ΑΝΑΡΤΗΤΕΟ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
2η Υ.ΠΕ ΠΕΙΡΑΙΩΣ & ΑΙΓΑΙΟΥ
ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΧΙΟΥ
« Σ Κ Υ Λ Ι Τ Σ Ε Ι Ο »
Ταχ. Δ/νση: Ελενας Βενιζελου

ΠΛΗΡΟΦΟΡΙΕΣ:

Τηλ.: 2271350106 Φαξ:2271350241

Email:paragelies@xioshosp.gr

ΧΙΟΣ: 21/10/2020

ΑΡ. ΠΡΩΤ.: οικ. 65

ΘΕΜΑ: ΔΗΜΟΣΙΑ ΑΝΟΙΚΤΗ ΔΙΑΔΙΚΑΣΙΑ ΣΥΛΛΟΓΗΣ ΠΡΟΣΦΟΡΩΝ

Το Γενικό Νοσοκομείο Χίου για την κάλυψη άμεσων και επιτακτικών αναγκών του, προσκαλεί τους ενδιαφερόμενους να καταθέσουν προσφορά για την **προμήθεια Ανανέωσης Αδειών Χρήσης Λογισμικού Αντιϊκής Προστασίας.**

Α. ΚΑΤΑΣΤΑΣΗ ΕΙΔΩΝ ΠΡΟΜΗΘΕΙΑΣ

Α/Α	ΚΩΔΙΚΟΣ ΝΟΣΟ-ΚΟΜΕΙΟΥ	ΠΕΡΙΓΡΑΦΗ ΥΛΙΚΟΥ	ΠΟΣΟ-ΤΗΤΑ	ΠΡΟΥΠΟΛΟΓΙΖΟ-ΜΕΝΗ ΤΙΜΗ ΜΟΝΑΔΑΣ ΧΩΡΙΣ ΦΠΑ	ΠΡΟΥΠΟΛΟΓΙ-ΣΜΟΣ ΧΩΡΙΣ ΦΠΑ	ΠΡΟΥΠΟΛΟΓΙ-ΣΜΟΣ ΜΕ ΦΠΑ 24%
1		Ανανέωση Αδειών Χρήσης Λογισμικού Αντιϊκής Προστασίας (Antivirus) ESET Endpoint Protection Advanced	**150**	**150Χ25,766**	**3.864,90**	**4.792,50**
	ΣΥΝΟΛΟ					

Β. ΠΛΗΡΟΦΟΡΙΕΣ ΓΙΑ ΤΗΝ ΠΡΟΜΗΘΕΙΑ

Αριθμός Αιτήματος	16854/24-09-2020
ΚΑΕ	7123.010
Προϋπολογισμός	4.792,50€
Κριτήριο Κατακύρωσης	Χαμηλότερη τιμή
Ημερομηνία έναρξης υποβολής προσφορών	Πέμπτη 22/10/2020
Ημερομηνία λήξης υποβολής προσφορών	**Δευτέρα 26/10/2020**
Τρόπος υποβολής προσφορών	**ΦΑΞ:2271350241** **e – mail**:paragelies@xioshosp.gr

Γ.ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

Υποστήριξη για τις εξής πλατφόρμες λειτουργικών συστημάτων: - MicrosoftWindows7, 8, 10 - Microsoft Windows 2008(R2), 2012(R2), 2016 - Linuxμε kernel 2.6.xκαι νεότερα - Mac OS X - Android 5 ή νεότερο	Δυνατότητα εξαγωγής ενιαίου πακέτου με το πρόγραμμα προστασίας, σύνδεση διαχείρισης, πολιτικές και την άδεια ενεργοποίησης
Δυνατότητα ανίχνευσης και καθαρισμού όλων των τύπων απειλών: viruses, malware, trojans, dialers, spyware, jokes,hoaxes, ransomware	Ξεχωριστό εργαλείο ανίχνευσης τερματικών και pushεγκατάστασης του παραπάνω ενιαίου πακέτου
Δυνατότητα αυτόματης ανίχνευσης & καθαρισμού των προαναφερθέντων απειλών σε πραγματικό χρόνο	Επικοινωνία του clientμόνο με IP, δηλαδή να δουλέψει σε περιπτώσεις όπου δεν υπάρχουν υπηρεσίες ονοματοδοσίας (DNSservers)
Δυνατότητα επιλογής ανίχνευσης malwareσε δικτυακές τοποθεσίες, on-demand και σε πραγματικό χρόνο	Αυτόματη ανίχνευση των τερματικών που βρίσκονται στο τοπικό δίκτυο, ακόμα κι αν αυτά δεν ανήκουν σε ActiveDirectory
ΠαρέχεταιCloudre putation data base για αμεσότερη προστασία από νέες απειλές	Εισαγωγή λίστας των τερματικών του δικτύου με τη χρήση CSV αρχείου
Υποστήριξη τεχνολογιών Advanced heuristics/DNAS ignatures/Script base data cks για δυνατότητα ανίχνευσης άγνωστων ιών	Η επικοινωνία των servers και των clients διασφαλίζεται μέσω certificate
Δυνατότητα για Intrusion Prevention System	Δυνατότητα ενεργοποίησης σε δίκτυο χωρίς σύνδεση στο internet (offlineactivation)
Δυνατότητα αποτροπής γνωστών exploits	Τα signaturefiles, πακέτα εγκατάστασης και οποιαδήποτε άλλη υπηρεσία απαιτείται μπορεί να διανέμεται μέσω τοπικού HTTP proxycache, με αυτόματη παράκαμψή του σε περίπτωση που δεν είναι διαθέσιμος ο proxyserver
Δυνατότητα αποτροπής ransomware	Περιλαμβάνεται έλεγχος και ειδοποίηση για το αν υπάρχουν ενημερώσεις για το λειτουργικό σύστημα, καθώς και η δυνατότητα να δοθεί εντολή ενημέρωσης λειτουργικού συστήματος
Δυνατότητα rollback των detection engines σε προηγούμενη έκδοση του με ταυτόχρονη παύση των ενημερώσεων, επιλέγοντας το κεντρικά ή	Παρακολούθηση όλων των clients και παραγωγή reports και στατιστικών σε πολλές μορφές (Προγραμματισμένα emails, PDF, PS, CSV, Charts)

απευθείας από το client	
Δυνατότητα κατεβάσματος ενημερώσεων με νεότερες engines που βρίσκονται σε δοκιμαστικό στάδιο, επιλέγοντας το κεντρικά ή απευθείας από το client	Δυνατότητα ενιαίας καραντίνας αρχείων που ανιχνεύθηκαν για όλο το δίκτυο, με δυνατότητες προβολής clients ανά απειλή, εξαγωγή και εξαίρεση
Δυνατότητα να μπορεί να γίνει ένα clientupdate server για τα υπόλοιπα clientstου δικτύου	Ο server διαχείρισης μπορεί να γίνει εγκατάσταση με τις παρακάτω μεθόδους. α) Αυτοματοποιημένα με τη μορφή Wizard β) Χειροκίνητα, εκτελώντας ανεξάρτητα τα τμήματα της εγκατάστασης γ) Ως προεγκατεστημένο Virtual Appliance με Linux OS
Δυνατότητα γιαSSL/TLS filtering στα πρωτόκολλα HTTPS, IMAPS, POP3S	Η εγκατάσταση της βάσης δεδομένων της κονσόλας γίνεται σε ένα υπολογιστή οπουδήποτε στο εσωτερικό δίκτυο της εταιρίας (όχι σε εξωτερικό δίκτυο π.χ. Cloud.)
Δυνατότητα μπλοκαρίσματος όλων των σελίδων του Internet σε ένα client καθώς και διαχείριση των σελίδων που μπορούν να είναι διαθέσιμες στο χρήστη ανά κατηγορία, π.χ. αποτροπή επίσκεψης σε σελίδες social media, streaming videos.	Παρέχεται εργαλείο ελέγχου κατάστασης αδειών και αριθμού ενεργοποιήσεων, ακόμα κι αν αυτές έχουν γίνει εκτός της κεντρικής κονσόλας (standaloneεγκαταστάσεις)
Δυνατότητα προστασίας σε δικτυακό επίπεδο με client based Firewall, με δυνατότητα φιλτραρίσματος σε επίπεδο θυρών και εφαρμογών σε εισερχόμενες και εξερχόμενες συνδέσεις.	Παρέχεται η δυνατότητα διαχείρισης Androidκαι iOS συσκευών μέσω της ίδιας κονσόλας (MDM)
Δυνατότητα προστασίας από δικτυακές απειλές και botnets	Παρέχεται η δυνατότητα agentless προστασίας μηχανημάτων σε περιβάλλον VMWare χωρίς εγκατάσταση λογισμικού antivirusστο λειτουργικό σύστημα του εικονικού μηχανήματος
Δυνατότητα εξαγωγής των ρυθμίσεων ενός client σε αρχείο και εισαγωγής των ρυθμίσεων σε άλλο clientαπό το ίδιο αρχείο.	Η είσοδος στην κονσόλα διαχείρισης μπορεί να κλειδωθεί με πιστοποίηση διπλού παράγοντα (2-factor authentication)
Ενσωματωμένη εφαρμογή που καταγράφει την κατάσταση του συστήματος (εφαρμογές, processes, services κ.α) – κατόπιν εντολής τοπικά ή από την κονσόλα - σε μία χρονική στιγμή (snapshot) και αποθηκεύει τα αποτελέσματα για σύγκριση τους με την κατάσταση του συστήματος	Δυνατότητα εξαγωγής των logs και events σε εξωτερικό σύστημα Syslog/SIEM με την υποστήριξη του IBM QRadar

από διαφορετική χρονική στιγμή.	
Παροχή Bootable Media που περιέχει το antivirus δίνοντας τη δυνατότητα για καθαρισμό του συστήματος χωρίς να χρειάζεται να ξεκινήσει το λειτουργικό σύστημα	Το μενού της κονσόλας διαχείρισης και του antivirusγια τα workstationsδιατίθεται και στην Ελληνική γλώσσα
Κεντρική διαχείριση όλων των clients των τερματικών και servers	Λειτουργία προσωρινής απενεργοποίησης πολιτικής ανά client
Υποστήριξη πολλαπλών ομάδων και υπό-ομάδων με δυνατότητα εφαρμογής διαφορετικών πολιτικών για κάθε περίπτωση	Δυνατότητα για ομάδες διαχείρισης με βάση ιδιότητες υπολογιστών, π.χ. αυτόματη ομαδοποίηση υπολογιστών με Windows 10
Εγκατάσταση & απεγκατάσταση της προστασίας μέσω κεντρικής κονσόλας (Remotedeployment)	

Δ. ΥΠΟΧΡΕΩΤΙΚΑ ΣΤΟΙΧΕΙΑ ΠΡΟΣΦΟΡΑΣ

Οι τιμές θα πρέπει να είναι σύμφωνα με τις τιμές του παρατηρητηρίου ή σύμφωνα με τις τιμές της τελευταίας σύμβασης. Η προσφορά που θα υποβληθεί θα πρέπει να αναφέρει τα πλήρη στοιχεία της εταιρείας:(ΑΦΜ, πλήρη επωνυμία, τηλέφωνο, φαξ, e-mail, και ΦΠΑ), ο χρόνος ισχύος της προσφοράς και να έχει την παρακάτω μορφή:

Αριθμός Αιτήματος	**Περιγραφή Υλικού**	**Τιμή μονάδας € (χωρίς ΦΠΑ)**	**Κωδικός Παρατ/ρίου**	**Τιμή Παρατ/ρίου**	**Κωδικό Εμπορίου**	**GMDN**	**Κωδικός ΕΚΑΠΤΥ**

Επιπλέον θα πρέπει να αναφέρεται – επί ποινή απόρριψης – ο χρόνος παράδοσης. Λόγω του επείγοντος της προμήθειας, το νοσοκομείο επιθυμεί τα προσφερόμενα να είναι **ετοιμοπαράδοτα,** σε διαφορετική περίπτωση διατηρεί το δικαίωμα να απορρίψει την προσφορά αν κρίνει ότι ο χρόνος παράδοσης είναι μεγάλος σε σχέση με τις ανάγκες του.

Σε περίπτωση που η τιμή προσφοράς του είδους υπερβαίνει την αντίστοιχη τιμή παρατηρητηρίου, αυτή υποχρεωτικά απορρίπτεται. Τέλος, σε περίπτωση που το είδος δεν αντιστοιχίζεται με το παρατηρητήριο τιμών, αυτό θα αναφέρεται στη στήλη κωδικός παρατηρητηρίου.

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

Επί της προσφοράς τους οι συμμετέχοντες θα πρέπει να δηλώνουν υπεύθυνα ότι δεν βρίσκονται σε μία από τις καταστάσεις των άρθρων 73 και 74 του Ν. 4412/2016 για τις οποίες οι οικονομικοί φορείς αποκλείονται ή μπορούν να αποκλεισθούν.

Η ΔΙΟΙΚΗΤΡΙΑ

Ε. ΚΑΝΤΑΡΑΚΗ