Ministry of Digital Governance
Digitally signed by Ministry of Digital Governance
Date: 2026.09.25 10:16:47 EEST
Reason:
Location: Athens

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Υγείας

Γενικό Νοσοκομείο Αθηνών
«Η Ε Λ Π Ι Σ»
Διεύθυνση: Διοικητική
Τμήμα:Γρ. Προμηθειών
Δημητσάνας 7, 115 22, Αθήνα
Τηλ.: 213 2039 136
email: **ekalampaliki@elpis.gr – promithion@elpis.gr**

Αθήνα: 24-09-2026
Αριθμ. Πρωτ. 11931

Αναρτητέα στο Κ.Η.Μ.ΔΗ.Σ.
στο Διαύγεια και στο Site του Νοσοκομείου

Προς την εταιρεία
«13CS SYSTEMS INTERGATION»
email: office@13cs.gr

ΠΡΟΣΚΛΗΣΗ ΥΠΟΒΟΛΗΣ ΠΡΟΣΦΟΡΑΣ

«Προμήθεια ειδικού Λογισμικού 24-ωρης Παρακολούθησης και Απόκρισης Κέντρου Επιχειρήσεων Ασφαλείας (SOC) με Υπηρεσίες Διαχειριζόμενης Ανίχνευσης και Απόκρισης (MDR), στο πλαίσιο εναρμόνισης του Γ.Ν.Α. «Η ΕΛΠΙΣ» με το Ν.5160/27-11-2024 - Οδηγία NIS2 για την εξασφάλιση υψηλού επιπέδου Κυβερνοασφάλειας», στην εταιρεία «13CS SYSTEMS INTERGATION » με δαπάνη 29.850,00€ πλέον ΦΠΑ.

ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ	**ΝΟΣΟΚΟΜΕΙΟ ΓΝΑ «Η ΕΛΠΙΣ»**
ΕΙΔΟΣ ΔΙΑΓΩΝΙΣΜΟΥ	**ΑΠΕΥΘΕΙΑΣ ΑΝΑΘΕΣΗ**
CPV	**72212730-5**
ΠΡΟΫΠΟΛΟΓΙΣΘΕΙΣΑ ΔΑΠΑΝΗ	**29.850,00 € πλέον Φ.Π.Α.**
ΤΟΠΟΣ ΥΠΟΒΟΛΗΣ ΠΡΟΣΦΟΡΩΝ	**ΔΗΜΗΤΣΑΝΑΣ 7, ΑΜΠΕΛΟΚΗΠΟΙ ΑΤΤΙΚΗΣ ΤΚ 11522**
ΚΑΤΑΛΗΚΤΙΚΗ ΗΜΕΡΟΜΗΝΙΑ ΥΠΟΒΟΛΗΣ ΠΡΟΣΦΟΡΑΣ	**Παρασκευή 02-10-2026 ώρα 14.00 μ.μ.**
ΔΙΑΡΚΕΙΑ ΙΣΧΥΟΣ ΠΡΟΣΦΟΡΑΣ	**ΕΝΑ (01) ΕΤΟΣ**

Το ΓΝΑ «Η ΕΛΠΙΣ» προτίθεται να αναθέσει υπηρεσίες για την «Προμήθεια ειδικού Λογισμικού 24-ωρης Παρακολούθησης και Απόκρισης Κέντρου Επιχειρήσεων Ασφαλείας (SOC) με Υπηρεσίες Διαχειριζόμενης Ανίχνευσης και Απόκρισης (MDR), στο πλαίσιο εναρμόνισης του Γ.Ν.Α. «Η ΕΛΠΙΣ» με το Ν.5160/27-11-2024 - Οδηγία NIS2 για την εξασφάλιση υψηλού επιπέδου Κυβερνοασφάλειας» **,** με τη διαδικασία της απευθείας ανάθεσης του άρθρου 118 του Ν.4412/16, σύμφωνα με την 201/3-09-2026 απόφαση του Δ.Σ. του Νοσοκομείου.

1. ΑΝΤΙΚΕΙΜΕΝΟ ΤΗΣ ΥΠΟ ΑΝΑΘΕΣΗΣ ΥΠΗΡΕΣΙΑΣ

Το αντικείμενο θα είναι η «Προμήθεια ειδικού Λογισμικού 24-ωρης Παρακολούθησης και Απόκρισης Κέντρου Επιχειρήσεων Ασφαλείας (SOC) με Υπηρεσίες Διαχειριζόμενης Ανίχνευσης και Απόκρισης (MDR), στο πλαίσιο εναρμόνισης του Γ.Ν.Α. «Η ΕΛΠΙΣ» με το Ν.5160/27-11-2024 - Οδηγία NIS2 για την εξασφάλιση υψηλού επιπέδου Κυβερνοασφάλειας». Την ευθύνη για τη υπηρεσία θα έχει αποκλειστικά και μόνο η ανάδοχος εταιρεία **«13CS SYSTEMS INTERGATION».**
Σημειώνεται ότι τα παραστατικά που τυχόν διατεθούν από τις Υπηρεσίες του Νοσοκομείου για τις ανάγκες παροχής υποστηρικτικών και συμβουλευτικών υπηρεσιών σε ζητήματα δημοσίων συμβάσεων, στην Ανάδοχο εταιρεία υπόκεινται στη διαδικασία εμπιστευτικότητας σύμφωνα με τον κανονισμό GDPR, η δε ανάδοχος εταιρεία δεσμεύεται απολύτως για την τήρηση του απορρήτου και της εμπιστευτικότητας.

Η τεχνική περιγραφή της ανωτέρω υπηρεσίας επισυνάπτεται στην παρούσα πρόσκληση (Παράρτημα Α).
Η εκτίμηση της αμοιβής ανέρχεται στο ποσό των 29.850,00 ευρώ πλέον Φ.Π.Α. για την κάλυψη της δαπάνης εκτέλεσής του έχει εκδοθεί η υπ' αριθμ. 2783/18-09-2026 απόφαση ανάληψης υποχρέωσης και η δέσμευση πίστωσης ποσού 37.014,00 ευρώ (με Φ.Π.Α.) σε βάρος του ΑΛΕ 24209030000101 του προϋπολογισμού οικ. έτους 2026.
Η παρούσα πρόσκληση θα δημοσιευτεί στο Κεντρικό Ηλεκτρονικό Μητρώο Δημοσίων Συμβάσεων (ΚΗΜΔΗΣ) την **25-09-2026** στον ιστότοπο http://et.diavgeia.gov.gr/ (ΠΡΟΓΡΑΜΜΑ ΔΙΑΥΓΕΙΑ) την **25-09-2026** και στην ιστοσελίδα της αναθέτουσας αρχής την **25-09-2026.**

2. ΚΑΤΑΡΤΙΣΗ ΚΑΙ ΥΠΟΒΟΛΗ ΠΡΟΣΦΟΡΩΝ

Η προσφορά υποβάλλεται μέχρι και την **02-10-2026** και ώρα **14.00 μ.μ.** στο πρωτόκολλο του Νοσοκομείου, ταχυδρομική Δ/νση Δημητσάνας 7 Αμπελόκηποι, Αθήνα Τ.Κ. 11522.

Περιεχόμενο φακέλου

Ο φάκελος θα περιλαμβάνει:

Α. ΕΝΤΥΠΟ ΤΕΧΝΙΚΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΚΗΣ ΠΡΟΣΦΟΡΑΣ του Παραρτήματος Β της παρούσας, με σφραγίδα και υπογραφή του προσφέροντος στην τελευταία σελίδα.

Εναλλακτική προσφοράς δεν θα γίνει δεκτή. Επίσης δεν γίνεται δεκτή, προσφορά που ξεπερνά τον προϋπολογισμό.

Β. ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ εκ μέρους του οικονομικού φορέα, σε περίπτωση φυσικού προσώπου, ή σε περίπτωση νομικού προσώπου την υποβολή αυτής εκ μέρους του νόμιμου εκπροσώπου, όπως αυτός προκύπτει από το ισχύον καταστατικό ή το πρακτικό εκπροσώπησής του κατά τον χρόνο υποβολής της προσφοράς ή το αρμοδίως εξουσιοδοτημένο φυσικό πρόσωπο να εκπροσωπεί τον οικονομικό φορέα για διαδικασίες σύναψης συμβάσεων ή για συγκεκριμένη διαδικασία σύναψης σύμβασης, όπου θα δηλώνεται ότι:

- Δεν συντρέχουν οι λόγοι αποκλεισμού της παραγράφου 1 του άρθρου 73 του Ν.4412/16.
- Έχει λάβει πλήρη γνώση των όρων της πρόσκλησης και των λοιπών συνημμένων εγγράφων του φακέλου δημόσιας σύμβασης: **«Προμήθεια ειδικού Λογισμικού 24-ωρης Παρακολούθησης και Απόκρισης Κέντρου Επιχειρήσεων Ασφαλείας (SOC) με Υπηρεσίες Διαχειριζόμενης Ανίχνευσης και Απόκρισης (MDR), στο πλαίσιο εναρμόνισης του Γ.Ν.Α. «Η ΕΛΠΙΣ» με το Ν.5160/27-11-2024 - Οδηγία NIS2 για την εξασφάλιση υψηλού επιπέδου Κυβερνοασφάλειας** και δηλώνει συμμετοχή στην διαδικασία ανάθεσής της.

Η ανωτέρω υπεύθυνη δήλωση γίνεται αποδεκτή εφόσον έχει συνταχθεί μετά την κοινοποίηση της παρούσας πρόσκλησης.

Επισημαίνεται ότι η ως άνω **Υπεύθυνη Δήλωση** θα πρέπει να φέρει Βεβαίωση του γνησίου της υπογραφής από αρμόδια Υπηρεσία ή Αρχή ή ισοδύναμα να έχει εκδοθεί μέσω της ηλεκτρονικής πλατφόρμας gov.gr.

Γ. Απόσπασμα του ποινικού μητρώου ή, ελλείψει 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 εν λόγω οικονομικός φορέας, από το οποίο προκύπτει ότι πληρούνται αυτές οι προϋποθέσεις, που να έχει εκδοθεί έως τρεις (3) μήνες πριν από την υποβολή του. Η υποχρέωση του προηγούμενου εδαφίου αφορά:

α) Στις περιπτώσεις εταιρειών περιορισμένης ευθύνης (Ε.Π.Ε.), προσωπικών εταιρειών (Ο.Ε. Ε.Ε.) και Ιδιωτικών Κεφαλαιουχικών Εταιρειών (Ι.Κ.Ε.), τους διαχειριστές.

β) Στις περιπτώσεις ανωνύμων εταιρειών (Α.Ε.) τον Διευθύνοντα Σύμβουλο, τα μέλη του Διοικητικού Συμβουλίου, καθώς και τα πρόσωπα στα οποία με απόφαση του Διοικητικού Συμβουλίου έχει ανατεθεί το σύνολο της διαχείρισης και εκπροσώπησης της εταιρείας.

γ) Στις περιπτώσεις των συνεταιρισμών, τα μέλη του Διοικητικού Συμβουλίου, ή
δ) στις υπόλοιπες περιπτώσεις νομικών προσώπων, τον κατά περίπτωση νόμιμο εκπρόσωπο.

Δ. Πιστοποιητικό φορολογικής ενημερότητας, που εκδίδεται από την Ανεξάρτητη Αρχή Δημοσίων Εσόδων (Α.Α.Δ.Ε.) σε ισχύ κατά την υποβολή της προσφοράς και κατά την υποβολή των δικαιολογητικών για τον οικονομικό φορέα.

Ε. Πιστοποιητικό ασφαλιστικής ενημερότητας

Τα φυσικά πρόσωπα υποβάλλουν σχετικό πιστοποιητικό για την κάλυψη κύριας και επικουρικής ασφάλισής τους. Οι εγκατεστημένες στην Ελλάδα εταιρείες υποβάλλουν αποδεικτικό ασφαλιστικής ενημερότητας από τον ΕΦΚΑ (κύριας και επικουρικής ασφάλισης) για το προσωπικό τους με σχέση εξαρτημένης εργασίας. Δεν αποτελούν απόδειξη ενημερότητας της προσφέρουσας εταιρίας, αποδεικτικά ασφαλιστικής ενημερότητας των φυσικών προσώπων που στελεχώνουν το πτυχίο της εταιρίας ως εταίροι.

ΣΤ. Υπεύθυνη δήλωση του προσφέροντος ότι:

- Δεν έχει εκδοθεί δικαστική ή διοικητική απόφαση με τελεσίδικη και δεσμευτική ισχύ για την αθέτηση των υποχρεώσεών του όσον αφορά στην καταβολή φόρων ή εισφορών κοινωνικής ασφάλισης.
- Δεν έχει εκδοθεί σε βάρος του απόφαση οριζόντιου αποκλεισμού.

Επισημαίνεται ότι η ως άνω **Υπεύθυνη Δήλωση** θα πρέπει να φέρει Βεβαίωση του γνησίου της υπογραφής από αρμόδια Υπηρεσία ή Αρχή ή ισοδύναμα να έχει εκδοθεί μέσω της ηλεκτρονικής πλατφόρμας gov.gr.

ΙΣΧΥΣ ΤΗΣ ΠΡΟΣΦΟΡΑΣ

Η προσφορά ισχύει και δεσμεύει για δώδεκα (12) μήνες από την επόμενη της καταληκτικής ημερομηνίας υποβολής προσφοράς. Εάν η προσφορά αναφέρει μικρότερο χρόνο ισχύος απορρίπτεται ως απαράδεκτη.

Η ανακοίνωση επιλογής του αναδόχου μπορεί να γίνει και μετά τη λήξη της ισχύος της προσφοράς, δεσμεύει όμως τον υποψήφιο ανάδοχο μόνο εφόσον αυτός την αποδεχθεί.

3. ΤΙΜΕΣ

Στις προσφερόμενες τιμές (χωρίς ΦΠΑ) θα περιλαμβάνονται:

- Η αξία της προσφερόμενης υπηρεσίας σε ΕΥΡΩ.
- Όλες οι υπέρ τρίτων κρατήσεις ως και δασμοί, τέλη καθώς και λοιπές δημοσιονομικές επιβαρύνσεις ή άλλες αμοιβές και επιβαρύνσεις.
- Εάν μετά την ημερομηνία της πρόσκλησης επιβληθούν τέλη και κρατήσεις ή καταργηθούν υφιστάμενοι, το ποσό πληρώνεται ή εκπίπτει αντιστοίχως από τους λογαριασμούς του αναδόχου.

4. ΕΙΔΙΚΟΙ ΟΡΟΙ-ΕΚΤΕΛΕΣΗ ΤΗΣ ΣΥΜΒΑΣΗΣ

Ο ανάδοχος υποχρεούται κατά την εκτέλεση της σύμβασης να τηρεί τις υποχρεώσεις στους τομείς περιβαλλοντικού, κοινωνικοασφαλιστικού και εργατικού δικαίου, που έχουν θεσπισθεί με το δίκαιο της Ένωσης, το εθνικό δίκαιο, συλλογικές: συμβάσεις j ή διεθνείς (διατάξεις περιβαλλοντικού, κοινωνικοασφαλιστικού και εργατικού δικαίου, οι οποίες απαριθμούνται στο Παράρτημα Χ του Προσαρτήματος Α του Ν. 4412/2016.

5. ΕΠΙΒΛΕΨΗ- ΠΑΡΑΛΑΒΗ

Σχετικά με την υπογραφή της σύμβασης, ισχύουν τα προβλεπόμενα στις παρ. 4,5,7,8 του άρθρου 105 καθώς και στο άρθρο 182 του ν. 4412/2016.

Τα έγγραφα της σύμβασης, με βάση τα οποία θα εκτελεσθεί η υπηρεσία είναι τα αναφερόμενα παρακάτω. Σε περίπτωση ασυμφωνίας των περιεχομένων σε αυτά όρων, η σειρά ισχύος καθορίζεται ως κατωτέρω:

1. Η σύμβαση, συμπεριλαμβανομένων, των παρασχεθεισών εξηγήσεων του οικονομικού φορέα, σύμφωνα με τα άρθρα 88 και 89 του ν. 4412/2016, ιδίως ως προς τον προσδιορισμό **οικονομικών μεγεθών με τις οποίες ο ανάδοχος διαμόρφωσε την προσφορά του**
2. Η παρούσα Πρόσκληση,

3. Η Οικονομική Προσφορά,
4. Η Τεχνική Προσφορά

Τα ανωτέρω έγγραφα , της σύμβασης ισχύουν όπως διαμορφώθηκαν, με τις συμπληρωματικές πληροφορίες και διευκρινίσεις που παρασχέθηκαν από την αναθέτουσα αρχή επί όλων των ανωτέρω.

Η αναθέτουσα αρχή θα ορίσει και θα γνωστοποιήσει σχετικά στον ανάδοχο τα πρόσωπα που θα επιβλέψουν την εκτέλεση των εργασιών της σύμβασης.

6. ΠΡΟΘΕΣΜΙΕΣ-ΧΡΟΝΟΔΙΑΓΡΑΜΜΑ

Ο συνολικός χρόνος της σύμβασης ανέρχεται σε δέκα πέντε(15) ημερών από την ημερομηνία υπογραφής της σύμβασης.

7. ΠΟΙΝΙΚΕΣ ΡΗΤΡΕΣ

Οι προβλεπόμενες βάσει του άρθρου 185 του Ν4412/2016, όπως τροποποιήθηκε με το Ν.4782/2021 και ισχύει.

8. ΠΡΟΥΠΟΛΟΓΙΣΜΟΣ ΚΑΙ ΤΡΟΠΟΣ ΠΛΗΡΩΜΗΣ

Ο προϋπολογισμός της υπό ανάθεσης υπηρεσίας ανέρχεται σε 37.014,00 € συμπεριλαμβανομένου του αναλογούντος Φ.Π.Α.
Η πληρωμή της αξίας των υπηρεσιών στον Προμηθευτή θα γίνει τμηματικά σύμφωνα με το πλάνο τμηματικών παραδόσεων και με τμηματική εξόφληση της συμβατικής αξίας που αναλογεί στο εκάστοτε παραδοθέν τμήμα.
Οι πληρωμές θα γίνονται σε ευρώ με την προσκόμιση των νομίμων παραστατικών και δικαιολογητικών που προβλέπονται από τις ισχύουσες διατάξεις καθώς και κάθε άλλου δικαιολογητικού προβλέπεται από τα έγραφα της σύμβασης και σε χρόνο προσδιοριζόμενο από την αναγκαία διοικητική διαδικασία για έκδοση των σχετικών χρηματικών ενταλμάτων.
Ο ανάδοχος υποχρεούται να προσκομίσει τα ακόλουθα δικαιολογητικά για την είσπραξή του:

- Τιμολόγιο του αναδόχου
- Αποδεικτικό Φορολογικής Ενημερότητας
- Αποδεικτικό ασφαλιστικής ενημερότητας που αφορά τον ίδιο, *αν* πρόκειται για φυσικό *πρόσωπο,* ή τις *ασφαλιστικές* υποχρεώσεις προς τους απασχολούμενους με σύμβαση εξαρτημένης εργασίας (ΙΚΑ, ΤΣΜΕΔΕ, κλπ), όταν πρόκειται για νομικό πρόσωπο. *Οι συμπράξεις και* κοινοπραξίες αποδεικνύουν την ασφαλιστική ενημερότητα όλων των μελών τους.

Ο *ανάδοχος* υποχρεούται *ακόμα να* προσκομίσει κατά αίτηση του εργοδότη και οποιοδήποτε άλλο δικαιολογητικό απαιτείται από την ελληνική νομοθεσία για την πληρωμή *της* απαίτησης. Διευκρινίζεται *ότι:*
Για όλες τις πληρωμές θα εκδίδονται τα απαραίτητα νόμιμα παραστατικά/ δικαιολογητικά. Από κάθε τιμολόγιο του Αναδόχου θα γίνονται όλες οι νόμιμες κρατήσεις, σύμφωνα με τους ισχύοντες κάθε φορά Νόμους και σχετικές Εγκυκλίους των αρμόδιων Υπουργείων.
Ο Ανάδοχος επιβαρύνεται με παρακράτηση φόρου εισοδήματος σύμφωνα με τις ισχύουσες διατάξεις όπως εκάστοτε ισχύουν.
Στην αμοιβή του Αναδόχου, περιλαμβάνονται οι υπέρ τρίτων νόμιμες κρατήσεις, ως και κάθε άλλη επιβάρυνση σύμφωνα με την κείμενη νομοθεσία, μη συμπεριλαμβανομένου Φ.Π.Α για την παράδοση της υπηρεσίας στον τόπο και με τον τρόπο που προβλέπεται στα έγγραφα της σύμβασης. Ιδίως βαρύνεται με τις ακόλουθες κρατήσεις:
α) Κράτηση ύψους 0,1% υπέρ ΕΑΔΗΣΥ επί όλων των συμβάσεων.
β) Κράτηση ύψους 0,02% υπέρ της ανάπτυξης και συντήρησης του ΟΠΣ ΕΣΗΔΗΣ , η οποία υπολογίζεται επί της αξίας ,εκτός ΦΠΑ ,της αρχικής , καθώς και κάθε συμπληρωματικής σύμβασης. Το ποσό αυτό παρακρατείται σε κάθε πληρωμή από την αναθέτουσα αρχή στο όνομα

και για λογαριασμό του Υπουργείου Ψηφιακής Διακυβέρνησης , σύμφωνα με την παρ.6 του άρθρου 36 του ν. 4412 / 2016.
γ) Κράτηση 2% Υπέρ οργανισμών ψυχικής Υγείας, Υπουργείου Υγείας.
Οι υπέρ τρίτων κρατήσεις υπόκεινται στο εκάστοτε ισχύον αναλογικό τέλος χαρτοσήμου και στην επ' αυτού εισφορά υπέρ ΟΓΑ
Με κάθε πληρωμή θα γίνεται η προβλεπόμενη από την κείμενη νομοθεσία παρακράτηση φόρου εισοδήματος επί του καθαρού ποσού.
Τα δικαιολογητικά που απαιτούνται είναι κατ' ελάχιστον τα εξής:
α) Πρωτόκολλο οριστικής παραλαβής του τμήματος που αφορά η πληρωμή ή του συνόλου του συμβατικού αντικείμενου.
β) Τιμολόγιο του Αναδόχου.
γ) Πιστοποιητικά Φορολογικής και Ασφαλιστικής Ενημερότητας, σύμφωνα με τις κείμενες διατάξεις.
Πέραν των ανωτέρω δικαιολογητικών η αναθέτουσα αρχή που διενεργεί τον έλεγχο και την πληρωμή, μπορεί να ζητήσουν και οποιοδήποτε άλλο δικαιολογητικό προβλέπεται στην κείμενη νομοθεσία.
Για την πληρωμή του Αναδόχου εφαρμόζονται και ισχύουν οι προβλεπόμενες διατάξεις του Ν 4152/2013 (ΦΕΚ Α/107/09-05-2013).
Όλα τα τιμήματα της παρούσας Σύμβασης (συνολικά και τιμές μονάδος), παραμένουν σταθερά και δεν υπόκε0ινται σε καμία αναθεώρηση ή αύξηση έως την συμβατική ημερομηνία ολοκλήρωσης της Σύμβασης και τυχόν παράτασης αυτής.
Καμία αποζημίωση ή άλλη χρηματική καταβολή δεν δικαιούται ο Ανάδοχος στις περιπτώσεις αδράνειας, παύσης κλπ. της σύμβασης, ιδίως δε γιατί δεν παρουσιάστηκε ανάγκη χρησιμοποίησης των συμβατικών υπηρεσιών.
Ο ανάδοχος υποχρεούται στην έκδοση ηλεκτρονικού τιμολογίου μέσω Ε.Δ.Η.Τ.

9. ΛΗΞΗ ΤΗΣ ΣΥΜΒΑΣΗΣ-ΠΑΡΑΛΑΒΗ ΤΟΥ ΑΝΤΙΚΕΙΜΕΝΟΥ ΤΗΣ

Η λήξη της σύμβασης, εφόσον δε συντρέχουν λόγοι πρόωρης λύσης (έκπτωση του αναδόχου ή διάλυση της σύμβασης), πιστοποιείται με την παραλαβή των εργασιών του αναδόχου και την έκδοση σχετικής απόφασης από το αρμόδιο αποφαινόμενο όργανο.

10. ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Εφόσον, υφίσταται επεξεργασία προσωπικών δεδομένων, τα δύο μέρη συμφωνούν να τηρούνται τα άρθρα του Γενικού Κανονισμού Προστασίας Δεδομένων 2016 / 679 (GDPR).

Η Συντάξασα

Ο Πρόεδρος του Δ.Σ.

Σταύρος Γεωργόπουλος

ΠΑΡΑΡΤΗΜΑ Ι - «ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ - ΑΠΑΙΤΗΣΕΙΣ» - ΠΙΝΑΚΑΣ ΣΥΜΜΟΡΦΩΣΗΣ ΤΕΧΝΙΚΗΣ ΠΡΟΣΦΟΡΑΣ

Τεχνικές Προδιαγραφές Έργου «Προμήθεια ειδικού Λογισμικού 24-ωρης Παρακολούθησης και Απόκρισης Κέντρου Επιχειρήσεων Ασφαλείας (SOC) με Υπηρεσίες Διαχειριζόμενης Ανίχνευσης και Απόκρισης (MDR), στο πλαίσιο εναρμόνισης του Γ.Ν.Α. «Η ΕΛΠΙΣ» με το Ν.5160/27-11-2024 - Οδηγία NIS2 για την εξασφάλιση υψηλού επιπέδου Κυβερνοασφάλειας».

Σκοπός του Έργου

Σκοπός του έργου είναι η εξασφάλιση υψηλού επιπέδου Κυβερνοασφάλειας του Γ.Ν.Α. «Η ΕΛΠΙΣ» (εφεξής Νοσοκομείο), προς συμμόρφωση με τις απαιτήσεις της Ευρωπαϊκής Οδηγίας NIS2, η οποία ενσωματώνεται στον **Ν.5160/27-11-2024** και προς :

- αποφυγή προστίμων,
- μείωση των κινδύνων διαρροών Ευαίσθητων Προσωπικών Δεδομένων,
- διασφάλιση της Επιχειρησιακής Συνέχειας του Νοσοκομείου σε περίπτωση Κυβερνοεπίθεσης,
- ενίσχυση της Φήμης του Νοσοκομείου ως ασφαλούς φορέα.

Αντικείμενο του Έργου

Σύμφωνα με την Οδηγία NIS2 της ΕΕ και την προσαρμογή της στην Ελληνική Νομοθεσία με το Ν.5160/27-11-2024 και συγκεκριμένα το Μέρος Α', Κεφ. Β', Άρθρο 15, παρ. 6, προκειμένου να αποδειχθεί η συμμόρφωση με τις απατήσεις της Νομοθεσίας, δύναται να απαιτηθεί από τους Φορείς να χρησιμοποιούν συγκεκριμένα προϊόντα ΤΠΕ (Τεχνολογίες Πληροφοριών και Επικοινωνιών) είτε σε Hardware (Υλικός Εξοπλισμός), είτε σε Software (Λογισμικό), υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ, που αναπτύσσονται από τον φορέα ή παρέχονται από τρίτους και πιστοποιούνται στο πλαίσιο Ευρωπαϊκών Συστημάτων πιστοποίησης Κυβερνοασφάλειας

Αντικείμενο του έργου αποτελεί η προμήθεια ειδικού Λογισμικού 24-ωρης Παρακολούθησης και Απόκρισης Κέντρου Επιχειρήσεων Ασφαλείας (SOC: Security Operations Center) με Υπηρεσίες Διαχειριζόμενης Ανίχνευσης και Απόκρισης (MDR), προκειμένου να επιτευχθεί η εξασφάλιση υψηλού επιπέδου Κυβερνοασφάλειας του Νοσοκομείου και η δυνατότητα απόδειξης της συμμόρφωσης με την κείμενη Νομοθεσία.

Η συνεχής παρακολούθηση και προστασία της Υποδομής του Νοσοκομείου είναι επιβεβλημένη. Η παρακολούθηση αυτή θα πρέπει να γίνεται επί 24ωρου βάσης 365 ημέρες τον χρόνο από επαγγελματίες και εξειδικευμένο προσωπικό στην Κυβερνοασφάλεια. Το Νοσοκομείο είναι αδύνατο να δημιουργήσει και να διατηρήσει μια εσωτερική ομάδα, η οποία θα εξελίσσει διαρκώς τις δεξιότητες που απαιτούνται για την επίτευξη του στόχου της Ασφάλειας της Πληροφορίας.

Για την επίτευξη του περιορισμού των διαρκώς αναπτυσσόμενων ψηφιακών κινδύνων, προκύπτει η ανάγκη της ανάθεσης της Ασφάλειας των Πληροφοριών και της Διαχείρισης Κινδύνων (Information Security and Risk Management) σε εξειδικευμένο και αξιόπιστο πάροχο υπηρεσιών Ασφάλειας (Managed Security Services).

Το Επιχειρησιακό Κέντρο Ασφαλείας (SOC) θα παρέχει στο Νοσοκομείο το αιτούμενο επίπεδο Ασφάλειας της Πληροφορίας και την αντοχή τους σε Κακόβουλες Επιθέσεις σε ένα βέλτιστο επιχειρησιακό και αποτελεσματικό επίπεδο, 24x7χ365 ημέρες το χρόνο.

ΑΠΑΙΤΟΥΜΕΝΕΣ ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΤΟΥ ΕΡΓΟΥ

Στο πλαίσιο του έργου, ο Ανάδοχος οφείλει να προσφέρει Λογισμικό Cloud **Software-as-a-Service** που να ενεργοποιείται μέσω δικής του Συσκευής προώθησης δεδομένων iCollector (κεντρική παρακολούθηση και ανάλυση συμβάντων Κυβερνοασφάλειας σε πραγματικό χρόνο), που να μπορεί να είναι on-premise, στο Cloud ή σε υβριδικό περιβάλλον και η διαχείρισή του να υλοποιείται μέσω Κεντρικής Κονσόλας Web Portal.
Το Λογισμικό πρέπει να :

1. παρέχει σε πραγματικό χρόνο ευφυή ανάλυση σε βάθος και συσχέτιση δεδομένων και συμβάντων που συλλέγονται από ετερογενείς πηγές δεδομένων, σε συνδυασμό με τεκμηριωμένη γνώση των αναδυόμενων απειλών και ευπαθειών για την παραγωγή πληροφοριών.
2. τη δυνατότητα άμεσης ανταπόκρισης σε απειλές και αξιολόγησης περιστατικών Ασφαλείας/Incidents, προς μείωση του χρόνου διακοπής λειτουργίας του Νοσοκομείου και αποτύπωσης των σχετικών εκθέσεων Ελέγχου και Συμμόρφωσης.
3. δίνει τη δυνατότητα για τον έγκαιρο εντοπισμό και την αντιμετώπιση προηγμένων κακόβουλων κυβερνοεπιθέσεων και ύποπτων δραστηριοτήτων χρηστών, με τη χρήση της ενορχήστρωσης και αυτοματοποίησης ασφάλειας (Security Orchestration & Response), της προηγμένης μηχανικής μάθησης (Machine Learning - ML) και της Τεχνητής Νοημοσύνης (Artificial Intelligence - AI).
4. χρησιμοποιεί αλγορίθμους μηχανικής μάθησης (ML) και Τεχνητής Νοημοσύνης (AI) για να βελτιώσει δραστικά τις δυνατότητες ανίχνευσης και πρόβλεψης που σχετίζονται με ύποπτες/ κακόβουλες Κυβερνοαπειλές, συμπεριλαμβανομένης της μη φυσιολογικής δραστηριότητας/ συμπεριφοράς χρηστών.

Διαδικασία διαχείρισης απειλών (Threat Management Process)

Το Λογισμικό θα πρέπει απλοποιεί τη διαδικασία διαχείρισης απειλών επιταχύνοντας σημαντικά τις προληπτικές δυνατότητες ανίχνευσης και απόκρισης απειλών, μειώνοντας έτσι δραστικά το "Detection Deficit" (χρόνος μεταξύ παραβίασης και ανακάλυψης). Ταυτόχρονα, θα πρέπει να διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα ευαίσθητων πληροφοριών που βρίσκονται στα δεδομένα.

Υπηρεσίες διαχείρισης πληροφοριών και περιστατικών ασφάλειας (Security Information and Event Management - SIEM)

Η αυξανόμενη πολυπλοκότητα και εξάρτηση από το οικοσύστημα πληροφορικής δημιουργεί άγνωστους ψηφιακούς κινδύνους, καθώς και νέα είδη απειλών.

Η πλατφόρμα του λογισμικού θα πρέπει να έχει σε γενικές γραμμές τη δυνατότητα:

- παροχής πληροφοριών σε πραγματικό χρόνο σχετικά με την κατάσταση ασφαλείας του Νοσοκομείου (Cybersercurity posture),
- αποτελεσματικής υποστήριξης κρίσιμων λειτουργιών, όπως προηγμένα αναλυτικά μοντέλα ασφαλείας,
- βοήθειας στη βελτίωση της ανίχνευσης απειλών, της διαχείρισης συμβάντων, της έρευνας σε πραγματικό χρόνο και της έξυπνης ανάλυσης ιστορικών ή/και τρεχόντων δεδομένων καταγραφής και συμβάντων,
- παροχής αυτοματοποιημένης ειδοποίησης,
- διευκόλυνσης της ουσιαστικής επιχειρησιακής και κανονιστικής υποβολής εκθέσεων,
- ενίσχυσης των δυνατοτήτων αντιμετώπισης περιστατικών του Νοσοκομείου,
- βοήθειας για την αντιμετώπιση της κανονιστικής συμμόρφωσης.

Πλεονεκτήματα των υπηρεσιών Managed Security Services επόμενης γενιάς

- Ενσωματωμένη ευφυΐα.
- Μηδενική αρχική επένδυση.
- Καμία απαξίωση υλικού (hardware).
- Επεκτασιμότητα.
- Μειωμένος χρόνος για την επίτευξη αποτελεσμάτων.
- Νοημοσύνη απειλών (Threat Intelligence).
- Μειωμένα λειτουργικά έξοδα.

Τα αιτούμενα χαρακτηριστικά της πλατφόρμας του Λογισμικού

Έξυπνη ανάλυση (μοντέλα AI & ML)
Βελτιωμένος έγκαιρος εντοπισμός και απόκριση σε προηγμένες επιθέσεις, παραβιάσεις δεδομένων ή/και ύποπτη/κακόβουλη συμπεριφορά του χρήστη με χρήση προγνωστικών/μηχανικών μοντέλων μάθησης, που καθιστούν δυνατή την ανίχνευση μη φυσιολογικής συμπεριφοράς ή/και κακόβουλων πληροφοριών-απειλών που διαφορετικά θα περνούσαν απαρατήρητες/ μη ανιχνεύσιμες με την χρήση συμβατικών συστημάτων πληροφοριών ασφαλείας και διαχείρισης συμβάντων.
Ευελιξία
Επιτρέπει την ικανότητα συλλογής, επεξεργασίας και ανάλυσης νέων τύπων δεδομένων καταγραφής και συμβάντων σε περιβάλλοντα IT και Τεχνολογιών (Operational Technology - OT), παρέχοντας δυνατότητα αποθήκευσης, επεξεργασίας και ανάλυσης διαφορετικών τύπων δεδομένων καταγραφής και συμβάντων από διάφορους τύπους συσκευών, είτε δομημένων είτε μη δομημένων.
Επεξεργαστική ισχύς
Δυνατότητα επεξεργασίας πολύ πιο τρεχόντων και ιστορικών δεδομένων καταγραφής και συμβάντων σε πραγματικό χρόνο, σε κλάσμα του χρόνου.
iCollector
Ο iCollector είναι μια έξυπνη συσκευή που συλλέγει και αναλύει έξυπνα, σε πραγματικό χρόνο, δεδομένα καταγραφής και συμβάντων από εκατοντάδες διαφορετικούς τύπους δεδομένων. Προσφέρεται ως φυσική ή εικονική συσκευή και μπορεί να αναπτυχθεί είτε on-premise, cloud ή και στα δύο για υβριδικά περιβάλλοντα.

iCollector Τρόπος Λειτουργίας
Εκτελώντας μια σειρά λειτουργιών, ο iCollector Συλλέγει (Collect), Αρχειοθετεί – Archive (Digitally Signs/Encrypts), Ομαλοποιεί (Normalize), Αναλύει Έξυπνα (Intelligently Analyze) και Συσχετίζει (Correlate) τεράστιους όγκους ετερογενών δεδομένων. Αξιοποιεί πληροφορίες για αναδυόμενες απειλές, ευπάθειες, για τον έγκαιρο εντοπισμό και την αντιμετώπιση στοχευμένων επιθέσεων και παραβιάσεων δεδομένων. Για τη διασφάλιση της εμπιστευτικότητας και τη διατήρηση της ακεραιότητας ευαίσθητων πληροφοριών, τα δεδομένα αρχείου καταγραφής και συμβάντων που συλλέγονται δύναται να υποβληθούν σε διαδικασία συγκάλυψης (Mask).

Collect
Συλλέγονται τεράστιοι όγκοι ετερογενών συνόλων δεδομένων που παράγονται από διάφορες συσκευές ασφαλείας, υποδομές δικτύου, συστήματα και εφαρμογές.

Archive
Τα δεδομένα καταγραφής και συμβάντων που συλλέγονται συμπιέζονται σε αναλογία έως και 96%, υπογράφονται ψηφιακά και κρυπτογραφούνται προαιρετικά πριν αρχειοθετηθούν. Με αυτόν τον τρόπο, συλλέγονται δεδομένα καταγραφής και συμβάντων και διατηρούνται σε κατάσταση που θα μπορούσε επίσης να χρησιμοποιηθεί για εγκληματολογική έρευνα ή νομικά αποδεικτικά στοιχεία, εάν προκύψει ανάγκη.

Normalize

Τα δεδομένα καταγραφής και συμβάντων που συλλέγονται ομαλοποιούνται και αποθηκεύονται σε κοινή μορφή, κατά τη στιγμή της συλλογής δεδομένων, για περαιτέρω επεξεργασία.

Intelligently Analyse
Έξυπνη επεξεργασία, συγκέντρωση και ανάλυση δεδομένων καταγραφής και συμβάντων με τη χρήση μοντέλων Συμπεριφοράς Χρήστη & Οντότητας, Τεχνητής Νοημοσύνης, Πρόβλεψης και Μηχανικής Μάθησης, ενσωματώνοντας contextual πληροφορίες για την πρόβλεψη ύποπτης και την ανίχνευση μη φυσιολογικής συμπεριφοράς.

Correlate
Η συσχέτιση των δεδομένων και συμβάντων χρησιμοποιεί, όχι μόνο μια σειρά από στατιστικών και ευρετικών (heuristic) μοντέλων, αλλά και μια σειρά προκαθορισμένων κανόνων ευφυούς συσχέτισης σε συνδυασμό με τεκμηριωμένη γνώση των αναδυόμενων απειλών και τρωτών σημείων, επιτρέποντας με αυτόν τον τρόπο τον έγκαιρο εντοπισμό και την αντιμετώπιση επιθέσεων και παραβιάσεων δεδομένων.

Mask
Οι ευαίσθητες πληροφορίες που βρίσκονται στα δεδομένα μπορούν προαιρετικά να αποκρύπτονται για τη διασφάλιση της εμπιστευτικότητας.

Secure Web Portal (SWP)
Το Λογισμικό πρέπει να διαθέτει μία Web Portal (SWP) κεντρική κονσόλα διαχείρισης, παρέχοντας στο Νοσοκομείο σαφή ορατότητα σε πραγματικό χρόνο σημαντικών συμβάντων, μετρήσεων, δεικτών και αξιολόγησης κινδύνου μέσω έξυπνων, πλήρως προσαρμόσιμων έξυπνων πινάκων εργαλείων.

Threat Intelligence
Το Λογισμικό πρέπει να διαθέτει τεχνολογία Threat Intelligence, η οποία ενημερώνει για νέες ευπάθειες και αναδυόμενες απειλές στον κυβερνοχώρο. Αποτελεί βασικό πυλώνα γιατί παρέχει μια συνεχώς ενημερωμένη και αναλυμένη ροή τεκμηριωμένων γνώσεων σχετικά με αναδυόμενες απειλές και ευπάθειες στον κυβερνοχώρο. Αντλεί δεδομένα από έγκυρα feeds Threat Intelligence και τα επεξεργάζεται για να εξάγει πολύτιμες πληροφορίες που σχετίζονται με το Νοσοκομείο. Αναλύει δεδομένα και συμπεριφορές για να υποστηρίξει την προληπτική άμυνα του Νοσοκομείου. Επιπλέον, το Threat Anticipation αξιοποιεί τη συνεχή συλλογή πληροφοριών απειλής σε συνδυασμό με το Advanced Security Analytics για να εντοπίσει τη σοβαρότητα και το αντίκτυπο των απειλών στον κυβερνοχώρο σε σχέση με τα χαρακτηριστικά του Νοσοκομείου, παρέχοντας μια ολοκληρωμένη αξιολόγηση και ανάλυση των Δεικτών Επίθεσης (Indicators of Attack - IOA), με χρήσιμες πληροφορίες, Threat Hunting και την εξάλειψη απειλών στο επόμενο επίπεδο.

Η βελτιστοποίηση του Risk Exposure είναι μια συνεχής διαδικασία προληπτικής προσαρμογής στο συνεχώς μεταβαλλόμενο τοπίο απειλών στον κυβερνοχώρο.

Στόχος :
- Η Απόκτηση γενικής εικόνας του Risk Susceptibility του Νοσοκομείου.
- Η Ενημέρωση για το συνεχώς μεταβαλλόμενο τοπίο Κυβερνοαπειλών.
- Η Συνεχής βελτιστοποίησή του Security Posture.
- Η Ταυτοποίηση και πρόβλεψη Κυβερνοαπειλών και Ευπαθειών.
- Η Λήψη τεκμηριωμένων αποφάσεων κατά τη διερεύνηση ειδοποιήσεων Ασφαλείας.
- Η Εξάλειψη των απειλών πριν τη διείσδυση.

Compliance

Διαχείριση μέσω ενός user-friendly περιβάλλοντος των απαιτήσεων των Προτύπων και Κανονισμών. Παρακολούθηση σε πραγματικό χρόνο της κατάστασης συμμόρφωσης μέσω προσαρμόσιμων dashboards και reports.

Dashboards
Διατήρηση του Security Posture. Επίγνωση της κατάστασης των μετρήσεων Ασφαλείας για τη λήψη των σωστών αποφάσεων, έγκαιρα και αποτελεσματικά. Προσαρμοσμένα dashboards, αριθμήσιμα, ώστε να εμφανίζονται οι πληροφορίες που είναι πιο χρήσιμες και αποτελεσματικές στη διατήρηση μιας επισκόπησης της κατάστασης ειδοποιήσεων ασφαλείας, της απόδοσης, και της διαθεσιμότητας.

Reports
Εξαγωγή κατάλληλων και ακριβών reports για την παρακολούθηση των υποχρεώσεων συμμόρφωσης (compliance), καθώς και των απαιτήσεων Εσωτερικού Ελέγχου (audit).

Event Management
Παροχή έγκαιρης έρευνας, κατηγοριοποίησης, εκχώρησης και επίλυσης ειδοποιήσεων Ασφαλείας - διαχείρισης Συμβάντων Ασφαλείας. Ταξινόμηση των απειλών της ENISA για την αποτελεσματική παρακολούθηση και διαχείριση των Περιστατικών Ασφαλείας.

Performance & Availability – NOC
Προληπτική παρακολούθηση της απόδοσης και της διαθεσιμότητας των συσκευών δικτύου (NOC), των συστημάτων και των συνδέσεων επικοινωνίας, συλλέγοντας και επεξεργάζοντας δεδομένα Netflow και SNMP. Επίτευξη ελαχιστοποίησης του χρόνου διακοπής λειτουργίας και του σχετικού επιχειρηματικού κόστους που προκαλείται από διακοπές υπηρεσιών.

ΠΡΟΫΠΟΘΕΣΕΙΣ ΕΠΑΓΓΕΛΜΑΤΙΚΗΣ ΚΑΙ ΤΕΧΝΙΚΗΣ ΙΚΑΝΟΤΗΤΑΣ ΚΑΙ ΕΜΠΕΙΡΟΓΝΩΣΙΑΣ ΑΝΑΔΟΧΟΥ

Το Σύστημα SOC ή οι Άδειες SOC πρέπει να είναι πιστοποιημένο/ες κατά ISO 27001 και SOC II Type II.

Ο Ανάδοχος του έργου θα πρέπει να διαθέτει τις παρακάτω πιστοποιήσεις :

- ISO 9001-2015,
- ISO 14001-2015,
- ISO 20000-2018,
- ISO 22301-2019,
- ISO 27001-2022,
- ISO 27701-2019,
- ISO 37001-2016,

Ο Ανάδοχος οφείλει να έχει υλοποιήσει αντίστοιχο έργο σε τουλάχιστον ένα Δημόσιο Νοσοκομείο τα τελευταία δυο (2) έτη και να προσκομίσει αντίστοιχη Σύμβαση ενεργή ή ολοκληρωμένη.

Το προσωπικό του Λογισμικού SOC, ανάλογα με την εμπειρία, τις δεξιότητες και τα καθήκοντα, θα πρέπει να διαβαθμίζεται στα εξής επίπεδα:

Αναλυτής Επιπέδου 1

- Παρακολούθηση των alerts σε πραγματικό χρόνο.
- Παρακολούθηση της διαθεσιμότητας των συστημάτων του Νοσοκομείου.
- Αρχική συλλογή πληροφοριών.

Αναλυτής Επιπέδου2

- Κλιμάκωση των alerts ανάλογα με την σοβαρότητα τους.
- Συλλογή πληροφοριών εις βάθος.
- Ανταπόκριση σε αιτήματα διαχείρισης συμβάντων.
- Επικοινωνία με τα στελέχη του Νοσοκομείου.

Αναλυτής Επιπέδου3

- Ανάλυση εις βάθος και εμπλουτισμός των αναφορών συμβάντων.
- Threat Hunting.
- Ανάλυση Ευπαθειών.
- Αξιοποίηση πληροφοριών Threat Intelligence.

Υπεύθυνος Ομάδας

- Διασφάλιση ποιότητας και έλεγχος εργασιών.
- Προγραμματισμός βαρδιών.
- Συνεχιζόμενη εκπαίδευση των Αναλυτών.
- Δημιουργία, διαχείριση και βελτίωση των Κανόνων Συσχέτισης.
- Δημιουργία αναφορών.
- Επίβλεψη των Αναλυτών.

Διευθυντής

- Υπεύθυνος για την συνολική λειτουργία του SOC.
- Διασφάλιση της εύρυθμης λειτουργίας (άνθρωποι, διαδικασίες, συστήματα).
- Συνεχής επίβλεψη, επίλυση προβλημάτων και βελτίωση της λειτουργίας.
- Επικοινωνία με το Νοσοκομείο, κυρίως για σοβαρά συμβάντα ή ευαίσθητα θέματα.
- Διασφάλιση του SLA (Συμφωνία Επίπεδου Υπηρεσίας).
- Διασφάλιση της συνολικής ποιότητας.
- Συντονισμός ανάμεσα σε εξωτερικούς και εσωτερικούς συνεργάτες.
- Υλοποίηση της στρατηγικής του τμήματος.

ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

Ο Ανάδοχος, χωρίς προηγούμενη γραπτή συναίνεση του Νοσοκομείου δεν επιτρέπεται να αποκαλύπτει εμπιστευτικές πληροφορίες που του δόθηκαν ή που ο ίδιος ανακάλυψε κατά την εκτέλεση του παρόντος έργου, ούτε να κοινοποιεί στοιχεία, έγγραφα και πληροφορίες των οποίων λαμβάνει γνώση σε σχέση με τη παρούσα Σύμβαση. Υποχρεούται δε να μεριμνά ώστε το προσωπικό του και κάθε συνεργάτης του να τηρήσει την ως άνω υποχρέωση.
Σε περίπτωση αθέτησης της ανωτέρω υποχρέωσης του Αναδόχου, το Νοσοκομείο δικαιούται να απαιτήσει την αποκατάσταση τυχόν ζημίας με κάθε νόμιμο τρόπο και την παύση κοινοποίησης των εμπιστευτικών πληροφοριών.
Ο Ανάδοχος οφείλει να τηρήσει πλήρη εμπιστευτικότητα και εχεμύθεια σε όποια πληροφορία περιέλθει σε γνώση του και αφορά προσωπικά δεδομένα ασθενών, εργαζομένων, συνεργατών, προμηθευτών του Νοσοκομείου και σύμφωνα με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ – GDPR) 2016/679 της Ε.Ε.

ΧΡΟΝΟΣ ΥΛΟΠΟΙΗΣΗΣ - ΔΙΑΡΚΕΙΑ ΤΟΥ ΕΡΓΟΥ

Ο Ανάδοχος οφείλει να εγκαταστήσει την πλατφόρμα του Λογισμικού 24-ωρης Παρακολούθησης και Απόκρισης Κέντρου Επιχειρήσεων Ασφαλείας (SOC: Security Operations Center) με

Υπηρεσίες Διαχειριζόμενης Ανίχνευσης και Απόκρισης (MDR) στις υποδομές του Νοσοκομείου, εντός **δυο (2) εβδομάδων** από την έναρξη της Σύμβασης του έργου και κατόπιν συνεννόησης με το Τμήμα Πληροφορικής του Νοσοκομείου. Οι άδειες χρήσης του Λογισμικού θα είναι ετήσιες και αφορούν τον Κεντρικό ΙΤ Εξοπλισμό και τις 210 θέσεις Εργασίας του Νοσοκομείου.

ΠΙΘΑΝΟ ΚΟΣΤΟΣ ΔΑΠΑΝΗΣ

Το πιθανό Κόστος του έργου διαμορφώνονται σύμφωνα με τον παρακάτω πίνακα :

Α/Α	**ΠΕΡΙΓΡΑΦΗ ΄ΕΡΓΟΥ**	**ΤΜΧ**	**ΤΙΜΗ ΜΟΝΑΔΟΣ ΧΩΡΙΣ ΦΠΑ**	**ΣΥΝΟΛΙΚΗ ΠΡΟΫΠΟΛΟΓΙΣΘΕΙΣΑ ΔΑΠΑΝΗ, ΧΩΡΙΣ ΦΠΑ**
1	Υπηρεσίες 24ωρης παρακολούθησης και απόκρισης με χρήση Λογισμικού SOC με 30 ημέρες περίοδο ενεργής αποθήκευσης, με Υπηρεσία Διαχειριζόμενης Ανίχνευσης και Απόκρισης για: 20 Servers 2 Firewalls 210 Επιτραπέζιους Υπολογιστές, με 5 Αιτήματα Αλλαγών ανά μήνα, Υποστήριξη 8x5 και 24ωρη Παρακολούθηση.	1	29.850,00	29.850,00
ΣΥΝΟΛΟ ΧΩΡΙΣ ΦΠΑ				**29.850,00€**

1. **ΠΙΝΑΚΑΣ ΣΥΜΜΟΡΦΩΣΗΣ ΤΕΧΝΙΚΗΣ ΠΡΟΣΦΟΡΑΣ**

Α/Α	ΠΕΡΙΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ/ ΠΑΡΑΤΗΡΗΣΕΙΣ
1	**Σκοπός του Έργου** Σκοπός του έργου είναι η εξασφάλιση υψηλού επιπέδου Κυβερνοασφάλειας του Γ.Ν.Α. «Η ΕΛΠΙΣ» (εφεξής Νοσοκομείο), προς συμμόρφωση με τις απαιτήσεις της Ευρωπαϊκής Οδηγίας NIS2, η οποία ενσωματώνεται στον **Ν.5160/27-11-2024** και προς : • αποφυγή προστίμων, • μείωση των κινδύνων διαρροών Ευαίσθητων Προσωπικών Δεδομένων, • διασφάλιση της Επιχειρησιακής Συνέχειας του Νοσοκομείου σε περίπτωση Κυβερνοεπίθεσης, • ενίσχυση της Φήμης του Νοσοκομείου ως ασφαλούς φορέα.	ΝΑΙ		
2	**Αντικείμενο του Έργου** Σύμφωνα με την Οδηγία NIS2 της ΕΕ και την προσαρμογή της στην Ελληνική Νομοθεσία με το Ν.5160/27-11-2024 και συγκεκριμένα το Μέρος Α', Κεφ. Β', Άρθρο 15, παρ. 6, προκειμένου να αποδειχθεί η συμμόρφωση με τις απατήσεις της Νομοθεσίας, δύναται να απαιτηθεί από τους Φορείς να χρησιμοποιούν συγκεκριμένα προϊόντα ΤΠΕ (Τεχνολογίες Πληροφοριών και Επικοινωνιών) είτε σε Hardware (Υλικός Εξοπλισμός), είτε σε Software (Λογισμικό), υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ, που αναπτύσσονται από τον φορέα ή παρέχονται από τρίτους και πιστοποιούνται στο πλαίσιο Ευρωπαϊκών Συστημάτων πιστοποίησης Κυβερνοασφάλειας Αντικείμενο του έργου αποτελεί η προμήθεια ειδικού Λογισμικού 24-ωρης Παρακολούθησης και Απόκρισης Κέντρου Επιχειρήσεων Ασφαλείας (SOC: Security Operations Center) με Υπηρεσίες Διαχειριζόμενης Ανίχνευσης και Απόκρισης (MDR), προκειμένου να επιτευχθεί η εξασφάλιση υψηλού επιπέδου Κυβερνοασφάλειας του Νοσοκομείου και η δυνατότητα απόδειξης της συμμόρφωσης με την κείμενη Νομοθεσία. Η συνεχής παρακολούθηση και προστασία της Υποδομής του Νοσοκομείου είναι επιβεβλημένη. Η παρακολούθηση αυτή θα πρέπει να γίνεται επί 24ωρου βάσης 365 ημέρες τον χρόνο από επαγγελματίες και εξειδικευμένο προσωπικό στην Κυβερνοασφάλεια. Το Νοσοκομείο είναι αδύνατο να δημιουργήσει και να διατηρήσει μια εσωτερική ομάδα, η	ΝΑΙ		

	οποία θα εξελίσσει διαρκώς τις δεξιότητες που απαιτούνται για την επίτευξη του στόχου της Ασφάλειας της Πληροφορίας. Για την επίτευξη του περιορισμού των διαρκώς αναπτυσσόμενων ψηφιακών κινδύνων, προκύπτει η ανάγκη της ανάθεσης της Ασφάλειας των Πληροφοριών και της Διαχείρισης Κινδύνων (Information Security and Risk Management) σε εξειδικευμένο και αξιόπιστο πάροχο υπηρεσιών Ασφάλειας (Managed Security Services). Το Επιχειρησιακό Κέντρο Ασφαλείας (SOC) θα παρέχει στο Νοσοκομείο το αιτούμενο επίπεδο Ασφάλειας της Πληροφορίας και την αντοχή τους σε Κακόβουλες Επιθέσεις σε ένα βέλτιστο επιχειρησιακό και αποτελεσματικό επίπεδο, 24x7χ365 ημέρες το χρόνο.			
3	**ΑΠΑΙΤΟΥΜΕΝΕΣ ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΤΟΥ ΕΡΓΟΥ** Στο πλαίσιο του έργου, ο Ανάδοχος οφείλει να προσφέρει Λογισμικό Cloud Software-as-a-Service που να ενεργοποιείται μέσω δικής του Συσκευής προώθησης δεδομένων iCollector (κεντρική παρακολούθηση και ανάλυση συμβάντων Κυβερνοασφάλειας σε πραγματικό χρόνο), που να μπορεί να είναι on-premise, στο Cloud ή σε υβριδικό περιβάλλον και η διαχείρισή του να υλοποιείται μέσω Κεντρικής Κονσόλας Web Portal. Το Λογισμικό πρέπει να : **5.** παρέχει σε πραγματικό χρόνο ευφυή ανάλυση σε βάθος και συσχέτιση δεδομένων και συμβάντων που συλλέγονται από ετερογενείς πηγές δεδομένων, σε συνδυασμό με τεκμηριωμένη γνώση των αναδυόμενων απειλών και ευπαθειών για την παραγωγή πληροφοριών. **6.** τη δυνατότητα άμεσης ανταπόκρισης σε απειλές και αξιολόγησης περιστατικών Ασφαλείας/Incidents, προς μείωση του χρόνου διακοπής λειτουργίας του Νοσοκομείου και αποτύπωσης των σχετικών εκθέσεων Ελέγχου και Συμμόρφωσης. **7.** δίνει τη δυνατότητα για τον έγκαιρο εντοπισμό και την αντιμετώπιση προηγμένων κακόβουλων κυβερνοεπιθέσεων και ύποπτων δραστηριοτήτων χρηστών, με τη χρήση της ενορχήστρωσης και	ΝΑΙ		

	αυτοματοποίησης ασφάλειας (Security Orchestration & Response), της προηγμένης μηχανικής μάθησης (Machine Learning - ML) και της Τεχνητής Νοημοσύνης (Artificial Intelligence - AI). **8.** χρησιμοποιεί αλγορίθμους μηχανικής μάθησης (ML) και Τεχνητής Νοημοσύνης (AI) για να βελτιώσει δραστικά τις δυνατότητες ανίχνευσης και πρόβλεψης που σχετίζονται με ύποπτες/ κακόβουλες Κυβερνοαπειλές, συμπεριλαμβανομένης της μη φυσιολογικής δραστηριότητας/ συμπεριφοράς χρηστών. Διαδικασία διαχείρισης απειλών (Threat Management Process) Το Λογισμικό θα πρέπει απλοποιεί τη διαδικασία διαχείρισης απειλών επιταχύνοντας σημαντικά τις προληπτικές δυνατότητες ανίχνευσης και απόκρισης απειλών, μειώνοντας έτσι δραστικά το "Detection Deficit" (χρόνος μεταξύ παραβίασης και ανακάλυψης). Ταυτόχρονα, θα πρέπει να διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα ευαίσθητων πληροφοριών που βρίσκονται στα δεδομένα. Υπηρεσίες διαχείρισης πληροφοριών και περιστατικών ασφάλειας (Security Information and Event Management - SIEM) Η αυξανόμενη πολυπλοκότητα και εξάρτηση από το οικοσύστημα πληροφορικής δημιουργεί άγνωστους ψηφιακούς κινδύνους, καθώς και νέα είδη απειλών. Η πλατφόρμα του λογισμικού θα πρέπει να έχει σε γενικές γραμμές τη δυνατότητα: • παροχής πληροφοριών σε πραγματικό χρόνο σχετικά με την κατάσταση ασφαλείας του Νοσοκομείου (Cybersercurity posture), • αποτελεσματικής υποστήριξης κρίσιμων λειτουργιών, όπως προηγμένα αναλυτικά μοντέλα ασφαλείας,			

	• βοήθειας στη βελτίωση της ανίχνευσης απειλών, της διαχείρισης συμβάντων, της έρευνας σε πραγματικό χρόνο και της έξυπνης ανάλυσης ιστορικών ή/και τρεχόντων δεδομένων καταγραφής και συμβάντων, • παροχής αυτοματοποιημένης ειδοποίησης, • διευκόλυνσης της ουσιαστικής επιχειρησιακής και κανονιστικής υποβολής εκθέσεων, • ενίσχυσης των δυνατοτήτων αντιμετώπισης περιστατικών του Νοσοκομείου, • βοήθειας για την αντιμετώπιση της κανονιστικής συμμόρφωσης. Πλεονεκτήματα των υπηρεσιών Managed Security Services επόμενης γενιάς • Ενσωματωμένη ευφυΐα. • Μηδενική αρχική επένδυση. • Καμία απαξίωση υλικού (hardware). • Επεκτασιμότητα. • Μειωμένος χρόνος για την επίτευξη αποτελεσμάτων. • Νοημοσύνη απειλών (Threat Intelligence). • Μειωμένα λειτουργικά έξοδα. Τα αιτούμενα χαρακτηριστικά της πλατφόρμας του Λογισμικού Έξυπνη ανάλυση (μοντέλα AI & ML) Βελτιωμένος έγκαιρος εντοπισμός και απόκριση σε προηγμένες επιθέσεις, παραβιάσεις δεδομένων ή/και ύποπτη/κακόβουλη συμπεριφορά του χρήστη με χρήση προγνωστικών/μηχανικών μοντέλων μάθησης, που καθιστούν δυνατή την ανίχνευση μη φυσιολογικής συμπεριφοράς ή/και κακόβουλων πληροφοριών-απειλών			

	που διαφορετικά θα περνούσαν απαρατήρητες/ μη ανιχνεύσιμες με την χρήση συμβατικών συστημάτων πληροφοριών ασφαλείας και διαχείρισης συμβάντων. Ευελιξία Επιτρέπει την ικανότητα συλλογής, επεξεργασίας και ανάλυσης νέων τύπων δεδομένων καταγραφής και συμβάντων σε περιβάλλοντα IT και Τεχνολογιών (Operational Technology - OT), παρέχοντας δυνατότητα αποθήκευσης, επεξεργασίας και ανάλυσης διαφορετικών τύπων δεδομένων καταγραφής και συμβάντων από διάφορους τύπους συσκευών, είτε δομημένων είτε μη δομημένων. Επεξεργαστική ισχύς Δυνατότητα επεξεργασίας πολύ πιο τρεχόντων και ιστορικών δεδομένων καταγραφής και συμβάντων σε πραγματικό χρόνο, σε κλάσμα του χρόνου. iCollector Ο iCollector είναι μια έξυπνη συσκευή που συλλέγει και αναλύει έξυπνα, σε πραγματικό χρόνο, δεδομένα καταγραφής και συμβάντων από εκατοντάδες διαφορετικούς τύπους δεδομένων. Προσφέρεται ως φυσική ή εικονική συσκευή και μπορεί να αναπτυχθεί είτε on-premise, cloud ή και στα δύο για υβριδικά περιβάλλοντα. iCollector Τρόπος Λειτουργίας Εκτελώντας μια σειρά λειτουργιών, ο iCollector Συλλέγει (Collect), Αρχειοθετεί – Archive (Digitally Signs/Encrypts), Ομαλοποιεί (Normalize), Αναλύει Έξυπνα (Intelligently Analyze) και Συσχετίζει (Correlate) τεράστιους όγκους ετερογενών δεδομένων. Αξιοποιεί πληροφορίες για αναδυόμενες απειλές, ευπάθειες, για τον έγκαιρο εντοπισμό και την αντιμετώπιση στοχευμένων επιθέσεων και παραβιάσεων δεδομένων. Για τη διασφάλιση της εμπιστευτικότητας και τη διατήρηση της ακεραιότητας ευαίσθητων πληροφοριών, τα δεδομένα αρχείου καταγραφής και συμβάντων που συλλέγονται δύναται να υποβληθούν σε διαδικασία συγκάλυψης (Mask). Collect Συλλέγονται τεράστιοι όγκοι ετερογενών συνόλων δεδομένων που παράγονται από διάφορες συσκευές ασφαλείας, υποδομές δικτύου, συστήματα και εφαρμογές.			

	Archive Τα δεδομένα καταγραφής και συμβάντων που συλλέγονται συμπιέζονται σε αναλογία έως και 96%, υπογράφονται ψηφιακά και κρυπτογραφούνται προαιρετικά πριν αρχειοθετηθούν. Με αυτόν τον τρόπο, συλλέγονται δεδομένα καταγραφής και συμβάντων και διατηρούνται σε κατάσταση που θα μπορούσε επίσης να χρησιμοποιηθεί για εγκληματολογική έρευνα ή νομικά αποδεικτικά στοιχεία, εάν προκύψει ανάγκη. Normalize Τα δεδομένα καταγραφής και συμβάντων που συλλέγονται ομαλοποιούνται και αποθηκεύονται σε κοινή μορφή, κατά τη στιγμή της συλλογής δεδομένων, για περαιτέρω επεξεργασία. Intelligently Analyse Έξυπνη επεξεργασία, συγκέντρωση και ανάλυση δεδομένων καταγραφής και συμβάντων με τη χρήση μοντέλων Συμπεριφοράς Χρήστη & Οντότητας, Τεχνητής Νοημοσύνης, Πρόβλεψης και Μηχανικής Μάθησης, ενσωματώνοντας contextual πληροφορίες για την πρόβλεψη ύποπτης και την ανίχνευση μη φυσιολογικής συμπεριφοράς. Correlate Η συσχέτιση των δεδομένων και συμβάντων χρησιμοποιεί, όχι μόνο μια σειρά από στατιστικών και ευρετικών (heuristic) μοντέλων, αλλά και μια σειρά προκαθορισμένων κανόνων ευφυούς συσχέτισης σε συνδυασμό με τεκμηριωμένη γνώση των αναδυόμενων απειλών και τρωτών σημείων, επιτρέποντας με αυτόν τον τρόπο τον έγκαιρο εντοπισμό και την αντιμετώπιση επιθέσεων και παραβιάσεων δεδομένων. Mask Οι ευαίσθητες πληροφορίες που βρίσκονται στα δεδομένα μπορούν προαιρετικά να αποκρύπτονται για τη διασφάλιση της εμπιστευτικότητας.			

	Secure Web Portal (SWP) Το Λογισμικό πρέπει να διαθέτει μία Web Portal (SWP) κεντρική κονσόλα διαχείρισης, παρέχοντας στο Νοσοκομείο σαφή ορατότητα σε πραγματικό χρόνο σημαντικών συμβάντων, μετρήσεων, δεικτών και αξιολόγησης κινδύνου μέσω έξυπνων, πλήρως προσαρμόσιμων έξυπνων πινάκων εργαλείων. Threat Intelligence Το Λογισμικό πρέπει να διαθέτει τεχνολογία Threat Intelligence, η οποία ενημερώνει για νέες ευπάθειες και αναδυόμενες απειλές στον κυβερνοχώρο. Αποτελεί βασικό πυλώνα γιατί παρέχει μια συνεχώς ενημερωμένη και αναλυμένη ροή τεκμηριωμένων γνώσεων σχετικά με αναδυόμενες απειλές και ευπάθειες στον κυβερνοχώρο. Αντλεί δεδομένα από έγκυρα feeds Threat Intelligence και τα επεξεργάζεται για να εξάγει πολύτιμες πληροφορίες που σχετίζονται με το Νοσοκομείο. Αναλύει δεδομένα και συμπεριφορές για να υποστηρίξει την προληπτική άμυνα του Νοσοκομείου. Επιπλέον, το Threat Anticipation αξιοποιεί τη συνεχή συλλογή πληροφοριών απειλής σε συνδυασμό με το Advanced Security Analytics για να εντοπίσει τη σοβαρότητα και το αντίκτυπο των απειλών στον κυβερνοχώρο σε σχέση με τα χαρακτηριστικά του Νοσοκομείου, παρέχοντας μια ολοκληρωμένη αξιολόγηση και ανάλυση των Δεικτών Επίθεσης (Indicators of Attack - IOA), με χρήσιμες πληροφορίες, Threat Hunting και την εξάλειψη απειλών στο επόμενο επίπεδο. Η βελτιστοποίηση του Risk Exposure είναι μια συνεχής διαδικασία προληπτικής προσαρμογής στο συνεχώς μεταβαλλόμενο τοπίο απειλών στον κυβερνοχώρο. Στόχος : • Η Απόκτηση γενικής εικόνας του Risk Susceptibility του Νοσοκομείου. • Η Ενημέρωση για το συνεχώς μεταβαλλόμενο τοπίο Κυβερνοαπειλών. • Η Συνεχής βελτιστοποίησή του Security Posture.			

	• Η Ταυτοποίηση και πρόβλεψη Κυβερνοαπειλών και Ευπαθειών. • Η Λήψη τεκμηριωμένων αποφάσεων κατά τη διερεύνηση ειδοποιήσεων Ασφαλείας. • Η Εξάλειψη των απειλών πριν τη διείσδυση. Compliance Διαχείριση μέσω ενός user-friendly περιβάλλοντος των απαιτήσεων των Προτύπων και Κανονισμών. Παρακολούθηση σε πραγματικό χρόνο της κατάστασης συμμόρφωσης μέσω προσαρμόσιμων dashboards και reports. Dashboards Διατήρηση του Security Posture. Επίγνωση της κατάστασης των μετρήσεων Ασφαλείας για τη λήψη των σωστών αποφάσεων, έγκαιρα και αποτελεσματικά. Προσαρμοσμένα dashboards, αριθμήσιμα, ώστε να εμφανίζονται οι πληροφορίες που είναι πιο χρήσιμες και αποτελεσματικές στη διατήρηση μιας επισκόπησης της κατάστασης ειδοποιήσεων ασφαλείας, της απόδοσης, και της διαθεσιμότητας. Reports Εξαγωγή κατάλληλων και ακριβών reports για την παρακολούθηση των υποχρεώσεων συμμόρφωσης (compliance), καθώς και των απαιτήσεων Εσωτερικού Ελέγχου (audit). Event Management Παροχή έγκαιρης έρευνας, κατηγοριοποίησης, εκχώρησης και επίλυσης ειδοποιήσεων Ασφαλείας - διαχείρισης Συμβάντων Ασφαλείας. Ταξινόμηση των απειλών της ENISA για την αποτελεσματική παρακολούθηση και διαχείριση των Περιστατικών Ασφαλείας. Performance & Availability – NOC			

	Προληπτική παρακολούθηση της απόδοσης και της διαθεσιμότητας των συσκευών δικτύου (NOC), των συστημάτων και των συνδέσεων επικοινωνίας, συλλέγοντας και επεξεργάζοντας δεδομένα Netflow και SNMP. Επίτευξη ελαχιστοποίησης του χρόνου διακοπής λειτουργίας και του σχετικού επιχειρηματικού κόστους που προκαλείται από διακοπές υπηρεσιών.			
4	**ΠΡΟΫΠΟΘΕΣΕΙΣ ΕΠΑΓΓΕΛΜΑΤΙΚΗΣ ΚΑΙ ΤΕΧΝΙΚΗΣ ΙΚΑΝΟΤΗΤΑΣ ΚΑΙ ΕΜΠΕΙΡΟΓΝΩΣΙΑΣ ΑΝΑΔΟΧΟΥ** Το Σύστημα SOC ή οι Άδειες SOC πρέπει να είναι πιστοποιημένο/ες κατά ISO 27001 και SOC II Type II. Ο Ανάδοχος του έργου θα πρέπει να διαθέτει τις παρακάτω πιστοποιήσεις : • ISO 9001-2015, • ISO 14001-2015, • ISO 20000-2018, • ISO 22301-2019, • ISO 27001-2022, • ISO 27701-2019, • ISO 37001-2016, Ο Ανάδοχος οφείλει να έχει υλοποιήσει αντίστοιχο έργο σε τουλάχιστον ένα Δημόσιο Νοσοκομείο τα τελευταία δυο (2) έτη και να προσκομίσει αντίστοιχη Σύμβαση ενεργή ή ολοκληρωμένη. Το προσωπικό του Λογισμικού SOC, ανάλογα με την εμπειρία, τις δεξιότητες και τα καθήκοντα, θα πρέπει να διαβαθμίζεται στα εξής επίπεδα:	ΝΑΙ		

	Αναλυτής Επιπέδου 1 • Παρακολούθηση των alerts σε πραγματικό χρόνο. • Παρακολούθηση της διαθεσιμότητας των συστημάτων του Νοσοκομείου. • Αρχική συλλογή πληροφοριών. Αναλυτής Επιπέδου2 • Κλιμάκωση των alerts ανάλογα με την σοβαρότητα τους. • Συλλογή πληροφοριών εις βάθος. • Ανταπόκριση σε αιτήματα διαχείρισης συμβάντων. • Επικοινωνία με τα στελέχη του Νοσοκομείου. Αναλυτής Επιπέδου3 • Ανάλυση εις βάθος και εμπλουτισμός των αναφορών συμβάντων. • Threat Hunting. • Ανάλυση Ευπαθειών. • Αξιοποίηση πληροφοριών Threat Intelligence. Υπεύθυνος Ομάδας • Διασφάλιση ποιότητας και έλεγχος εργασιών. • Προγραμματισμός βαρδιών. • Συνεχιζόμενη εκπαίδευση των Αναλυτών. • Δημιουργία, διαχείριση και βελτίωση των Κανόνων Συσχέτισης. • Δημιουργία αναφορών. • Επίβλεψη των Αναλυτών.			

	Διευθυντής • Υπεύθυνος για την συνολική λειτουργία του SOC. • Διασφάλιση της εύρυθμης λειτουργίας (άνθρωποι, διαδικασίες, συστήματα). • Συνεχής επίβλεψη, επίλυση προβλημάτων και βελτίωση της λειτουργίας. • Επικοινωνία με το Νοσοκομείο, κυρίως για σοβαρά συμβάντα ή ευαίσθητα θέματα. • Διασφάλιση του SLA (Συμφωνία Επίπεδου Υπηρεσίας). • Διασφάλιση της συνολικής ποιότητας. • Συντονισμός ανάμεσα σε εξωτερικούς και εσωτερικούς συνεργάτες. • Υλοποίηση της στρατηγικής του τμήματος.			
5	**ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ** Ο Ανάδοχος, χωρίς προηγούμενη γραπτή συναίνεση του Νοσοκομείου δεν επιτρέπεται να αποκαλύπτει εμπιστευτικές πληροφορίες που του δόθηκαν ή που ο ίδιος ανακάλυψε κατά την εκτέλεση του παρόντος έργου, ούτε να κοινοποιεί στοιχεία, έγγραφα και πληροφορίες των οποίων λαμβάνει γνώση σε σχέση με τη παρούσα Σύμβαση. Υποχρεούται δε να μεριμνά ώστε το προσωπικό του και κάθε συνεργάτης του να τηρήσει την ως άνω υποχρέωση. Σε περίπτωση αθέτησης της ανωτέρω υποχρέωσης του Αναδόχου, το Νοσοκομείο δικαιούται να απαιτήσει την αποκατάσταση τυχόν ζημίας με κάθε νόμιμο τρόπο και την παύση κοινοποίησης των εμπιστευτικών πληροφοριών. Ο Ανάδοχος οφείλει να τηρήσει πλήρη εμπιστευτικότητα και εχεμύθεια σε όποια πληροφορία περιέλθει σε γνώση του και αφορά προσωπικά δεδομένα ασθενών, εργαζομένων, συνεργατών, προμηθευτών του Νοσοκομείου και σύμφωνα με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ – GDPR) 2016/679 της Ε.Ε.	ΝΑΙ		

<table>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>6</td><td>

ΧΡΟΝΟΣ ΥΛΟΠΟΙΗΣΗΣ - ΔΙΑΡΚΕΙΑ ΤΟΥ ΕΡΓΟΥ

Ο Ανάδοχος οφείλει να εγκαταστήσει την πλατφόρμα του Λογισμικού 24-ωρης Παρακολούθησης και Απόκρισης Κέντρου Επιχειρήσεων Ασφαλείας (SOC: Security Operations Center) με Υπηρεσίες Διαχειριζόμενης Ανίχνευσης και Απόκρισης (MDR) στις υποδομές του Νοσοκομείου, εντός δυο (2) εβδομάδων από την έναρξη της Σύμβασης του έργου και κατόπιν συνεννόησης με το Τμήμα Πληροφορικής του Νοσοκομείου. Οι άδειες χρήσης του Λογισμικού θα είναι ετήσιες και αφορούν τον Κεντρικό ΙΤ Εξοπλισμό και τις 210 θέσεις Εργασίας του Νοσοκομείου.

ΠΙΘΑΝΟ ΚΟΣΤΟΣ ΔΑΠΑΝΗΣ

Το πιθανό Κόστος του έργου διαμορφώνονται σύμφωνα με τον παρακάτω πίνακα :

Α/Α	ΠΕΡΙΓΡΑΦΗ ΈΡΓΟΥ	ΤΜΧ	ΤΙΜΗ ΜΟΝΑΔΟΣ ΧΩΡΙΣ ΦΠΑ	ΣΥΝΟΛΙΚΗ ΠΡΟΫΠΟΛΟΓΙΣΘΕΙΣΑ ΔΑΠΑΝΗ, ΧΩΡΙΣ ΦΠΑ
1	Υπηρεσίες 24ωρης παρακολούθησης και απόκρισης με χρήση Λογισμικού SOC με 30 ημέρες περίοδο ενεργής αποθήκευσης, με Υπηρεσία Διαχειριζόμε	1	29.850,00	29.850,00

</td><td>ΝΑΙ</td><td></td><td></td></tr>
</table>

		νης Ανίχνευσης και Απόκρισης για: 20 Servers 2 Firewalls 210 Επιτραπέζιους Υπολογιστές, με 5 Αιτήματα Αλλαγών ανά μήνα, Υποστήριξη 8x5 και 24ωρη Παρακολούθηση.						
	ΣΥΝΟΛΟ ΧΩΡΙΣ ΦΠΑ			**29.850,00€**				

Τα αναγραφόμενα στον πίνακα συμμόρφωσης, στον οποίο περιγράφεται αναλυτικά το προσφερόμενο είδος με το σύνολο των τεχνικών προδιαγραφών της πρόσκλησης, πρέπει να τεκμηριώνονται με παραπομπές στα επίσημα τεχνικά φυλλάδια (prospectus) του κατασκευαστικού οίκου ή με την προσκόμιση επίσημων βεβαιώσεων του κατασκευαστή ή (και) άλλων επίσημων εγγράφων για ότι δεν αναγράφεται στα τεχνικά φυλλάδια. Προσφορές οι οποίες θα αντιγράφουν τις τεχνικές προδιαγραφές της πρόσκλησης ή θα απαντούν μονολεκτικά ("ΝΑΙ" ή "συμφωνούμε" κ.λ.π.), χωρίς τεκμηρίωση και πλήρη παραπομπή – αντιστοιχία, μεταξύ κειμένου ανά παράγραφο και prospectus θα αποκλείονται.
Ο πίνακας συμμόρφωσης της Πρόσκλησης πρέπει να υποβληθεί με την τεχνική προσφορά, συμπληρωμένος σύμφωνα με τις παρακάτω επεξηγήσεις και οδηγίες, τις οποίες ο υποψήφιος είναι υποχρεωμένος να ακολουθήσει:

1. Στη Στήλη «ΤΕΧΝΙΚΗ ΠΡΟΔΙΑΓΡΑΦΗ», περιγράφονται αναλυτικά οι αντίστοιχοι τεχνικοί όροι, υποχρεώσεις ή επεξηγήσεις για τα οποία θα πρέπει να δοθούν αντίστοιχες απαντήσεις.
2. Στη στήλη «ΑΠΑΝΤΗΣΗ ΥΠΟΨΗΦΙΟΥ» σημειώνεται η απάντηση του υποψηφίου Αναδόχου που έχει τη μορφή ΝΑΙ/ ΟΧΙ εάν η αντίστοιχη προδιαγραφή πληρούται ή όχι από την προσφορά ή ένα αριθμητικό μέγεθος που δηλώνει την ποσότητα του αντίστοιχου χαρακτηριστικού στην προσφορά. Απλή κατάφαση ή επεξήγηση δεν αποτελεί απόδειξη πλήρωσης της προδιαγραφής και η αρμόδια Επιτροπή έχει την υποχρέωση ελέγχου και επιβεβαίωσης της πλήρωσης της απαίτησης.
3. Στη στήλη «ΠΑΡΑΠΟΜΠΗ» θα καταγραφεί η σαφής παραπομπή σε ενότητα της τεχνικής προσφοράς, η οποία θα περιλαμβάνει αριθμημένα Τεχνικά Φυλλάδια κατασκευαστών, ή αναλυτικές τεχνικές περιγραφές των υπηρεσιών, του εξοπλισμού ή του τρόπου διασύνδεσης και λειτουργίας ή αναφορές μεθοδολογίας εγκατάστασης και υποστήριξης κλπ., που κατά την κρίση του υποψηφίου Αναδόχου τεκμηριώνουν τα στοιχεία του Πίνακα Συμμόρφωσης.
4. Είναι υποχρεωτική η πλήρης συμπλήρωση των παραπομπών, οι οποίες πρέπει να είναι κατά το δυνατόν συγκεκριμένες (π.χ. Τεχνικό Φυλλάδιο 3, Σελ. 4 Παράγραφος 4, κ.λ.π.). Αντίστοιχα στο τεχνικό φυλλάδιο ή στην αναφορά θα υπογραμμιστεί το σημείο που τεκμηριώνει τη συμφωνία και θα σημειωθεί η αντίστοιχη παράγραφος του Πίνακα Συμμόρφωσης, στην οποία καταγράφεται η ζητούμενη προδιαγραφή (π.χ. Προδ. 4.18).

ΠΑΡΑΡΤΗΜΑ ΙΙ-ΥΠΟΔΕΙΓΜΑ ΟΙΚΟΝΟΜΙΚΗΣ ΠΡΟΣΦΟΡΑΣ

Α/Α	ΠΕΡΙΓΡΑΦΗ	ΠΟΣΟΤΗΤΑ	ΤΙΜΗ ΠΛΕΟΝ Φ.Π.Α	ΣΥΝΟΛΟ ΣΥΜΠ. Φ.Π.Α
	Προμήθεια ειδικού Λογισμικού 24-ωρης Παρακολούθησης και Απόκρισης Κέντρου Επιχειρήσεων Ασφαλείας (SOC) με Υπηρεσίες Διαχειριζόμενης Ανίχνευσης και Απόκρισης (MDR), στο πλαίσιο εναρμόνισης του Γ.Ν.Α. «Η ΕΛΠΙΣ» με το Ν.5160/27-11-2024 - Οδηγία NIS2 για την εξασφάλιση υψηλού επιπέδου Κυβερνοασφάλειας»,	1		

ΥΠΟΔΕΙΓΜΑ ΥΠΕΥΘΥΝΗΣ ΔΗΛΩΣΗΣ

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ
(άρθρο 8 Ν.1599/1986)

Η ακρίβεια των στοιχείων που υποβάλλονται με αυτή τη δήλωση μπορεί να ελεγχθεί με βάση το αρχείο άλλων υπηρεσιών (άρθρο 8 παρ. 4 Ν. 1599/1986)							
ΠΡΟΣ[(1)]:	ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΑΘΗΝΩΝ «Η ΕΛΠΙΣ»						
Ο – Η Όνομα:		Επώνυμο:					
Όνομα και Επώνυμο Πατέρα:							
Όνομα και Επώνυμο Μητέρας:							
Ημερομηνία γέννησης[(2)]:							
Τόπος Γέννησης:							
Αριθμός Δελτίου Ταυτότητας:		Τηλ:					
Τόπος Κατοικίας:		Οδός:		Αριθ:		ΤΚ:	
Αρ. Τηλεομοιοτύπου (Fax):		Δ/νση Ηλεκτρ. Ταχυδρομείου (Email):					

Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [(3)], που προβλέπονται από τις διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:
Αναφερόμενοι στην πρόσκληση με αριθμό…… για την προμήθεια «……» ως νόμιμος εκπρόσωπος/μέλος του Δ.Σ./διαχειριστής της εταιρείας/ της ατομικής επιχείρησης …….μέχρι και την ημέρα υποβολής της προσφοράς, δεν έχω καταδικαστεί με αμετάκλητη απόφαση για κάποιο τα αδικήματα της παρ. 1 του άρθρου 73 του Ν 4412/2016, δηλαδή για κάποιο από τα ακόλουθα:
α) συμμετοχή σε εγκληματική οργάνωση, όπως αυτή ορίζεται στο άρθρο 2 της απόφασης πλαίσιο 2008/841/ ΔΕΥ του Συμβουλίου της 24ης Οκτωβρίου 2008, για την καταπολέμηση του οργανωμένου εγκλήματος (ΕΕ L 300 της 11.11.2008 σ. 42) και τα εγκλήματα του άρθρου 187 του Ποινικού Κώδικα (εγκληματική οργάνωση),

β) ενεργητική δωροδοκία, όπως ορίζεται στο άρθρο 3 της σύμβασης περί της καταπολέμησης της δωροδοκίας στην οποία ενέχονται υπάλληλοι των Ευρωπαϊκών Κοινοτήτων ή των κρατών μελών της Ένωσης (ΕΕ C 195 της 25.6.1997, σ. 1) και στην παρ. 1 του άρθρου 2 της απόφασης πλαίσιο 2003/568/ΔΕΥ του Συμβουλίου της 22ας Ιουλίου 2003, για την καταπολέμηση της δωροδοκίας στον ιδιωτικό τομέα (ΕΕ L 192 της 31.7.2003, σ. 54), καθώς και, όπως ορίζεται στο εθνικό δίκαιο του οικονομικού φορέα, και τα εγκλήματα των άρθρων 159Α (δωροδοκία πολιτικών προσώπων), 236 (δωροδοκία υπαλλήλου), 237 παρ. 2-4 (δωροδοκία δικαστικών λειτουργών), 237Α παρ. 2 (εμπορία επιρροής μεσάζοντες), 396 παρ. 2 (δωροδοκία στον ιδιωτικό τομέα) του Ποινικού Κώδικα,

γ) απάτη εις βάρος των οικονομικών συμφερόντων της Ένωσης, κατά την έννοια των άρθρων 3 και 4 της Οδηγίας (ΕΕ) 2017/1371 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 5ης Ιουλίου 2017 σχετικά με την καταπολέμηση, μέσω του ποινικού δικαίου, της απάτης εις βάρος των

οικονομικών συμφερόντων της Ένωσης (L 198/28.07.2017) και τα εγκλήματα των άρθρων 159Α (δωροδοκία πολιτικών προσώπων), 216 (πλαστογραφία), 236 (δωροδοκία υπαλλήλου), 237 παρ. 2-4 (δωροδοκία δικαστικών λειτουργών), 242 (ψευδής βεβαίωση, νόθευση κ.λπ.), 374 (διακεκριμένη κλοπή), 375 (υπεξαίρεση), 386 (απάτη), 386Α (απάτη με υπολογιστή), 386Β (απάτη σχετική με τις επιχορηγήσεις), 390 (απιστία) του Ποινικού Κώδικα και των άρθρων 155 επ. του Εθνικού Τελωνειακού Κώδικα (ν. 2960/2001, Α' 265), όταν αυτά στρέφονται κατά των οικονομικών συμφερόντων της Ευρωπαϊκής Ένωσης ή συνδέονται με την προσβολή αυτών των συμφερόντων, καθώς και τα εγκλήματα των άρθρων 23 (διασυνοριακή απάτη σχετικά με τον ΦΠΑ) και 24 (επικουρικές διατάξεις για την ποινική προστασία των οικονομικών συμφερόντων της Ευρωπαϊκής Ένωσης) του ν. 4689/2020 (Α' 103),

δ) τρομοκρατικά εγκλήματα ή εγκλήματα συνδεόμενα με τρομοκρατικές δραστηριότητες, όπως ορίζονται, αντιστοίχως στα άρθρα 3-4 και 5-12 της Οδηγίας (ΕΕ) 2017/541 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Μαρτίου 2017 για την καταπολέμηση της τρομοκρατίας και την αντικατάσταση της απόφασης πλαισίου 2002/475/ΔΕΥ του Συμβουλίου και για την τροποποίηση της απόφασης 2005/671/ΔΕΥ του Συμβουλίου (ΕΕ L 88/31.03.2017) ή ηθική αυτουργία ή συνέργεια ή απόπειρα διάπραξης εγκλήματος, όπως ορίζονται στο άρθρο 14 αυτής, και τα εγκλήματα των άρθρων 187Α και 187Β του Ποινικού Κώδικα, καθώς και τα εγκλήματα των άρθρων 32-35 του ν. 4689/2020 (Α' 103),

ε) νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή χρηματοδότηση της τρομοκρατίας, όπως αυτές ορίζονται στο άρθρο 1 της Οδηγίας (ΕΕ) 2015/849 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ης Μαΐου 2015, σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας, την τροποποίηση του κανονισμού (ΕΕ) αριθμ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, και την κατάργηση της οδηγίας 2005/60/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και της οδηγίας 2006/70/ΕΚ της Επιτροπής (ΕΕ L 141/05.06.2015) και τα εγκλήματα των άρθρων 2 και 39 του ν. 4557/2018 (Α' 139),

στ) παιδική εργασία και άλλες μορφές εμπορίας ανθρώπων, όπως ορίζονται στο άρθρο 2 της Οδηγίας 2011/36/ ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 5ης Απριλίου 2011, για την πρόληψη και την καταπολέμηση της εμπορίας ανθρώπων και για την προστασία των θυμάτων της, καθώς και για την αντικατάσταση της απόφασης πλαίσιο 2002/629/ΔΕΥ του Συμβουλίου (ΕΕ L 101 της 15.4.2011, σ. 1) και τα εγκλήματα του άρθρου 323Α του Ποινικού κώδικα (εμπορία ανθρώπων).

τηρεί το σύνολο της ελληνικής Εργατικής κι Ασφαλιστικής Νομοθεσίας
αποδέχονται ανεπιφύλακτα τους όρους της παρούσας πρόσκλησης,
η προσφορά συντάχθηκε σύμφωνα με τους όρους της παρούσας πρόσκλησης, των οποίων ο προσφέρων έλαβε πλήρη και ανεπιφύλακτη γνώση,
τα προσφερόμενα είδη/υπηρεσίες καλύπτουν τις τεχνικές προδιαγραφές της παρούσας πρόσκλησης,
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, ακύρωση ή ματαίωση της πρόσκλησης,
συμμετέχει με μόνο μία προσφορά στο πλαίσιο της παρούσας πρόσκλησης,
τηρεί και θα εξακολουθεί να τηρεί κατά την εκτέλεση της σύμβασης, εφόσον επιλεγεί, τις υποχρεώσεις του που απορρέουν από τις διατάξεις της περιβαλλοντικής κοινωνικοασφαλιστικής και εργατικής νομοθεσίας, που έχουν θεσπιστεί με το δίκαιο της Ένωσης, το εθνικό δίκαιο, συλλογικές συμβάσεις ή διεθνείς διατάξεις περιβαλλοντικού, κοινωνικού κι εργατικού δικαίου, οι οποίες απαριθμούνται στο Παράρτημα Χ του Προσαρτήματος Α του ν. 4412/2016,
δεν θα ενεργήσει αθέμιτα, παράνομα ή καταχρηστικά καθ' όλη τη διάρκεια της διαδικασίας ανάθεσης αλλά και κατά το στάδιο εκτέλεσης της σύμβασης εφόσον επιλεγεί,

λαμβάνει τα κατάλληλα μέτρα για να διαφυλάξει την εμπιστευτικότητα των πληροφοριών που έχουν χαρακτηριστεί ως τέτοιες και
κατά τη διάρκεια εκτέλεσης της σύμβασης δεσμεύεται για την απαρέγκλιτη τήρηση των διατάξεων του με αρ. 2016/679 Κανονισμού (ΕΕ) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και του ν. 4624/2019 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

Ημερομηνία: …….20……
Ο – Η Δηλ.
(Υπογραφή)
(1) Αναγράφεται από τον ενδιαφερόμενο πολίτη ή Αρχή ή η Υπηρεσία του δημόσιου τομέα, που απευθύνεται η αίτηση.
(2) Αναγράφεται ολογράφως.
(3) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση του άρθρου 8 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.
(4) Σε περίπτωση ανεπάρκειας χώρου η δήλωση συνεχίζεται στην πίσω όψη της και υπογράφεται από τον δηλούντα ή την δηλούσα.