



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
2^η Υ.ΠΕ ΠΕΙΡΑΙΩΣ & ΑΙΓΑΙΟΥ
ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΧΙΟΥΑΡ.
« ΣΚΥΛΙΤΣΕΙΟ »
Ταχ. Δ/ση: Ελενας Βενιζελου

ΑΝΑΡΤΗΤΕΟ

ΧΙΟΣ: 21/10/2020

ΠΡΩΤ.: οικ. 65

ΠΛΗΡΟΦΟΡΙΕΣ:

ΟΡΘΗ ΕΠΑΝΑΛΗΨΗ

Τηλ.: 2271350106 Φαξ:2271350241

Email:paragelies@xioshosp.gr

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 ΝΟΣΟΚΟΜΕΙΟΥ	ΠΕΡΙΓΡΑΦΗ ΥΛΙΚΟΥ	ΠΟΣΟΤΗΤΑ	ΠΡΟΥΠΟΛΟΓΙΖΟΜΕΝΗ ΤΙΜΗ ΜΟΝΑΔΑΣ ΧΩΡΙΣ ΦΠΑ	ΠΡΟΥΠΟΛΟΓΙΣΜΟΣ ΧΩΡΙΣ ΦΠΑ	ΠΡΟΥΠΟΛΟΓΙΣΜΟΣ ΜΕ ΦΠΑ 24%
1		Ανανέωση Αδειών Χρήσης Λογισμικού Αντιϊκής Προστασίας (Antivirus) ESET Endpoint Protection Advanced (ΓΙΑ ΤΡΙΑ ΕΤΗ)	150	150X25,766	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: - Microsoft Windows 7, 8, 10 - Microsoft Windows 2008(R2), 2012(R2), 2016 - Linux με kernel 2.6. και 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 push εγκατάστασης του παραπάνω ενιαίου πακέτου
Δυνατότητα αυτόματης ανίχνευσης & καθαρισμού των προαναφερθέντων απειλών σε πραγματικό χρόνο	Επικοινωνία του client μόνο με IP, δηλαδή να δουλέψει σε περιπτώσεις όπου δεν υπάρχουν υπηρεσίες ονοματοδοσίας (DNS servers)
Δυνατότητα επιλογής ανίχνευσης malware σε δικτυακές τοποθεσίες, on-demand και σε πραγματικό χρόνο	Αυτόματη ανίχνευση των τερματικών που βρίσκονται στο τοπικό δίκτυο, ακόμα κι αν αυτά δεν ανήκουν σε Active Directory
Παρέχεται Cloud reputation data base για αμεσότερη προστασία από νέες απειλές	Εισαγωγή λίστας των τερματικών του δικτύου με τη χρήση CSV αρχείου
Υποστήριξη τεχνολογιών Advanced heuristics/DNS signatures/Script base data checks 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 (offline activation)
Δυνατότητα αποτροπής γνωστών exploits	Τα signature files, πακέτα εγκατάστασης και οποιαδήποτε άλλη υπηρεσία απαιτείται μπορεί να διανέμεται μέσω τοπικού HTTP proxy cache, με αυτόματη παράκαμψή του σε περίπτωση που δεν είναι διαθέσιμος ο proxy server
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 client του 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 για SSL/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 (standalone εγκαταστάσεις)
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 Android και 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 antivirus στο λειτουργικό σύστημα του εικονικού μηχανήματος
Δυνατότητα εξαγωγής των ρυθμίσεων ενός client σε αρχείο και εισαγωγής των ρυθμίσεων σε άλλο client από 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 antivirus για τα workstations διατίθεται 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 περισσότερων 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