**ΕΝΤΥΠΟ TEXNIKH ΠΡΟΣΦΟΡΑΣ**

Της ατομικής επιχείρησης / ημεδαπούς νομικού προσώπου ……………………………με έδρα τ Οδός Αριθ Τ.Κ Τηλ.

Fax Email:

Αφού έλαβα γνώση των όρων της μελέτης για την προμήθεια με τίτλο :

**«Προμήθεια εξοπλισμού και λογισμικού πληροφορικής»**

Αφού έλαβα γνώση των όρων της διακήρυξης του διαγωνισμού που αναγράφεται στον τίτλο & των λοιπών στοιχείων της μελέτης, υποβάλλω την παρούσα προσφορά και δηλώνω ότι - Τα προσφερόμενα είδη πληρούν τις προδιαγραφές της μελέτης. Αποδέχομαι πλήρως και χωρίς επιφύλαξη όλα αυτά και αναλαμβάνω την εκτέλεση της προμήθειας με τις ακόλουθες τεχνικές προδιαγραφές.

1. **Τεχνικές Προδιαγραφές Ομάδας Α plotter/scanner σχεδίων**

Αναλυτικά, το Plotter θα πρέπει να έχει τις παρακάτω ελάχιστες τεχνικές προδιαγραφές:

|  |  |  |
| --- | --- | --- |
| Α/Α | Είδος | Ελάχιστα Τεχνικά Χαρακτηριστικά |
| 1. | Σχεδιαγράφος (Plotter) | * Ασπρόμαυρη / Έγχρωμη εκτύπωση * Πλάτος υλικών εκτύπωσης: 917mm * Πάχος Υλικών: Ρολό/Φύλλο: 0.07-0.8mm * Χρώματα: 5 * Ανάλυση Εκτύπωσης: 2.400 Χ 1.200 dpi * Ακρίβεια Γραμμής: +- 0,1% ή λιγότερο * Βήμα ακροφυσίων: 1200dpi X 2 * Σύστημα ανίχνευσης και αντιστάθμισης αδρανών ακροφυσίων: ΝΑΙ * Παρεχόμενα Αρχικά μελάνια:330ml για όλα τα χρώματα. * Συμβατότητα με λειτ. Συστήματα: 32bit και 64bit WIN7, WIN10, WIN11. * Μνήμη: 128GB (φυσική μνήμη 2GB) * Σκληρός Δίσκος: 500GB * Ταχύτητα Εκτύπωσης σχεδίου CAD. Για χαρτί Α1: 0:18 (Κατάσταση γρήγορης οικονομικής λειτουργίας) 3,2 σελ/ λεπτό. Για χαρτί Α0: 0:34 (Κατάσταση γρήγορης οικονομικής λειτουργίας, 0:37 (γρήγορη), 1:04 (Στάνταρ) * Ταχύτητα Εκτύπωσης σχεδίου Πόστερ Για χαρτί Α0 0:37 (Κατάσταση γρήγορη οικονομικής εκτύπωσης), 0:42 (Γρήγορη), 1:15 (Στανταρ). * Ethernet: 10/100/1000 base-T * Wireless LAN: IEEE802.11n/IEEE802.11g/IEEE802.11b * Θα πρέπει να περιλαμβάνει και 2 επιπλέον σειρές μελάνια όλων των χρωμάτων των 330ml * Θα πρέπει να περιλαμβάνει ένα Maintenance Cartridge KIT |
|  |  | * Ασπρόμαυρη / Έγχρωμη εκτύπωση * Print/Copy/Scan * Τεχνολογία Σάρωσης: SingleSensor * Οπτική ανάλυση (dpi): 1200dpi * Πλάτος Σάρωσης: 914mm * Ελάχιστο πλάτος Σάρωσης: 150mm * Ταχύτητα Σάρωσης, κλίμακα του γκρι και μονόχρωμα 8-bit στα 200dpi: 13’’/sec * Σάρωση σε PC: Ταχύτητα σάρωσης χρώμα 24 bit στα 200 dpi: 3’’/sec * H συσκευασία του Σαρωτή θα πρέπει να περιλαμβάνει όλα τα απαραίτητα για τη σύνδεση του σαρωτή με τον plotter. * Σύστημα:Win10 * SSD: 256GB * RAM: 8GB DDR4 * Οθόνη: Αφής * 3ΧUSB3 * 1XUSB2 * Χρώματα: 5 ΜΒΚ/ΒΚ/C/M/Y * χρόνος ανταπόκρισης σε βλάβη 1 ώρα * Εγκατάσταση και επίδειξη εξοπλισμού |
|  |  | * Εγγύηση: 2 Χρόνια |

1. **Τεχνικές Προδιαγραφές Ομάδας Β Λογισμικού Προστασίας από Ιούς (Anti-Virus)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A/A** | **ΠΡΟΔΙΑΓΡΑΦΗ** | **ΑΠΑΙΤΗΣΗ** | **ΑΠΑΝΤΗΣΗ** | **ΠΑΡΑΠΟΜΠΗ ΤΕΚΜΗΡΙΩΣΗΣ** |
| **1** | **Γενικά** |  |  |  |
| 1.1 | Να αναφερθεί ο κατασκευαστής και το όνομα/έκδοση του λογισμικού προστασίας από ιούς. | ΝΑΙ |  |  |
| 1.2 | Το λογισμικό προστασίας να υποστηρίζει τα εξής λειτουργικά συστήματα:  MS Windows 8, 10  MS Windows Server 2008, 2012, 2016  Linux (kernel 2.6.x και νεότερο), MAC OS X | NAI |  |  |
| 1.3 | Οι ελάχιστες απαιτήσεις συστήματος να είναι 0.3 GB ελεύθερη διαθέσιμη μνήμη (RAM) και 1 GB ελεύθερος χώρος στον σκληρό δίσκο. | ΝΑΙ |  |  |
| **2** | **Αντιική Προστασία** |  |  |  |
| 2.1 | Η εγκατάσταση της κεντρικής βάσης malware θα γίνει σε server στο εσωτερικό δίκτυο του φορέα και όχι σε εξωτερικό δίκτυο (πχ στο cloud ή σε server που είναι εγκατεστημένος σε server εκτός εγκαταστάσεων του φορέα). Να προσφερθούν όλα τα απαραίτητα για τον εν λόγω server (φυσικό ή εικονικό). | ΝΑΙ |  |  |
| 2.2 | Να υπάρχει η δυνατότητα ο κεντρικός Server να παρασχεθεί σε μορφή εικονικής μηχανής (VM Appliance). | ΝΑΙ |  |  |
| 2.3 | Να υποστηρίζεται ανίχνευση και καθαρισμός όλων των τύπων απειλών malware: viruses, malware, trojans, dialers, spyware, jokes, hoaxes,ransomware. | ΝΑΙ |  |  |
| 2.4 | Να υποστηρίζεται αυτόματη ανίχνευση και καθαρισμός των προαναφερθέντων απειλών σε πραγματικό χρόνο. | ΝΑΙ |  |  |
| 2.5 | Να υποστηρίζεται on-demand ανίχνευση και καθαρισμός των προαναφερθέντων απειλών. | ΝΑΙ |  |  |
| 2.6 | Να υποστηρίζεται IPS (intrusion prevention system). | ΝΑΙ |  |  |
| 2.7 | Να υποστηρίζονται τεχνολογίες advanced heuristics (ενδεικτικά: DNA, smart signatures, Behavioral Analysis) για δυνατότητα ανίχνευσης άγνωστου malware. | ΝΑΙ |  |  |
| 2.8 | Προστασία για SSL/TLS filtering στα πρωτόκολλα HTTPS, IMAPS, POP3S. | ΝΑΙ |  |  |
| 2.9 | Δυνατότητα αποτροπής γνωστών exploits | ΝΑΙ |  |  |
| 2.10 | 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. | ΝΑΙ |  |  |
| 2.11 | Δυνατότητα προστασίας σε δικτυακό επίπεδο με client based Firewall, με δυνατότητα φιλτραρίσματος σε επίπεδο θυρών και εφαρμογών σε εισερχόμενες και εξερχόμενες συνδέσεις. | ΝΑΙ |  |  |
| 2.12 | Δυνατότητα προστασίας από δικτυακές απειλές και botnets | ΝΑΙ |  |  |
| 2.13 | Δυνατότητα ενιαίας καραντίνας αρχείων που ανιχνεύθηκαν για όλο το δίκτυο, με δυνατότητες προβολής clients ανά απειλή, εξαγωγή και εξαίρεση | ΝΑΙ |  |  |
| 2.14 | Δυνατότητα προστασίας απο Brute Force Attack | ΝΑΙ |  |  |
| **3** | **Κεντρική διαχείριση** |  |  |  |
| 3.1 | Να υποστηρίζεται η κεντρική διαχείριση όλων των λογισμικών προστασίας των σταθμών εργασίας / servers (antivirus client) μέσω κεντρικής κονσόλας. | ΝΑΙ |  |  |
| 3.2 | Να υποστηρίζεται η δημιουργία πολλαπλών ομάδων με δυνατότητα εφαρμογής διαφορετικών πολιτικών / ρυθμίσεων για κάθε ομάδα. | ΝΑΙ |  |  |
| 3.3 | Λειτουργία προσωρινής απενεργοποίησης πολιτικής ανά client | ΝΑΙ |  |  |
| 3.4 | Να υποστηρίζεται η διαχείριση των ιστοσελίδων (επιτρεπόμενες, μη επιτρεπόμενες) σε ένα σταθμό εργασίας / server όπου είναι εγκατεστημένος ο antivirus client. | ΝΑΙ |  |  |
| 3.5 | Να υποστηρίζεται η αυτόματη ανίχνευση των σταθμών εργασίας που βρίσκονται στο τοπικό δίκτυο δεδομένων ακόμα κι αν αυτά δεν ανήκουν σε υπηρεσία ενεργού καταλόγου. | ΝΑΙ |  |  |
| 3.6 | Να υποστηρίζεται η εγκατάσταση και απεγκατάσταση του λογισμικού προστασίας (antivirus client) μέσω της κεντρικής κονσόλας. | ΝΑΙ |  |  |
| 3.7 | Να υποστηρίζεται ενεργοποίηση άδειας antivirus client σε σταθμό εργασίας ή server μέσω δικτύου χωρίς σύνδεση στο διαδίκτυο internet (offline activation). | ΝΑΙ |  |  |
| 3.8 | Να υπάρχει η δυνατότητα εξαγωγής πακέτου με το πρόγραμμα προστασίας, διαχείρισης, τις αντίστοιχες πολιτικές - ρυθμίσεις τους και την άδεια ενεργοποίησης για τοπικές εγκαταστάσεις. | ΝΑΙ |  |  |
| 3.9 | Να μπορεί να γίνει εισαγωγή λίστας των υπολογιστών του δικτύου με τη χρήση ενδεικτικά CSV αρχείου ή text file ή Active Directory Scan ή Active Directory import ή Network Pool ή IP range κτλ. | ΝΑΙ |  |  |
| 3.10 | Να υποστηρίζεται έλεγχος και ειδοποίηση στην κεντρική κονσόλα για το αν υπάρχουν ενημερώσεις για λειτουργικά συστήματα Windows των σταθμών εργασίας / server όπου είναι εγκατεστημένος ο antivirus client. | ΝΑΙ |  |  |
| 3.11 | Να υποστηρίζεται η παρακολούθηση όλων των antivirus client και η παραγωγή αναφορών και στατιστικών σε μορφές (ενδεικτικά) PDF, PS, CSV, Charts καθώς και η αποστολή αυτοματοποιημένων emails των προαναφερόμενων αναφορών/στατιστικών. | ΝΑΙ |  |  |
| 3.12 | Η επικοινωνία του κεντρικού server και των antivirus clients θα διασφαλίζεται μέσω certificate. | ΝΑΙ |  |  |
| 3.13 | Να υπάρχει η δυνατότητα αυτόματων αναβαθμίσεων του προϊόντος. | ΝΑΙ |  |  |
| **4** | **Ενημερώσεις** |  |  |  |
| 4.1 | Οι ενημερώσεις από το διαδίκτυο για της κεντρικής βάσης malware θα γίνονται αυτόματα σε κεντρικό σημείο (server διαχείρισης) από το οποίο στην συνέχεια θα ενημερώνονται όλοι οι σταθμοί εργασίας και οι servers. Σε περίπτωση που δεν είναι διαθέσιμος ο server διαχείρισης, να υποστηρίζεται αυτόματη παράκαμψή του. | ΝΑΙ |  |  |
| 4.2 | Οι προαναφερόμενες ενημερώσεις θα προσφέρονται έως τη λήξη της περιόδου εγγυημένης λειτουργίας προμήθειας. | ΝΑΙ |  |  |
| 4.3 | Rollback σε προηγούμενη έκδοση του Signature File με ταυτόχρονη παύση των ενημερώσεων, επιλέγοντας το κεντρικά ή απευθείας από τον client. | ΝΑΙ |  |  |
| 4.4 | Να παρέχεται cloud reputation database για αμεσότερη προστασία από νέες απειλές. | ΝΑΙ |  |  |
| **5** | **On boot scan** |  |  |  |
| 5.1 | Να υποστηρίζεται σάρωση και καθαρισμός κατά την εκκίνηση του σταθμού εργασίας / server (on-boot scan) χωρίς να χρειάζεται να ξεκινήσει το λειτουργικό σύστημα. | ΝΑΙ |  |  |
| **6** | **Ειδικές απαιτήσεις** |  |  |  |
| 6.1 | Να υποστηρίζεται η εξαγωγή των ρυθμίσεων ενός antivirus client σε αρχείο και εισαγωγής των ρυθμίσεων σε άλλον από το ίδιο αρχείο. | ΝΑΙ |  |  |
| 6.2 | Να υποστηρίζεται η προστασία εικονικών μηχανών σε περιβάλλον VMWare χωρίς εγκατάσταση λογισμικού προστασίας (agent / antivirus client) στο λειτουργικό σύστημα της κάθε εικονικής μηχανής είτε με την εγκατάσταση ενός light agent. | ΝΑΙ |  |  |
| 6.3 | Να περιέχεται εφαρμογή που να καταγράφει την κατάσταση των agents / antivirus clients (εφαρμογές, processes, services κ.α) σε μία χρονική στιγμή (snapshot) και προαιρετικά να μπορεί να γίνει σύγκριση με προηγούμενη κατάσταση. | ΝΑΙ |  |  |
| 6.4 | Επικοινωνία του software μόνο με IP δηλαδή να δουλέψει σε περιπτώσεις όπου δεν υπάρχουν υπηρεσίες ονοματοδοσίας (DNS server). | ΝΑΙ |  |  |
| 6.5 | Το μενού της κονσόλας διαχείρισης και των antivirus clients για τους σταθμούς εργασίας να διατίθεται και στην ελληνική γλώσσα και να γίνει εκπαίδευση χρήσης στους υπευθύνους υπαλλήλους του Δήμου | ΝΑΙ |  |  |

**Λογισμικό κρυπτογράφησης**

| **ive** | **ΠΡΟΔΙΑΓΡΑΦΗ** | **ΑΠΑΙΤΗΣΗ** | **ΑΠΑΝΤΗΣΗ** | **ΠΑΡΑΠΟΜΠΗ ΤΕΚΜΗΡΙΩΣΗΣ** |
| --- | --- | --- | --- | --- |
| **1** | **Γενικά** |  |  |  |
| 1.1 | Να αναφερθεί ο Κατασκευαστής και ο τύπος | NAI |  |  |
| 1.2 | Υποστήριξη για τις εξής πλατφόρμες λειτουργικών συστημάτων:  - Microsoft Windows 10, 8.1, 8, 7  - Microsoft Windows Server 2019, 2016, 2012R2, 2012, 2008R2 | ΝΑΙ |  |  |
| 1.3 | Υποστήριξη των παρακάτω αλγόριθμων κρυπτογράφησης:  - AES 128 bit - 256 bit File & Folder RME  - Triple DES 112dit  - Blowfish 128 bit  - Password encryption με 192-bit AES key | ΝΑΙ |  |  |
| **2** | **Εξειδίκευση των απαιτήσεων κρυπτογράφησης** |  |  |  |
| 2.1 | Δυνατότητα κρυπτογράφησης επιλεγμένων φακέλων | ΝΑΙ |  |  |
| 2.2 | Δυνατότητα δημιουργίας κρυπτογραφημένων εικονικών δίσκων | ΝΑΙ |  |  |
| 2.3 | Η κρυπτογράφηση νέων αρχείων να γίνεται με τη μετακίνησή τους στο φάκελο ή τον εικονικό δίσκο | ΝΑΙ |  |  |
| 2.4 | Το άνοιγμα και η επεξεργασία των κρυπτογραφημένων αρχείων να γίνεται διάφανα από το χρήστη χωρίς επιπλέον διαδικασίες | ΝΑΙ |  |  |
| 2.5 | Δυνατότητα κρυπτογράφησης μεμονωμένων αρχείων για αποστολή μέσω email ή μεταφορά σε εξωτερικά μέσα | ΝΑΙ |  |  |
| 2.6 | Δυνατότητα ενσωμάτωσης σε Microsoft Outlook για αποστολή κρυπτογραφημένων emails | ΝΑΙ |  |  |
| 2.7 | Η κρυπτογράφηση των emails να γίνεται με κλειδί κρυπτογράφησης ή με κωδικό password | ΝΑΙ |  |  |
| 2.8 | Παροχή δωρεάν λογισμικού αποκρυπτογράφησης των emails με password από τρίτους εξουσιοδοτημένους χρήστες | ΝΑΙ |  |  |
| 2.9 | Δυνατότητα κρυπτογράφησης usb flash disk/hard drives και οπτικών μέσων CD/DVD |  |  |  |
| 2.10 | Δυνατότητα κρυπτογράφησης απλού κειμένου | ΝΑΙ |  |  |
| 2.11 | Παροχή εργαλείου ασφαλούς διαγραφής αρχείων | ΝΑΙ |  |  |
| **3** | **Απαιτήσεις απομακρυσμένης και κεντρικής διαχείρισης** |  |  |  |
| 3.1 | Παροχή Web κονσόλας διαχείρισης των τερματικών και χρηστών | ΝΑΙ |  |  |
| 3.2 | Δυνατότητα διαχείρισης τερματικών μέσω cloud και τοπικού δικτύου | ΝΑΙ |  |  |
| 3.3 | Δυνατότητα σύνδεσης με Active Directory | ΝΑΙ |  |  |
| 3.4 | Δυνατότητα δημιουργίας πολλαπλών κλειδιών κρυπτογράφησης | ΝΑΙ |  |  |
| 3.5 | Τα κλειδιά κρυπτογράφησης να έχουν τη δυνατότητα διαμοιρασμού μεταξύ χρηστών (shared keys) | ΝΑΙ |  |  |
| 3.6 | Δυνατότητα δημιουργίας ομάδων χρηστών και τερματικών | ΝΑΙ |  |  |
| 3.7 | Δυνατότητα ορισμού πολιτικών ανά ομάδα | ΝΑΙ |  |  |
| 3.8 | Δυνατότητα εύρεσης τερματικών και απομακρυσμένης εγκατάστασης του λογισμικού κρυπτογράφησης | ΝΑΙ |  |  |

**Λογισμικό καταγραφής**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Α/Α** | **ΠΡΟΔΙΑΓΡΑΦΗ** | **ΑΠΑΙΤΗΣΗ** | **ΑΠΑΝΤΗΣΗ** | **ΠΑΡΑΠΟΜΠΗ ΤΕΚΜΗΡΙΩΣΗΣ** |
| **1** | **Γενικά** |  |  |  |
| 1.1 | Να αναφερθεί ο Κατασκευαστής και ο τύπος |  |  |  |
| 1.2 | Υποστήριξη για τις εξής πλατφόρμες: - Υποστήριξη Windows 7, 8.1 και 10 | ΝΑΙ |  |  |
| -                      Υποστήριξη macOS 10.15 και νεότερο |
| -                      Microsoft Windows Server 2012 και νεότερο |
| -                      Υποστήριξη MS SQL 2012 database server και νεότερο, MS SQL Express 2016 και νεότερο, Azure SQL |
| 1.3 | Integration με Microsoft Active Directory | ΝΑΙ |  |  |
| 1.4 | Υποστήριξη οπτικής αναγνώρισης χαρακτήρων(OCR) | ΝΑΙ |  |  |
| 1.5 | Να μην απαιτείται αγορά λογισμικού τρίτου κατασκευαστή για τη λειτουργία του, π.χ. για βάσεις δεδομένων κλπ. | ΝΑΙ |  |  |
| **2** | **Εξειδικευμένες Απαιτήσεις** |  |  |  |
| 2.1 | Υποστήριξη Microsoft terminal server | ΝΑΙ |  |  |
| 2.2 | Προσαρμόσιμη κεντρική κονσόλα διαχείρισης | ΝΑΙ |  |  |
| 2.3 | Προσαρμόσιμα δικαιώματα πρόσβασης σε αναφορές, ρυθμίσεις και διαχείριση δικαιωμάτων των διαχειριστών | ΝΑΙ |  |  |
| 2.4 | Δυνατότητα απόκρυψης εγκατάστασης και διεργασιών από χρήστες και διαχειριστές | ΝΑΙ |  |  |
| 2.5 | Προστασία τερματισμού διεργασίας του λογισμικού προστασίας από χρήστες ή διαχειριστές | ΝΑΙ |  |  |
| 2.6 | Προστασίας ανεπιθύμητης απεγκατάστασης του λογισμικού προστασίας | ΝΑΙ |  |  |
| 2.7 | Δυνατότητα αποτροπής έναρξης του συστήματος σε ασφαλή λειτουργία | ΝΑΙ |  |  |
| 2.8 | Η προστασία να ισχύει ακόμα κι όταν το τερματικό είναι offline, ή συνδεδεμένο σε άλλο δίκτυο | ΝΑΙ |  |  |
| 2.9 | Η σουίτα να διαθέτει ενσωματωμένη δυνατότητα backup στοιχείων εφαρμογής, καταγραφών και των πολιτικών | ΝΑΙ |  |  |
| 2.10 | Ειδοποίηση με email σε περίπτωση συμβάντων, με δυνατότητα ρύθμισης επιπέδου ευαισθησίας και ιδιοτήτων συμβάντων | ΝΑΙ |  |  |
| 2.11 | Αποστολή αναφορών με email με τη δυνατότητα παραμετροποίησης σε πλήρες βαθμό (ποσότητα πληροφοριών, χρήστες, συχνότητα αποστολής, παραλήπτες) | ΝΑΙ |  |  |
| 2.12 | Δυνατότητα αποστολής καταγραφών σε συστήματα SIEM | ΝΑΙ |  |  |
| 2.13 | Να υπάρχει δυνατότητα multi-domain | ΝΑΙ |  |  |
| 2.14 | Να παρέχει εργαλείο πληροφόρησης (κονσόλα) για παρακολούθηση αναφορών από χρήστες χωρίς δικαιώματα διαχειριστή | ΝΑΙ |  |  |
| 2.15 | Να μπορεί να στείλει αρχεία καταγραφής σε σύστημα SIEM | ΝΑΙ |  |  |
| 2.16 | Δυνατότητα διασύνδεσης με FortiGate | ΝΑΙ |  |  |
| 2.17 | Δυνατότητα ενσωμάτωσης με άλλα εργαλεία ανάλυσης δεδομένων μέσω API. (όπως Power BI, Tableau, κτλ) | ΝΑΙ |  |  |
| **3** | **Απαιτήσεις Ελέγχου Ασφάλειας - Πληροφόρησης** |  |  |  |
| 3.1 | Λεπτομερής πληροφόρηση για τον χρόνο εκκίνησης εφαρμογών, καθώς και τον ενεργό χρόνο χρήσης τους. Οι εφαρμογές να κατηγοριοποιούνται ανάλογα τον τύπο τους για ταχύτερη αξιολόγηση | ΝΑΙ |  |  |
| 3.2 | Πληροφόρηση σχετικά με τον ενεργό χρόνο χρήσης ιστοσελίδων, με λεπτομερή πληροφόρηση σχετικά με το URL, πρωτόκολλο και τίτλο ιστοσελίδας, ανεξάρτητα από τον τύπο | ΝΑΙ |  |  |
| 3.3 | φυλλομετρητή που χρησιμοποιείται. Οι ιστοσελίδες να παρουσιάζονται κατηγοριοποιημένες ανάλογα με τον τύπο τους |  |  |  |
| 3.4 | Πληροφόρηση σχετικά με εξωτερικές συσκευές(USB, κινητά τηλέφωνα, εκτυπωτές, κλπ). Οι συσκευές κατηγοριοποιούνται ανάλογα τον τύπο τους για ταχύτερη αξιολόγηση | ΝΑΙ |  |  |
| 3.5 | Πληροφόρηση σχετικά με τις εκτυπώσεις(εκτυπώτές, ετκυπωμένα έγγραφα, αριθμός σελίδων, τύπος εκτύπωσης). Οι εκτυπώσεις κατηγοριοποιούνται ανάλογα τον τύπο τους για ταχύτερη αξιολόγηση | ΝΑΙ |  |  |
| 3.6 | Πληροφόρηση σχετικά με την δικτυακή κίνηση(στατιστικά δικτυακής κίνησης, downloads, uploads,). Οι πληροφορίες κατηγοριοποιούνται ανάλογα με την εφαρμογή, για ταχύτερη αξιολόγηση | ΝΑΙ |  |  |
| 3.7 | Πληροφορίες σχετικά με τα εξερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου(Θέμα, τομέας αποστολέα/παραλήπτη, συννημένα αρχεία,κλπ) | ΝΑΙ |  |  |
| 3.8 | Πληροφορίες σχετικά με λειτουργίες αρχείων(Uploads/Downloads απο το διαδύκτιο, αντιγραφή, αποκοπή, δημιουργία, διαγραφή, άνοιγμα, μεταφορές FTP, κλπ). Στις πληροφορίες υπάρχουν: όνομα αρχείου, ημερομηνία και ώρα, πηγής και προορισμός, κλπ) | ΝΑΙ |  |  |
| 3.9 | Δυνατότητα εξαγωγής αναφορών σε XLS, PDF | ΝΑΙ |  |  |
| 3.10 | Δυνατότητα καταγραφής αποστολής αρχείων μέσω πάσης φύσεως λογισμικών email client και instant messaging | ΝΑΙ |  |  |
| 3.11 | Λεπτομερής πληροφόρηση για την χρήση αρχείων, π.χ. ποιος χρήστης άνοιξε, αντέγραψε, διέγραψε το αρχείο και από που | ΝΑΙ |  |  |
| 3.12 | Καταγραφή αρχείων που εκτυπώθηκαν | ΝΑΙ |  |  |
| 3.13 | Υποστήριξη POP3, IMAP, MAPI / Exchange protocol καθώς και SSL encrypting | ΝΑΙ |  |  |
| 3.14 | Η σουίτα να παρακολουθεί κάθε είδους email client, π.χ. MS Outlook, Thunderbird, κλπ | ΝΑΙ |  |  |
| 3.15 | Καταγραφή κινήσεων HTTP και HTTPS με κάθε είδους φυλλομετρητή | ΝΑΙ |  |  |
| 3.16 | Δραστηριότητα τερματικών: | ΝΑΙ |  |  |
| - Καταγραφή εκκίνησης/τερματισμού υπολογιστή |
| - Καταγραφή εισόδου/εξόδου λογαριασμών υπολογιστή |
| - Καταγραφή λειτουργίας sleep/wake up |
| 3.17 | Δραστηριότητα δικτύου: | ΝΑΙ |  |  |
| - Καταγραφή όγκου απεσταλμένων/ληφθέντων δεδομένων |
| 3.18 | Δυνατότητα παρακολούθησης αρχείων στην υπηρεσία Office 365 | ΝΑΙ |  |  |
| **4** | **Δυνατότητες κατηγοριοποίησης / ευρετηρίασης** |  |  |  |
| 4.1 | Κατηγοριοποίηση αρχείων με βάση την τοποθεσία τους, είτε είναι τοπική ή δικτυακή | ΝΑΙ |  |  |
| 4.2 | Κατηγοριοποίηση αρχείων που εξάγονται από web εφαρμογές, π.χ. Intranet site | ΝΑΙ |  |  |
| 4.3 | Κατηγοριοποίηση αρχείων που εξάγονται από Windows εφαρμογές, π.χ. σουΐτα ERP | ΝΑΙ |  |  |
| 4.4 | Δυνατότητα κατηγοριοποίησης αρχείων απο τον χρήστη (Userbased data classification) | ΝΑΙ |  |  |
| 4.5 | Ανίχνευση αρχείων που περιέχουν ευαίσθητες πληροφορίες, όπως αριθμούς πιστωτικών καρτών, IBAN, αριθμό ΑΜΚΑ κλπ | ΝΑΙ |  |  |
| 4.6 | Δυνατότητα ορισμού keywords ή regular expressions για την κατηγοριοποίηση αρχείων | ΝΑΙ |  |  |
| **5** | **Δυνατότητες προστασίας** |  |  |  |
| 5.1 | Μετά την κατηγοριοποίηση ευαίσθητων δεδομένων να μπορεί να περιοριστεί η μετακίνηση και η επεξεργασία αυτών. Π.χ. επιτρεπόμενα μέσα για μεταφορές, επιτρεπόμενες ιστοσελίδες για μεταφόρτωση, επιτρεπόμενοι παραλήπτες email, επιτρεπόμενα λογισμικά επεξεργασίας | ΝΑΙ |  |  |
| 5.2 | Δυνατότητα ορισμού πολιτικών για συγκεκριμένες εφαρμογές ή πηγές, π.χ. συγκεκριμένα δεδομένα, πρόσβαση σε εξωτερικές συσκευές, δίκτυο | ΝΑΙ |  |  |
| 5.3 | Δυνατότητες εφαρμογής κανόνων σε λειτουργία δοκιμής, ενημέρωσης ή αποτροπής | ΝΑΙ |  |  |
| 5.4 | Αποτροπή ενεργειών σε αρχεία, όπως αντιγραφή, μετακίνηση, μεταφόρτωση στο Web, σε FTP, σε εξωτερική συσκευή, με αναφορά πηγής και προορισμού, τη διαδρομή, τύπο συσκευών | ΝΑΙ |  |  |
| 5.5 | Αποτροπή αντιγραφής μέσω clipboard και screen capture | ΝΑΙ |  |  |
| 5.6 | Κρυπτογράφηση: | ΝΑΙ |  |  |
| -                      Δυνατότητα Full Disk Encryption μέσω BitLocker service, όπου αυτό είναι διαθέσιμο |
| -                      Κρυπτογράφηση δίσκων USB Flash μέσω BitLocker |
| 5.7 | Device Control: | ΝΑΙ |  |  |
| -                      Ολικός περιορισμός σε συσκευές USB, firewire, κάρτες μνήμης, LPT, COM, Bluetooth, CD, DVD, Blue-ray - |
| Δυνατότητα read-only λειτουργίας συσκευών |
| -                      Καταγραφή συνδέσεων εξωτερικών συσκευών |
| 5.8 | Δυνατότητα application control για την αποτροπή εκτέλεσης ορισμένων κατηγοριών λογισμικών | ΝΑΙ |  |  |
| 5.9 | Δυνατότητα web control για την αποτροπή επίσκεψης σε ορισμένες κατηγορίες ιστοσελίδων | ΝΑΙ |  |  |
| 5.10 | Δυνατότητα print control για προσαρμογή ορίων εκτύπωσης σε χρήστες | ΝΑΙ |  |  |