ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ & ΚΟΙΝΩΝΙΚΗΣ ΑΛΛΗΛΕΓΓΥΗΣ – ΔΙΟΙΚΗΣΗ 1ης ΥΠΕ ΑΤΤΙΚΗΣ
ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΑΤΤΙΚΗΣ ΣΙΣΜΑΝΟΓΛΕΙΟ - ΑΜΑΛΙΑ ΦΛΕΜΙΓΚ Ν.Π.Δ.Δ.

ΔΙΕΥΘΥΝΣΗ ΔΙΟΙΚΗΤΙΚΟΥ
ΥΠΟΔΙΕΥΘΥΝΣΗ ΟΙΚΟΝΟΜΙΚΟΥ
ΤΜΗΜΑ ΠΡΟΜΗΘΕΙΩΝ- ΔΙΑΧΕΙΡΙΣΗΣ ΥΛΙΚΟΥ
ΓΡΑΦΕΙΟ ΠΡΟΜΗΘΕΙΩΝ
ΠΛΗΡ: Α. Οικονομοπούλου
ΤΗΛ: 213 2058539
E-mail: a.oikonomopoulou@sismanoglio.gr

ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΚΗΜΔΗΣ

ΑΡ.ΠΡΩΤ.: 23676
ΗΜΕΡ: 17-09-2025

ΠΡΟΣ ΚΑΘΕ ΕΝΔΙΑΦΕΡΟΜΕΝΟ

ΠΡΟΣΚΛΗΣΗ ΥΠΟΒΟΛΗΣ ΠΡΟΣΦΟΡΩΝ ΓΙΑ ΤΗΝ ΑΠΕΥΘΕΙΑΣ ΑΝΑΘΕΣΗ Νο ΑΑ 13/2025 ΓΙΑ ΤΗΝ ΑΝΑΔΕΙΞΗ ΑΝΑΔΟΧΟΥ ΓΙΑ ΤΙΣ «ΥΠΗΡΕΣΙΕΣ ΕΚΠΟΝΗΣΗΣ ΜΕΛΕΤΗΣ ΓΙΑ ΤΗΝ ΑΞΙΟΛΟΓΗΣΗ ΤΩΝ ΕΥΠΑΘΕΙΩΝ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΕΚΤΙΜΗΣΗΣ ΚΙΝΔΥΝΟΥ (GAP ANALYSIS- RISK ASSESSMENT» (CPV: 79417000-0)

ΑΝΤΙΚΕΙΜΕΝΟ ΤΟΥ ΔΙΑΓΩΝΙΣΜΟΥ – ΣΥΝΟΠΤΙΚΑ ΣΤΟΙΧΕΙΑ

Είδος διαγωνισμού	ΑΠΕΥΘΕΙΑΣ ΑΝΑΘΕΣΗ
Αναθέτουσα Αρχή	ΝΠΔΔ Γ.Ν.Α «Σισμανόγλειο- Αμαλία Φλέμιγκ»
Κριτήριο Κατακύρωσης	πλέον συμφέρουσα από οικονομική άποψη προσφορά αποκλειστικά βάσει τιμής
Τόπος υποβολής Προσφορών	Πρωτόκολλο Γ.Ν.Α «Σισμανόγλειο- Αμαλία Φλέμιγκ» και Γραφείο Προμηθειών, Σισμανογλείου 1, 151 26- Μαρούσι
Ημερομηνία Λήξης Κατάθεσης Προσφορών	**09/10/2025 ημέρα ΠΕΜΠΤΗ ώρα 14:00μμ**
Χρόνος Διενέργειας	**10/10/2025 ημέρα ΠΑΡΑΣΚΕΥΗ ώρα 11:00πμ**
Τόπος Διενέργειας	Γραφείο Προμηθειών του Νοσοκομείου, Σισμανογλείου 1, 151 26- Μαρούσι
Περιγραφή Είδους/Υπηρεσίας	**ΓΙΑ ΤΗΝ ΑΝΑΔΕΙΞΗ ΑΝΑΔΟΧΟΥ ΓΙΑ ΤΙΣ «ΥΠΗΡΕΣΙΕΣ ΕΚΠΟΝΗΣΗΣ ΜΕΛΕΤΗΣ ΓΙΑ ΤΗΝ ΑΞΙΟΛΟΓΗΣΗ ΤΩΝ ΕΥΠΑΘΕΙΩΝ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΕΚΤΙΜΗΣΗΣ ΚΙΝΔΥΝΟΥ (GAP ANALYSIS- RISK ASSESSMENT» (CPV: 79417000-0)**
Προϋπολογισθείσα ετήσια δαπάνη	**30.000,00 € πλέον ΦΠΑ**
Διάρκεια της σύμβασης	Από την υπογραφή της και για ένα (1) έτος
Χρόνος και Τόπος Παράδοσης	Γ.Ν.Α «Σισμανόγλειο- Αμαλία Φλέμιγκ

Έχοντας υπόψη τις διατάξεις όπως έχουν τροποποιηθεί και ισχύουν:

1. του Ν 4412/2016 (ΦΕΚ 147/Α/08-08-2016) «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών (Προσαρμογή στις οδηγίες 2014/24/ΕΕ και 201/25/ΕΕ).
2. 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»
3. του Ν. 4727/2020 Ψηφιακή Διακυβέρνηση- Ηλεκτρονικές Υπηρεσίες.
4. το Ν.4412/2016 (ΦΕΚ 147/8-8-2016 τ.Α΄) «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών (προσαρμογή στις Οδηγίες 2014/24/ΕΕ και 2014/25/ΕΕ)»
5. του Ν.4542/2016 (Α΄95) άρθρο τέταρτο «Ρυθμίσεις για την Εθνική Κεντρική Αρχή Προμηθειών Υγείας»
6. το Ν.4152/2013, υποπαρ.Ζ5 περί συναλλαγών μεταξύ επιχειρήσεων και δημοσίων αρχών.
7. τις διατάξεις του Ν.3918/11, άρ.13 «Διαρθρωτικές αλλαγές στο σύστημα υγείας και άλλες διατάξεις»

8.τις διατάξεις του Ν.3329/05 (ΦΕΚ 81 Α'/4-4-05) «Εθνικό Σύστημα Υγείας και Κοινωνικής Αλληλεγγύης και λοιπές διατάξεις»

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

10. τις άμεσες και επιτακτικές ανάγκες του Νοσοκομείου «ΣΙΣΜΑΝΟΓΛΕΙΟ – ΑΜΑΛΙΑ ΦΛΕΜΙΓΚ»

11. Την υπ' αρίθμ. 23070/10-09-2025 απόφαση της Διοικήτριας του «ΓΝΑ ΣΙΣΜΑΝΟΓΛΕΙΟ- ΑΜ. ΦΛΕΜΙΓΚ», λόγω έλλειψης Διοικητικού Συμβουλίου.

12. την απόφαση ανάληψης υποχρέωσης με ΑΔΑ: ΨΖΡΠ4690Ω5-ΩΗΥ.

13. 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.

ΠΡΟΣΚΑΛΟΥΜΕ

σε κατάθεση γραπτής και σφραγισμένης προσφοράς, **ΓΙΑ ΤΗΝ ΑΝΑΔΕΙΞΗ ΑΝΑΔΟΧΟΥ ΓΙΑ ΤΙΣ «ΥΠΗΡΕΣΙΕΣ ΕΚΠΟΝΗΣΗΣ ΜΕΛΕΤΗΣ ΓΙΑ ΤΗΝ ΑΞΙΟΛΟΓΗΣΗ ΤΩΝ ΕΥΠΑΘΕΙΩΝ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΕΚΤΙΜΗΣΗΣ ΚΙΝΔΥΝΟΥ (GAP ANALYSIS- RISK ASSESSMENT» (CPV: 79417000-0).**

Η αποσφράγιση της προσφοράς θα γίνει στο Νοσοκομείο (Γραφείο Προμηθειών) ενώπιον επιτροπής, στις 10-10-2025, ημέρα ΠΑΡΑΣΚΕΥΗ, ώρα 11.00π.μ.

Η ημερομηνία λήξης κατάθεσης των προσφορών είναι η προηγούμενη (εργάσιμη) ημέρα από την ημερομηνία διενέργειας του διαγωνισμού, δηλαδή στις 09-10-2025 ημέρα ΠΕΜΠΤΗ και ώρα 14:00 ήτοι τουλάχιστον πέντε (5) ημέρες μετά τη δημοσίευση της παρούσας στο ΚΗΜΔΗΣ. Η κατάθεση των προσφορών θα γίνεται στο Γραφείο Προμηθειών αφού προηγουμένως πρωτοκολληθούν στη Γραμματεία του Νοσοκομείου. Προσφορές που κατατίθενται στην Υπηρεσία μετά την παραπάνω ημερομηνία είναι εκπρόθεσμες και θα επιστρέφονται χωρίς να αποσφραγισθούν.

Η διάρκεια της σύμβασης ορίζεται σε ένα (1) έτος από την υπογραφή της σχετικής σύμβασης.

Διευκρινήσεις:

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

2. Το πλήρες κείμενο της πρόσκλησης δημοσιεύτηκε στον ιστότοπο του ΓΝΑ ΣΙΣΜΑΝΟΓΛΕΙΟ- ΑΜ. ΦΛΕΜΙΓΚ www.sismanoglio.gr

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

4. 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 του διενεργούντος το διαγωνισμό και την ημερομηνία διενέργειας).

5. Μέσα στον κυρίως φάκελο τοποθετούνται τα παρακάτω:

Α) Καλά σφραγισμένος υποφάκελος με τα ανωτέρω 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.
- Συμμετέχει σε μια μόνο σε μια μόνο προσφορά στο πλαίσιο του παρόντος διαγωνισμού. Στην περίπτωση νομικών προσώπων, η υπογραφή της ως άνω Υπεύθυνης Δήλωσης απαιτείται από τον κατά περίπτωση νόμιμο εκπρόσωπο του οικονομικού φορέα

Α2) Παραστατικό εκπροσώπησης εφόσον οι προμηθευτές συμμετέχουν με αντιπρόσωπο τους

Β) Καλά σφραγισμένος υποφάκελος με την ένδειξη **ΤΕΧΝΙΚΗ ΠΡΟΣΦΟΡΑ** στον οποίο τοποθετείται η τεχνική προσφορά με τα απαιτούμενα δικαιολογητικά και αντίγραφο αυτής σε έντυπη και ηλεκτρονική μορφή. Στην τεχνική προσφορά ο προσφέρων θα δηλώνει αναλυτικά τη συμμόρφωση ή μη των προσφερόμενων ειδών σε σχέση με τις αντίστοιχες προδιαγραφές της Διακήρυξης (ΠΑΡΑΡΤΗΜΑ Α΄).

Γ) Καλά σφραγισμένος υποφάκελος με τα ανωτέρω στοιχεία και την ένδειξη **ΟΙΚΟΝΟΜΙΚΗ ΠΡΟΣΦΟΡΑ** στον οποίο τοποθετείται η οικονομική προσφορά και αντίγραφο αυτής σε έντυπη μορφή και ηλεκτρονική μορφή.

6. 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.

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

8. Κατά την αποσφράγιση των προσφορών δικαιούνται να παρίστανται οι προσφέροντες στο διαγωνισμό ή οι νόμιμοι εκπρόσωποι αυτών, που απαραίτητα θα πρέπει να έχουν νόμιμο παραστατικό εκπροσώπησης.

9. Κατά την αξιολόγηση η Υπηρεσία διατηρεί το δικαίωμα να ζητήσει οποιοδήποτε διευκρίνιση ή στοιχείο κρίνει απαραίτητο.

10. Ο τελικός 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 κατά την υπογραφή της σύμβασης τα παρακάτω δικαιολογητικά κατακύρωσης σύμφωνα με το άρθρο 80 του Ν.4412/2016**. Ήτοι:**

α. Απόσπασμα ποινικού μητρώου. Που εκδίδεται έως τρεις (3) μήνες πριν από την υποβολή τους Η υποχρέωση αφορά ιδίως: αα) στις περιπτώσεις εταιρειών περιορισμένης ευθύνης (Ε.Π.Ε.) και προσωπικών εταιρειών (Ο.Ε. και Ε.Ε.), τους διαχειριστές, ββ) στις περιπτώσεις ανωνύμων εταιρειών (Α.Ε.), τον Διευθύνοντα Σύμβουλο, καθώς και όλα τα μέλη του Διοικητικού Συμβουλίου, γγ) στις περιπτώσεις των συνεταιρισμών τα μέλη του Διοικητικού συμβουλίου.

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).

Σε περίπτωση αδυναμίας προσκόμισης των ανωτέρω πιστοποιητικών εντός δέκα (10) ημερών από τη σχετική πρόσκληση ο υποψήφιος ανάδοχος αποκλείεται από τη διαδικασία και καλείται ο αμέσως επόμενος στην κατάταξη συμμετέχων.

11. **Με την υπογραφή** της σύμβασης, ο προμηθευτής υποχρεούται στην έκδοση εγγυητικής επιστολής καλής εκτέλεσης, ίση με το 4% της συμβατικής αξίας χωρίς να υπολογίζεται ο ΦΠΑ, ισχύος τουλάχιστον δύο (2) μήνες επιπλέον της λήξης της σύμβασης.
12. **Οι προσφορές** θα ισχύουν για χρονικό διάστημα τουλάχιστον εκατόν ογδόντα (180) ημερών και θα αναγράφουν την αποδοχή των όρων της πρόσκλησης.
13. **Τρόπος Πληρωμής**: Όλες οι πληρωμές θα γίνονται σε ευρώ (€) μετά τη διαδικασία της οριστικής παραλαβής των προς προμήθεια ειδών 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».
14. **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:

- 0,2% υπέρ Οργανισμών Ψυχικής Υγείας (ΦΕΚ 545 Β’ /24-3-’09).
- 0,1% υπέρ ΕΑΑΔΗΣΥ (Ν.4912/17.3.22 ΦΕΚ Α 59)
- 8% παρακράτηση φόρου εισοδήματος, σύμφωνα με το άρθρο 24 του Ν.2198/1994.
- Υπέρ Γ.Δ.Δ.Σ.Π. 0,02% (άρθρο 36 παρ 6 Ν. 4412/2016) - εκκρεμεί η έκδοση ΚΥΑ

15. Σε περίπτωση αθέτησης των όρων της Σύμβασης, ο ανάδοχος κηρύσσεται έκπτωτος (άρθρο 203 του Ν 4412/16).
16. Για κάθε θέμα που δεν αναφέρεται ρητώς στη διακήρυξη, ισχύει η κείμενη Νομοθεσία**.**
17. 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.
18. 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 αποτέλεσμά της ή να αποφασίσει την επανάληψή της από το σημείο που εμφιλοχώρησε το σφάλμα ή η παράλειψη. Κατά τα λοιπά εφαρμόζονται οι διατάξεις του άρθρου 106 του Ν.4412.2016.

Ειδικοί Όροι

1. Σύμφωνα με την υπ΄ αριθμ. 52445ΕΞ2023 (ΦΕΚ 2385/12.04.2023)ΚΥΑ από 01.06.2024 οικονομικοί φορείς υποχρεούνται να υποβάλλουν ηλεκτρονικά τιμολόγια, για συμβάσεις αξίας μεγαλύτερης των 2.500 €.
2. Στην προσφορά πρέπει να δηλώνεται η δυνατότητα του προμηθευτή για την έκδοση ηλεκτρονικού τιμολογίου

Η Διοικήτρια
του Νοσοκομείου

Ζωή Ρακοπούλου

ΠΑΡΑΡΤΗΜΑ Α

ΑΝΑΛΥΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΦΥΣΙΚΟΥ ΑΝΤΙΚΕΙΜΕΝΟΥ – ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

Α. ΑΝΤΙΚΕΙΜΕΝΟ

Αντικείμενο της παρούσας σύνταξης προδιαγραφών είναι η παροχή υπηρεσιών με σκοπό την προσαρμογή και εναρμόνιση του Γενικού Νοσοκομείου Σισμανόγλειο – Αμ. Φλέμιγκ (Νοσοκομειακή Μονάδα «Σισμανόγλειο» και Νοσοκομειακή Μονάδα Αμαλία Φλέμιγκ) (εφεξής Φορέας) στις διατάξεις του Ν.5160/2024 «Ενσωμάτωση της Οδηγίας (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του Κανονισμού (ΕΕ) 910/2014 και της Οδηγίας (ΕΕ) 2018/1972, και την κατάργηση της Οδηγίας (ΕΕ) 2016/1148 (Οδηγία NIS2) και άλλες διατάξεις», της κοινής υπουργικής απόφασης Υπουργείων «Εθνικής Οικονομίας και Οικονομικών» και «Ψηφιακής Διακυβέρνησης» σχετικά με «Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων» (ΦΕΚ Β’ 186/06.05.2025) και γενικά την ενίσχυση της ανθεκτικότητας του Φορέα απέναντι στους κινδύνους του Κυβερνοχώρου.

Β. ΤΟΠΟΣ ΚΑΙ ΧΡΟΝΟΣ ΠΑΡΟΧΗΣ ΤΗΣ ΥΠΗΡΕΣΙΑΣ

Ο Ανάδοχος θα παρέχει τις υπηρεσίες από την έδρα του και στους χώρους των δύο Νοσοκομειακών Μονάδων «Σισμανόγλειο» και «Αμαλία Φλέμιγκ» του Γενικού Νοσοκομείου Σισμανόγλειο - Αμ. Φλέμιγκ.

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

Γ. ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

Στο αντικείμενο του έργου συμπεριλαμβάνονται:

1. Καταγραφή Πληροφοριακών Assets

Συγκέντρωση, ανάλυση και καταγραφή όλων των πληροφοριακών και τεχνολογικών Assets του Φορέα.

2. Internal Penetration test

- Port Scanning – Vulnerability assessment – Pen Test.
- Report Ευρημάτων – Κατηγοριοποίηση – Προτάσεις αποκατάστασης.

3. External Penetration test

- Port Scanning – Vulnerability assessment – Pen Test.
- Report Ευρημάτων – Κατηγοριοποίηση – Προτάσεις αποκατάστασης.
- Phishing Campaign.

Πραγματοποίηση ελέγχου/ων δοκιμής/ων παρείσδυσης, εσωτερικά και εξωτερικά και ανάλυσης κινδύνων, με στόχο την ανάδειξη ευπαθειών ασφαλείας στις υποδομές πληροφορικής, την περιγραφή των επιπτώσεων τους στην εύρυθμη και ασφαλή λειτουργία του Φορέα, την πρόταση αντίμετρων για την μείωση του κινδύνου, ώστε να γίνει και συμμόρφωση με την οδηγία NIS 2.

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

4. IT Security Audit

- Audit – Καταγραφή ευρημάτων – Αναφορά κινδύνων σχετιζόμενων με ευρήματα.
- Κατηγοριοποίηση ευρημάτων ανά επικινδυνότητα και κόστος αποκατάστασης.

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.

5. Gap Analysis για NIS2

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

NIS 2 Gap Analysis. Αναλυτική περιγραφή των υποδομών, των πολιτικών και διαδικασιών που απαιτούνται ώστε να συμμορφώνεται με το NIS 2.

Υπηρεσία ISMS Implementation (Ανάπτυξη Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών) με στόχο τη διαχείριση και αντιμετώπιση των κινδύνων ασφάλειας που σχετίζονται με την ψηφιακή πληροφορία, ώστε ο Φορέας να συμμορφώνεται με την οδηγία NIS 2.

6. Πολιτικές ασφαλείας για συμμόρφωση κατά NIS2

- Πολιτικές Ασφάλειας Διαχείρισης των κινδύνων του πληροφοριακού συστήματος του οργανισμού από απειλές όπως, οι κυβερνοεπιθέσεις, οι παραβιάσεις των συστημάτων, οι διαρροές δεδομένων ή η κλοπή, συμμορφούμενες κατά NIS 2.

7. Risk Assessment

- Εκτίμηση κινδύνων.
- Σημεία εφαρμογής αντίμετρων.

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 εμφάνιση της. Το αποτέλεσμα της διαδικασίας αυτής θα αναδείξει τα σημεία της πληροφοριακής υποδομής, τα οποία χρίζουν επιπλέον αντίμετρα ώστε να μειωθεί το ρίσκο.

8. Πραγματοποίηση εκπαιδεύσεων

Πραγματοποίηση μίας τουλάχιστον εκπαίδευσης των Υπαλλήλων της Υποδιεύθυνσης Πληροφορικής σε θέματα Κυβερνοασφάλειας, προκειμένου να αποκτήσουν επαρκείς γνώσεις και δεξιότητες που θα τους επιτρέπουν να εντοπίζουν τους κινδύνους και να αξιολογούν τις πρακτικές διαχείρισης κινδύνων στον τομέα της Κυβερνοασφάλειας και τον αντίκτυπο τους στις υπηρεσίες που παρέχει η οντότητα.

Αναλυτικότερα:

ΚΑΤΑΓΡΑΦΗ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ASSETS

Στόχος του είναι η πλήρης χαρτογράφηση των υποδομών πληροφορικής και επικοινωνιών σε συνεργασία με την Υποδιεύθυνση Πληροφορικής.

- Δημιουργία καταλόγων που θα περιλαμβάνουν:
  - Υποδομές πληροφορικής και επικοινωνιών, όπως σταθμοί εργασίας, διακομιστές (servers), δικτυακές συσκευές, εκτυπωτές, αποθηκευτικά μέσα και λοιπές τεχνολογικές εγκαταστάσεις.
  - Λογισμικά που χρησιμοποιούνται στον οργανισμό, όπως λειτουργικά συστήματα, εφαρμογές διαχείρισης δεδομένων, λογισμικά ασφαλείας και εξειδικευμένες εφαρμογές του Φορέα.
  - Πληροφοριακά αγαθά ταξινομημένα ανά κτιριακή υποδομή, προκειμένου να υπάρχει σαφής εικόνα της γεωγραφικής κατανομής των συστημάτων και της διαχείρισης των δεδομένων.
  - Καθώς επίσης τα πληροφοριακά συστήματα cloud, όλες τις διαλειτουργικότητες των πληροφοριακών συστημάτων με εθνικές ψηφιακές πλατφόρμες και μητρώα.

EXTERNAL-INTERNAL PENETRATION TEST

Σκοπός του έργου είναι η πραγματοποίηση ελέγχου/ων δοκιμής/ων παρείσδυσης και ανάλυσης κινδύνων, με στόχο την ανάδειξη ευπαθειών ασφαλείας στις υποδομές πληροφορικής, την περιγραφή των επιπτώσεων τους στην εύρυθμη και ασφαλή λειτουργία του Φορέα και την πρόταση αντίμετρων 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 αναγνώρισης τους. Η διαδικασία αυτή θα αναλυθεί στα ακόλουθα επίπεδα:

α. Σε επίπεδο εφαρμογής χωρίς γνώση (Black Box) (μόνο στην δικτυακή διεύθυνση της εφαρμογής).

β. 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:

α. Σε επίπεδο εφαρμογής χωρίς γνώση (Black Box) (μόνο στην δικτυακή διεύθυνση της εφαρμογής).

β. 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 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:

i. Πραγματοποίηση δοσοληψίων χωρίς εξουσιοδότηση.
ii. Απόκτηση δικαιωμάτων πρόσβασης σε ευαίσθητα δεδομένα χωρίς την κατάλληλη εξουσιοδότηση.
iii. Μη εξουσιοδοτημένη αλλαγή ή καταστροφή δεδομένων.
iv. 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 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.**
Στα πλαίσια αυτού του παραδοτέου, θα περιγράφουν 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 ο Φορέας 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 ο Φορέας 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 αποκατάστασης τους.
- Παρέχει προτάσεις για συνολική ασφάλεια, σε όλες τις παραμέτρους της μηχανογραφικής υποδομής.

Extented 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 Cybersecurity Framework και ελέγχονται τόσο τα υφιστάμενα τεχνικά αντίμετρα, όσο και η ύπαρξη επιμέρους εταιρικών πολιτικών για κρίσιμους τομείς της ασφάλειας.

GAP ANALYSIS για το NIS2

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 πάροχους 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.

Η Υπηρεσία 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.

Ανάπτυξη Πολιτικής Ασφαλείας κατά NIS2

Οι πολιτικές ασφάλειας ISMS (Information Security Management System), αποτελούν το θεμέλιο για τη διαχείριση της ασφάλειας 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. Η Υπηρεσία θα 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.

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 Φορέα αναφορικά με την ασφάλεια των πληροφοριακών συστημάτων, των δικτύων και την προστασία δεδομένων. Στόχος είναι να διασφαλιστεί καλύτερα η εμπιστευτικότητα (Confidentiality), η ακεραιότητα (Integrity) και η διαθεσιμότητα (Availability) 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 ασφάλειας 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 ασφάλειας.

Ο ανάδοχος θα επικαιροποιήσει τις πολιτικές ασφαλείας του Φορέα και θα αναπτύξει πολιτικές ασφαλείας όπου χρειάζεται, σε συνεργασία με την Υποδιεύθυνση 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 ασφάλειας. Εδώ αξιολογείται η κάθε απειλή που μπορεί να συμβεί στο πληροφοριακό σύστημα του Φορέα, βάσει της πιθανότητας να εμφανιστεί και του αντικτύπου που θα έχει μια πιθανή εμφάνισή της. Το αποτέλεσμα της διαδικασίας αυτής, θα αναδείξει τα σημεία των πληροφοριακών συστημάτων και του δικτύου τα οποία χρήζουν 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 Φορέα (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 απειλών, καταγραφή απειλών, κινδύνων κυβερνοασφάλειας και ασφάλειας πληροφοριών του Φορέα (Risk Registry).
- Διενέργεια άσκησης Εκτίμησης Επιχειρησιακού Αντικτύπου (Business Impact Analysis).
- Υπολογισμός πρωταρχικών κινδύνων (Inherent Risk Rating).
- Διενέργεια άσκησης αξιολόγησης των δικλείδων ασφάλειας του Φορέα (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.

Οι παρακάτω εργασίες απαιτείται να ολοκληρωθούν σε περίοδο 2 μηνών, εφόσον υπάρχει η σχετική διαθεσιμότητα της Υποδιεύθυνσης Πληροφορικής του Φορέα.

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

Ο Φορέας θα διευκολύνει τον Ανάδοχο να συλλέξει τα απαραίτητα στοιχεία για την καταγραφή της πληροφοριακής υποδομής του και θα να συνεργαστεί μαζί του παρέχοντας πρόσβαση σε απαραίτητους πόρους ώστε να μπορεί να ασκεί τα καθήκοντά του στις εγκαταστάσεις του Φορέα.

<u>Χρόνος Παράδοσης:</u> 2 μήνες από την υπογραφή της σύμβασης.

<u>Σημείωση:</u>

- Όλα τα παραδοτέα reports θα είναι γραμμένα στα Ελληνικά.
- Τα παραδοτέα reports θα είναι διακριτά για κάθε Νοσοκομειακή Μονάδα «Σισμανόγλειο» και «Αμαλία Φλέμιγκ» του Γενικού Νοσοκομείου Σισμανόγλειο - Αμ. Φλέμιγκ.

<u>Δ. ΠΡΟΫΠΟΘΕΣΕΙΣ ΕΠΑΓΓΕΛΜΑΤΙΚΗΣ ΚΑΙ ΤΕΧΝΙΚΗΣ ΙΚΑΝΟΤΗΤΑΣ</u>

Ο υποψήφιος ανάδοχος θα πρέπει:

1. Να είναι πιστοποιημένος κατά:

- ISO 9001:2015 (Πρότυπο για Σύστημα Διαχείρισης Ποιότητας).
- ISO 20000-1:2018 (Πρότυπο για Διαχείριση Υπηρεσιών Πληροφορικής).
- ISO 27001:2022 (Πρότυπο για Σύστηματα Διαχείρισης Ασφάλειας Πληροφοριών).
- ISO 37001:2016 (Πρότυπο για Συστήματα Διαχείρισης κατά της Δωροδοκίας/Διαφθοράς).

2. Η ομάδα έργου θα πρέπει να διαθέτει τουλάχιστον 6 από τις παρακάτω πιστοποιήσεις:

- ISO 27001 Lead Auditor.
- OSCP – Offensive Security Certified Professional.
- CISSP - Certified Information Systems Security Professional.
- OSWE – Offensive Security Web Expert.
- CIH – Certified Incident Handler.
- CPTS - Hackthebox Certified Penetration Testing Specialist.
- CCT INF - CREST Certified Tester – Infrastructure.
- ISC2 CCSP - Certified Cloud Security Professional certification from ISC2.
- Certified Information Security Manager (CISM).

και:

- πτυχία Πανεπιστημιακής Εκπαίδευσης.

- αποδεδειγμένη συμμετοχή σε ολοκληρωμένα έργα ασφάλειας πληροφοριών.

3. Η ομάδα έργου θα πρέπει να αποτελείται από εργαζόμενους του Αναδόχου με μόνιμη σχέση εργασίας η οποία θα πρέπει να αποδεικνύεται από μισθοδοτικές καταστάσεις προσωπικού. Όλα τα μέλη της ομάδας έργου θα πρέπει να πραγματοποιήσουν 1 τουλάχιστον φυσική παρουσία στους χώρους του Φορέα, καθώς και όποτε απαιτείται.

4. Να προσκομισθούν τα βιογραφικά της ομάδας έργου και οι ανωτέρω τουλάχιστον 6 πιστοποιήσεις.

5. Ο Ανάδοχος θα πρέπει να έχει πραγματοποιήσει δοκιμές παρείσδυσης (penetration tests) την τελευταία πενταετία σε τουλάχιστον 4 δημόσιους φορείς/οργανισμούς, εκ των οποίων τουλάχιστον 2 θα πρέπει να είναι οργανισμοί/φορείς υγείας. Η προϋπηρεσία θα πιστοποιείται με προσκόμιση σχετικών βεβαιώσεων από τους Φορείς.

Σε περίπτωση ύπαρξης υπεργολάβου ή ένωσης οικονομικών φορέων, οι παραπάνω ελάχιστες απαιτήσεις καλύπτονται αθροιστικά από τα μέλη της ένωσης, ή από τον ανάδοχο και τον υπεργολάβο του.

Ε. ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

Χωρίς την προηγούμενη γραπτή συναίνεση του Φορέα, ο Ανάδοχος δεν θα αποκαλύπτει εμπιστευτικές πληροφορίες, που θα του δοθούν ή που ο ίδιος ανακαλύψει κατά την υλοποίηση του έργου, ούτε θα κοινοποιεί στοιχεία, έγγραφα και πληροφορίες των οποίων λάβει γνώση. Υποχρεούται δε, να μεριμνά ώστε το προσωπικό του, και κάθε συνεργαζόμενος με αυτόν να τηρήσει την ως άνω υποχρέωση. Σε περίπτωση αθέτησης από τον Ανάδοχο της ως άνω υποχρέωσης του, ο Φορέας δικαιούται να απαιτήσει την αποκατάσταση τυχόν ζημίας του και την παύση κοινοποίησης των εμπιστευτικών πληροφοριών και την παράλειψη της στο μέλλον.