ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ
2η ΥΓΕΙΟΝ. ΠΕΡΙΦΕΡΕΙΑ ΠΕΙΡΑΙΩΣ & ΑΙΓΑΙΟΥ
ΚΡΑΤΙΚΟ ΘΕΡΠ/ΡΙΟ-Γ.Ν.-Κ.Υ. ΛΕΡΟΥ
Α.Φ.Μ.: 099591588/Δ.Ο.Υ. Κω
ΟΙΚΟΝΟΜΙΚΗ ΥΠΟΔΙΕΥΘΥΝΣΗ
ΓΡΑΦΕΙΟ ΠΡΟΜΗΘΕΙΩΝ
Πληροφορίες: Μπουράκη Σεβαστή
Τηλέφωνο: 2247022131
e-mail: promithies@leros-hospital.gr
promithies1@leros-hospital.gr
promithies2@leros-hospital.gr
promithies3@leros-hospital.gr

ΛΕΡΟΣ:19/09/2025

ΑΡ. ΠΡΩΤ.: 9623

ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΚΗΜΔΗΣ

Πρόσκληση Εκδήλωσης Ενδιαφέροντος Νο -73-

«ΑΝΑΔΕΙΞΗ ΠΑΡΟΧΟΥ ΓΙΑ ΤΟ ΣΧΕΔΙΟ ΑΝΑΛΥΣΗΣ ΚΙΝΔΥΝΟΥ ΚΑΙ ΕΝΙΑΙΑ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΠΡΟΣΑΡΜΟΓΗ ΣΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΔΗΓΙΑ 2022/2555 - ΥΠΗΡΕΣΙΕΣ ΥΑΣΠΕ, ΓΙΑ ΕΝΑ ΕΤΟΣ»

Το Κρατικό Θεραπευτήριο – Γ.Ν.-Κ.Υ. Λέρου για την κάλυψη άμεσων και επιτακτικών αναγκών του και έχοντας υπόψη:

1. Τις διατάξεις του Ν. 4412/16 (Δημόσιες Συμβάσεις , έργων , προμηθειών και υπηρεσιών) όπως τροποποιήθηκε με το άρθρο 43 του Ν. 4605/19, το άρθρο 33 του Ν. 4608/19 και το άρθρο 56 του Ν. 4609/19.
2. Τις τροποποιήσεις του Ν. 4782/2021 για τον εκσυγχρονισμό, απλοποίηση και αναμόρφωση του ρυθμιστικού πλαισίου των δημοσίων συμβάσεων.
3. Τον Ν.3329/2005 (ΦΕΚ 81/Α/4-4-2005) «Εθνικό σύστημα υγείας και Κοινωνικής Αλληλεγγύης και λοιπές διατάξεις».
4. Τον Ν.3580/2007 (ΦΕΚ 134/Α/18-6-2007)«Προμήθειες φορέων εποπτευόμενων από το Υπουργείο Υγείας και Κοινωνικής Αλληλεγγύης και άλλες διατάξεις».
5. Τον Ν.4412/2016 (ΦΕΚ 147/Α/8-8-2016) «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών (προσαρμογή στις Οδηγίες 2014/24/ΕΕ και 2014/25/ΕΕ)», όπως τροποποιήθηκε και ισχύει.
6. Την υπ΄αριθ. 1/30-1-2025 (Θέμα 7), απόφαση Δ.Σ. περί προγραμματισμό συμβάσεων 2025- Έγκριση σκοπιμότητας διαγωνισμών προμηθειών και υπηρεσιών του Κ.Θ.-Γ.Ν.- Κ.Υ. Λέρου (ΑΔΑ:ΨΦ8Ι46904Ρ-9Τ8).
7. Την Ευρωπαϊκή Οδηγία 2022/2555 (NIS2) περί μέτρων για κοινό υψηλό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ευρώπη.
8. Τον Ν. 4961/27-07-2022 (ΦΕΚ 146Α/2022) περί αναδυομένων τεχνολογιών πληροφορικής – επικοινωνίας και ενίσχυση της ψηφιακής διακυβέρνησης.
9. Το Ν. 5160/27-11-2024 (ΦΕΚ 195Α/2022) περί ενσωμάτωσης της οδηγίας ΕΕ2022/2555 του ευρωπαϊκού κοινοβουλίου, σχετικά με τα μέτρα για κοινό υψηλό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ευρώπη.
10. Το υπ’ αριθ. 7141/7-7-2025 αίτημα του τμήματος πληροφορικής.

11. Την υπ' αριθ. 18/11-09-2025 (θέμα 6) Απόφ. Δ/κού Σ/λίου με ΑΔΑ: ΨΞ6346904Ρ-ΤΑΚ, ΑΔΑΜ:25REQ017567967 με την οποία εγκρίθηκε η σκοπιμότητα για συμβάσεις προμηθειών και υπηρεσιών.
12. Την υπ' αριθ.500/17-09-2025 με ΑΔΑ:6τ7946904ρ-8κ3, ΑΔΑΜ:25REQ017577845 απόφαση ανάληψης υποχρέωσης και καταχώρησης στο βιβλίο εγκρίσεων και εντολών πληρωμής, σύμφωνα με την εγκύκλιο 02/18993/ΔΠΔΣΜ/28-02-2014 περί τήρησης μητρώου δεσμεύσεων,

προσκαλεί τους ενδιαφερόμενους να καταθέσουν προσφορά για την παρακάτω υπηρεσία:

Γενική Περιγραφή του Έργου

Αντικείμενο του έργου αυτού είναι η παροχή υπηρεσιών, καθώς και η προσαρμογή του Φορέα με τις απαιτήσεις του Ν.4961/2022, του Ν.5160/2024 καθώς και της Ευρωπαϊκής Οδηγίας 2022/2555 (NIS2). Το έργο θα αφορά την προσαρμογή στις διατάξεις του εν λόγω Κανονισμού και στην ενίσχυση της ανθεκτικότητας του Νοσοκομείου, απέναντι στους κινδύνους του Κυβερνοχώρου.

Βάσει της οδηγίας της ΕΕ 2022/2555 (NIS2) πρέπει να ληφθούν τα κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά την ασφάλεια συστημάτων δικτύου και πληροφοριακών συστημάτων που χρησιμοποιούν για τις δραστηριότητές τους ή για την παροχή των υπηρεσιών τους και για την πρόληψη ή ελαχιστοποίηση των επιπτώσεων των περιστατικών στους αποδέκτες των υπηρεσιών τους ή σε άλλες υπηρεσίες και οργανισμούς.

Συγκεκριμένα, το έργο θα περιλαμβάνει υπηρεσίες για τη διενέργεια μελέτης για την εναρμόνιση του Φορέα έναντι του ν.5160/2024 (και τις σχετικές ΚΥΑ που έχουν στο μεταξύ δημοσιευθεί), του προγενέστερου ν.4961/2022 και της ΟΔΗΓΙΑΣ 2022/2555 (NIS2).

Η μελέτη ωριμότητας θα αξιολογεί όλους τους τομείς δραστηριότητας του Φορέα ως προς την ετοιμότητα και όπου απαιτούνται ενέργειες συμμόρφωσης, θα εμβαθύνει στις ανωτέρω περιοχές, θα προτείνει συγκεκριμένα μέτρα, ώστε ο Φορέας να ξεκινήσει την υλοποίηση όλων των διορθωτικών ενεργειών συμμόρφωσης. Επίσης θα παρέχει συμβουλευτικές υπηρεσίες όποτε απαιτηθούν από το Φορέα από την έναρξη της σύμβασης.

Στο αντικείμενο του έργου συμπεριλαμβάνονται:

- Η κατάρτιση καταλόγου με τις υποδομές Πληροφορικής του Φορέα.
- Report Συνολικού Κινδύνου του Φορέα.
- Vulnerability Assessment στα συστήματα του Φορέα.
- Compliance Plan - Σχέδιο για την Υλοποίηση διορθωτικών ενεργειών.
- Δημιουργία Πολιτικών για την ασφάλεια των Συστημάτων Πληροφορικής.
- Προσαρμογή στα άρθρα 15 και 16 του Ν. 5160/2024.

Αντικείμενο εργασίας

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

- Ανάλυση της τρέχουσας κατάστασης των πληροφοριακών συστημάτων και δικτυακών υποδομών, των λογισμικών, και όλων των εφαρμογών καθώς και κάθε στοιχείο που επηρεάζει την επιχειρησιακή συνέχεια του Φορέα σε όλες τις δραστηριότητες, τα τμήματα, τα παραρτήματα και τις διευθύνσεις του οργανισμού.
- Δημιουργία Καταλόγου με όλες τις εκτιμώμενες απειλές που ενδέχεται να εκδηλωθούν στους καταγεγραμμένους πόρους Πληροφορικής
- Διενέργεια Vulnerability Assessment προκειμένου να εκτιμηθούν αναλυτικά οι κίνδυνοι και να καταγραφούν οι ενδεχόμενες ευπάθειες των συστημάτων πληροφορικής και επικοινωνιών του Φορέα, που είναι δυνατό να αποτελέσουν αντικείμενο εκμετάλλευσης από συγκεκριμένες πηγές απειλών.
- Σύνταξη προτάσεων για βελτίωση του επιπέδου ασφάλειας του Φορέα σε σχέση με την Κυβερνοασφάλεια και τα πληροφοριακά του συστήματα.
- Σύνταξη των απαραίτητων προτάσεων για Πολιτικές Ασφάλειας Πληροφοριών και Ασφάλειας συστημάτων Πληροφορικής.

Η ανωτέρω αξιολόγηση θα περιλαμβάνει τουλάχιστον τα εξής:

- Αξιολόγηση δυνατότητας ικανοποίησης των δικαιωμάτων των φυσικών προσώπων.
- Αξιολόγηση ικανοποιητικού επιπέδου ασφαλείας και επιχειρησιακής συνέχειας.
- Αξιολόγηση επαρκούς οργανωτικής δομής.
- Αξιολόγηση Πληροφοριακών Συστημάτων και πολιτικών που επιβάλλονται από την Πληροφορική.
- Αξιολόγηση σχετικών γραπτών πολιτικών και διαδικασιών.
- Αξιολόγηση των υποδομών Πληροφορικής και Επικοινωνιών του Φορέα.
- Αξιολόγηση των ευπαθειών και των κινδύνων που θα προκύψουν από τη Μελέτη.

Με σκοπό την επιτυχή υλοποίηση των σκοπών του έργου ο Ανάδοχος θα:

- Συμπεριλάβει ανάλυση της τρέχουσας κατάστασης των πληροφοριακών συστημάτων και δικτυακών υποδομών, των υφιστάμενων πολιτικών, διαδικασιών και πρακτικών, οι οποίες σχετίζονται με την ασφάλεια των πληροφοριών, την επιχειρησιακή συνέχεια και την προστασία των επιχειρησιακών δεδομένων του Φορέα.
- Με επιτόπια παρουσία καταγράφει τον εξοπλισμό και τις πολιτικές που ακολουθούνται (με την αρωγή του τμ. Μηχανογράφησης του Φορέα), διεξάγει συνεντεύξεις με αρμόδια στελέχη προκειμένου να:
    a. Δημιουργήσει λεπτομερές πλάνο ενεργειών αντιμετώπισης και διαχείρισης των ευρημάτων, έτσι ώστε οι επικεφαλής των αρμόδιων επιχειρησιακών μονάδων να είναι σε θέση να εφαρμόσουν τις απαραίτητές ενέργειες
    b. Πραγματοποιήσει αξιολόγηση όλων των πρακτικών που σχετίζονται με την επεξεργασία των προσωπικών δεδομένων και να παρέχει συγκεκριμένες και λεπτομερείς προτάσεις για δράσεις συμμόρφωσης
    c. Διενεργήσει Vulnerability Assessment προκειμένου να εκτιμηθούν οι ευπάθειες που ενδέχεται να έχουν τα συστήματα του Φορέα.

d. Προσδιορίσει τον κίνδυνο καθώς και τον τρόπο αντιμετώπισής των κινδύνων, με τεχνικά και οργανωτικά μέτρα για την αποτελεσματικότερη προστασία του Οργανισμού.

Φάσεις του έργου - Παραδοτέα

ΦΑΣΗ 1: Έναρξη έργου – Οργάνωση Δράσεων

Η Φάση αυτή περιλαμβάνει τις ακόλουθες δράσεις:

- Καταγραφή εργασιών και αλληλεξάρτηση αυτών.
- Καθορισμό των παραδοτέων και των χρονικών οροσήμων.
- Συστηματική παρακολούθηση της προόδου του έργου και των παραδοτέων.
- Τρόπος παρακολούθησης της κρίσιμης διαδρομής, επισήμανση τομέων ανησυχίας και πρόταση διορθωτικών ενεργειών σε περίπτωση αποκλίσεων από το σχέδιο και στις επί μέρους Ομάδες Εργασίας που θα συσταθούν στο πλαίσιο υλοποίησης του ανωτέρου έργου.
- Εκτίμηση απαιτούμενων ανθρωποημερών με αναφορά στην:
  - Αντιστοίχιση εργασιών με απαιτούμενους ανθρώπινους πόρους της εταιρείας και του Φορέα.
  - Εκτίμηση Επάρκειας Πόρων.
  - Οργάνωση συναντήσεων.
  - Προγραμματισμός Συναντήσεων.
  - Πρακτικά Συναντήσεων.

Παραδοτέα Φάσης 1: Πλάνο Υλοποίησης Έργου (Περιγραφή του Έργου, καθώς και του τρόπου με τον οποίο θα εκτελεστεί) – Εγχειρίδιο Παράδοσης του Έργου.

ΦΑΣΗ 2: Συλλογή Δεδομένων / Καταγραφή Πληροφοριακών assets

Η Φάση αυτή περιλαμβάνει τις ακόλουθες δράσεις:

Συγκέντρωση των απαιτούμενων πληροφοριών για την καταγραφή του εξοπλισμού.

Συγκεκριμένα η καταγραφή πρέπει να περιλαμβάνει:

- Κατάλογο με τις υποδομές πληροφορικής και επικοινωνιών, όπως ιδίως σταθμούς εργασίας, διακομιστές, δικτυακές συσκευές, εκτυπωτές κλπ.
- Κατάλογο με τα λογισμικά που χρησιμοποιούνται από το Φορέα, όπως ιδίως τα λειτουργικά συστήματα και οι εφαρμογές.
- Κατάλογο με τα πληροφοριακά αγαθά του Φορέα ανά κτιριακή υποδομή.
- Ταξινόμηση των δεδομένων και αγαθών που διαχειρίζεται ο Φορέας, σε διακριτά επίπεδα, με βάση τις απαιτήσεις εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητάς τους. Η αντιστοίχιση κάθε αγαθού και συνόλου δεδομένων με ένα επίπεδο ταξινόμησης, γίνεται ανάλογα με την ευαισθησία, κρισιμότητα και επιχειρηματική τους αξία.
- Κατάλογο με τις διαφορετικές εκτιμώμενες απειλές, που δύνανται να εκδηλωθούν στους πόρους του Φορέα, όπως αυτοί καταγράφηκαν προηγουμένως.
- Θα ορίσει τις κρίσιμες υποδομές του Φορέα που πρέπει να προστατευτούν βάσει του αρ. 15 του ν. 5160/2024.

Παραδοτέα Φάσης 2: Κατάλογος Πληροφοριακών Assets του Φορέα - Κατάλογος Εκτιμώμενων Απειλών - Ορισμός Κρίσιμων Υποδομών του Φορέα.

ΦΑΣΗ 3: Vulnerability Assessment

Η Φάση αυτή περιλαμβάνει τις εξής ενέργειες:

- Προσδιορισμός των περιουσιακών στοιχείων του Φορέα στα οποία πρόκειται να πραγματοποιηθεί διενέργεια ευπάθειας των συστημάτων.
- Προτεραιοποίηση των στοιχείων που αποτελούν βασικά επιχειρησιακά εργαλεία για τον Φορέα.
- Σάρωση ευπάθειας των στοιχείων σε δίκτυα, σταθμούς εργασίας κτλ, όσον αφορά κινδύνους από κακόβουλο λογισμικό, επιθέσεις, μη εγκεκριμένη πρόσβαση κτλ.
- Διενέργεια ελέγχων παρείσδυσης (penetrationtests) στα συστήματα δικτύου και πληροφοριών, με βάση το σχήμα ταξινόμησης των αγαθών και των δεδομένων.
- Ανάλυση αποτελεσμάτων.
- Προσδιορισμός συνολικού κινδύνου, ως συνδυασμού της πιθανότητας πραγματοποίησης των απειλών που έχουν αναγνωριστεί και της εκτίμησης της επίπτωσής τους στις υποδομές, αγαθά, τις λειτουργίες και το προσωπικό του Φορέα, καθώς και σε άλλους φορείς.

Penetration Testing

- Αναγνώριση ευπαθειών σε δίκτυα, εφαρμογές και συστήματα.
- Αξιολόγηση της αποτελεσματικότητας των υφιστάμενων μέτρων ασφαλείας.
- Παροχή συστάσεων για τη μείωση κινδύνων.

Το PenTest θα καλύψει το εσωτερικό και εξωτερικό δίκτυο του Φορέα, τους διακομιστές (web, email), τις φυσικές συσκευές καθώς και συστήματα τα οποία ενδεχομένως θα υποδείξει ο Φορέας.

Για να πραγματοποιηθεί το PenTest θα χρησιμοποιηθεί η χαρτογράφηση των συστημάτων, ενώ θα παρασχεθεί από το Φορέα η χαρτογράφηση του Δικτύου.

Παράλληλα το pentest θα γίνει ως εξής:

- Παθητική αναγνώριση (OSINT).
- Ενεργητική Σάρωση για εντοπισμό ανοιχτών θυρών και υπηρεσιών.
- Χρήση εργαλείων για εντοπισμό ευπαθειών.
- Επαλήθευση για τα falsepositives.
- Προσομοίωση επιθέσεων (SQL Injections).

Παραδοτέα Φάσης 3: Vulnerability Assessment - Penetration Test - Report Συνολικού Κινδύνου.

ΦΑΣΗ 4: Ανάπτυξη σχεδίου διορθωτικών ενεργειών

Η Φάση αυτή περιλαμβάνει τις ακόλουθες δράσεις:

Σύνταξη αναλυτικού και σαφούς σχεδίου στο οποίο θα:

- Συμπεριλαμβάνονται οι προτάσεις βελτίωσης, με βάση τα προηγούμενα Παραδοτέα, με σκοπό την αντιμετώπιση των ελλείψεων ή/και αποκλίσεων σε σχέση με τις απαιτήσεις του ευρύτερου κανονιστικού πλαισίου και των προτύπων, όπως αναλύεται παραπάνω.
- Προσδιορίζονται συγκεκριμένες, σαφείς και προτεραιοποιημένες ενέργειες και εργασίες, ώστε να βελτιωθεί -κατά τον δυνατόν συντομότερα - το επίπεδο εναρμόνισης και ανθεκτικότητας του Φορέα, από τις απειλές του Κυβερνοχώρου.
- Περιλαμβάνονται προτάσεις με σκοπό τη συμμόρφωση με τον Κανονισμό μέσω:
  - της τροποποίησης του περιβάλλοντος λειτουργίας των πληροφοριακών συστημάτων,
  - της διατήρησης στο μέλλον ικανοποιητικού επιπέδου συμμόρφωσης,
  - της συστηματικής βελτίωσης του επιπέδου ανθεκτικότητας του Φορέα,
  - οργανωτικών μέτρων,
  - τεχνικών μέτρων.

Παραδοτέα Φάσης 4: Compliance Plan για βελτίωση της ανθεκτικότητας του Φορέα σε επιθέσεις στον Κυβερνοχώρο.

ΦΑΣΗ 5: Δημιουργία Πολιτικής Κυβερνοασφάλειας

Στη Φάση αυτή πρόκειται να καταρτιστεί ενιαία πολιτική ασφάλειας συστημάτων πληροφορικής και επικοινωνιών η οποία θα περιλαμβάνει κατ' ελάχιστον:

Α) τους στόχους ασφάλειας του Φορέα και την προσέγγιση της διαχείρισής του,
Β) τον τρόπο διαχείρισης των απαιτήσεων που δημιουργούνται από:
Βα) την επιχειρησιακή στρατηγική του Φορέα,
Ββ) τις νομοθετικές, κανονιστικές και συμβατικές υποχρεώσεις,
Βγ) το διεθνές περιβάλλον Κυβερνοαπειλών,
Γ) την ανάθεση γενικών και ειδικών ρόλων και αντίστοιχων ευθυνών για τη διαχείριση της ασφάλειας των πληροφοριακών συστημάτων,
Δ) διαδικασίες για τον χειρισμό αποκλίσεων και εξαιρέσεων
Για την εκπόνηση της Ενιαίας Πολιτικής Ασφάλειας, θα ληφθούν υπόψη και τα οριζόμενα στην ΚΥΑ 1689/6-5-2025. Οι επιμέρους πολιτικές θα περιλαμβάνουν κατ' ελάχιστο:

- Πολιτική ασφάλειας δικτύων.
- Πολιτική Διαχείρισης ταυτότητας και ελέγχου πρόσβασης.
- Πολιτική διαχείρισης αγαθών.
- Πολιτική ορθής χρήσης αγαθών και δεδομένων.
- Πολιτική αφαιρούμενων μέσων αποθήκευσης.
- Πολιτική αντιγράφων ασφαλείας.
- Πολιτική κρυπτογράφησης δεδομένων και επικοινωνιών.
- Πολιτική φυσικής και περιβαλλοντικής ασφάλειας.
- Πολιτική διαχείρισης περιστατικών κυβερνοασφάλειας.
- Πολιτική Ανάκαμψης από Καταστροφή και Επιχειρησιακής Συνέχειας.
- Πολιτική ασφάλειας εφοδιαστικής αλυσίδας.
- Πολιτική διενέργειας ελέγχων κυβερνοασφάλειας και Αξιολόγησης Αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον τομέα της Κυβερνοασφάλειας.

Παραδοτέα Φάσης 5: Πολιτική Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών

Φάση 6: Εγκατάσταση Λογισμικού CyberSecurity

Το Λογισμικό θα διέπεται από τις παρακάτω γενικές αρχές:

• Την ανθεκτικότητα και τη βιωσιμότητα του Νοσοκομείου, διασφαλίζοντας τη δυνατότητα αποτροπής των συστημάτων και των υπηρεσιών από επιθέσεις ασφαλείας και την προσαρμογή τους, ενδεχομένως και τον μετασχηματισμό τους σε συνθήκες πίεσης ή κρίσης όπως αυτές της απομακρυσμένης εργασίας, διάσκεψης, εξυπηρέτησης και εκπαίδευσης.

• Την προστασία υποδομών και υπηρεσιών, προστατεύοντας τα συστήματα και τις ηλεκτρονικές υπηρεσίες του Νοσοκομείου από επιθέσεις και συμβάντα, που απειλούν την ακεραιότητα των δεδομένων, τη διαθεσιμότητα και την εμπιστευτικότητά τους, συμπεριλαμβανομένων των προσπαθειών υποκλοπής ευαίσθητων δεδομένων των πολιτών ή πληροφοριών του Οργανισμού.

Για τους σταθμούς εργασίας έχει προβλεφθεί προστασία η οποία ενσωματώνεται στα αντίστοιχα λειτουργικά συστήματα με τη μορφή λογισμικού και με αυτόν τον τρόπο παρέχεται υψηλό επίπεδο ασφάλειας και πρόληψης μολύνσεων από κακόβουλο λογισμικό μηδενικού χρόνου (0-day).

Το λογισμικό θα έχει τη δυνατότητα live response προς επιλεγμένους χρήστες, σε περίπτωση που συμβεί οποιαδήποτε κακόβουλη ενέργεια, καθώς και της δυνατότητας threat intelligence, προκειμένου να βελτιστοποιεί τη δυνατότητα του Φορέα να ανταπεξέρχεται σε επιθέσεις.

Το Λογισμικό θα πρέπει να καλύπτει επίσης να περιλαμβάνει:

Κεντρική Διαχείριση και Ενοποίηση

1. Ενιαία κονσόλα: Διαχείριση πολλών παραγόντων (endpoints, cloudworkloads) από μια ενιαία διεπαφή.
2. Αυτόματη ανακάλυψη: Αυτόματη ανακάλυψη και εγγραφή νέων συστημάτων στο περιβάλλον.
3. Ομαδοποίηση παραγόντων: Ομαδοποίηση συστημάτων για ευκολότερη διαχείριση και εφαρμογή πολιτικών.
4. Ειδοποιήσεις και Απόκριση: Όταν εντοπιστούν απειλές, να δημιουργεί ειδοποιήσεις και μπορεί να ενεργοποιήσει αυτοματοποιημένες ενέργειες απόκρισης.
5. Anomaly Detection: Η ανίχνευση ανωμαλιών είναι μια κρίσιμη τεχνική στην κυβερνοασφάλεια που περιλαμβάνει τον εντοπισμό μοτίβων που αποκλίνουν από το κανονικό. Με τον εντοπισμό αυτών των ανωμαλιών, οι οργανισμοί μπορούν να προληπτικά να εντοπίσουν πιθανές απειλές και να ανταποκριθούν αποτελεσματικά.

Μέθοδοι εντοπισμού ανώμαλης συμπεριφοράς:

- Καθιέρωση Βασικής Γραμμής: Να καθιερώνει μια βασική γραμμή της κανονικής συμπεριφοράς του συστήματος αναλύοντας ιστορικά δεδομένα.
- Ανίχνευση Απόκλισης: Οποιαδήποτε σημαντική απόκλιση από αυτή τη βασική γραμμή σημαδεύεται ως ανωμαλία, υποδεικνύοντας πιθανή κακόβουλη δραστηριότητα.

Μηχανική Μάθηση:

- Αναγνώριση Μοτίβων: Οι αλγόριθμοι μηχανικής μάθησης μπορούν να αναγνωρίσουν πολύπλοκα μοτίβα που ενδεχομένως να μην είναι εύκολα ανιχνεύσιμα μέσω παραδοσιακών μεθόδων.
- Προσαρμοστική Μάθηση: Αυτοί οι αλγόριθμοι μπορούν συνεχώς να μαθαίνουν και να

προσαρμόζονται στα εξελισσόμενα τοπία απειλών.

- Ανίχνευση Βασισμένη σε Κανόνες:
- Προσαρμόσιμοι Κανόνες: Μπορείτε να ορίσετε συγκεκριμένους κανόνες για να ανιχνεύσετε ανωμαλίες με βάση προκαθορισμένα κριτήρια.
- Ευέλικτη Ρύθμιση: Αυτοί οι κανόνες μπορούν να προσαρμοστούν στις συγκεκριμένες ανάγκες και το προφίλ απειλών του οργανισμού σας.

Ο Ανάδοχος θα εγκαταστήσει το Λογισμικό σε πόρους που δύναται να του διαθέσει ο Φορέας (Εικονικές Μηχανές VM), άλλως υποχρεούται να παραχωρήσει για το σκοπό αυτό, προς χρήση από τη Μονάδα, δικό του server, χωρίς πρόσθετο κόστος και μέχρι το πέρας της Σύμβασης.

Το λογισμικό αυτό θα παρέχει στο Νοσοκομείο:

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

Στο τέλος του έργου ακολουθεί η Παρουσίαση των Αποτελεσμάτων στην Ομάδα Παραλαβής, στον Υπεύθυνο Κυβερνοασφάλειας ΥΑΣΠΕ και στη Διοίκηση του Νοσοκομείου.

Παραδοτέα Φάσης 6: Εγκατάσταση λογισμικού για monitoring και προστασία από τις Κυβερνοεπιθέσεις .

ΦΑΣΗ 7: Υπηρεσίες Συμβούλου ΥΑΣΠΕ

Βάσει των άρθρων 15 -παρ. 5α)- του Ν.5160/24 και 18, 19 του Ν.4961/22, κάθε Δημόσιος Οργανισμός είναι υποχρεωμένος να ορίσει έναν Υπεύθυνο Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (από εδώ και στο εξής ΥΑΣΠΕ) προκειμένου να λάβει οργανωτικά μέτρα για την βελτίωση της ανθεκτικότητας του Οργανισμού σε Κυβερνοεπιθέσεις.

Η Ανάδοχος Εταιρεία, θα αναλάβει να υποστηρίξει με συμβουλευτικές υπηρεσίες τον ΥΑΣΠΕ, του οποίου οι αρμοδιότητες είναι οι εξής:

α) η διαρκής μέριμνα για την ασφάλεια των Συστημάτων Δικτύου και Πληροφοριών του Φορέα κατά την έννοια της περ. 2 του άρθρου 3 του ν. 4577/2018 (Α’ 199),
β) η συνεργασία με τους αρμόδιους φορείς στον τομέα της Κυβερνοασφάλειας και η μέριμνα για την εφαρμογή των κατευθυντήριων οδηγιών, απαιτήσεων και μέτρων
ασφαλείας που εκδίδουν,
γ) η τήρηση Μητρώου του Φορέα με τις υποδομές Πληροφορικής και Επικοινωνιών, το λογισμικό και τα πληροφοριακά αγαθά,
δ) η συμμετοχή στη διενέργεια ελέγχων σε Συστήματα Πληροφορικής και Επικοινωνιών του Φορέα για τη διακρίβωση του υφιστάμενου επιπέδου ασφάλειας,
ε) η εποπτεία της τήρησης της Πολιτικής Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών του φορέα,

στ) η παρακολούθηση και αξιοποίηση νέων τεχνολογιών και εργαλείων ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών για την ενίσχυση του επιπέδου Κυβερνοασφάλειας του φορέα και

ζ) η διενέργεια αξιολογήσεων του επιπέδου Κυβερνοασφάλειας του Φορέα σε συνεργασία με τις κατά περίπτωση αρμόδιες Αρχές.

Ενδεικτικά, αλλά όχι περιοριστικά, ο Ανάδοχος θα συνδράμει τον ΥΑΣΠΕ με:

- βοήθεια στον καθορισμό πλάνου ενεργειών από τον ΥΑΣΠΕ, σε τακτική βάση, ώστε να ελέγχεται και να επικαιροποιείται το αντικείμενο της Σύμβασης (Παραδοτέα Φασεων 1-5)
- μεταφορά τεχνογνωσίας, διαρκή ενημέρωση για κινδύνους, πρακτικές, μέτρα αντιμετώπισης
- συνδρομή σε περιπτώσεις Κυβερνοεπίθεσης, ή άλλων θεμάτων ασφαλείας, για:
  - υποστήριξη στην επικοινωνία με τους αρμόδιους Φορείς Ασφαλείας
  - συνδρομή των αρμόδιων Αρχών στη Διερεύνηση Περιστατικού
  - καταγραφή των χαρακτηριστικών της επίθεσης
  - εκτίμηση της έκτασής της στους πόρους της Υπηρεσίας
  - άμεσες ενέργειες αντιμετώπισης
  - Εγκατάσταση Λογισμικού Προστασίας από Κυβερνοεπιθέσεις

Προκειμένου να υλοποιηθεί, μέσω μιας ολιστικής προσέγγισης, το αρ.15 του Ν.5160/24 και τα οριζόμενα στην ΚΥΑ 1689/06-05-2025, ο Ανάδοχος πρόκειται να εγκαταστήσει Λογισμικό, το οποίο θα διατηρεί και θα επικαιροποιεί, προκειμένου να προστατεύει αποτελεσματικά το Νοσοκομείο, από τις απειλές του Κυβερνοχώρου. Ο Ανάδοχος θα παρέχει κατά τη διάρκεια της Σύμβασης στο Νοσοκομείο επικαιροποιήσεις του Λογισμικού που θα εγκαταστήσει και θα παρακολουθεί τη λειτουργία του, ενημερώνοντας τον ΥΑΣΠΕ για τα ευρήματα, καθορίζοντας ανάλογα το πλάνο ενεργειών του Φορέα.

Το χρονοδιάγραμμα όλου του έργου είναι :
-Για τις Φάσεις 1-6 ένας μήνας από την υπογραφή της σύμβασης.
-Για την Φάση 7 ένα έτος από την υπογραφή της σύμβασης.

Παραθέτουμε πίνακα με ενδεικτικό κόστος:

Α/Α	**ΠΕΡΙΓΡΑΦΗ**	**ΦΑΣΗ**	**ΕΝΔΕΙΚΤΙΚΟ ΚΟΣΤΟΣ ΑΝΕΥ ΦΠΑ 24%**
1	Πλάνο Υλοποίησης Έργου – Οργάνωση Δράσεων	Φάση 1	10.000,00 €
2	Συλλογή Δεδομένων Κατάλογος Πληροφοριακών Assets	Φάση 2	
3	Vulnerability Assessment – Penetration Test - Report Κινδύνου	Φάση 3	
4	Compliance Plan	Φάση4	
5	Πολιτική Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών	Φάση 5	
6	Εγκατάσταση λογισμικού προστασίας από κυβερνοεπιθέσεις	Φάση 6	
7	Υπηρεσίες Συμβούλου ΥΑΣΠΕ	Φάση 7	12.000,00 €
	Σύνολο	**Φάσεις 1-7**	**22.000,00 €**

Προϋποθέσεις επαγγελματικής και τεχνικής ικανότητας και εμπειρογνωσίας

Ο υποψήφιος Ανάδοχος θα πρέπει:

1. Να είναι πιστοποιημένος με ISO 27001, ISO 9001, ISO 20000-1, ISO 37001, ISO 22301, ISO27701
2. Να έχει υλοποιήσει τουλάχιστον δύο (2) Έργα Συμμόρφωσης(ενεργή Σύμβαση η Βεβαίωση Καλής Εκτέλεσης) με το GDPR σε Δημόσιο Φορέα.
3. Να έχει υλοποιήσει τουλάχιστον πέντε (5) Έργα Συμμόρφωσης με τον Ν.4961/2022 σε Δημόσια Νοσοκομεία και να έχει βεβαίωση καλής εκτέλεσης.
4. Να διαθέτει κατάλληλη Ομάδα Έργου, που να καλύπτει τις προϋποθέσεις για την υλοποίηση του έργου.

Συγκεκριμένα θα πρέπει να διαθέτει ομάδα με τουλάχιστον έξι (6) μέλη για την ολοκλήρωση του Έργου. Η ομάδα θα πρέπει να διαθέτει τουλάχιστον μέλη με τους εξής ρόλους και προσόντα:

Υπεύθυνος Έργου / ProjectManager: ο οποίος θα έχει τη συνολική ευθύνη των εργασιών του Αναδόχου, τη διοίκηση, την πρόοδο και τον συντονισμό όλων των στελεχών της ομάδας έργου, θα είναι υπεύθυνος για τη διασφάλιση της ποιότητας του έργου, καθώς και την τήρηση όλων των προδιαγραφών πληρότητας που θέτει η Αναθέτουσα Αρχή. Επίσης, θα αναλάβει τη λειτουργική εκπροσώπηση του Αναδόχου για το συγκεκριμένο έργο, έναντι της αρμόδιας για την παρακολούθηση της Σύμβασης υπηρεσίας της Αναθέτουσας Αρχής, καθώς και της Επιτροπής Παραλαβής του Έργου. Ο Υπεύθυνος Έργου θα πρέπει να διαθέτει τουλάχιστον τα προσόντα και την εμπειρία, που αναφέρονται παρακάτω και αυτά να αποδεικνύονται επαρκώς:

- Πανεπιστημιακό δίπλωμα ή πτυχίο σπουδών (ΑΕΙ) της ημεδαπής ή αντίστοιχου ιδρύματος της αλλοδαπής.
- Εικοσαετή (20 έτη) επαγγελματική εμπειρία στην υλοποίηση ή/και διοίκηση έργων πληροφορικής.

Υπεύθυνος Νομικός Σύμβουλος: Θα πρέπει να διαθέτει τουλάχιστον τα προσόντα και την εμπειρία που αναφέρονται παρακάτω και να αποδεικνύεται επαρκώς:

- Μεταπτυχιακό Τίτλο σπουδών από την ημεδαπή ή αντίστοιχου ιδρύματος της αλλοδαπής σε αντικείμενο σχετικό με το Δίκαιο της Πληροφορικής.
- Πανεπιστημιακό Δίπλωμα (ΑΕΙ) από την ημεδαπή ή αντίστοιχο πανεπιστήμιο της αλλοδαπής .
- Πιστοποίηση ISO/IEC 17024 για Υπεύθυνους Προστασίας Δεδομένων (DPO Executives).
- ΠιστοποίησηCertified Information Privacy Manager (CIPM).

Υπεύθυνος Ασφάλειας Πληροφοριακών Συστημάτων. Για την επιτυχή ολοκλήρωση του Έργου είναι απαραίτητο να υπάρχει άτομο το οποίο να έχει εμπειρία από ασφάλεια των πληροφοριακών συστημάτων και ειδικότερα των δεδομένων που κυκλοφορούν στα συστήματα αυτά. Το άτομο που θα αναλάβει το ρόλο αυτό θα πρέπει να διαθέτει τουλάχιστον τα εξής προσόντα:

- Πανεπιστημιακό Δίπλωμα (ΑΕΙ) από την ημεδαπή ή αντίστοιχο πανεπιστήμιο της αλλοδαπής.

- Μεταπτυχιακό Δίπλωμα (ΑΕΙ) από την ημεδαπή ή αντίστοιχο πανεπιστήμιο της αλλοδαπής.
- Διδακτορικό Δίπλωμα από την ημεδαπή ή αντίστοιχο πανεπιστήμιο της αλλοδαπής, σε αντικείμενο σχετικό με την προστασία δεδομένων σε ψηφιακά περιβάλλοντα.
- Συμμετοχή σε δραστηριότητες προτυποποίησης με δημοσιευμένο επιστημονικό έργο.

Υπεύθυνος Κυβερνοασφάλειας: Είναι απαραίτητο να υπάρχει τουλάχιστον ένα (1) άτομο στην ομάδα έργου τα οποία να έχουν αναπτυγμένες γνώσεις αναφορικά με το περιβάλλον της Κυβερνοασφάλειας. Συγκεκριμένα και οι δύο θα πρέπει:

- Πανεπιστημιακό Δίπλωμα (ΑΕΙ) από την ημεδαπή ή αντίστοιχο πανεπιστήμιο της αλλοδαπής.
- Μεταπτυχιακό Τίτλο σπουδών από την ημεδαπή ή αντίστοιχου ιδρύματος της αλλοδαπής .
- Πενταετή (5 έτη) εμπειρία στο κομμάτι του RiskGovernance.

Β΄ ΠΛΗΡΟΦΟΡΙΕΣ ΓΙΑ ΤΙΣ ΥΠΗΡΕΣΙΕΣ

ΚΑΕ	0433.01
Προϋπολογισθείσα δαπάνη (προ ΦΠΑ 24%)	22.000,00 €
Προϋπολογισθείσα δαπάνη (συμπερ/νου του ΦΠΑ 24%)	27.280,00 €
CPV: Πακέτα λογισμικού ασφάλειας δεδομένων	48732000-8
Κριτήριο κατακύρωσης	Πλέον οικονομική προσφορά βάσει τιμής (Χαμηλότερη τιμή) στο σύνολο.
Ημερομηνία έναρξης υποβολής προσφορών	Από την ανάρτηση της παρούσας στο ΔΙΑΥΓΕΙΑ
Ημερομηνία και ώρα λήξης υποβολής προσφορών	**Πέμπτη 2 Οκτωβρίου 2025, έως ώρα 13:00**
Ημερομηνία και ώρα διαγωνισμού	**Παρασκευή 3 Οκτωβρίου 2025, ώρα 12:00**

Τρόπος υποβολής προσφορών	**Με e-mail, σε ένα από τα κάτωθι**: promithies@leros-hospital.gr **ή** promithies1@leros-hospital.gr **ή** promithies2@leros-hospital.gr **ή** promithies3@leros-hospital.gr **ή σε έντυπη μορφή, στα γραφεία της υπηρεσίας μας (Πρωτόκολλο)** (λαμβάνεται υπ' όψιν η ημερομηνία και ώρα παραλαβής από το πρωτόκολλο, όχι της σφραγίδας του ταχυδρομείου).

Γ΄ Στοιχεία Αναθέτουσας Αρχής

Επωνυμία	ΚΡΑΤΙΚΟ ΘΕΡ/ΡΙΟ – Γ.Ν.- Κ.Υ. ΛΕΡΟΥ
Αριθμός Φορολογικού Μητρώου (Α.Φ.Μ.)	099591588
Κωδικός Αναθέτουσας Αρχής για την ηλεκτρονική τιμολόγηση*	1015.Ε00199.0001
Ταχυδρομική διεύθυνση	Λακκί
Πόλη	Λέρος
Ταχυδρομικός Κωδικός	85400
Χώρα	Ελλάδα
Τηλέφωνο	2247022131
Ηλεκτρονικό Ταχυδρομείο (e-mail)	Promithies1@leros-hospital.gr
Αρμόδιος για πληροφορίες	Παγιοπούλου Θεοδότα, Βηλάκη Δήμητρα, Μπουράκη Σεβαστή
Γενική Διεύθυνση στο διαδίκτυο (URL)	www.leros-hospital.gr
Διεύθυνση του προφίλ αγοραστή στο διαδίκτυο (URL)	www.leros-hospital.gr

Κωδικός Αναθέτουσας Αρχής για την ηλεκτρονική τιμολόγηση: 1015.Ε00199.0001

*__ΟΙ ΟΙΚΟΝΟΜΙΚΟΙ ΦΟΡΕΙΣ ΥΠΟΧΡΕΟΥΝΤΑΙ ΣΤΗΝ ΕΚΔΟΣΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΤΙΜΟΛΟΓΙΩΝ ΣΥΜΦΩΝΑ ΜΕ ΤΗΝ Υπ' Αριθ. 52445 ΕΞ 2023 /04-04-2023__ Κοινή Υπουργική Απόφαση των Υπουργών Οικονομικών, Ανάπτυξης και Επενδύσεων, Ψηφιακής Διακυβέρνησης, Υποδομών και Μεταφορών, με τίτλο : ***"Υποχρέωση υποβολής ηλεκτρονικών τιμολογίων από τους οικονομικούς Φορείς"*.**

Η ΥΠΟΧΡΕΩΣΗ ΙΣΧΥΕΙ ΜΟΝΟ ΓΙΑ ΤΙΜΟΛΟΓΙΑ Η ΣΥΜΒΑΣΕΙΣ ΑΝΩ ΤΩΝ 2.500,00€

Δ΄ ΥΠΟΧΡΕΩΤΙΚΑ ΣΤΟΙΧΕΙΑ ΠΡΟΣΦΟΡΑΣ

Η προσφορά που θα υποβληθεί θα πρέπει να αναφέρει τα πλήρη στοιχεία της εταιρείας: ΑΦΜ, Δ.Ο.Υ, πλήρη επωνυμία, διεύθυνση, τηλέφωνο, e-mail, τον συντελεστή ΦΠΑ (να τονίζεται σε περίπτωση που αυτός είναι διαφορετικός του ισχύοντος , 17%), τον χρόνο ισχύος της προσφοράς και να έχει την παρακάτω μορφή:

Α/Α	Περιγραφή εργασιών	Κόστος χωρίς ΦΠΑ	Κόστος με ΦΠΑ

Σε περίπτωση που η τιμή προσφοράς του είδους υπερβαίνει την προϋπολογισθείσα δαπάνη αυτή υποχρεωτικά απορρίπτεται.

Ο ανάδοχος κατά την πληρωμή υπόκεινται στις παρακάτω κρατήσεις επί του Τιμολογίου:

α. Υπέρ ΕΑΔΗΣΥ 0,1% επί της καθαρής αξίας.

β. Υπέρ Ψυχικής Υγείας 2% επί της καθαρής αξίας αφαιρουμένων των προηγούμενων κρατήσεων.

γ. Φόρος 8% επί της καθαρής αξίας αφαιρουμένων των προηγούμενων κρατήσεων (για υπηρεσίες).

-Ο ΦΠΑ βαρύνει το Θεραπευτήριο.

Εναλλακτικές προσφορές και αντιπροσφορές δεν γίνονται δεκτές. Σε περίπτωση δύο ή περισσοτέρων εναλλακτικών προσφορών, ως κύρια θεωρείται αυτή με την χαμηλότερη τιμή, οι υπόλοιπες δεν θα αξιολογούνται.

Δικαιολογητικά που συνοδεύουν την οικονομική-τεχνική προσφορά καθαρής αξίας άνω των 2.500,00:

Στις περιπτώσεις που η εκτιμώμενη καθαρή αξία της προσφοράς είναι μεγαλύτερη των 2.500,00€, οι οικονομικοί φορείς υποχρεούνται να προσκομίσουν τα ακόλουθα δικαιολογητικά:

- Ποινικό μητρώο (τελευταίου τριμήνου).
- Πιστοποιητικό φορολογικής ενημερότητας, σε ισχύ.
- Πιστοποιητικό ασφαλιστικής ενημερότητας , σε ισχύ.
- Βεβαίωση πρωτοδικείου περί δικαστικής φερεγγυότητας (τελευταίου τριμήνου).
- Εγγραφή στο οικείο Επιμελητήριο.
- Πιστοποιητικό εκπροσώπησης ΓΕΜΗ (για νομικά πρόσωπα).

ΔΙΑΡΚΕΙΑ ΣΥΜΒΑΣΗΣ

Η σύμβαση που θα προκύψει θα έχει ισχύ ένα (1) έτος από την ημερομηνία ανάρτησής της στο ΚΗΜΔΗΣ.

Κανόνες Δημοσιότητας

- Η Πρόσκληση Εκδήλωσης Ενδιαφέροντος καταχωρήθηκε στο Κεντρικό Ηλεκτρονικό Μητρώο Δημοσίων Συμβάσεων (ΚΗΜΔΗΣ).
- Η Πρόσκληση Εκδήλωσης Ενδιαφέροντος αναρτήθηκε στο διαδίκτυο, στον ιστότοπο http//diavgeia.gov.gr/(ΠΡΟΓΡΑΜΜΑ ΔΙΑΥΓΕΙΑ).

Η ΣΥΝΤΑΚΤΡΙΑ Η ΤΜΗΜ/ΡΧΗΣ ΟΙΚ/ΚΟΥ ΥΠΟΔ/ΝΤΡΙΑ ΟΙΚ/ΚΟΥ Ο Δ/ΚΟΣ Δ/ΝΤΗΣ Ο ΔΙΟΙΚΗΤΗΣ

STAMATIOS KARDASIS
21/09/2025 13:39