωση Ελέγχου**

Ο έλεγχος ολοκληρώνεται με τη καταγραφή των προβλημάτων, τη κατηγοριοποίησή τους ανάλογα με τη σοβαρότητά τους, την ανάλυση των κινδύνων κάθε ευρήματος και τέλος με προτάσεις για διορθώσεις και βελτιώσεις, ώστε το νοσοκομείο να αποκτήσει το επιθυμητό επίπεδο ασφάλειας.

Το IT Security Audit θα είναι ειδικά σχεδιασμένο για να:

- Αναγνωριστούν οι αδυναμίες και τα προβλήματα του δικτύου.
- Κατηγοριοποιηθούν τα προβλήματα ανάλογα με τη σημασία, την ευκολία ή το κόστος αποκατάστασής τους.
- Παρέχει προτάσεις για συνολική ασφάλεια, σε όλες τις παραμέτρους της μηχανογραφικής υποδομής.

### **Extended IT Security Audit**

Στο Extended IT Security Audit, ο έλεγχος θα γίνει βάσει των απαιτήσεων που έχει θέσει ο NIST (National Institute of Standards and Technology), στο Cyber security Framework και ελέγχονται τόσο τα υφιστάμενα τεχνικά αντίμετρα, όσο και η ύπαρξη επιμέρους εταιρικών πολιτικών για κρίσιμους τομείς της ασφάλειας.

### **NIS 2 GAP ANALYSIS**

Η οδηγία NIS 2 (Ασφάλεια των Συστημάτων Δικτύου και Πληροφοριών), ενισχύει σημαντικά τους κανονισμούς για την κυβερνοασφάλεια, σε ολόκληρη την Ευρωπαϊκή Ένωση και εφαρμόζεται σε ένα ευρύτερο φάσμα επιχειρήσεων, που δραστηριοποιούνται σε τομείς και υπηρεσίες ζωτικής σημασίας για βασικές κοινωνικές και οικονομικές δραστηριότητες, όπως είναι εταιρείες διαχείρισης λυμάτων, ταχυδρομικές υπηρεσίες, κατασκευαστικές εταιρείες και πάροχοι ψηφιακών υπηρεσιών.

Οι βασικοί στόχοι της οδηγίας είναι να θεσπίσει ένα κοινό κανονιστικό πλαίσιο, επιβάλλοντας μέτρα για την κυβερνοασφάλεια, όπως πρακτικές διαχείρισης κινδύνου, υποχρεώσεις αναφοράς συμβάντων και αξιολογήσεις ασφάλειας της εφοδιαστικής αλυσίδας. Δεύτερον, στοχεύει στη βελτίωση της συνεργασίας των μελών της ΕΕ σε επίπεδο απειλών κυβερνοασφάλειας, καθώς θα υποχρεώνει τις αρμόδιες αρχές, τις αρχές διαχείρισης κρίσεων στον κυβερνοχώρο και τις ομάδες αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (CSIRT), σε κάθε κράτος μέλος, να συνεργάζονται και να ανταλλάσσουν μεταξύ τους πληροφορίες.

Το Νοσοκομείο καλείται να επιτύχει, με την βοήθεια της πολιτικής ασφαλείας των πληροφοριακών συστημάτων, τους παρακάτω στόχους:

- Συμμόρφωση προς συγκεκριμένους κανόνες προστασίας.
- Συμμόρφωση προς συγκεκριμένους κανονισμούς.
- Βελτιστοποίηση της χρήσης οικονομικών πόρων και ανθρώπινου δυναμικού.

Το Cyber Security Policy Consulting, είναι συμβουλευτικές υπηρεσίες για την διαμόρφωση της Πολιτικής Ψηφιακής Ασφάλειας, που αφορούν την ορθή διαχείριση και αντιμετώπιση κινδύνων ασφαλείας της ψηφιακής πληροφορίας.

Η Υπηρεσία θα πρέπει να περιλαμβάνει

- Αποτύπωση αναγκών και υπάρχουσας κατάστασης.
- Ανάλυση και καταγραφή.
- Πολιτικές κατά NIS2.

### **ΑΝΑΠΤΥΞΗ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ ΚΑΤΑ NIS 2**

Οι πολιτικές ασφαλείας ISMS (Information Security Management System), αποτελούν το θεμέλιο για τη διαχείριση της ασφαλείας των πληροφοριών σε έναν οργανισμό, καθορίζοντας τις κατευθυντήριες γραμμές και τις διαδικασίες που εξασφαλίζουν την προστασία των δεδομένων και των συστημάτων. Περιλαμβάνουν την καθορισμένη κατανομή ρόλων και ευθυνών για την ασφάλεια, πολιτικές πρόσβασης για τον έλεγχο της πρόσβασης σε ευαίσθητα δεδομένα, διαδικασίες διαχείρισης κινδύνων για την αναγνώριση και αξιολόγηση απειλών, και μέτρα προστασίας για την αποφυγή απωλειών ή ζημιών. Αυτές οι πολιτικές βοηθούν στην εξασφάλιση της συμμόρφωσης με κανονισμούς και πρότυπα ασφαλείας, ενώ παρέχουν έναν οργανωμένο τρόπο για την προστασία των πληροφοριών και τη διαχείριση των σχετικών κινδύνων.

Η πολιτική ασφαλείας των πληροφοριακών συστημάτων, περιγράφει το σύνολο των κανόνων και των πρακτικών, που καθορίζουν τον τρόπο με τον οποίο ένας οργανισμός, πρέπει να διαχειρίζεται και να προστατεύει τους πόρους του, έτσι ώστε να πετύχει την μέγιστη δυνατή ασφάλεια.

Περιλαμβάνει ένα σύνολο πολιτικών και διαδικασιών, που έχουν ως στόχο τη διαχείριση των κινδύνων του πληροφοριακού συστήματος του οργανισμού, από απειλές όπως οι κυβερνοεπιθέσεις, οι παραβιάσεις των συστημάτων, οι διαρροές δεδομένων ή η κλοπή.

Το Νοσοκομείο θα επιτύχει, με την εφαρμογή της Πολιτικής Ασφάλειας Πληροφοριακών Συστημάτων, τους ακόλουθους στόχους:

- Συμμόρφωση με το ισχύον κανονιστικό και θεσμικό πλαίσιο προστασίας πληροφοριών και πληροφοριακών συστημάτων.
- Συμμόρφωση με τις απαιτήσεις εθνικών και διεθνών κανονισμών και προτύπων κυβερνοασφάλειας.
- Βελτιστοποίηση της χρήσης των διαθέσιμων οικονομικών πόρων και του ανθρώπινου δυναμικού, μέσω της εφαρμογής δομημένων διαδικασιών διαχείρισης ασφαλείας πληροφοριών.
- Ενίσχυση της δυνατότητας παρακολούθησης, ανάλυσης και διαχείρισης συμβάντων ασφαλείας μέσω εγκατάστασης και λειτουργίας πλατφόρμας παρακολούθησης ασφαλείας (Security Platform), η οποία θα υποστηρίζει τη συλλογή και ανάλυση αρχείων καταγραφής (Log Management & Log Analysis), την ενίσχυση της ορατότητας της πληροφοριακής υποδομής και του δικτύου (Infrastructure & Network Visibility), την αναγνώριση και ταξινόμηση συμβάντων και απειλών (Security Event Identification and Threat Classification), την παραγωγή ειδοποιήσεων βάσει κανόνων και τεχνικών Τεχνητής Νοημοσύνης (Rule-based and AI/ML Alerting), την παρακολούθηση συμμόρφωσης (Compliance Monitoring), την υποστήριξη της διαχείρισης ενημερώσεων ασφαλείας (Security Patch Management), καθώς και την παραγωγή αναφορών (Reporting) για την τεκμηρίωση της αξιολόγησης κινδύνου και της συμμόρφωσης.
- Ενίσχυση της τεχνικής επάρκειας του προσωπικού μέσω παροχής πρόσβασης σε πλατφόρμα εκπαίδευσης κυβερνοασφάλειας (Cyber Defense Academy), η οποία θα παρέχει

εξειδικευμένη τεχνική εκπαίδευση σε τεχνικούς χρήστες, δυνατότητα παρακολούθησης της εκπαιδευτικής προόδου και παροχή πιστοποίησης (Certification), συμβάλλοντας στη διαρκή ενίσχυση της επιχειρησιακής ετοιμότητας και συμμόρφωσης του Νοσοκομείου.

Η Πολιτική Ψηφιακής Ασφάλειας, αποτελεί κατευθυντήρια γραμμή στη διαχείριση και αντιμετώπιση κινδύνων ασφαλείας, που αφορούν τη ψηφιακή πληροφορία. Καθορίζει τη δέσμευση της Διοίκησης και την προσέγγιση του νοσοκομείου αναφορικά με την ασφάλεια των πληροφοριακών συστημάτων και δικτύων και την προστασία δεδομένων. Στόχος είναι να διασφαλιστεί καλύτερα η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των πληροφοριών μέσω της συνεχούς βελτίωσης του επιπέδου ασφαλείας.

Ο στόχος επιτυγχάνεται θέτοντας τις βασικές αρχές για:

α) τα οργανωτικά μέτρα ασφαλείας αναφορικά με τους ρόλους και τις αρμοδιότητες του προσωπικού, την εκπαίδευση του προσωπικού, τη διαχείριση περιστατικών ασφαλείας, την διαχείριση των εξωτερικών συνεργατών, καθώς και για την καταστροφή δεδομένων.

β) τα τεχνικά μέτρα ασφαλείας αναφορικά με τη διαχείριση των χρηστών του πληροφοριακού συστήματος, την αυθεντικοποίηση των χρηστών, την ασφάλεια των επικοινωνιών, τη λειτουργία των αρχείων καταγραφής του πληροφοριακού συστήματος, την εξαγωγή αντιγράφων ασφαλείας.

γ) τα μέτρα φυσικής ασφαλείας.

Ο ανάδοχος θα αναπτύξει τις πολιτικές ασφαλείας σε συνεργασία με το τμήμα πληροφορικής και τη διοίκηση, για να καλυφθούν όλες οι απαιτήσεις του NIS2.

### **RISK ASSESSMENT**

Το Risk Assessment σκοπεύει στην εκτίμηση των κινδύνων στην περίπτωση συμβάντος ασφαλείας. 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 χρίζουν επιπλέον αντίμετρα, 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 ασφαλείας πληροφοριών του νοσοκομείου (Risk Registry).
- Διενέργεια άσκησης Εκτίμησης Επιχειρησιακού Αντικτύπου (Business Impact Analysis).
- Υπολογισμός πρωταρχικών κινδύνων (Inherent Risk Rating).
- Διενέργεια άσκησης αξιολόγησης των δικλείδων ασφαλείας 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 ασφαλείας 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.

### **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 (Cybersecurity Consulting Services), συμπεριλαμβανομένης υποστήριξης στη χρήση εργαλείων παρακολούθησης ασφάλειας, αξιολόγησης ευρημάτων vulnerability assessment και penetration testing, τεκμηρίωσης συμμόρφωσης με NIS2 και ανάπτυξης σχεδίων μετριασμού κινδύνων, 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.

Υπηρεσίες Υποστήριξης ΥΑΣΠΕ του ΓΝΑ Κοργιαλένιο Μπενάκειο ΕΕΣ.

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:

- 1) Διαρκής μέριμνα για την ασφάλεια των συστημάτων δικτύου και πληροφοριών.
- 2) Συνεργασία με τους αρμόδιους φορείς κυβερνοασφάλειας και εφαρμογή κατευθυντήριων οδηγιών και μέτρων.
- 3) Τήρηση μητρώου του φορέα με υποδομές πληροφορικής και επικοινωνιών, λογισμικό και πληροφοριακά αγαθά.
- 4) Συμμετοχή στη διενέργεια ελέγχων για διακρίβωση του υφιστάμενου επιπέδου ασφάλειας.
- 5) Εποπτεία της τήρησης της πολιτικής ασφάλειας συστημάτων πληροφορικής και επικοινωνιών.
- 6) Παρακολούθηση και αξιοποίηση νέων τεχνολογιών και εργαλείων ασφάλειας για ενίσχυση του επιπέδου κυβερνοασφάλειας.
- 7) Διενέργεια αξιολογήσεων του επιπέδου κυβερνοασφάλειας σε συνεργασία με τις αρμόδιες αρχές.
- 8) Εγκατάσταση και επικαιροποίηση λογισμικού προστασίας από κυβερνοεπιθέσεις, παρέχοντας:
- 9) Threat Detection και Παρακολούθηση σε Πραγματικό Χρόνο.
- 10) Ανάλυση Δεδομένων Καταγραφής και Integrity Monitoring με ταυτόχρονη παρακολούθηση υποδομών και δικτύου (Infrastructure and Network Monitoring)
- 11) Compliance Management και Vulnerability Detection.
- 12) Security Configuration Assessment.
- 13) Email Alerts για αντιμετώπιση Συμβάντων.
- 14) Ο ανάδοχος θα παρέχει επικαιροποιήσεις και ανανεώσεις του λογισμικού καθ' όλη τη διάρκεια της Σύμβασης.
- 15) Σύνταξη προτάσεων για βελτίωση του επιπέδου ασφάλειας του Φορέα σε σχέση με την Κυβερνοασφάλεια και τα πληροφοριακά συστήματα.
- 16) Σύνταξη των απαραίτητων προτάσεων για Πολιτικές Ασφάλειας Πληροφοριών και Ασφάλειας συστημάτων Πληροφορικής.
- 17) Σύνταξη διαδικασίας για την επικοινωνία με την Εθνική Αρχή Κυβερνοασφάλειας σε περίπτωση περιστατικών.
- 18) Σύνταξη Disaster Recovery Plan.
- 19) Εκτίμηση του ρίσκου που λαμβάνει ο Φορέας βάσει των υποδομών του.

Η συνολική διάρκεια των υπηρεσιών του αναδόχου θα είναι έξι (6) μήνες από την υπογραφή της Σύμβασης.

Παραδοτέα:

- 2 μηνιαία 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.

**Ο υποψήφιος ανάδοχος, επί ποινής αποκλεισμού οφείλει:**

- Να είναι πιστοποιημένος κατά:
  - ISO 27001
  - ISO 14001
  - ISO 22301
  - ISO 9001

- Να διαθέτει τουλάχιστον τρεις τεχνικούς με τις παρακάτω πιστοποιήσεις:
  - Cyber Security Foundations: A Beginner's Guide to Awareness and Protection
  - Cybersecurity Compliance Framework, Standards & Regulations: NIS2 Essentials
  - SOC Analyst Tier 1
- Να διαθέτει την παρακάτω πιστοποίηση:
  - Πιστοποιημένος Υπεύθυνος Ασφάλειας Συστημάτων- NIS2
- Προς απόδειξη να καταθέσει αντίγραφο των ανωτέρω σχετικών πιστοποιητικών και πιστοποιήσεων.

#### **ΠΡΟΫΠΟΘΕΣΕΙΣ ΓΙΑ ΤΟΝ ΑΝΑΔΟΧΟ**

Οι παρακάτω εργασίες απαιτείται να ολοκληρωθούν σε περίοδο 6 μηνών, εφόσον υπάρχει η σχετική διαθεσιμότητα του τμήματος πληροφορικής του νοσοκομείου.

- External Pen test
- Internal Pen test
- IT Audit
- NIS 2 GAP analysis
- NIS 2 Πολιτικές
- Risk Assessment

#### **ΧΡΟΝΟΣ ΠΑΡΑΔΟΣΗΣ ΤΩΝ ΥΠΗΡΕΣΙΩΝ**

Η συνολική διάρκεια υλοποίησης της υπηρεσίας ορίζεται στους έξι (6) μήνες από την υπογραφή της σύμβασης.

Ουδεμία μεταβολή του προγράμματος παράδοσης επιτρέπεται χωρίς την έγκριση της Αναθέτουσας Αρχής, ο δε συμβατικός χρόνος παράδοσης δύναται να παραταθεί υπό τις κάτωθι σωρευτικές προϋποθέσεις:

Α) η τροποποίηση της σύμβασης λόγω της παρατάσεως αυτής να είναι σύμφωνη με τους περιορισμούς του άρθρου 132 του ν.4412/2016.

Β) να έχει εκδοθεί αιτιολογημένη απόφαση του αρμόδιου αποφαινόμενου οργάνου της αναθέτουσας αρχής μετά από γνωμοδότηση αρμοδίου συλλογικού οργάνου είτε με πρωτοβουλία της αναθέτουσας αρχής και εφόσον συμφωνεί ο ανάδοχος είτε ύστερα από σχετικό αίτημα του αναδόχου, το οποίο υποβάλλεται υποχρεωτικά πριν από τη λήξη του συμβατικού χρόνου παράδοσης.

Γ) η παράταση έως του 50% από τον αρχικό συμβατικό χρόνο παράδοσης.

Στην περίπτωση παράτασης του συμβατικού χρόνου παράδοσης, ο χρόνος παράτασης δεν συνυπολογίζεται στο συμβατικό χρόνο παράδοσης.

Εάν λήξει ο συμβατικός χρόνος παράδοσης, χωρίς να υποβληθεί εγκαίρως αίτημα παράτασης ή, εάν λήξει ο παραταθείς, κατά τα ανωτέρω, χρόνος, χωρίς να παραδοθεί η υπηρεσία, ο ανάδοχος κηρύσσεται έκπτωτος.

#### **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.

### **ΠΑΡΑΡΤΗΜΑ Β'**

#### **Υπόδειγμα Οικονομικής Προσφοράς**

Οικονομικές προσφορές των συμμετεχόντων θα υποβληθούν με τη συμπλήρωση του παρακάτω πίνακα:

|                           |                                                           |
|---------------------------|-----------------------------------------------------------|
| Επωνυμία εταιρείας        |                                                           |
| Έδρα                      |                                                           |
| ΑΦΜ                       |                                                           |
| Όνομα προσφέροντος        |                                                           |
| Στοιχεία επικοινωνίας     |                                                           |
| Διάρκεια ισχύος προσφοράς | 180 ημέρες από την ημερομηνία διενέργειας της Πρόσκλησης. |
| Υπογραφή                  |                                                           |
| Σφραγίδα                  |                                                           |

#### **ΚΟΙΝΟΠΟΙΗΣΗ**

Γρ. Προέδρου Δ.Σ.  
Γρ. Διοικητή  
Γρ. Αν. Διοικητή  
Δ/νση Διοικ.-Οικ. Υπηρεσίας  
Υποδ/νση Οικονομικού  
Τμήμα Πληροφορικής και Οργάνωσης