ΓΝΘ "ΑΓΙΟΣ ΠΑΥΛΟΣ"
Αριθμ. Πρωτ.: 4977
Ημ/νία: 14/04/2026

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
4η Υ.ΠΕ. ΜΑΚΕΔΟΝΙΑΣ ΚΑΙ ΘΡΑΚΗΣ
ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΘΕΣ/ΝΙΚΗΣ
«ΑΓΙΟΣ ΠΑΥΛΟΣ»
(Εθν. Αντίστασης 161 ΤΚ 55134 ΘΕΣ/ΝΙΚΗ)

Διεύθυνση: ΔΙΟΙΚΗΤΙΚΟΥ Τμήμα : Οικονομικού Γραφείο: Προμηθειών Πληροφορίες: Γούλη Ευαγγελία Τηλέφωνο : 2313 304 461/464 Email: promagpavlos@outlook.com		

ΠΡΟΣΚΛΗΣΗ ΣΥΛΛΟΓΗΣ ΠΡΟΣΦΟΡΩΝ ΜΕ ΑΡΙΘ. 2026-25/ΣΠ
«ΣΥΣΤΗΜΑΤΟΣ ΠΡΟΣΤΑΣΙΑΣ ΙΩΝ ΚΑΙ ΑΠΕΙΛΩΝ - ANTIVIRUS» CPV:48761000-0

Πρόσκληση εκδήλωσης ενδιαφέροντος, αναφορικά με την προμήθεια 300 αδειών του «ΣΥΣΤΗΜΑΤΟΣ ΠΡΟΣΤΑΣΙΑΣ ΙΩΝ ΚΑΙ ΑΠΕΙΛΩΝ - ANTIVIRUS» CPV:48761000-0, προϋπολογισθείσας δαπάνης 15.000,00€ άνευ ΦΠΑ και 18.600,00€ συμπεριλαμβανομένου ΦΠΑ 24%, χρονικής διάρκειας 3 ετών, με κριτήριο κατακύρωσης την πλέον συμφέρουσα από οικονομική άποψη προσφορά βάσει τιμής, σε εφαρμογή του Προγραμματισμού Συμβάσεων διαχειριστικού έτους 2026, σύμφωνα με τα οριζόμενα στο άρθρο 118 του ν. 4412/2016.

Το Γ.Ν.Θ. «ΑΓΙΟΣ ΠΑΥΛΟΣ», έχοντας υπόψη:

Α. Τις διατάξεις όπως αυτές ισχύουν:

1. Ο ν. 4412 (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.

2. Ο ν. 4782/2021 (ΦΕΚ 36/Α) «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 π.δ. 80/2016 (Α΄145) «Ανάληψη υποχρεώσεων από τους Διατάκτες».

Β. Τις αποφάσεις –έγγραφα:

1. Την με αριθ. Β2/1ης ΣΥΝ/11-03-2026 (ΑΔΑ: 9ΑΞ446906Ι-4Ι2) Απόφαση ΔΣ του ΓΝΘ Άγιος Παύλος έγκρισης της Πρώτης τροποποίησης του αρχείου του Ετήσιου Προγράμματος Συμβάσεων στο Μητρώο Κεντρικών Προμηθειών της Ε.Κ.Α.Π.Υ. του διαχειριστικού έτους 2026, οποία εγκρίθηκε με την με αριθμ. 128/ ΣΥΝ 409/17-03-2026 απόφαση του ΔΣ της ΕΚΑΠΥ.

2. Την με αριθ. πρωτ. 1200/23-01-2026 (ΑΔΑ: 6ΖΝΤ46906Ι-4ΜΧ) Πράξη Διοικήτριας περί ορισμού επιτροπής σύνταξης τεχνοοικονομικής μελέτης του διαγωνισμού.

3. Το με αριθ. πρωτ. 3287/09-03-2026 πρακτικό τεχνικών προδιαγραφών της αρμόδιας επιτροπής.

4. Την με αριθμ. Β8/6ης ΣΥΝ/16-03-2026 (ΑΔΑ: ΡΕΑΩ46906Ι-ΘΦΝ) Απόφαση ΔΣ του ΓΝΘ Άγιος Παύλος έγκρισης της διενέργειας διαγωνισμού για την προμήθεια 300 αδειών του «ΣΥΣΤΗΜΑΤΟΣ ΠΡΟΣΤΑΣΙΑΣ ΙΩΝ ΚΑΙ ΑΠΕΙΛΩΝ - ANTIVIRUS» CPV:48761000-0

5. Την απόφαση δέσμευσης δαπάνης με αριθ. πρωτ. 4268/27-03-2026 (ΑΔΑ: ΨΙΨ46906Ι-ΛΙΩ) με α/α 392 η οποία θα βαρύνει τον ΑΛΕ: 31203010000001.

Το Γ.Ν.Θ. «ΑΓΙΟΣ ΠΑΥΛΟΣ» προβαίνει σε αναζήτηση προσφορών σύμφωνα με τις διατάξεις του άρθρου 118 του ν. 4412/2016, αναφορικά με την προμήθεια 300 αδειών του «ΣΥΣΤΗΜΑΤΟΣ ΠΡΟΣΤΑΣΙΑΣ ΙΩΝ ΚΑΙ ΑΠΕΙΛΩΝ - ANTIVIRUS» CPV:48761000-0, προϋπολογισθείσας δαπάνης 15.000,00€ άνευ ΦΠΑ και 18.600,00€ συμπεριλαμβανομένου ΦΠΑ 24%, χρονικής διάρκειας 3 ετών, με κριτήριο κατακύρωσης την πλέον συμφέρουσα από οικονομική άποψη προσφορά βάσει τιμής, σε εφαρμογή του Προγραμματισμού Συμβάσεων διαχειριστικού έτους 2026.

Αντικείμενο του διαγωνισμού-συνοπτικά στοιχεία

Αναθέτουσα Αρχή	Γενικό Νοσοκομείο Θεσσαλονίκης Άγιος Παύλος
Είδος διαγωνισμού	Συλλογή προσφορών σύμφωνα με τα οριζόμενα στο άρθρο 118 του ν. 4412/2016.
Αριθμός διαγωνισμού	2026-25/ΣΠ
Αντικείμενο διαγωνισμού	Προμήθεια 300 αδειών του «ΣΥΣΤΗΜΑΤΟΣ ΠΡΟΣΤΑΣΙΑΣ ΙΩΝ ΚΑΙ ΑΠΕΙΛΩΝ - ANTIVIRUS»
Κωδικός CPV	48761000-0
Προϋπολογισθείσα δαπάνη άνευ ΦΠΑ	15.000,00€
Προϋπολογιζόμενη δαπάνη με ΦΠΑ 24%	18.600,00€
Κωδικός Αριθμός Εξόδου (ΑΛΕ)	31203010000001
Κριτήριο κατακύρωσης:	Η πλέον συμφέρουσα από οικονομική άποψη προσφορά, αποκλειστικά βάσει τιμής.
Έναρξη υποβολής προσφορών	Τετάρτη 15-04-2026
Καταληκτική ημερομηνία υποβολής προσφορών	Τετάρτη 29-04-2026, ώρα 14:30 μ.μ
Τόπος – τρόπος υποβολής προσφορών	Γ.Ν.Θ. «ΑΓΙΟΣ ΠΑΥΛΟΣ», έντυπα στη διεύθυνση του Γ.Ν.Θ. «ΑΓΙΟΣ ΠΑΥΛΟΣ» (Εθνικής Αντίστασης 161, Τ.Κ. 55134, Θεσσαλονίκη) στο Γραφείο της Γραμματείας (πρωτόκολλο).
Χρόνος διενέργειας	Πέμπτη 30-04-2026, ώρα 11:00
Τόπος διενέργειας	Γ.Ν.Θ. «ΑΓΙΟΣ ΠΑΥΛΟΣ» Εθνικής Αντίστασης 161, ΤΚ 55134 Θεσσαλονίκη.

Διάρκεια σύμβασης	Τρία (3) έτη.
Κρατήσεις επί της τιμής των ειδών	Οι τιμές υπόκεινται στις υπέρ του Δημοσίου και τρίτων νόμιμες κρατήσεις.
Χρόνος Ισχύος Προσφοράς	Τριακόσιες εξήντα πέντε (365) ημερολογιακές ημέρες από την επόμενη της διενέργειας του διαγωνισμού.
Διεύθυνση Ιστοσελίδας Ανάρτησης Τεύχους Πρόσκλησης	www.agpavlos.gr

<u>ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ</u>

Α/Α	***ΠΕΡΙΓΡΑΦΗ***	
	Γενικές Πληροφορίες	
1.	***Αριθμός αδειών: 300***	
	Λειτουργίες Προστασίας / Εντοπισμού	*Δυνατότητες του προϊόντος για προστασία ενάντια και / ή εντοπισμό σύγχρονων επιθέσεων*
2.	*Προστασία / Πρόληψη από γνωστά Malware*	*Αναγνώριση και προσθήκη σε καραντίνα για γνωστούς τύπους malware και των παραλλαγών τους είτε αυτόματα είτε μετά από απαίτηση.*
3.	*Προστασία / Εντοπισμός από άγνωστα Malware*	*Αναγνώριση και προσθήκη σε καραντίνα για άγνωστους τύπους malware και παραλλαγών τους είτε αυτόματα είτε μετά από απαίτηση.*
4.	*Εντοπισμός / Πρόληψη Κακόβουλων Διεργασιών*	*Αναγνώριση προτύπων και τερματισμός αυτών των διεργασιών οι οποίες έχουν κακόβουλη συμπεριφορά (π.χ. με ανάλυση συμπεριφοράς των binaries).*
5.	*Προστασία / εντοπισμός από Exploit*	*Προστασία ενάντια σε Flash exploits, ευπάθειες browser exploits και άλλων τεχνικών που χρησιμοποιούνται σε επιθέσεις.*
6.	*Προληπτική δράση*	⇨ *Θα πρέπει να δρα προληπτικά κατά των απειλών και να αποκλείει τις επιθέσεις, ανεξάρτητα από το μέσο εξάπλωσής τους, USB stick, δίκτυο, κλπ.* ⇨ *Να προσφέρει σάρωση σε pre-execution στάδιο με machine learning μηχανισμούς για την ανίχνευση εξελιγμένων επιθέσεων.* ⇨ *Να υποστηρίζει τη δυνατότητα ανίχνευσης exploits καθώς και αποκλεισμού τους.* ⇨ *Να υποστηρίζει sandboxing τεχνολογία μέσα από την ίδια κονσόλα διαχείρισης χωρίς να απαιτείται καμία επιπλέον εγκατάσταση client.*
7.	*Τύποι απειλών*	*Να παρέχει δυνατότητα ανίχνευσης και καθαρισμού όλων των τύπων απειλών (viruses, Trojans, dialers, spyware, jokes, hoaxes , ransomware κλπ.).*
8.	*Τεχνολογίες ανίχνευσης απειλών*	*Να υποστηρίζει τεχνολογίες ανίχνευσης απειλών όπως signature-based, machine learning, heuristic-based και anti-stealth (rootkit detection), καθώς και file-less επιθέσεων και για την ανίχνευση αγνώστων απειλών.*

9.	*Πολιτικές Προστασίας*	*Δυνατότητα εφαρμογής διαφορετικών πολιτικών προστασίας για διαφορετικές ομάδες endpoints. Για παράδειγμα:* ⇨ *Laptops* ⇨ *Desktops* ⇨ *Servers*
10.	*Προστασία από Ransomware*	⇨ *Παροχή προστασίας των περιεχομένων των φακέλων ενάντια σε ransomware και την διεργασία κρυπτογράφησης αυτών. Η λύση αποτρέπει την κρυπτογράφηση ή οποιαδήποτε άλλη μορφή αλλοίωσης από μη επιτρεπόμενες εφαρμογές.* ⇨ *Να υπάρχει η δυνατότητα επαναφοράς των αρχείων που δέχτηκαν ransomware επίθεση ώστε τα αρχεία να παραμένουν διαρκώς ασφαλή.*
11.	*Mobile Workforce*	*Το προϊόν πρέπει να είναι δυνατό να παρέχει ασφάλεια σε χρήστες που συνδέονται:* ⇨ *εντός των ορίων του δικτύου του οργανισμού ή* ⇨ *μέσω ενός δημοσίου δικτύου*
12.	*Αποκλεισμός Botnet*	*Αποκλεισμός DNS resolution queries βασισμένο στην κατάσταση ασφαλείας του domain.*
13.	*Collaboration Security*	⇨ *Έλεγχος κατά την πρόσβαση όταν γίνεται ανέβασμα ή κατέβασμα αρχείων ή κατά την εκτέλεση νέων αρχείων.* ⇨ *Τα αρχεία που βρίσκονται στον collaboration server ελέγχονται συχνά στο παρασκήνιο χρησιμοποιώντας τις πιο πρόσφατες ταυτότητες κακόβουλου λογισμικού.*
14.	*Προστασία από αλλοίωση*	*Εξασφάλιση ότι η προστασία των endpoint δεν θα μπορεί να απενεργοποιηθεί, τροποποιηθεί ή απεγκατασταθεί από μη εξουσιοδοτημένο χρήστη.*
15.	*Anti-Tampering*	*Να διαθέτει λειτουργία Anti-Tampering που εντοπίζει τόσο ευάλωτους drivers σε endpoints και όσο και προηγμένες προσπάθειες επίθεσης με σκοπό την απενεργοποίηση του agent. Επίσης να διαθέτει αυτόματο action σε Isolate ή Reboot.*
16.	*Brute force επιθέσεις, password stealers, port scanning επιθέσεις*	*Να παρέχει προστασία από απειλές οι οποίες εκμεταλλεύονται δικτυακές ευπάθειες όπως brute force επιθέσεις ή password stealers. Επίσης να προστατεύει από port scanning επιθέσεις.*
17.	*Έλεγχος εκτέλεσης εφαρμογών*	⇨ *Η λύση πρέπει να παρέχει δυνατότητα ελέγχου εφαρμογών. Μέσω του ελέγχου εφαρμογών πρέπει να ελέγχεται η εγκατάσταση και η εκτέλεση εφαρμογών, καθώς και η μεταφόρτωση εξωτερικών στοιχείων (πχ αρχεία dll).* ⇨ *Ο διαχειριστής θα πρέπει να μπορεί να ορίζει κανόνες για συγκεκριμένες εφαρμογές καθώς και τα δικαιώματα εκτέλεσης αυτών.*
18.	*Έλεγχος αλληλογραφίας*	⇨ *Έλεγχος και προστασία εισερχόμενου και εξερχομένου ηλεκτρονικού ταχυδρομείου όλων των χρηστών.* ⇨ *Να παρέχεται antispam προστασία για την εισερχόμενη αλληλογραφία σε με σάρωση που ελέγχει για κυριλλικούς/ασιατικούς χαρακτήρες, URLs, σεξουαλικό περιεχόμενο καθώς και να γίνεται έλεγχος βάσει RBL servers και heuristic μηχανισμών.* ⇨ *Να υπάρχει η δυνατότητα δημιουργίας κανόνων βάσει keywords ή ολόκληρων φράσεων στο subject ή στο κύριο μέρος των μηνυμάτων.* ⇨ *Να υπάρχει η δυνατότητα δημιουργίας κανόνων βάσει keywords ή ολόκληρων φράσεων στο subject ή στο κύριο μέρος των μηνυμάτων.*
19.	*Αποστολή δεδομένων*	*Να παρέχει τη δυνατότητα ελέγχου αποστολής δεδομένων μέσω email ή web traffic.*
20.	*Ενημερώσεις*	*Να αναζητά ενημερώσεις μέσω δικτύου τουλάχιστον ανά μία ώρα χωρίς να απαιτείται η παρέμβαση του χρήστη.*

21.	*Encryption*	⇨ *Να υποστηρίζει τη προσθήκη δυνατότητας εγκατάστασης και διαχείρισης της κρυπτογράφησης δίσκου μέσα από το ίδιο περιβάλλον διαχείρισης ασφαλείας, χωρίς να απαιτείται κάποιος επιπλέον client.* ⇨ *Στην encryption λειτουργία να υποστηρίζεται full disk encryption για Windows και Mac λειτουργικά.* ⇨ *Στην encryption λειτουργία τα κλειδιά κρυπτογράφησης να είναι αποθηκευμένα στην κονσόλα διαχείρισης ώστε να είναι εφικτή η ανάκτησή τους.*
22.	*Ανάλυση χρηστών*	*Να υποστηρίζει τη προσθήκη δυνατότητας ανάλυσης της συμπεριφοράς των χρηστών και των εφαρμογών που χρησιμοποιούν με AI μηχανισμούς. Να δημιουργεί προφίλ για τον κάθε χρήστη, να μαθαίνει πρότυπα χρήσης και να προτείνει μέτρα προστασίας.*
23.	*Συμβατότητα Οργανισμού*	*Να παρέχεται η προσθήκη δυνατότητας δημιουργίας report που να δείχνει κατά πόσο ο οργανισμός είναι συμβατός με κανονισμούς όπως το NIS2, ISO , SOC2, DORA κτλ*
	Ενσωμάτωση Firewall	*Προστασία ενάντια σε μη εξουσιοδοτημένη πρόσβαση από το internet και ενάντια σε επιθέσεις που προέρχονται από το εσωτερικό δίκτυο.*
24.	*Προκαθορισμένα Προφίλ*	*Το προϊόν πρέπει αν έχει σετ από προκαθορισμένους κανόνες βασισμένους στην τοποθεσία και πολιτική ασφαλείας του χρήστη.*
25.	*Έλεγχος εφαρμογών*	*Αποκλεισμός πρόσβασης στο δίκτυο από εφαρμογές που βρίσκονται στα endpoints.*
26.	*Αναγνώριση τοποθεσίας*	*Αυτόματη επιλογή του προφίλ του τοίχους προστασίας βάσει της τοποθεσίας του endpoint (π.χ. εταιρικό δίκτυο, δημόσιο δίκτυο, οικιακό δίκτυο κλπ)*
27.	*Καραντίνα δικτύου*	*Αυτόματος αποκλεισμός της πρόσβασης στο δίκτυο για τα endpoints που παρουσιάζουν πρόβλημα (π.χ. παλιοί ορισμοί ιών, απενεργοποιημένη προστασία ελέγχου σε πραγματικό χρόνο). Επίσης, να υποστηρίζει τη δυνατότητα προγραμματισμού της ολικής ενεργοποίησης ή απενεργοποίησης της πρόσβασης στο διαδίκτυο τόσο για έναν υπολογιστή όσο και για ολόκληρες ομάδες*
28.	*Αποκλεισμός ιστοσελίδων*	*Αποκλεισμός πρόσβασης σε ιστοσελίδες που παραβιάζουν την πολιτική του οργανισμού, βάσει κατηγοριών ιστοσελίδων.* *Δυνατότητα αποκλεισμού ιστοσελίδων κατά απαίτηση.*
29.	*Web filtering*	*Να παρέχεται η δυνατότητα web filtering με scheduling επιλογές.*
	Έλεγχος συσκευών	*Δυνατότητα ελέγχου της πρόσβασης σε εξωτερικές συσκευές που συνδέονται στα endpoints.*
30.	*Πρόσβαση σε συσκευές υλικού*	*Δυνατότητα ελέγχου της πρόσβασης σε ομάδες συσκευών όπως:* ⇨ *DVD/CD ROM Drives* ⇨ *Imaging Devices* ⇨ *Modems* ⇨ *Εκτυπωτές* ⇨ *USB Συσκευές αποθήκευσης*
31.	*Αφαιρούμενα μέσα αποθήκευσης*	⇨ *Αποκλεισμός πρόσβασης εγγραφής* ⇨ *Αποκλεισμός εκτελέσιμων αρχείων*
32.	*Device Whitelisting*	*Δυνατότητα πρόσβασης σε συγκεκριμένες συσκευές*
	Ανάλυση επιθέσεων	*Ανθεκτικότητα ενάντια σε νέες επιθέσεις εμπλουτίζοντας τις αναλυτικές δυνατότητες στο cloud, σε αντίθεση με το να χρειάζεται μόνο ενημέρωση των τοπικών endpoint*
33.	*Εκτεταμένη ανάλυση*	*Ενσωμάτωση νέων και εξελισσόμενων τεχνολογιών μέσω cloud για το δυναμικό εντοπισμό και αποκλεισμό επιθέσεων.*

34.	*Χρήση ευριστικών αλγορίθμων*	*Χρήση ευριστικών αλγορίθμων για τον εντοπισμό κακόβουλης συμπεριφοράς και βελτίωση της προστασίας των endpoint.*
35.	*Πηγές ανάλυσης Απειλών*	*Συγκέντρωση ανάλυσης απειλών από πολλαπλές πηγές που είναι ενσωματωμένες στη λύση*
	Καταγραφή και αναφορές	*Δυνατότητα πρόσβασης στα γεγονότα ασφαλείας και τις πληροφορίες των επιθέσεων*
36.	*Καταγραφή εντοπισμών*	*Καταγραφή όλων των αποτελεσμάτων του εντοπισμού κακόβουλου λογισμικού ή συμπεριφοράς.*
37.	*Καταγραφή ενεργειών αντιμετώπισης*	*Καταγραφή όλων των ενεργειών αντιμετώπισης που έγιναν ως απόκριση σε κάποιο εντοπισμό κακόβουλου λογισμικού ή συμπεριφοράς*
38.	*Αναγνωσιμότητα της Μορφή Καταγραφών*	*Παρουσίαση όλων των καταγεγραμμένων πληροφοριών σε μορφή αναγνώσιμη από ανθρώπους ανεξαρτήτως από το περιβάλλον διεπαφής του διαχειριστή.*
39.	*Δυνατότητα διεπαφής με άλλα εργαλεία*	*Δυνατότητα διεπαφής για ενσωμάτωση με άλλα εργαλεία όπως SIEM συστήματα ή syslog servers, για πιο ευρεία δυνατότητα ανίχνευσης και υποστήριξης.*
40.	*Αναφορές*	*Παραγωγή αναφορών & στατιστικών σε διάφορες μορφές (txt, csv, charts) για ανάγνωση τόσο με on-demand όσο και προγραμματισμένη εκτέλεση.* *Οι διαθέσιμες αναφορές πρέπει να περιλαμβάνουν χωρίς να περιορίζονται σε αυτά, τα ακόλουθα:* ⇨ *Περιστατικά μόλυνσης* ⇨ *Παραλειπόμενα patches* ⇨ *Κατάσταση των Endpoints* ⇨ *Εγκατεστημένες εκδόσεις του προϊόντος* *Οι αναφορές πρέπει να δημιουργούνται κατά απαίτηση ή αν στέλνονται αυτόματα μέσω email.* *Οι αναφορές που εξάγονται θα πρέπει να επιτρέπουν την παραμετροποίηση της μορφής τους ή τουλάχιστον κάποιων εκ των παραπάνω μορφών μετά την εξαγωγή.*
	Απόκριση και αποκατάσταση	*Παροχή απόκρισης και αποκατάστασης στο endpoint.*
41.	*Ανίχνευση κακόβουλου λογισμικού*	⇨ *Κατά την ανίχνευση κακόβουλου λογισμικού οι ακόλουθες ενέργειες πρέπει να είναι διαθέσιμες ως αυτόματη απόκριση.* ⇨ *Καθαρισμός μόλυνσης από το αρχείο* ⇨ *Προσθήκη σε καραντίνα* ⇨ *Διαγραφή του αρχείου* ⇨ *Να υποστηρίζει τη δυνατότητα σύνδεσης μέσω terminal στο τελικό σημείο για την αποστολή εντολών που αφορούν διερεύνηση ή αποκατάσταση. Επιπλέον η λειτουργία αυτή να είναι διαθέσιμη και για non windows λειτουργικά.*
42.	*Επιπρόσθετες ενέργειες απόκρισης*	*Αποκλεισμός όλης της κίνησης δικτύου στο endpoint.*
43.	*Blacklist Files*	*Δυνατότητα προσθήκης σε blacklist νέων εντοπισμένων κακόβουλων αρχείων.*
44.	*Διαχείριση καραντίνας*	*Προσθήκη μολυσμένων αρχείων ή επικίνδυνου λογισμικού σε καραντίνα.* *Οι διαθέσιμες ενέργειες για τα περιεχόμενα της καραντίνας θα πρέπει να είναι:* ⇨ *Διαγραφή* ⇨ *Απελευθέρωση* *Οι διαχειριστές θα πρέπει να μπορούν να εκτελούν απομακρυσμένα αυτές τις ενέργειες στις καραντίνες των endpoint.*

45.	*Application Whitelists/ Blacklists*	⇨ *Έλεγχος των εφαρμογών που επιτρέπεται να εκτελούνται στα endpoints βάσει hash των αρχείων.* ⇨ *Να παρέχει τη δυνατότητα αποκλεισμού εκτέλεσης εγκατεστημένων εφαρμογών (blacklisting) μέσω κανόνων.* ⇨ *Να παρέχει λίστα των εφαρμογών που χρησιμοποιούνται καθώς και να προσφέρεται η δυνατότητα εκτέλεσης μόνο συγκεκριμένων εφαρμογών (whitelisting).*
	Επιδόσεις	*Βεβαίωση ελάχιστου αντίκτυπου στους πόρους των endpoint.*
46.	*Endpoint User Experience: Impact*	*Παροχή προστασίας, συμπεριλαμβανομένης αναγνώρισης νέων, πιθανών κακόβουλων συμπεριφορών, με ελάχιστο αντίκτυπο στην εμπειρία του χρήστη στο endpoint.*
47.	*Endpoint System Resource Offload*	*Να υποστηρίζει για endpoints μικρών επιδόσεων, τη σάρωση κακόβουλου λογισμικού και έλεγχο για content reputation από κάποιο on-premises virtual appliance.*
	Enterprise Management	*Ευκολία στη χρήση του προϊόντος και διαλειτουργικότητα με άλλα επιχειρηματικά εργαλεία.*
48.	*Management Server*	*Ο Server ή η κεντρική κονσόλα διαχείρισης θα βρίσκεται είτε στις εγκαταστάσεις του οργανισμού είτε σε περιβάλλον cloud.*
49.	*Κονσόλα διαχείρισης*	*Να παρέχεται μια διεπαφή χρήστη για σύνδεση στο server ή την κεντρική κονσόλα διαχείρισης με καλό σχεδιασμό και ευκολία χρήσης με σύστημα κεντρικής διαχείρισης για όλα τα απαιτούμενα εργαλεία προστασίας και δυνατότητα απομακρυσμένης εγκατάστασης / απεγκατάστασης.*
50.	*Management Proxy*	*Δυνατότητα να μπορούν τα endpoints να συνδεθούν στο Proxy διαχείρισης ή στα endpoints που θα επιλεχθούν ως proxy διαχειριστές εφόσον υπάρχει αυτή η δυνατότητα για την παραλαβή virus definitions και ενημερώσεις λογισμικού, ώστε να μειώνεται ο φόρτος κίνησης του Server διαχείρισης.*
51.	*Σάρωση*	*Υποστήριξη για αυτόματη (π.χ. σε προγραμματισμένο χρόνο, η επαναλαμβανόμενη με ρύθμιση από το διαχειριστή) καθώς και κατά απαίτηση (π.χ. έναρξη από το διαχειριστή / χρήστη) σάρωση & καθαρισμό απειλών για τις προστατευμένες συσκευές.*
52.	*Ανάλυση των επιθέσεων*	*Να παρέχεται forensic ανάλυση των επιθέσεων που ανιχνεύονται και αντιμετωπίζονται αυτόματα. Επίσης να υπάρχει η δυνατότητα ενεργειών έρευνας αλλά και αποκατάστασης μέσα από το ίδιο περιβάλλον.*
53.	*Παρακολούθηση κατάστασης*	*Υποστήριξη παρακολούθησης κατάστασης περιλαμβανομένου:* ⇨ *Dashboard που να αντικατοπτρίζει την γενική κατάσταση των συνδεδεμένων endpoints.* ⇨ *Κατάσταση του κάθε μεμονωμένου endpoint.* ⇨ *Alerts και warnings σχετικά με την ανίχνευση κακόβουλου λογισμικού / κακόβουλης συμπεριφοράς.* ⇨ *Δυνατότητα συλλογής, επεξεργασίας και ανάλυσης αρχείων καταγραφής από πολλές πηγές (τερματικά σημεία, διακομιστές, δίκτυα και υπηρεσίες cloud) σε πραγματικό χρόνο. Η λύση να υποστηρίζεται από τον ίδιο κατασκευαστή μέσα από την ίδια κονσόλα διαχείρισης.* ⇨ *Να παρέχεται η δυνατότητα αποστολής ειδοποιήσεων μέσω email.* ⇨ *Μέσα από το περιβάλλον διαχείρισης και χωρίς την εγκατάσταση επιπλέον client, να υποστηρίζεται η λειτουργία ελέγχου των λειτουργικών, των εφαρμογών καθώς και ευπαθειών που προέρχονται από τον ανθρώπινο παράγοντα με σκοπό την ελαχιστοποίηση του κινδύνου επίθεσης (Risk Management) από λανθασμένες ρυθμίσεις, ευπάθειες εφαρμογών ή ενέργειες χρηστών. Επίσης να παρέχονται περισσότερες πληροφορίες για το κάθε θέμα μαζί με την αλλαγή που συνιστάται στην εκάστοτε ρύθμιση. Επιπλέον, μέσα από το ίδιο περιβάλλον να παρέχεται και η δυνατότητα εφαρμογής των*

		διορθωτικών ενεργειών.
54.	*Καταγραφή Audit*	*Παρακολούθηση και συλλογή στατιστικών για την υγεία του συστήματος για την ένδειξη του χρόνου λειτουργίας του agent και συμμόρφωσης με την πολιτική.*
55.	*Διαγνωστικά*	*Ο Server ή η κεντρική κονσόλα διαχείρισης θα πρέπει να συλλέγει διαγνωστικές αναφορές κατά απαίτηση από τα endpoint για την αντιμετώπιση προβλημάτων.*
56.	*Sensors*	*Να υποστηρίζει τη δυνατότητα εισαγωγής επιπλέον sensors ώστε να είναι εφικτή η πρόσβαση σε επιπλέον πληροφορίες που αφορούν Active Directory, Cloud εφαρμογές όπως το Office ή και το εσωτερικό δίκτυο για την προστασία και IoT συσκευών (XDR). Η διαχείριση να γίνεται μέσα από την ίδια κονσόλα χωρίς την εγκατάσταση επιπλέον client.*
57.	*Active Directory*	*Δυνατότητα ενσωμάτωσης του Active Directory στην κονσόλα διαχείρισης.*
58.	*Ανίχνευση Υπολογιστών*	*Να μπορεί να γίνει αυτόματη ανίχνευση των υπολογιστών που βρίσκονται στο τοπικό δίκτυο, ακόμα και αν αυτά δεν ανήκουν σε Active Directory.*
59.	*Ενσωμάτωση Τεχνολογιών*	*Δυνατότητα ενσωμάτωσης των Microsoft Azure, Amazon EC2, VMware NSX-V, VMware NSX-T & Nutanix Prism στην κονσόλα διαχείρισης.*
60.	*Δεδομένα ασφαλείας και λειτουργίας*	*Δυνατότητα συγκέντρωσης, εμπλουτισμού και ανάλυσης δεδομένων ασφαλείας και λειτουργίας από όλη την υποδομή της επιχείρησης σε μία ενιαία διεπαφή.*
61.	*Integration hub*	*Να υπάρχει ενσωματωμένο integration hub το οποίο να παρέχει κεντρικό έλεγχο για να συνδέεται, να παρακολουθείται και να επεκτείνεται εύκολα το οικοσύστημα της κυβερνοασφάλειας του οργανισμού.*
62.	*Ομάδες χρηστών*	*Υποστήριξη διαφορετικών ομάδων & υποομάδων χρηστών με δυνατότητα εφαρμογής διαφορετικών ρυθμίσεων για κάθε μια.*
63.	*Ρυθμίσεις ασφαλείας (πολιτικών)*	*Δυνατότητα αυτόματης αλλαγής των ρυθμίσεων ασφαλείας (πολιτικών) βάσει δικτυακών κανόνων ή βάσει συγκεκριμένων χρηστών.*
64.	*EDR*	*Να υπάρχει δυνατότητα διαχείρισης EDR τεχνολογίας μέσα από την ίδια κονσόλα διαχείρισης χωρίς να απαιτείται επιπλέον client*
65.	*Patch management*	*Να υποστηρίζει την προσθήκη δυνατότητας εγκατάστασης και διαχείρισης patching μέσα από το ίδιο περιβάλλον διαχείρισης ασφαλείας, χωρίς να απαιτείται κάποιος επιπλέον client. Στην patch management λειτουργία, να υποστηρίζεται patching και για 3rd party windows εφαρμογές όπως και Linux, Mac λειτουργικών.*
66.	*Integrity Monitoring*	*Να παρέχει την προσθήκη της δυνατότητας Integrity Monitoring η οποία ελέγχει και επικυρώνει τις αλλαγές που πραγματοποιούνται σε Windows και Linux τερματικά, μέσα από την ίδια κονσόλα χωρίς την εγκατάσταση επιπλέον client.*
67.	*Storages*	*Να παρέχεται η προσθήκη δυνατότητας προστασίας storages.*
68.	*Updates*	*Να υποστηρίζεται διαδικασία staging για τα updates.*
	Διαχείριση Endpoint	*Βασικές λειτουργίες για τη διαχείριση των endpoint.*
69.	*Endpoint Deployment*	*Υποστήριξη αυτόματου καθώς και χειροκίνητου τρόπου για την εγκατάσταση των agent, όπως απομακρυσμένο push και τοπική εγκατάσταση στον client.*
70.	*Παραμετροποίηση Endpoint*	*Υποστήριξη πολλαπλών μεθόδων για την εφαρμογή των αλλαγών της πολιτικής ασφαλείας, συμπεριλαμβάνοντας αυτόματου (κεντρικά διαχειριζόμενου) καθώς και τοπικά (ελεγχόμενο από το χρήστη του endpoint).*
71.	*Ενημερώσεις Endpoint*	*Υποστήριξη πολλαπλών μεθόδων για την ενημέρωση των endpoints, συμπεριλαμβάνοντας αυτόματου (κεντρικά διαχειριζόμενου), τοπικά (ελεγχόμενο από το χρήστη του endpoint) ή offline μεθόδους.*

72.	*Documentation*	*Το documentation θα πρέπει να είναι διαθέσιμο σε μια ή παραπάνω από τις ακόλουθες μορφές:* ⇨ *Ηλεκτρονικά μέσα* ⇨ *Έγγραφο* ⇨ *Online*
73.	*Κάλυψη ενημερώσεων, αναβαθμίσεων και τεχνικής υποστήριξης.*	*3 έτη*
	Υποστηριζόμενα λειτουργικά - πλατφόρμες	*Παροχή προστασίας ενδεικτικά στα παρακάτω λογισμικά*
74.	*Windows*	*7, 8, 10, 11, Server 2016, Server 2019, Server 2022*
75.	*Linux*	*Ubuntu, openSUSE, Fedora, Debian, Oracle, Linux*
76.	*Mac*	*MacOS Sequoia, MacOS Sonoma, MacOS Ventura, MacOS Monterey*
77.	*Λογισμικά / Πλατφόρμες*	*Δυνατότητα εγκατάστασης της κονσόλας διαχείρισης ενδεικτικά σε VMware, Citrix, Hyper-V, Nutanix Prism, Red Hat Enterprise virtualization, Oracle VM*
	Διακρίσεις	*Ύπαρξη διακρίσεων από διεθνείς οργανισμούς και φορείς*
78.	*Διακρίσεις από Οργανισμούς*	*Να έχει διακρίσεις σε συγκριτικά τεστ από αξιόπιστους διεθνείς οργανισμούς.*
79.	*Διακρίσεις από φορείς*	*Να έχει διακριθεί τουλάχιστον από τρεις διεθνείς φορείς.*

Η τιμολόγηση για το σύνολο του «ΣΥΣΤΗΜΑΤΟΣ ΠΡΟΣΤΑΣΙΑΣ ΙΩΝ ΚΑΙ ΑΠΕΙΛΩΝ-ANTIVIRUS» θα γίνει αμέσως μετά την ενεργοποίηση των τριακοσίων (300) αδειών.

Συνολικός Προϋπολογισμός Συστήματος Προστασίας Ιών και απειλών και υποστήριξης τύπου SOC: 15.000,00€ + 3.600,00€ ΦΠΑ = 18.600,00€.….»

ΤΡΟΠΟΣ ΑΠΟΣΤΟΛΗΣ-ΤΟΠΟΣ ΚΑΙ ΧΡΟΝΟΣ ΥΠΟΒΟΛΗΣ ΠΡΟΣΦΟΡΑΣ:

Οι προσφορές, όσων επιθυμούν να συμμετέχουν, υποβάλλονται έντυπα στη διεύθυνση του Γ.Ν.Θ. «ΑΓΙΟΣ ΠΑΥΛΟΣ» (Εθνικής Αντίστασης 161, Τ.Κ. 55134, Θεσσαλονίκη) στο Γραφείο της Γραμματείας (πρωτόκολλο), μέχρι και την Τετάρτη 29-04-2026, ώρα 14:30 μ.μ

Σε κλειστό φάκελο εξωτερικά θα αναγράφεται:

- Ο τίτλος: φάκελος προσφοράς για την πρόσκληση εκδήλωσης ενδιαφέροντος για την προμήθεια 300 αδειών του «ΣΥΣΤΗΜΑΤΟΣ ΠΡΟΣΤΑΣΙΑΣ ΙΩΝ ΚΑΙ ΑΠΕΙΛΩΝ - ANTIVIRUS» CPV:48761000-0.
- Ο Αριθ. Πρόσκλησης: 2026-25/ΣΠ
- Τα στοιχεία της εταιρείας
- Η διευκρίνιση: «Να μην ανοιχθεί από την ταχυδρομική υπηρεσία ή τη γραμματεία».

Διευκρινίζεται ότι οι προσφορές που τυχόν υποβληθούν εκπρόθεσμα, δεν θα γίνουν αποδεκτές.

ΠΕΡΙΕΧΟΜΕΝΟ ΠΡΟΣΦΟΡΩΝ:

Ο φάκελος της προσφοράς θα περιλαμβάνει:

1. Δικαιολογητικά συμμετοχής στον οποίο θα περιέχονται τα εξής:

α) **Υπεύθυνη Δήλωση** του εκπροσώπου του οικονομικού φορέα, στην οποία θα δηλώνονται τα παρακάτω:

- η αποδοχή όλων των όρων της πρόσκλησης,
- η μη ύπαρξη σε βάρος του οικονομικού φορέα, (εάν πρόκειται για μεμονωμένο φυσικό ή νομικό πρόσωπο) αμετάκλητης καταδικαστικής απόφασης για ένα ή περισσότερο από τα ακόλουθα εγκλήματα: α) συμμετοχή σε εγκληματική οργάνωση, β) ενεργητική δωροδοκία, γ) απάτη εις βάρος των οικονομικών συμφερόντων της Ένωσης, δ) τρομοκρατικά εγκλήματα ή εγκλήματα συνδεόμενα με τρομοκρατικές δραστηριότητες, ε) νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή χρηματοδότηση της τρομοκρατίας, στ) παιδική εργασία και άλλες μορφές εμπορίας ανθρώπων.

  Η περίπτωση αποκλεισμού οικονομικού φορέα εφαρμόζεται επίσης όταν το πρόσωπο εις βάρος του οποίου εκδόθηκε αμετάκλητη καταδικαστική απόφαση είναι μέλος του διοικητικού, διευθυντικού ή εποπτικού οργάνου του εν λόγω οικονομικού φορέα ή έχει εξουσία εκπροσώπησης, λήψης αποφάσεων ή ελέγχου σε αυτό.

  Εάν στις ως άνω περιπτώσεις η κατά τα ανωτέρω, περίοδος αποκλεισμού δεν έχει καθοριστεί με αμετάκλητη απόφαση, αυτή ανέρχεται σε πέντε (5) έτη από την ημερομηνία της καταδίκης με αμετάκλητη απόφαση.
- η μη αθέτηση των υποχρεώσεων που προβλέπονται στην παρ. 2 του άρθρου 18 του ν. 4412/2016, περί αρχών που εφαρμόζονται στις διαδικασίες σύναψης δημοσίων συμβάσεων, ήτοι παραβίαση των περιβαλλοντικών, κοινωνικών και επιβαλλόμενων από την εργατική νομοθεσία υποχρεώσεων, κατά την εκτέλεση των δημοσίων συμβάσεων.

β) **Απόσπασμα σχετικού ποινικού μητρώου** ή, ελλείψει αυτού, ισοδύναμο έγγραφο που εκδίδεται από αρμόδια δικαστική ή διοικητική αρχή του κράτους-μέλους ή της χώρας καταγωγής ή της χώρας όπου είναι εγκατεστημένος ο οικονομικός φορέας, από το οποίο προκύπτει ότι πληρούνται αυτές οι προϋποθέσεις, *που να έχει εκδοθεί έως τρεις (3) μήνες πριν από την υποβολή του*.

Η υποχρέωση προσκόμισης του ως άνω αποσπάσματος αφορά και στα μέλη του διοικητικού, διευθυντικού ή εποπτικού οργάνου του εν λόγω οικονομικού φορέα ή στα πρόσωπα που έχουν εξουσία εκπροσώπησης, λήψης αποφάσεων ή ελέγχου σε αυτό.

γ) Για την **καταβολή φόρων, αποδεικτικά ενημερότητας για χρέη προς το ελληνικό δημόσιο** *εφόσον είναι σε ισχύ κατά το χρόνο υποβολής τους*, άλλως, στην περίπτωση που δεν αναφέρεται σε αυτό χρόνος ισχύος, που να έχει εκδοθεί έως τρεις (3) μήνες πριν από την υποβολή τους.

δ) Για την **καταβολή εισφορών κοινωνικής ασφάλισης**, πιστοποιητικά που εκδίδονται από την αρμόδια, κατά περίπτωση, αρχή του ελληνικού κράτους, ότι έχουν εκπληρωθεί οι υποχρεώσεις του φορέα, σύμφωνα με την ισχύουσα ελληνική νομοθεσία (θα αφορά την κύρια και την επικουρική ασφάλιση), *εφόσον είναι εν ισχύ κατά το χρόνο υποβολής τους*, άλλως, στην περίπτωση που δεν αναφέρεται σε αυτό χρόνος ισχύος, που να έχουν εκδοθεί έως τρεις (3) μήνες πριν από την υποβολή τους.

ε) **Πιστοποιητικό/ βεβαίωση του οικείου επαγγελματικού ή εμπορικού μητρώου** – αριθμός καταχώρησης στο ΓΕΜΗ (παρ. 2 άρθρου 75) του Παραρτήματος XI του Προσαρτήματος Α' του ν. 4412/2016, με το οποίο πιστοποιείται η εγγραφή τους σε αυτό, καθώς και το ειδικό επάγγελμά τους κατά την ημέρα διενέργειας του διαγωνισμού, οι εκάστοτε τροποποιήσεις του καταστατικού, *εφόσον έχει εκδοθεί έως τριάντα (30) εργάσιμες ημέρες πριν από την υποβολή τους.*

στ) Για την **απόδειξη της νόμιμης σύστασης και εκπροσώπησης**, στις περιπτώσεις που ο οικονομικός φορέας είναι νομικό πρόσωπο, προσκομίζει τα κατά περίπτωση νομιμοποιητικά έγγραφα σύστασης και νόμιμης εκπροσώπησης *εφόσον έχουν εκδοθεί έως τριάντα (30) εργάσιμες ημέρες πριν από την υποβολή τους* (όπως πιστοποιητικό Γ.Ε.ΜΗ. τροποποιήσεων του καταστατικού ΦΕΚ σύστασης και εκπροσώπησης σε περίπτωση Α.Ε., κλπ., ανάλογα με τη νομική μορφή του διαγωνιζομένου).

ζ) **Υπεύθυνη Δήλωση** του, ανά περίπτωση, νόμιμου εκπροσώπου του νομικού προσώπου/ οντότητας, στην οποία δηλώνει ότι το <u>νομικό πρόσωπο / οντότητα</u>, το οποίο εκπροσωπεί νόμιμα, δεν έχει καταδικαστεί αμετάκλητα για κανένα από τα αδικήματα δωροδοκίας του άρθρου 73 παρ. 1 του ν. 4412/2016, κατ' εφαρμογή των διατάξεων των άρθρων 134-135 του ν. 5090/2024

2. Τεχνική προσφορά

Οι υποψήφιοι οφείλουν να υποβάλουν στην τεχνική τους προσφορά συμπληρωμένο τον Πίνακα Συμμόρφωσης σύμφωνα με το Υπόδειγμα, το οποίο αναρτάται στο διαδίκτυο και συγκεκριμένα στην ιστοσελίδα του Νοσοκομείου.

3. Οικονομικοτεχνική προσφορά

Ο φάκελος της προσφοράς θα περιέχει την οικονομοτεχνική προσφορά, δηλαδή τα τεχνικά στοιχεία της προσφοράς που πρέπει να είναι σύμφωνα με τις τεχνικές προδιαγραφές που αναφέρονται στην παρούσα πρόσκληση, καθώς και τα οικονομικά στοιχεία της προσφοράς του.

Οι συμμετέχοντες οικονομικοί φορείς υποβάλουν Προσφορές για το σύνολο της προμήθειας των 300 αδειών.

Εναλλακτικές προσφορές δε γίνονται δεκτές και απορρίπτονται ως απαράδεκτες.

Η οικονομική προσφορά, θα περιέχει συμπληρωμένους τους παρακάτω πίνακες:

ΣΧΕΔΙΟ ΠΙΝΑΚΑ ΟΙΚΟΝΟΜΙΚΗΣ ΠΡΟΣΦΟΡΑΣ

Α/Α	ΚΩΔΙΚΟΣ ΕΙΔΟΥΣ ΓΡΑΦΕΙΟΥ ΠΡΟΜΗΘΕΙΩΝ	ΠΕΡΙΓΡΑΦΗ ΕΙΔΟΥΣ	ΣΥΝΟΛΙΚΗ ΤΙΜΗ ΠΡΟΣΦΟΡΑΣ ΧΩΡΙΣ ΦΠΑ	ΦΠΑ 24%	ΣΥΝΟΛΙΚΗ ΤΙΜΗ ΠΡΟΣΦΟΡΑΣ ΜΕ ΦΠΑ	ΠΡΟΫΠΟΛΟΓΙΣΘΕΙΣΑ ΔΑΠΑΝΗ ΜΕ ΦΠΑ 24%
1	200780010000007 ΑΠΟΘΗΚΗ ΜΗ ΑΝΑΛΩΣΙΜΩΝ	«ΣΥΣΤΗΜΑΤΟΣ ΠΡΟΣΤΑΣΙΑΣ ΙΩΝ ΚΑΙ ΑΠΕΙΛΩΝ-ΑΝΤΙVIRUS» CPV:48761000-0				

Οι τιμές των προσφορών θα εκφράζονται σε ευρώ. Στις τιμές θα συμπεριλαμβάνονται οι τυχόν υπέρ τρίτων κρατήσεις, ως και κάθε άλλη επιβάρυνση, εκτός του ΦΠΑ, ο οποίος θα αναφέρεται ξεχωριστά.

Οικονομική προσφορά που είναι ανώτερη της συνολικής προϋπολογισθείσας δαπάνης απορρίπτεται.

Η κατακύρωση θα γίνει στον ανάδοχο που θα προσφέρει την πλέον συμφέρουσα από οικονομική άποψη προσφορά, αποκλειστικά βάσει της τιμής, με την προϋπόθεση ότι με την προσφορά του ικανοποιούνται οι όροι της πρόσκλησης.

ΑΠΟΣΦΡΑΓΙΣΗ ΠΡΟΣΦΟΡΩΝ

Η αποσφράγιση των προσφορών θα πραγματοποιηθεί στις **30 Απριλίου 2026 ημέρα Πέμπτη και ώρα 11:00** στο Γραφείο προμηθειών του Γ.Ν.Θ. «ΑΓΙΟΣ ΠΑΥΛΟΣ», ενώπιον αρμόδιας επιτροπής.

Διευκρινίζεται ότι οι νόμιμοι εξουσιοδοτημένοι εκπρόσωποι των συμμετεχόντων εταιρειών, μπορούν να λάβουν γνώση για το σύνολο των κατατεθειμένων προσφορών του διαγωνισμού, εφόσον προηγηθεί τηλεφωνική επικοινωνία με τον αρμόδιο υπάλληλο του γραφείου προμηθειών ώστε να οριστεί συγκεκριμένη ημέρα και ώρα αυτού.

ΑΞΙΟΛΟΓΗΣΗ ΠΡΟΣΦΟΡΩΝ – ΚΑΤΑΚΥΡΩΣΗ

Η αρμόδια επιτροπή αποσφραγίζει τις προσφορές στον ορισμένο από την παρούσα χρόνο και προβαίνει στην αξιολόγηση των προσφορών με κριτήριο τη χαμηλότερη τιμή, συντάσσοντας πρακτικό με το οποίο γνωμοδοτεί για τον ανάδοχο, το οποίο επικυρώνεται με απόφαση του αρμοδίου οργάνου της Αναθέτουσας αρχής, η οποία κοινοποιείται με επιμέλεια αυτής στους προσφέροντες.

Επισημαίνεται ότι αν παρουσιαστούν ελλείψεις ή ήσσονος αξίας ατέλειες ή πρόδηλα τυπικά ή υπολογιστικά σφάλματα η Επιτροπή μπορεί να καλέσει εγγράφως τους προσφέροντες να τα διευκρινίσουν, σύμφωνα με το άρθρο 102 παρ. 4 του ν.4412/2016.

Σε περίπτωση ισοτιμίας, η αναθέτουσα αρχή επιλέγει τον ανάδοχο με κλήρωση μεταξύ των υποψηφίων που υπέβαλαν ισότιμες προσφορές.

Για δημόσιες συμβάσεις με εκτιμώμενη αξία κατώτερη ή ίση των ορίων του άρθρου 118, περί απευθείας ανάθεσης, όποιος έχει έννομο συμφέρον, μπορεί να ζητήσει την ακύρωση πράξης ή παράλειψης της αναθέτουσας αρχής, καθώς και την αναστολή εκτέλεσης, ενώπιον του Διοικητικού Εφετείου της έδρας της αναθέτουσας αρχής, σύμφωνα με όσα ορίζονται στα άρθρα 45 έως 56 του π.δ. 18/1989 (Α’ 8), το οποίο αποφαίνεται αμετακλήτως χωρίς να επιτρέπεται η προηγούμενη άσκηση άλλης ειδικής ή ενδικοφανούς διοικητικής προσφυγής. Το παράβολο για την άσκηση της αίτησης ακύρωσης και της αίτησης αναστολής ορίζεται ίσο με το πέντε τοις εκατό (5%) επί της εκτιμώμενης αξίας της σύμβασης.

ΚΑΤΑΡΤΙΣΗ ΚΑΙ ΥΠΟΓΡΑΦΗ ΣΥΜΒΑΣΗΣ

Μετά από την οριστικοποίηση της απόφασης κατακύρωσης η αναθέτουσα αρχή προσκαλεί τον ανάδοχο, να προσέλθει για την υπογραφή του συμφωνητικού.

Τυχόν υποβολή σχεδίων σύμβασης από τους υποψήφιους μαζί με τις προσφορές τους, δε δημιουργεί καμία δέσμευση για την αναθέτουσα αρχή.

Η σύμβαση που θα προκύψει θα είναι διάρκειας τριών (3) ετών.

ΤΟΠΟΣ, ΧΡΟΝΟΣ ΚΑΙ ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ – ΠΑΡΑΛΑΒΗ

Ως τόπος εκτέλεσης της προμήθειας ορίζεται η έδρα του Νοσοκομείου: Εθνικής Αντίστασης 161, Τ.Κ. 55134 Θεσσαλονίκη.

Ο Ανάδοχος υποχρεούται να παρέχει την προμήθεια του στο χρονικό διάστημα και με τον τρόπο που καθορίζεται στην παρούσα και ειδικότερα σύμφωνα με τους όρους των τεχνικών προδιαγραφών και της τεχνικής προσφοράς του.

Μη εμπρόθεσμη υποβολή των παραδοτέων από τον Ανάδοχο επάγεται την κήρυξη αυτού ως έκπτωτου.

Η παραλαβή των παραδοτέων γίνεται από αρμόδια επιτροπή, η οποία ορίζεται με απόφαση της Α.Α. και θα εκδίδει το σχετικό πρωτόκολλο οριστικής και ποιοτικής παραλαβής.

ΤΡΟΠΟΣ ΠΛΗΡΩΜΗΣ – ΚΡΑΤΗΣΕΙΣ

Η πληρωμή του αναδόχου θα πραγματοποιηθεί με τον πιο κάτω τρόπο:

Η πληρωμή του συμβατικού τιμήματος θα γίνεται με την προσκόμιση από τον Ανάδοχο των νομίμων παραστατικών και δικαιολογητικών που προβλέπονται από τις διατάξεις του άρθρου 200 παρ. 4 του ν. 4412/2016, καθώς και κάθε άλλου δικαιολογητικού που τυχόν ήθελε ζητηθεί από τις αρμόδιες υπηρεσίες που διενεργούν τον έλεγχο και την πληρωμή.

Η αναθέτουσα αρχή υποχρεούται να παραλαμβάνει και να επεξεργάζεται και ηλεκτρονικά τιμολόγια που είναι σύμφωνα με το ευρωπαϊκό πρότυπο έκδοσης ηλεκτρονικών τιμολογίων, όπως αυτό ορίζεται στην

περίπτωση 12 του άρθρου 149 του ν. 4601/2019 (Α΄44) και των, κατ΄ εξουσιοδότηση του άρθρου 154 του νόμου αυτού, κανονιστικών αποφάσεων, στην ηλεκτρονική διεύθυνση:

ilektronika.timologia@agpavlos.gr, με κωδικό τιμολόγησης «1015.Ε00224.0001».

Τον Ανάδοχο βαρύνουν οι υπέρ τρίτων κρατήσεις, ως και κάθε άλλη επιβάρυνση, σύμφωνα με την κείμενη νομοθεσία, μη συμπεριλαμβανομένου Φ.Π.Α., για την παράδοση του υλικού στον τόπο και με τον τρόπο που προβλέπεται στα έγγραφα της σύμβασης.

Ο Φ.Π.Α. επί της αξίας του τιμολογίου βαρύνει το Γ.Ν.Θ. «ΑΓΙΟΣ ΠΑΥΛΟΣ».

ΤΡΟΠΟΠΟΙΗΣΗ ΣΥΜΒΑΣΗΣ

Η σύμβαση μπορεί να τροποποιείται κατά τη διάρκειά της, χωρίς να απαιτείται νέα διαδικασία σύναψης σύμβασης, μόνο σύμφωνα με τους όρους και τις προϋποθέσεις του άρθρου 132 του ν. 4412/2016 και κατόπιν γνωμοδότησης της Επιτροπής της περ. β της παρ. 11 του άρθρου 221 του ν. 4412/2016.

ΛΟΙΠΟΙ ΟΡΟΙ:

- Οι προσφορές ισχύουν και δεσμεύουν τους συμμετέχοντες για ένα (1) έτος από την επόμενη μέρα της διενέργειας της πρόσκλησης εκδήλωσης ενδιαφέροντος. Προσφορά η οποία ορίζει χρόνο ισχύος μικρότερο από τον ανωτέρω προβλεπόμενο απορρίπτεται.
- Εγγυητική επιστολή συμμετοχής καθώς και καλής εκτέλεσης, δεν απαιτείται.
- Η παρούσα πρόσκληση εκδήλωσης ενδιαφέροντος αναρτάται στο ΚΗΜΔΗΣ και στο διαδίκτυο και συγκεκριμένα στην ιστοσελίδα του Νοσοκομείου στη διαδρομή (URL) http://www.agpavlos.gr./ΑΝΑΚΟΙΝΩΣΕΙΣ/ΠΡΟΜΗΘΕΙΕΣ/ΠΡΟΚΗΡΥΞΕΙΣ-ΔΙΑΓΩΝΙΣΜΟΙ.
- Για ότι δεν προβλέπεται στην παρούσα πρόσκληση εκδήλωσης ενδιαφέροντος, ισχύουν οι διατάξεις των νόμων και προεδρικών διαταγμάτων, όπως έχουν τροποποιηθεί και συμπληρωθεί.

Επισημαίνεται ότι οι ενδιαφερόμενοι οφείλουν να επισκέπτονται την ως άνω ιστοσελίδα του Νοσοκομείου για να ενημερώνονται για τυχόν αλλαγές.

Η ΔΙΟΙΚΗΤΡΙΑ ΤΟΥ ΝΟΣΟΚΟΜΕΙΟΥ

ΙΩΑΝΝΑ ΚΟΣΜΟΠΟΥΛΟΥ

14.04.2026 10:16:06
ΨΗΦΙΑΚΑ
ΥΠΟΓΕΓΡΑΜΜΕΝΟ
ΑΠΟ
ΙΟΑΝΝΑ
KOSMOPOULOU