ΑΝΑΡΤΗΤΕΟ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
2η Υ.ΠΕ ΠΕΙΡΑΙΩΣ & ΑΙΓΑΙΟΥ
ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΧΙΟΥΑΡ.
« 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: 03-10-2017

ΠΡΩΤ.:οικ. 61

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 των παρακάτω ειδών.

Α. ΚΑΤΑΣΤΑΣΗ ΕΙΔΩΝ ΠΡΟΜΗΘΕΙΑΣ

Α/Α	ΚΩΔΙΚΟΣ ΝΟΣΟΚΟΜΕΙΟΥ	ΠΕΡΙΓΡΑΦΗ ΥΛΙΚΟΥ	ΠΟΣΟΤΗΤΑ	ΠΡΟΥΠΟΛΟΓΙΖΟΜΕΝΗ ΤΙΜΗ ΜΟΝΑΔΑΣ ΧΩΡΙΣ ΦΠΑ	ΠΡΟΥΠΟΛΟΓΙΣΜΟΣ ΧΩΡΙΣ ΦΠΑ	ΠΡΟΥΠΟΛΟΓΙΣΜΟΣ ΜΕ ΦΠΑ
1		Λογισμικό Αντιικής Προστασίας (ESET Endpoint Protection Advanced)	**150**	**150Χ30**	**4.500,00**	**5.580,00**
	ΣΥΝΟΛΟ					

Β. ΠΛΗΡΟΦΟΡΙΕΣ ΓΙΑ ΤΗΝ ΠΡΟΜΗΘΕΙΑ

Αριθμός Αιτήματος	14479/28-9-2017
ΚΑΕ	7123.01
Κριτήριο Κατακύρωσης	Χαμηλότερη τιμή
Ημερομηνία έναρξης υποβολής προσφορών	06-10-2017
Ημερομηνία λήξης υποβολής προσφορών	**11-10-2017**
Τρόπος υποβολής προσφορών	**ΦΑΞ:2271350241** **e – mail**:paragelies@xioshosp.gr

ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

Προτείνεται η προμήθεια Λογισμικού Αντιικής Προστασίας (όπως το ESET Endpoint Protection Advanced), 150 αδειών χρήσης, με τα παρακάτω γενικά χαρακτηριστικά:

1. Να είναι ενοποιημένη λύση ενός κατασκευαστή.
2. Να παραδοθεί η νεότερη έκδοση της εφαρμογής.

3. Να γίνει ηλεκτρονική παράδοση του λογισμικού.
4. Να περιλαμβάνεται Κονσόλα Κεντρικής Διαχείρισης: εγκατάσταση/ απεγκατάσταση του λογισμικού στα τερματικά, αυτόματη λήψη ενημερώσεων, κεντρική συλλογή συμβάντων, έκδοση αναφορών, κα.
5. Να έχει Εγγύηση – Υποστήριξη (είτε on demand, είτε προληπτικά) για το σύνολο των ετών ισχύος του λογισμικού.
6. Να έχει δυνατότητα για εξαίρεση συγκεκριμένων, απειλών, συγκεκριμένων αρχείων, επεκτάσεων και φακέλων, κλπ.
7. Το παρεχόμενο λογισμικό να διαθέτει κατάλληλο μηχανισμό προστασίας του δικτύου από κακόβουλο λογισμικό που προέρχεται από αφαιρούμενες συσκευές – μέσα (USB STICK,DVD,CD,EXTERNAL HDD κλπ).
8. Να υπάρχει η δυνατότητα εγκατάστασης βάση επιλογής τερματικού ή αποκλεισμού εγκατάστασης βάση επιλογής υπολογιστή.
9. Να υπάρχει η δυνατότητα on demand scan από τους χρήστες.
10. Η εφαρμογή να διαθέτει εξελιγμένη ευρετική μηχανή προς εξουδετέρωση άγνωστων ιών.
11. Η εφαρμογή να διαθέτει τεχνολογία αυτόματης ανάλυσης συμπεριφοράς των εφαρμογών και να εξουδετερώνει τυχόν ύποπτες δραστηριότητες.
12. Η εταιρεία για τον χρόνο ισχύος της σύμβασης, υποχρεούται σε κάθε νέα έκδοση της εφαρμογής και της κονσόλας διαχείρισης να την εγκαθιστά χωρίς οικονομική επιβάρυνση, μετά από συνεννόηση με το Τμήμα Πληροφορικής.

Α/Α	**ΠΡΟΔΙΑΓΡΑΦΗ**
1	**Γενικά**
1.1	Για την προστασία από κακόβουλο λογισμικό στα τερματικά και τους εξυπηρετητές του έργου θα προσφερθούν άδειες antivirus χρονικής διάρκειας **τριών (3)** ετών
1.2	Να αναφερθεί ο Κατασκευαστής και ο τύπος
1.3	Υποστήριξη για τις εξής πλατφόρμες λειτουργικών συστημάτων: - Microsoft Windows: XP, Vista, 7, 8, 10 - Microsoft Windows Server 2003(R2), 2008(R2), 2012(R2), 2016 - Linux με kernel 2.6.x και νεότερα - Mac OS X - Android 4 ή νεότερο
2	**Εξειδίκευση των απαιτήσεων προστασίας**
2.1	Δυνατότητα ανίχνευσης και καθαρισμού όλων των τύπων απειλών: viruses, trojans, dialers, spyware, jokes, hoaxes
2.2	Δυνατότητα αυτόματης ανίχνευσης & καθαρισμού των προαναφερθέντων απειλών σε πραγματικό χρόνο
2.3	Δυνατότητα επιλογής ανίχνευσης malware σε δικτυακές τοποθεσίες, on-demand και σε πραγματικό χρόνο
2.4	Να παρέχεται cloud reputation database για αμεσότερη προστασία από νέες απειλές
2.5	Υποστήριξη τεχνολογίων Advanced heuristics/ DNA/ Smart Signatures για δυνατότητα ανίχνευσης άγνωστων ιών
2.6	Δυνατότητα για host intrusion prevention system
2.7	Η ανανέωση των signature files να είναι incremental
2.8	Δυνατότητα Rollback των Signature Files σε προηγούμενη έκδοση του με ταυτόχρονη παύση των ενημερώσεων, επιλέγοντας το κεντρικά ή απευθείας από το client
2.9	Δυνατότητα κατεβάσματος ενημερώσεων με νεότερες engines που βρίσκονται σε δοκιμαστικό στάδιο, επιλέγοντας το κεντρικά ή απευθείας από το client
2.10	Δυνατότητα να μπορεί να γίνει ένα client update server για τα υπόλοιπα clients του δικτύου χωρίς την εγκατάσταση τμήματος της κονσόλας διαχείρισης ή άλλου εξωτερικού software
2.11	Δυνατότητα για SSL/TLS filtering στα πρωτόκολλα HTTPS, IMAPS, POP3S
2.12	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.
2.13	Δυνατότητα προστασίας σε δικτυακό επίπεδο με client based Firewall, με δυνατότητα φιλτραρίσματος σε επίπεδο θυρών και εφαρμογών σε εισερχόμενες και εξερχόμενες συνδέσεις.
2.14	Δυνατότητα ανίχνευσης και αποτροπής botnet malware
2.15	Δυνατότητα εξαγωγής των ρυθμίσεων ενός client σε αρχείο και εισαγωγής των ρυθμίσεων σε άλλο client από το ίδιο αρχείο.
2.16	Να υπάρχει ενσωματωμένη εφαρμογή που να καταγράφει την κατάσταση του συστήματος (εφαρμογές, processes, services, κα) – κατόπιν εντολής τοπικά ή από την κονσόλα - σε μία χρονική στιγμή (snapshot) και να αποθηκεύει τα αποτελέσματα για σύγκριση τους με την κατάσταση του συστήματος από διαφορετική χρονική στιγμή.

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ
2.17	Παροχή Bootable Media που να περιέχει το antivirus ώστε να δίνει τη δυνατότητα για καθαρισμό του συστήματος χωρίς να χρειάζεται να ξεκινήσει το λειτουργικό σύστημα
3	**Απαιτήσεις απομακρυσμένης και κεντρικής διαχείρισης**
3.1	Κεντρική διαχείριση όλων των clients των τερματικών και servers
3.2	Υποστήριξη πολλαπλών ομάδων και υπο-ομάδων με δυνατότητα εφαρμογής διαφορετικών πολιτικών για κάθε περίπτωση
3.3	Λειτουργία προσωρινής απενεργοποίησης πολιτικής ανά client
3.4	Δυνατότητα για ομάδες διαχείρισης με βάση ιδιότητες υπολογιστών, π.χ. αυτόματη ομαδοποίηση υπολογιστών με Windows 10
3.5	Εγκατάσταση &απεγκατάσταση της προστασίας μέσω κεντρικής κονσόλας (Remote deployment)
3.6	Να υπάρχει η δυνατότητα εξαγωγής ενιαίου πακέτου με το πρόγραμμα προστασίας, σύνδεση διαχείρισης, πολιτικές και την άδεια ενεργοποίησης
3.7	Να παρέχεται ξεχωριστό εργαλείο ανίχνευσης τερματικών και push εγκατάστασης του παραπάνω ενιαίου πακέτου
3.8	Επικοινωνία του software μόνο με IP, δηλαδή να δουλέψει σε περιπτώσεις όπου δεν υπάρχουν υπηρεσίες ονοματοδοσίας (DNS servers)
3.9	Να μπορεί να γίνει αυτόματη ανίχνευση των τερματικών που βρίσκονται στο τοπικό δίκτυο, ακόμα κι αν αυτά δεν ανήκουν σε Active Directory
3.10	Να μπορεί να γίνει εισαγωγή λίστας των τερματικών του δικτύου με τη χρήση CSV αρχείου
3.11	Η επικοινωνία των servers και των clients να διασφαλίζεται μέσω certificate
3.12	Να μπορεί να γίνει ενεργοποίηση σε δίκτυο χωρίς σύνδεση στο internet (offline activation)
3.13	Να γίνεται ενημέρωση από το Internet από κεντρικό σημείο, από το οποίο στην συνέχεια θα ενημερωθούν όλοι οι clients του δικτύου
3.14	Τα antivirus να μπορούν να λάβουν signature files μέσω HTTP proxy cache, με αυτόματη παράκαμψή του σε περίπτωση που δεν είναι διαθέσιμος ο proxy server
3.15	Να περιλαμβάνεται έλεγχος και ειδοποίηση για το αν υπάρχουν ενημερώσεις για το λειτουργικό σύστημα, καθώς και η δυνατότητα να δοθεί εντολή ενημέρωσης λειτουργικού συστήματος
3.16	Παρακολούθηση όλων των clients και παραγωγή reports και στατιστικών σε πολλές μορφές (Προγραμματισμένα emails, PDF, PS, CSV, Charts)
3.17	Δυνατότητα ενιαίας καραντίνας αρχείων που ανιχνεύθηκαν για όλο το δίκτυο, με δυνατότητες προβολής clients ανά απειλή, εξαγωγή και εξαίρεση
3.18	Ο server διαχείρισης να 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
3.19	Η εγκατάσταση της βάσης δεδομένων της κονσόλας θα πρέπει απαραίτητα να γίνεται σε ένα υπολογιστή οπουδήποτε στο εσωτερικό δίκτυο της εταιρίας και όχι σε εξωτερικό δίκτυο π.χ. Cloud.
3.20	Να παρέχεται εργαλείο ελέγχου κατάστασης αδειών και αριθμού ενεργοποιήσεων, ακόμα κι αν αυτές έχουν γίνει εκτός της κεντρικής κονσόλας. (standalone εγκαταστάσεις)
3.21	Να παρέχεται η δυνατότητα διαχείρισης Android και iOS συσκευών μέσω της ίδιας κονσόλας
3.22	Να παρέχεται η δυνατότητα agentless προστασίας μηχανημάτων σε περιβάλλον VMWare χωρίς εγκατάσταση λογισμικού antivirus στο λειτουργικό σύστημα του εικονικού μηχανήματος
3.23	Η είσοδος στην κονσόλα διαχείρισης να μπορεί να κλειδωθεί με πιστοποίηση διπλού παράγοντα (2-factor authentication)
3.24	Δυνατότητα εξαγωγής των logs και events σε εξωτερικό σύστημα Syslog/ SIEM με την υποστήριξη του IBM QRadar
3.25	Το μενού της κονσόλας διαχείρισης και του antivirus για τα workstations να διατίθεται και στην Ελληνική γλώσσα

Γ. ΥΠΟΧΡΕΩΤΙΚΑ ΣΤΟΙΧΕΙΑ ΠΡΟΣΦΟΡΑΣ

Οι τιμές των προσφερόμενων ειδών 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	**Κωδικός Νοσοκομείου**	**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 των προσφερόμενων ειδών. Λόγω του επείγοντος της προμήθειας, το νοσοκομείο επιθυμεί τα προσφερόμενα είδη 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.

Οι εταιρείες που θα αποστείλουν προσφορά για ιατροτεχνολογικά προϊόντα θα πρέπει απαραίτητα να διαθέτουν τα νόμιμα πιστοποιητικά για τη διακίνηση και διανομή τους, και τα είδη θα πρέπει απαραίτητα να φέρουν την αντίστοιχη πιστοποίηση CE.

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.

Τέλος το νοσοκομείο διατηρεί το δικαίωμα να ζητήσει δείγμα προκειμένου να αξιολογήσει τις προσφορές και οι συμμετέχουσες εταιρείες υποχρεούνται - επί ποινή απόρριψης – να το αποστείλουν άμεσα.

Η ΔΙΟΙΚΗΤΡΙΑ

Ε. ΚΑΝΤΑΡΑΚΗ