

ΕΠΙΤΡΟΠΗ ΚΑΤΑΡΤΙΣΗΣ ΣΧΕΔΙΟΥ ΤΕΥΧΟΥΣ ΤΕΧΝΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ ΓΙΑ ΤΗΝ ΠΡΟΜΗΘΕΙΑ ΟΛΟΚΛΗΡΩΜΕΝΟΥ ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΕΦΑΡΜΟΓΗΣ ΠΟΛΙΤΙΚΩΝ ΠΡΟΣΤΑΣΙΑΣ ΜΕ ΣΚΟΠΟ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΤΗ ΔΙΑΡΡΟΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ (DATA LOSS PREVENTION) ΔΙΚΤΥΟΥ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

Συστήθηκε και λειτούργησε με την υπ' αριθμ. 8028/1/304 από 13-01-2016 Απόφαση κ. Γενικού Γραμματέα Δημόσιας Τάξης (ΑΔΑ: ΩΜΣ1465ΦΘΕ-ΑΡΣ) και λειτουργεί με την υπ' αριθμ. 8028/1/304-στ' από 12-09-2016 Απόφαση Επανασύστασης Επιτροπής κ. Γενικού Γραμματέα Δημόσιας Τάξης (ΑΔΑ: 6ΝΤΚ465ΦΘΕ-Β77)

ΣΧΕΔΙΟ ΤΕΥΧΟΥΣ ΤΕΧΝΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ

1. ΣΚΟΠΟΣ ΠΡΟΜΗΘΕΙΑΣ

Αντικείμενο του έργου είναι η προμήθεια και υλοποίηση ενός ολοκληρωμένου συστήματος διαχείρισης και εφαρμογής πολιτικών με σκοπό την προστασία από τη διαρροή διαβαθμισμένων πληροφοριών (Data Loss Prevention) για Υπηρεσίες της Ελληνικής Αστυνομίας όπως:

- Διεύθυνση Αντιμετώπισης Ειδικών Εγκλημάτων Βίας
- Διεύθυνση Εγκληματολογικών Ερευνών
- Υποδιεύθυνση Εγκληματολογικών Ερευνών Βορείου Ελλάδος
- Διεύθυνση Διαχείρισης και Ανάλυσης Πληροφοριών
- Διεύθυνση Κρατικής Ασφάλειας
- Διεύθυνση Αλλοδαπών
- Διεύθυνση Προστασίας Συνόρων

Η εν λόγω υλοποίηση υπαγορεύεται από το γεγονός ότι με τις υφιστάμενες παρεχόμενες λειτουργικότητες και υπηρεσίες του Πανελλαδικού Δικτύου Πληροφορικής της Ελληνικής Αστυνομίας υφίσταται κίνδυνος διαρροής δεδομένων των παραπάνω Υπηρεσιών μέσω εκτυπώσεων, μεταφοράς αρχείων με εξωτερικά μέσα αποθήκευσης, αποστολής με e-mail κ.α.

Το έργο περιλαμβάνει:

1) Την υλοποίηση των δύο παρακάτω υποσυστημάτων:

Υποσύστημα «1» δημιουργίας τομέα (domain) για τον καθορισμό, διαχείριση και εφαρμογή πολιτικών ασφαλείας για το σύνολο των διαχειρισθέντων σταθμών εργασίας του έργου με τις αντίστοιχες άδειες χρήσης.

Υπηρεσίες εγκατάστασης, δημιουργίας, παραμετροποίησης και συντήρησης ενός νέου ασφαλούς τομέα στο υπάρχον δίκτυο της Ελληνικής Αστυνομίας με τα εξής χαρακτηριστικά:

- Δημιουργία ενός νέου τομέα (Active Directory) στο υπάρχον εσωτερικό δίκτυο της Ελληνικής Αστυνομίας με εφαρμογή πρόσθετων χαρακτηριστικών και πολιτικών ασφαλείας που συνάδουν με τη διαχείριση τερματικών τα οποία επεξεργάζονται διαβαθμισμένη πληροφορία. Ο τομέας αυτός θα πρέπει να επικοινωνεί υπό συνθήκες εμπιστοσύνης με τον υπάρχον τομέα (SAMBA Active Directory) τόσο σε επίπεδο χρηστών όσο και παρεχόμενης λειτουργικότητας.
- Διαχείριση πολιτικών και μέτρων ασφαλείας από κεντρικό σημείο πρόσβασης για όλον το νέο τομέα.
- Υπηρεσίες διασύνδεσης και διαλειτουργικότητας του νέου τομέα με τις υπάρχουσες υπηρεσίες του Police on Line και όλα τα απαραίτητα υποσυστήματα αυτού (αυθεντικοποίηση και πρόσβαση των χρηστών και του εξοπλισμού τους) με σκοπό τη διασφάλιση της υπάρχουσας λειτουργικότητας των υπηρεσιών και εφαρμογών του Police on Line.
- Παρακολούθηση του τρόπου εφαρμογής των πολιτικών και μέτρων ασφαλείας σε πραγματικό χρόνο και επισκόπησης των εξαιρέσεων όπου αυτές προκύπτουν (alerts, reports, κλπ)

- Προμήθεια των αδειών χρήσης οι οποίες απαιτούνται για την ένταξη των υπό προστασία τερματικών και χρηστών του υποσυστήματος «2» (που περιγράφεται παρακάτω), στον τομέα του υποσυστήματος «1».
- Εργασίες ένταξης-μετάπτωσης των υπό προστασία τερματικών και χρηστών της Ελληνικής Αστυνομίας του υποσυστήματος «2» στον τομέα του υποσυστήματος «1» με ταυτόχρονη διασφάλιση της υπάρχουσας λειτουργικότητας (ενημέρωση, πρόσβαση, λειτουργίες) των τελικών χρηστών στο Πανελλαδικό Δίκτυο Πληροφορικής της Ελληνικής Αστυνομίας (δίκτυο PoL).
- Υπηρεσίες καθορισμού, σχεδιασμού και εφαρμογής εξειδικευμένων κανόνων και πολιτικών ασφαλείας για τη διαχείριση του τομέα του υποσυστήματος «1» σύμφωνα με τις απαιτήσεις του έργου και του Αγοραστή.

Υποσύστημα «2» καθορισμού και διαχείρισης πολιτικών για αποτροπή διαρροής πληροφοριών και διασφάλιση του επιπέδου εμπιστευτικότητας αυτών στο σύνολο των σταθμών εργασίας του υποσυστήματος «1», με τις αντίστοιχες άδειες χρήσης.

Ο έλεγχος θα πραγματοποιείται στο σταθμό εργασίας των χρηστών (end user) και θα αφορά:

- περιπτώσεις πρόσβασης (αντιγραφής, επισύναψης) σε κατηγοριοποιημένα αρχεία δεδομένων με σκοπό την αποστολή, εκτύπωση ή αποθήκευσή τους σε προορισμούς κοινών αρχείων διαφορετικούς από τους προκαθορισμένους αποδεκτούς.
- περιπτώσεις απευθείας πρόσβασης σε βάσεις δεδομένων που εμπίπτουν στις κατηγορίες που περιγράφονται στην παράγραφο 3.8.2 του Πίνακα Τεχνικών Προδιαγραφών. Θα πρέπει να απαγορεύεται οποιαδήποτε είδους εξαγωγή δεδομένων από τις εφαρμογές αυτές σε καταλόγους αρχείων (file systems) διαφορετικούς από προκαθορισμένους επιτρεπτούς (download).
- περιπτώσεις πρόσβασης σε web εφαρμογές (http, https) του εσωτερικού δικτύου (intranet) του Οργανισμού από τελικούς χρήστες. Θα πρέπει να αποτρέπεται η δυνατότητα για print-screen και επικόλληση ή αποθήκευση της οθόνης του χρήστη ως εικόνα, η δυνατότητα για «Αποθήκευση ως» της τρέχουσας σελίδας του browser καθώς και εξαγωγής και αποθήκευσης οποιοδήποτε είδους report των εφαρμογών αυτών από οποιαδήποτε εφαρμογή του εσωτερικού δικτύου.
- περιπτώσεις πρόσβασης στο ηλεκτρονικό ταχυδρομείο (astynomia.gr) μέσω webmail και προγραμμάτων διαχείρισης εσωτερικού ηλεκτρονικού ταχυδρομείου. Θα ελέγχεται και αποτρέπεται η δυνατότητα χρηστών να επισυνάψουν, προωθήσουν, αντιγράψουν και επικολλήσουν κείμενο ή έγγραφο το οποίο θα περιέχει δεδομένα τα οποία εμπίπτουν στις κατηγορίες που περιγράφονται στην παράγραφο 3.8.2 του Πίνακα Τεχνικών Προδιαγραφών.
- περιπτώσεις ελέγχου και διαχείρισης των περιφερειακών συσκευών (device control) των υπό προστασία τερματικών σταθμών
- κρυπτογράφηση των υπό προστασία αρχείων βάση των πολιτικών και των κανόνων που εφαρμόζονται από το υποσύστημα «2» στους υπό προστασία σταθμούς εργασίας με σκοπό τη διασφάλιση του περιεχομένου σε περίπτωση κλοπής ή παραβίασης των μέσων αποθήκευσης (σκληροί δίσκοι, κ.λ.π.)

2) Προμήθεια και εγκατάσταση κεντρικών Εξυπηρετητών με τα αντίστοιχα λογισμικά και άδειες χρήσης αυτών. Εξυπηρετητές σε εικονικά μηχανήματα για την επέκταση της υπάρχουσας εικονικής υποδομής του φορέα για τη φιλοξενία των υπηρεσιών του έργου.

- 3) Προμήθεια και εγκατάσταση ενεργού και παθητικού Δικτυακού εξοπλισμού για τη διασύνδεση της υπό προμήθεια υποδομής εξυπηρετητών με το υφιστάμενο υποσύστημα αποθηκευτικού χώρου και την υποδομή δικτύου δεδομένων του Κέντρου Πληροφορικής της Ελληνικής Αστυνομίας.
- 4) Εγκατάσταση-παραμετροποίηση της προστασίας του συστήματος ενδεικτικά σε περίπου 200 υφιστάμενους Η/Υ Υπηρεσιών της Ελληνικής Αστυνομίας, με κατανομή περίπου 160 στο νομό Αττικής και 40 στο νομό Θεσσαλονίκης.
- 5) Εκπαίδευση προσωπικού της Ελληνικής Αστυνομίας για τη Διαχείριση των υποσυστημάτων «1» και «2» και για τη χρήση των σταθμών εργασίας των τελικών χρηστών του συστήματος.

Οι ειδικότερες απαιτήσεις του έργου περιγράφονται αναλυτικά στον ΠΙΝΑΚΑ ΤΕΧΝΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ.

Αν ο Υποψήφιος Ανάδοχος κρίνει ότι, με την περιγραφόμενη στην παρούσα διακήρυξη διαμόρφωση των απαιτήσεων ή/και τη σύνθεση του εξοπλισμού, η οποία αποτελεί την ελάχιστη απαιτούμενη, δεν ικανοποιούνται όλες οι λειτουργικές απαιτήσεις των προδιαγραφών, θα πρέπει να προσφέρει την κατάλληλη για την ικανοποίησή τους σύνθεση εξοπλισμού (H/W & S/W), αναβαθμίζοντας τα αναγκαία επί μέρους τμήματα.

Τυχόν αναβαθμίσεις και πρόσθετα προϊόντα, πέραν των ζητούμενων, που θα συμπεριληφθούν στη λύση, θα πρέπει να αναφερθούν.

2. ΥΠΑΡΧΟΥΣΑ ΥΠΟΔΟΜΗ

A) Το Πανελλαδικό Δίκτυο Πληροφορικής της Ελληνικής Αστυνομίας (POL), μέσω του οποίου υπάρχει η δυνατότητα πρόσβασης στο σύνολο των επιχειρησιακών εφαρμογών από τις Υπηρεσίες της Ελληνικής Αστυνομίας.

Οι Υπηρεσίες της Ελληνικής Αστυνομίας, όπως αυτές διαρθρώνονται σήμερα, είναι συνδεδεμένες στο ιδιωτικό Πανελλαδικό Δίκτυο Πληροφορικής της Ελληνικής Αστυνομίας (Police on Line), με περίπου 670 σημεία (κτίρια) σε όλη την Επικράτεια, μέσω του οποίου δίνεται πρόσβαση στο σύνολο των επιχειρησιακών εφαρμογών της Ελληνικής Αστυνομίας.

Η δικτυακή υποδομή βασίζεται σε τεχνολογίες και εξοπλισμό του κατασκευαστή Cisco.

Η διασύνδεση των περιφερειακών σημείων υλοποιείται μέσω δικτύου IP VPN/MPLS του ΟΤΕ (συνδέσεις LL,SHDSL,ME,ADSL και LMDS, τουλάχιστον 1 Mbps) και κεντρική διασύνδεση στο Α.Ε.Α συνολικού bandwidth 300Mbps. Η διακίνηση των πακέτων δεδομένων μέσα στο MPLS VPN δίκτυο του τηλεπικοινωνιακού παρόχου γίνεται με κρυπτογράφηση των δεδομένων (κατά κανόνα με την τεχνολογία Cisco GETVPN, ενώ για περίπου 80 σημεία με GRE-IPsec tunnels). Η πρόσβαση των περιφερειακών Υπηρεσιών στις εφαρμογές πληροφορικής της Ελληνικής Αστυνομίας γίνεται μέσω σύνδεσης σε κεντροποιημένο Server Farm το οποίο προστατεύεται από το υπόλοιπο Intranet από διάταξη Firewalls.

Υλοποιούνται υπηρεσίες εσωτερικής τηλεφωνίας (IP τηλεφωνία) πάνω από το δίκτυο PoL με τη χρήση της τεχνολογίας AVVID της Cisco (Cisco Architecture for Voice, Video, and Integrated Data) – συνολικά διασυνδέονται περίπου 1.450 συσκευές Cisco IP-phones και περίπου 165 τηλεφωνικά κέντρα (PBX's) για σκοπούς εσωτερικής τηλεφωνίας.

Σε κάθε Αστυνομική Υπηρεσία (συνολικά περίπου 1.500 Υπηρεσίες επιπέδου Τμήματος & άνω) υλοποιείται τοπικό δίκτυο Ethernet 100Mbps με μεταγωγείς (switches) Cisco 2950, 2960 και διαχωρισμένα VLANs για κάθε Υπηρεσία.

Σε κάθε VLAN υπάρχει πρόσθετη ασφάλεια με την προσθήκη access list, η οποία αποτρέπει την πρόσβαση στα κοινόχρηστα αρχεία των Windows από υπολογιστές των διαφορετικών VLANs.

Το Πανελλαδικό Δίκτυο Πληροφορικής της Ελληνικής Αστυνομίας (POL), διασυνδέεται κεντρικά (από το Αρχηγείο της Ελληνικής Αστυνομίας) με το Δίκτυο δημοσίου τομέα «ΣΥΖΕΥΞΙΣ» για τη διασύνδεσή του με άλλους φορείς και το Διαδίκτυο. Στην εν λόγω διασύνδεση μεσολαβεί διάταξη Firewalls.

Κεντρικά στην έδρα της Δ/νσης Πληροφορικής του Αρχηγείου της Ελληνικής Αστυνομίας, υπάρχουν μια σειρά από **συστήματα διαχείρισης** για την ομαλή λειτουργία του πληροφοριακού συστήματος:

- ο Για τη διαχείριση και πρόσβαση των τελικών χρηστών στο παραπάνω δίκτυο, χρησιμοποιούνται προϊόντα Tivoli της IBM και συγκεκριμένα TIM (Tivoli Identity Manager), TAM (Tivoli Access Manager), καθώς και 4 reverse proxy webSEAL με χρήση δομών LDAP για την απεικόνιση των χρηστών και πόρων του Πληροφοριακού Συστήματος. Η πρόσβαση στο δίκτυο γίνεται με active directory controller (Samba ver. 4.1.5) με σύστημα πιστοποίησης χρηστών RSA Sign-On Manager κάνοντας χρήση του username/password του χρήστη σε αποθηκευμένο user account σε έξυπνη κάρτα πρόσβασης (Smart Card).

- Συγκεκριμένα, η πρόσβαση των χρηστών στον υφιστάμενο τομέα (domain) "police.gov.ydt" επιτυγχάνεται με τη χρήση έξυπνης κάρτας ή/και με τη χρήση ονόματος χρήστη (username) / κωδικού πρόσβασης (password). Σε κάθε περίπτωση, τα διαπιστευτήρια (credentials) του χρήστη στέλνονται στο Samba Domain Server, ο οποίος επικοινωνεί με τον Tivoli Identity/Access Manager Server (TIM/TAM) για την αυθεντικοποίηση του χρήστη και την επιτυχή είσοδό του. Μετά την επιτυχή πρόσβαση του χρήστη στο domain, η πρόσβαση στις εφαρμογές Ιστοσελίδων (Police On Line) γίνεται με τη χρήση web browser (Internet Explorer v.8) από κεντρικό σημείο μέσω της αρχικής σελίδας (http://elas.ydt) του Intranet της Ελληνικής Αστυνομίας. Η πρόσβαση στις εφαρμογές του χρήστη πραγματοποιείται μέσω τεσσάρων (4) Webseals (reverse proxy), οι οποίοι διαμεσολαβούν μεταξύ των "user calls" των τελικών χρηστών και των εξυπηρετητών εφαρμογών (Application Servers) προστατεύοντας τη μεταξύ τους επικοινωνία.
- Για τη διενέργεια των ακόλουθων διεργασιών γίνεται χρήση έξυπνων καρτών (Smart Cards):
 - Ασφαλής σύνδεση στους Ηλεκτρονικούς Υπολογιστές του δικτύου που διαθέτουν Windows XP με user login στον domain controller, με δυνατότητα αυτόματου κλειδώματος του σταθμού εργασίας κατά την εξαγωγή της Έξυπνης Κάρτας από τον αναγνώστη),
 - Πρόσβαση στις εφαρμογές που έχει εξουσιοδοτηθεί ο εκάστοτε χρήστης
 - Single Sign on-TIM/TAM και
 - Ψηφιακή υπογραφή των εγγράφων που διακινούνται μεταξύ των υπηρεσιών.
 - Στο Μηχανογραφικό Κέντρο της Δ/νης Πληροφορικής λειτουργεί **φάρμα εξυπηρετητών IBM 3690 X5 – 7147ZHU, 16 CPU Intel®Xeon® E7-2820@2GHz με 256GB RAM** η οποία σε συνδυασμό με VMware ESXi v.5.1.0, διαχειριζόμενη από VMware vSphere Client v.5.1.0, υποστηρίζει μία ευρεία υποδομή εικονικοποίησης **στην οποία θα ενταχθούν και οι υπό προμήθεια εξυπηρετητές.**
 - Το Intranet Police on Line της Ελληνικής Αστυνομίας διαθέτει ένα σύνολο από περίπου 13.000 **σταθμούς εργασίας (PCs) βασισμένους ως επί το πλείστο σε Windows XP Pro SP3 (περίπου 10.000), Windows 7 Pro (περίπου 2.000) και Windows 8.1 Pro (περίπου 1.000).** Στους σταθμούς εργασίας εγκαθίστανται δύο προγράμματα ανάγνωσης καρτών, το Net iD client version 5.3.2.32 RC HEL1301 της SecMaker AB και το RSA Authentication client version 2.0.1, παρέχοντας τη σύνδεση-πρόσβαση των τελικών χρηστών στο Πληροφοριακό Σύστημα της Ελληνικής Αστυνομίας. Τα προγράμματα που κατ' ελάχιστο εγκαθίστανται στους σταθμούς εργασίας, είναι τα εξής:
 - Trend Micro OfficeScan Antivirus Client v11.0
 - Adobe Reader v10.1+ Ελληνικό
 - Internet Explorer (κυρίως έκδοση v8.0)
 - Mozilla Firefox
 - Java SE Runtime Environment (JRE) 6 Update 16
 - RSA Authentication Client v2.0.1 (μόνο σε Windows XP)
 - Net iD (version 5.3.2.32 UD, HEL1301 της εταιρείας SecMaker AB)
 - Tivoli Endpoint Manager 8.2.0.44 / BIG Fix
 - TeraTerm Pro v2.3.1
 - Drivers:
 - HP LaserJet P3005 Drivers
 - HP LaserJet M4345

- Wincor Nixdorf High Print 4915
 - Drivers Mini Lector USB Card Reader
 - HP USB Smart Card Keyboard Drivers
 - Lexmark XP Drivers
 - Lexmark 98 Drivers
 - SATA Driver
 - Passport Reader
- ο Ως **Σύστημα διαχείρισης των σταθμών εργασίας** από κεντρικό σημείο χρησιμοποιείται το σύστημα IBM Tivoli Endpoint Manager (TEM). Με τη χρήση του TEM δίνεται η δυνατότητα εκτέλεσης πλήθους ενεργειών σε όλους ή σε μέρος των σταθμών εργασίας. Μερικές από αυτές είναι:
- Software distribution: Μεταφορά και εκτέλεση εγκατάστασης ή/και απεγκατάστασης λογισμικού στους σταθμούς εργασίας
 - Εγκατάσταση ενημερώσεων Windows ή άλλων λειτουργικών
 - Εγκατάσταση ενημερώσεων τρίτων προγραμμάτων
 - Πραγματοποίηση Remote Control στο σταθμό για επίλυση προβλημάτων σε πραγματικό χρόνο σε συνεργασία με τον τελικό χρήστη
 - Εκτέλεση λειτουργιών στο σταθμό (restart, shutdown κλπ)
 - Αλλαγή δικαιωμάτων τοπικών χρηστών, αλλαγές Password, απενεργοποίηση χρηστών κλπ)

Σημειώνεται ότι το συγκεκριμένο σύστημα διαχείρισης ως σήμερα έχει ενεργοποιηθεί σε περισσότερους από 3.000 σταθμούς εργασίας.

Β) Υπηρεσία Ηλεκτρονικού Ταχυδρομείου (e-mail), στην οποία έχουν πρόσβαση οι χρήστες από τους φορείς:

- της Ελληνικής Αστυνομίας (@astynomia.gr)
- του πρώην Υπουργείου Δημόσιας Τάξης και Προστασίας του Πολίτη (@yptp.gr)
- της Υπηρεσίας Ασύλου (@asylo.gov.gr)
- του Κέντρου Μελετών Ασφαλείας (@kemea.gr)
- της Διεύθυνσης Διαβατηρίων και Εγγράφων Ασφαλείας (@diavatiria.gr).

Η πρόσβαση στο ηλεκτρονικό ταχυδρομείο γίνεται:

- i. από εφαρμογή ιστοσελίδων «Webmail».
- ii. από εφαρμογές διαχείρισης ηλεκτρονικού ταχυδρομείου με τη χρήση πρωτοκόλλου POP3 και IMAP.

Γ) Πρόσβαση σε ιστοσελίδες του Διαδικτύου, παρέχεται για τους χρήστες του δικτύου PoL μέσω της κεντρικής πρόσβασης στο Δίκτυο Δημοσίου Τομέα «ΣΥΖΕΥΞΙΣ» του κτιρίου του Αρχηγείου της Ελληνικής Αστυνομίας, με χρήση κεντρικών Proxy Servers που υποστηρίζουν λειτουργία Web και Application Filtering.

Πλέον των διατάξεων Firewalls, λειτουργεί διπλό **σύστημα περιμετρικής προστασίας και ελέγχου πρόσβασης** (Trend Micro IWSVA) για την περαιτέρω προστασία της περιμέτρου των δύο ανωτέρω δικτύων και τον ελεγχόμενο τρόπο πρόσβασης στο Διαδίκτυο για το σύνολο των χρηστών.

3. ΔΙΑΘΕΣΙΜΟΤΗΤΑ-ΡΗΤΡΕΣ

Ο Ανάδοχος υποχρεούται να υλοποιήσει το σύνολο του συστήματος παρέχοντας τις απαιτούμενες υπηρεσίες στο πλαίσιο της πενταετούς Εγγύησης και Τεχνικής Υποστήριξης και της Συντήρησης του Έργου, ώστε να τηρούνται τα ελάχιστα όρια διαθεσιμότητας που ορίζονται στην παρούσα.

Τονίζεται ότι οι απαιτήσεις διαθεσιμότητας της παρούσας παραγράφου ισχύουν και για την Περίοδο Καλής Λειτουργίας.

Ορισμοί:

Χρόνος απόκρισης βλάβης/δυσλειτουργίας είναι το μέγιστο επιτρεπόμενο χρονικό διάστημα από την αναγγελία της βλάβης ή δυσλειτουργίας μέχρι την άφιξη του Αναδόχου στο χώρο του Αγοραστή και ορίζεται σε 3 ώρες. Για κάθε επιπλέον ώρα που απαιτήθηκε για την άφιξη του Αναδόχου αυτή θα προσμετράται στο χρόνο εκτός λειτουργίας.

Διαθεσιμότητα Εξοπλισμού – Λογισμικού είναι η επί τοις εκατό αναλογία του απαιτούμενου χρόνου λειτουργίας μείον του χρόνου εκτός λειτουργίας προς τον απαιτούμενο χρόνο λειτουργίας και υπολογίζεται από τον παρακάτω τύπο:

$$\Delta = 100 * (\text{Απαιτούμενος Χρόνος Λειτουργίας} - \text{Χρόνος Εκτός Λειτουργίας}) / (\text{Απαιτούμενος Χρόνος Λειτουργίας})$$

Απαιτούμενος Χρόνος Λειτουργίας είναι το χρονικό διάστημα είκοσι τεσσάρων (24) ωρών ανά ημέρα για όλες τις ημέρες του έτους (365).

Χρόνος Εκτός Λειτουργίας είναι το χρονικό διάστημα από την αναγγελία της βλάβης μέχρι τη διόρθωσή της και την παράδοση της μονάδας σε πλήρη λειτουργία από το μηχανικό της εταιρείας στον υπεύθυνο του χώρου. Ο μέγιστος ανεκτός χρόνος απόκρισης αφαιρείται από το Χρόνο Εκτός Λειτουργίας του εξοπλισμού, ανεξαρτήτως του πραγματικού χρόνου απόκρισης, ο οποίος όμως δε δύναται να γίνει μικρότερος του μηδενός.

Κατηγορία Α: Εξοπλισμού – Λογισμικού ορίζεται ως το σύνολο των διακριτών μονάδων εξοπλισμού ή/και λογισμικού, η εύρυθμη λειτουργία των οποίων στηρίζει τη λειτουργικότητα του συστήματος, δηλ. εξυπηρετητές, στοιχεία της κεντρικής υποδομής, εφαρμογές, λειτουργικά συστήματα server, virtualization software, συστημικό (έτοιμο) λογισμικό server. Όπως και το υποσύστημα «1».

Κατηγορία Β: Εξοπλισμού - Λογισμικού ορίζεται το υποσύστημα «2» και η παροχή υποστήριξης των περιφερειακών διαχειριστών του DLP με σκοπό τη συνδρομή τους στη διαχείριση πολιτικών DLP.

Αποδεκτή ετήσια διαθεσιμότητα Μονάδας Κατηγορίας Α – Ρήτρες:

Η ελάχιστη ετήσια αποδεκτή διαθεσιμότητα των συστημάτων της Κατηγορίας Α είναι **99.5%**. Σε περίπτωση διαθεσιμότητας μικρότερης του ανωτέρω ετήσιου ποσοστού, επιβάλλεται στον Ανάδοχο ρήτρα ίση με 0,02 % επί του τρέχοντος ετήσιου κόστους συντήρησης του συνόλου του συστήματος, για κάθε επιπλέον ώρα μη αποκατάστασης.

Διευκρινίζεται ότι :

- 1) Ένα σύστημα / υποσύστημα / υπηρεσία θεωρείται ολικά μη διαθέσιμο/η εάν είναι μη διαθέσιμο έστω και ένα μικρό μέρος της λειτουργικότητας που παρέχει.
- 2) Σε περίπτωση που στοιχείο εξοπλισμού κεντρικής υποδομής βρίσκεται σε διάταξη υψηλής διαθεσιμότητας και η βλάβη/δυσλειτουργία του δεν επηρεάζει τη λειτουργικότητα του συστήματος (ή μέρος αυτής) και την παροχή ηλεκτρονικών υπηρεσιών, τότε αυτό λογίζεται ως μονάδα της Κατηγορίας Β.

Αποδεκτή ετήσια διαθεσιμότητα Μονάδας Κατηγορίας Β – Ρήτρες:

Η ελάχιστη ετήσια αποδεκτή διαθεσιμότητα των συστημάτων της Κατηγορίας Β είναι **99%**. Σε περίπτωση διαθεσιμότητας μικρότερης του ανωτέρω ετήσιου ποσοστού, επιβάλλεται στον Ανάδοχο ρήτρα ίση με 0,01 % επί του τρέχοντος ετήσιου κόστους συντήρησης του συνόλου του συστήματος, για κάθε επιπλέον ώρα μη αποκατάστασης.

Επιπρόσθετες ρήτρες ανεξαρτήτου Κατηγορίας Εξοπλισμού - Λογισμικού

Αν ένα υποσύστημα / υπηρεσία είναι μη διαθέσιμο/η (σε βλάβη ή δυσλειτουργία) για χρονική περίοδο άνω των 72 ωρών (εντός του Απαιτούμενου Χρόνου Λειτουργίας) αθροιστικά στο διάστημα ενός μήνα, οι ως άνω αναφερόμενες ρήτρες, υπολογίζονται στο τριπλάσιο.

Αν για μία μονάδα εξοπλισμού – λογισμικού (υπηρεσία) συμβεί το ανωτέρω για δύο (2) συνεχείς μήνες, πέρα από την επιβληθείσα ρήτρα, ο Ανάδοχος υποχρεούται να αντικαταστήσει μέσα σ' ένα μήνα, με δικό του κόστος, τη μονάδα που παρουσίασε επανειλημμένα την ίδια βλάβη με άλλη ισοδύναμη και σύγχρονη, ύστερα από έγγραφη ειδοποίηση του αγοραστή, και με τη σύμφωνη γνώμη του.

4. ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

Καθ' όλη τη διάρκεια της Σύμβασης αλλά και μετά τη λήξη ή λύση αυτής και για διάρκεια τουλάχιστον δέκα πέντε (15) ετών, ο Ανάδοχος θα αναλάβει την υποχρέωση να τηρήσει εμπιστευτικές και να μη γνωστοποιήσει σε οποιοδήποτε τρίτο, οποιαδήποτε έγγραφα ή πληροφορίες που θα περιέλθουν σε γνώση του κατά την εκτέλεση των υπηρεσιών και την εκπλήρωση των υποχρεώσεων του.

Επίσης θα αναλάβει την υποχρέωση να μην γνωστοποιήσει μέρος ή το σύνολο του Έργου που θα εκτελέσει χωρίς την προηγούμενη έγγραφη έγκριση του Αγοραστή.

Ειδικότερα:

- Ο Ανάδοχος υποχρεούται να τηρεί εχεμύθεια ως προς τις εμπιστευτικές πληροφορίες και τα στοιχεία που σχετίζονται με τις δραστηριότητες του Αγοραστή. Ως εμπιστευτικές πληροφορίες και στοιχεία νοούνται όσα δεν είναι γνωστά στους τρίτους, ακόμα και αν δεν έχουν χαρακτηριστεί από τον Αγοραστή ως εμπιστευτικά. Η τήρηση εμπιστευτικών πληροφοριών από τον Ανάδοχο διέπεται από τις κείμενες διατάξεις και το νομοθετικό πλαίσιο και πρέπει να είναι εφάμιλλη της εμπιστευτικότητας που τηρεί ο Ανάδοχος για το δικό του Οργανισμό και για τις δικές τους πληροφορίες εμπιστευτικού χαρακτήρα.
- Ο Ανάδοχος υποχρεούται να αποφεύγει οποιαδήποτε εμπλοκή των συμφερόντων του με τα συμφέροντα του Αγοραστή, να παραδώσει με τη λήξη της Σύμβασης όλα τα στοιχεία, έγγραφα κλπ. που έχει στην κατοχή του και αφορούν τον Αγοραστή, να τηρεί μια πλήρη σειρά των αρχείων και εγγράφων και του λοιπού υλικού που αφορά στην υλοποίηση και διοίκηση του Έργου καθώς και στις υπηρεσίες που θα παρέχονται στο πλαίσιο του Έργου από αυτόν.
- Ο Ανάδοχος υποχρεούται να προστατεύει το απόρρητο και τα αρχεία που αφορούν σε προσωπικά δεδομένα ατόμων και που τυχόν έχει στην κατοχή του για την υλοποίηση και παραγωγική λειτουργία του Έργου, ακόμη και μετά τη λήξη του Έργου, με βάση τα αναφερόμενα στη Σύμβαση.
- Ο Ανάδοχος οφείλει να λάβει όλα τα αναγκαία μέτρα προκειμένου να διασφαλίσει ότι και οι υπάλληλοι/ συνεργάτες / υπεργολάβοι του γνωρίζουν και συμμορφώνονται με τις παραπάνω υποχρεώσεις. Τα συμβαλλόμενα μέρη συμφωνούν ότι σε περίπτωση υπαιτιότητας του Αναδόχου στη μη τήρηση των παραπάνω υποχρεώσεων εχεμύθειας, ο Ανάδοχος θα καταβάλλει στον Αγοραστή ποινική ρήτρα ίση με το ποσό της αμοιβής του από τη Σύμβαση. Επίσης, ο Αγοραστής διατηρεί το δικαίωμα να απαιτήσει από τον Ανάδοχο την αποκατάσταση κάθε τυχόν περαιτέρω ζημίας.

5. ΧΡΟΝΟΔΙΑΓΡΑΜΜΑ – ΦΑΣΕΙΣ ΥΛΟΠΟΙΗΣΗΣ

Ο χρόνος υλοποίησης του Έργου ορίζεται σε **δέκα (10) μήνες** από την ημερομηνία υπογραφής της Σύμβασης.

Το σύνολο του Έργου διαχωρίζεται στις παρακάτω φάσεις. Ειδικότερα η περιγραφή του Έργου ανά **Φάση** έχει ως εξής:

Φάση	Διάρκεια Φάσης	Τίτλος Φάσης	Προϋπόθεση έναρξης
A	1 μήνας	Μελέτη Εφαρμογής	Έναρξη με την υπογραφή της Σύμβασης
B	4 μήνες	Αναγνώριση Κατηγοριών δεδομένων – Καθορισμός Πολιτικών Ασφαλείας	Έναρξη με την υπογραφή της Σύμβασης
Γ	3 μήνες	Εγκατάσταση Εξοπλισμού & Λογισμικού, Διασύνδεση και Ολοκλήρωση Υποσυστημάτων	Έναρξη με την παραλαβή της Α Φάσης
Δ	5 μήνες	Αυτοματοποιημένος Εντοπισμός Δεδομένων Παρακολούθηση αποτελεσμάτων, βελτιστοποίηση πολιτικών Ασφαλείας.	Έναρξη με την παραλαβή της Β και Γ Φάσης
Ε	2 μήνες	Εκπαίδευση	Έναρξη με την παραλαβή της Β και Γ Φάσης
ΣΤ	1 μήνας	Περίοδος Καλής Λειτουργίας	Έναρξη με την παραλαβή όλων των προηγούμενων Φάσεων

Παρατίθεται το συνοπτικό χρονοδιάγραμμα υλοποίησης του Έργου.

Φάσεις	ΧΡΟΝΟΣ ΣΕ ΜΗΝΕΣ									
	1	2	3	4	5	6	7	8	9	10
A: Μελέτη Εφαρμογής	X									
B: Αναγνώριση Κατηγοριών δεδομένων – Καθορισμός Πολιτικών Ασφαλείας	X	X	X	X						
Γ: Εγκατάσταση Εξοπλισμού & Λογισμικού, Διασύνδεση και Ολοκλήρωση Υποσυστημάτων		X	X	X						
Δ: Αυτοματοποιημένος Εντοπισμός Δεδομένων Παρακολούθηση αποτελεσμάτων, βελτιστοποίηση πολιτικών Ασφαλείας					X	X	X	X	X	
Ε: Εκπαίδευση					X	X				
ΣΤ: Περίοδος Καλής Λειτουργίας										X

6. ΟΜΑΔΕΣ ΚΑΙ ΣΥΝΤΕΛΕΣΤΕΣ ΚΡΙΤΗΡΙΩΝ ΤΕΧΝΙΚΗΣ ΑΞΙΟΛΟΓΗΣΗΣ

Η αξιολόγηση των προσφορών των υποψηφίων Αναδόχων, για την επιλογή του καταλληλότερου, θα γίνει με βάση τα ακόλουθα κριτήρια:

α/α	Κριτήρια	Συντελεστής βαρύτητας	
1	ΔΙΚΤΥΑΚΕΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΕΣ ΥΠΟΔΟΜΕΣ	40%	Σύμφωνα με παραγράφους:
1.1	Εξυπηρετητές: Επεξεργαστής	10%	2.1.7, 2.1.8, 2.1.9, 2.1.11
1.2	Εξυπηρετητές: Μνήμη	10%	2.1.14, 2.1.15
1.3	Εξυπηρετητές: Δίσκοι	5%	2.1.19, 2.1.22, 2.1.23, 2.1.24
1.4	Εξυπηρετητές: Λοιπά χαρακτηριστικά	5%	2.1.27, 2.1.28, 2.1.32, 2.1.33, 2.1.34
1.5	Δικτυακός εξοπλισμός: Αριθμός θυρών	5%	2.2.8, 2.2.9, 2.2.10
1.6	Δικτυακός εξοπλισμός: Ταχύτητα- δυναμικότητα	5%	2.2.15, 2.2.16, 2.2.17
2	ΛΟΓΙΣΜΙΚΟ ΥΠΟΔΟΜΗΣ	40%	
2.1	Δυνατότητες λογισμικού Υποσυστήματος DLP	10%	2.5.4, 2.5.17, 2.5.29, 2.5.34, 2.5.36
2.2	Αριθμός αδειών λογισμικού σταθμών εργασίας Υποσυστήματος DLP	17%	2.5.3
2.3	Άδειες Λογισμικού εξυπηρετητή Υποσυστήματος DLP	3%	2.5.3.1
2.4	Αριθμός αδειών λογισμικού Υποσυστήματος AD	10%	2.6.3
3	ΥΠΗΡΕΣΙΕΣ ΕΚΠΑΙΔΕΥΣΗΣ, ΕΓΓΥΗΣΗΣ ΚΑΙ ΤΕΧΝΙΚΗΣ ΥΠΟΣΤΗΡΙΞΗΣ, ΣΥΝΤΗΡΗΣΗΣ	20%	
3.1	Υπηρεσίες Εκπαίδευσης	4%	4.1.1, 4.1.2
3.2	Υπηρεσίες Εγγύησης και Τεχνικής Υποστήριξης	8%	5.1, 5.8

3.3	Υπηρεσίες Συντήρησης	8%	6.1, 6.10
ΣΥΝΟΛΟ		100%	

7. ΤΕΧΝΙΚΑ ΣΤΟΙΧΕΙΑ ΤΗΣ ΠΡΟΣΦΟΡΑΣ

Η προσφορά πρέπει να καλύπτει κάθε απαίτηση της διακήρυξης, γεγονός το οποίο θα αποδεικνύεται με παραπομπές σε τεχνικά φυλλάδια και άλλο υλικό τεκμηρίωσης.

1. ΤΡΟΠΟΣ ΣΥΜΠΛΗΡΩΣΗΣ ΤΩΝ ΠΙΝΑΚΩΝ ΣΥΜΜΟΡΦΩΣΗΣ

Οι πίνακες αναλυτικών τεχνικών προδιαγραφών που ακολουθούν θα συμπληρωθούν από τους Υποψήφιους Αναδόχους. Επεξήγηση των στηλών των πινάκων:

Στήλη ΠΡΟΔΙΑΓΡΑΦΗ

Στα κελιά της στήλης αυτής περιγράφονται αναλυτικά οι αντίστοιχοι τεχνικοί όροι, υποχρεώσεις ή επεξηγήσεις, για τα οποία θα πρέπει να δοθούν αντίστοιχες απαντήσεις.

Στήλη ΑΠΑΙΤΗΣΗ

Στα κελιά της στήλης αυτής έχουν συμπληρωθεί:

Η λέξη "ΝΑΙ", που σημαίνει ότι η αντίστοιχη προδιαγραφή είναι υποχρεωτική για τον Υποψήφιο Ανάδοχο. Για τις περιπτώσεις όπου υπάρχει «ΝΑΙ» σε τίτλο απαιτήσεων, ο οποίος αναλύεται σε επιμέρους χαρακτηριστικά θεωρείται ότι η απαίτηση περιλαμβάνει όλα τα επιμέρους χαρακτηριστικά και πρέπει να δοθεί απάντηση για το καθένα χωριστά. Η συγκεκριμένη επισήμανση δεν ισχύει όταν υπάρχει επιμέρους ανάλυση για την απαίτηση του κάθε ειδικού χαρακτηριστικού.

Ένας αριθμός που σημαίνει υποχρεωτικό αριθμητικό μέγεθος της προδιαγραφής (μέγιστο ή ελάχιστο).

Όπου υπάρχει κενό, εάν ρητώς δεν αναφέρεται διαφορετικά ή από οποιοδήποτε άλλο σημείο των προδιαγραφών δεν προκύπτει ότι πρόκειται περί υποχρεωτικής απαίτησης, η αντίστοιχη προδιαγραφή δεν είναι υποχρεωτική για τον Υποψήφιο Ανάδοχο, αλλά αποτελεί επιθυμητό χαρακτηριστικό.

Στήλη ΑΠΑΝΤΗΣΗ

Στα κελιά της στήλης αυτής σημειώνεται υποχρεωτικά η απάντηση του Υποψήφιου Αναδόχου που θα έχει:

Την ένδειξη "ΝΑΙ" εάν από την προσφορά πληρείται η αντίστοιχη προδιαγραφή ή αναλαμβάνεται η συγκεκριμένη υποχρέωση ή την ένδειξη "ΟΧΙ" σε αντίθετη περίπτωση.

Ένα αριθμητικό μέγεθος από το οποίο θα προκύπτει εάν ικανοποιείται ή όχι η αντίστοιχη προδιαγραφή.

Απλή κατάφαση ή επεξήγηση δεν αποτελεί απόδειξη εκπλήρωσης της προδιαγραφής και η επιτροπή αξιολόγησης κατά την κρίση της μπορεί να τη δεχθεί ή όχι.

Στήλη ΠΑΡΑΠΟΜΠΗ

Στη στήλη αυτή αναγράφονται υποχρεωτικά οι παραπομπές ανά κελί, σε άλλα σημεία της προσφοράς, τεχνικά φυλλάδια, εγχειρίδια ή φωτοτυπίες τμημάτων τους, δημοσιεύματα κλπ. από τα οποία τεκμηριώνονται και αιτιολογούνται πλήρως οι απαντήσεις της προηγούμενης στήλης της προσφοράς.

Όλο το παραπάνω υλικό τεκμηρίωσης θα αποτελέσει ξεχωριστό τόμο της προσφοράς ο οποίος και θα είναι αριθμημένος ανά σελίδα. Οι παραπομπές θα γίνονται σε συγκεκριμένη σελίδα ή σελίδες του τόμου αυτού. Γενικές αναφορές ή ασαφείς παραπομπές δύναται να αποτελέσουν λόγο απόρριψης της προσφοράς.

Τονίζεται ότι είναι υποχρεωτική η απάντηση και η αντίστοιχη παραπομπή, σε όλα τα σημεία των πινάκων και η παροχή όλων των πληροφοριών που ζητούνται.

2. ΓΕΝΙΚΟΙ ΟΡΟΙ ΤΩΝ ΤΕΧΝΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ.

2.1. ΑΝΤΙΓΡΑΦΟ ΤΩΝ ΠΙΝΑΚΩΝ ΤΗΣ ΟΙΚΟΝΟΜΙΚΗΣ ΠΡΟΣΦΟΡΑΣ.

Πλήρες αντίγραφο του οικονομικού πίνακα, **χωρίς τιμές**, θα πρέπει να περιλαμβάνεται στην τεχνική προσφορά. Έλλειψη των παραπάνω πινάκων (χωρίς τιμές) καθώς και η υποβολή του στο φάκελο των τεχνικών προδιαγραφών με τιμές **αποτελεί λόγο απόρριψης της συγκεκριμένης προσφοράς.**

2.2. ΕΛΕΓΧΟΙ ΠΟΥ ΘΑ ΠΡΑΓΜΑΤΟΠΟΙΗΘΟΥΝ ΓΙΑ ΤΗΝ ΑΠΟΔΟΧΗ ΚΑΙ ΠΑΡΑΛΑΒΗ.

Από την επιτροπή παραλαβής για την αποδοχή και παραλαβή του έργου θα πραγματοποιηθούν οι παρακάτω έλεγχοι:

- Ποσοτικός-ποιοτικός έλεγχος του υλικού-λογισμικού-αδειών χρήσης, τεχνικών εγχειριδίων, παραδοτέων των φάσεων κ.λπ.
- Έλεγχος καλής λειτουργίας του υλικού-λογισμικού.
- Έλεγχος της αρμονικής συνεργασίας των διαφόρων μερών.
- Κάθε άλλος έλεγχος που θα κριθεί απαραίτητος για να αποδειχθεί ότι τα είδη ανταποκρίνονται στις απαιτήσεις των προδιαγραφών.

Εφόσον με την εγκατάσταση του παρεχόμενου υλικού και λογισμικού διαπιστωθούν προβλήματα ή ασυμβατότητες, η προσφερόμενη λύση θα απορρίπτεται. Το καθεστώς το οποίο διέπει τη διαχείριση των δειγμάτων, ορίζεται βάσει του Ν.4412/2016, άρθρο 214.

2.3. ΥΠΟΧΡΕΩΣΕΙΣ ΣΥΜΜΕΤΟΧΗΣ ΣΤΟ ΔΙΑΓΩΝΙΣΜΟ.

- Εναλλακτικές προσφορές δε θα γίνονται δεκτές και θα απορρίπτονται.
- Οι προσφορές πρέπει να συνοδεύονται από τεχνικό εγχειρίδιο / λεπτομερές περιγραφικό φυλλάδιο του κατασκευαστή, στο οποίο θα αναγράφονται οι λεπτομέρειες για τη λειτουργία των συσκευών και θα περιγράφονται με σαφήνεια τα ειδικά τεχνικά χαρακτηριστικά και στοιχεία που ζητούνται με τις παρούσες προδιαγραφές. Σαφής περιγραφή θεωρείται εκείνη που περιλαμβάνει λεπτομερή ανάλυση της λειτουργικότητάς και της προτεινόμενης αρχιτεκτονικής, η οποία θα τεκμηριώνεται από τα αντίστοιχα τεχνικά εγχειρίδια. Υλικό που προσφέρεται με απλή αναφορά χωρίς περιγραφή δε θα λαμβάνεται υπόψη και θα θεωρείται ότι δεν περιλαμβάνεται στην προσφορά.

ΠΙΝΑΚΑΣ ΤΕΧΝΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ

Ο Υποψήφιος Ανάδοχος συμπληρώνει τους παρακάτω πίνακες συμμόρφωσης με την απόλυτη ευθύνη της ακρίβειας των δεδομένων.

1. ΓΕΝΙΚΟΙ ΟΡΟΙ – ΑΠΟΔΟΤΙΚΟΤΗΤΑ & ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ

A/A	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.1.	Όλα τα προς προμήθεια προϊόντα θα είναι καινούρια, άριστης ποιότητας και θα παραδοθούν εντός των χώρων της Δ/σης Πληροφορικής / Α.Ε.Α. ή όπως ορίζεται στον «ΠΙΝΑΚΑ ΤΕΧΝΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ».	ΝΑΙ		
1.2.	Ο Υποψήφιος Ανάδοχος θα πρέπει να περιγράψει με σαφήνεια την προτεινόμενη λύση. Σαφής περιγραφή θεωρείται εκείνη που περιλαμβάνει λεπτομερή ανάλυση της λειτουργικότητάς της και της αρχιτεκτονικής αυτής, η οποία και θα τεκμηριώνεται από τα αντίστοιχα τεχνικά εγχειρίδια από τα οποία θα προκύπτει εύλογα η ικανοποίηση της αντίστοιχης προδιαγραφής.	ΝΑΙ		
1.3.	Καταφατική απάντηση στις τεχνικές προδιαγραφές ισοδυναμεί με την προσφορά των αντίστοιχων υποσυστημάτων για την υποστήριξη της επιθυμητής λειτουργικότητας.	ΝΑΙ		
1.4.	Ο Ανάδοχος υποχρεούται να προσφέρει όλες τις απαιτούμενες λειτουργίες / υπηρεσίες (απεγκατάστασης - εγκατάστασης - ενεργοποίησης) της παρούσας διακήρυξης με τις αντίστοιχες άδειες χρήσεις εγκατεστημένες και ενεργοποιημένες.	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.5.	<p>Ο Υποψήφιος Ανάδοχος υποχρεούται να κατανείμει τις φάσεις υλοποίησης του Έργου σύμφωνα με τους όρους του κεφαλαίου «ΧΡΟΝΟΔΙΑΓΡΑΜΜΑ – ΦΑΣΕΙΣ ΥΛΟΠΟΙΗΣΗΣ» της παρούσας, στις οποίες θα εντάξει όλες τις απαραίτητες εργασίες της προσφοράς του.</p> <p>Τροποποίηση του χρονοδιαγράμματος είναι δυνατή μόνο κατά την αποδοχή του τεύχους μελέτης εφαρμογής και κατόπιν συμφωνίας του Αγοραστή.</p>	ΝΑΙ		
1.6.	<p>Ο Υποψήφιος Ανάδοχος υποχρεούται να υποβάλλει με την προσφορά του ολοκληρωμένο σχέδιο ένταξης των Η/Υ στο νέο τομέα του υπό προμήθεια Active Directory. Να περιγραφεί επίσης η προτεινόμενη μεθοδολογία που θα ακολουθήσει ο Ανάδοχος για την αυτοματοποιημένη εγκατάσταση του προσφερόμενου λογισμικού αποτροπής διαρροής πληροφοριών στους σταθμούς εργασίας, με ταυτόχρονη αναφορά στο βαθμό τυχόν αξιοποίησης υπάρχοντων συστημάτων της Ελληνικής Αστυνομίας. Η οριστική μέθοδος που θα χρησιμοποιηθεί κατά την υλοποίηση θα προκύψει στο Τεύχος Μελέτης Εφαρμογής του Αναδόχου.</p>	ΝΑΙ		
1.7.	<p>Σε περίπτωση που για μέρος υλοποίησης της λύσης απαιτείται εξοπλισμός διαφορετικός αυτού που προδιαγράφεται από την παρούσα, ο Υποψήφιος Ανάδοχος υποχρεούται να τον προσφέρει στην προσφορά του δικαιολογώντας το σχετικά. Να αναφερθεί το είδος και τα χαρακτηριστικά του εξοπλισμού.</p> <p>Σε περίπτωση που κατά την υλοποίηση προκύψει ανάγκη επιπλέον εξοπλισμού, λογισμικού ή αδειών</p>	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	χρήσης, για την κάλυψη των αναγκών που περιγράφονται στην παρούσα, ο Ανάδοχος υποχρεούται να τα προσφέρει χωρίς επιπλέον κόστος για το δημόσιο.			
1.8.	Σε περίπτωση που για την ικανοποίηση όλων των απαιτήσεων της παρούσας, ο Ανάδοχος ή υπεργολάβος του δημιουργήσει κατά παραγγελία λογισμικό, τα δικαιώματα κτήσης και χρήσης αυτού περιέρχονται στον Αγοραστή.	ΝΑΙ		
1.9.	Στην τεχνική προσφορά θα πρέπει απαραίτητως να αναγράφεται η μάρκα, το μοντέλο, ο τύπος, το εργοστάσιο κατασκευής και η χώρα προέλευσης των προσφερόμενων συσκευών και των τυχόν παρελκομένων τους.	ΝΑΙ		
1.10.	<p>Το προσφερόμενο λογισμικό αποτροπής διαρροής δεδομένων που θα εγκατασταθεί στους Η/Υ πρέπει να προέρχεται κατά το δυνατόν από έναν κατασκευαστή.</p> <p>Σε περίπτωση που για την επίτευξη όλων των απαιτήσεων προσφέρονται πρόσθετα λογισμικά τρίτων κατασκευαστών, αυτά θα πρέπει να είναι πλήρως συμβατά και να συνεργάζονται μεταξύ τους, ενώ θα πρέπει για όλα να επιτυγχάνεται η κεντρική διαχείρισή τους.</p> <p>Να αναφερθούν τα προσφερόμενα λογισμικά.</p>	ΝΑΙ		
1.11.	Ο Υποψήφιος Ανάδοχος πρέπει να συμπεριλάβει στην προσφορά του δηλώσεις αποδοχής εκτέλεσης της προμήθειας από τους κατασκευαστικούς οίκους ή τους αντιπροσώπους αυτών στην Ελλάδα,	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	για τα προϊόντα τα οποία έχει συμπεριλάβει στην προσφορά του.			
1.12.	Ο Υποψήφιος Ανάδοχος θα πρέπει να αποδεικνύει με πιστοποιητικό καλής υλοποίησης την εγκατάσταση, παραμετροποίηση και συντήρηση του βασικού προσφερόμενου λογισμικού DLP σε τρίτο Οργανισμό (τουλάχιστον 50 σταθμών εργασίας).	≥ 1		
1.13.	Το προσφερόμενο προϊόν για την προστασία των σταθμών εργασίας, να αναφέρεται στην κατηγορία "leaders" από τον οργανισμό GARTNER, στην πλέον πρόσφατη αξιολόγησή του.	ΝΑΙ		
1.14.	<p>Το προσφερόμενο σύστημα και όλα τα λογισμικά θα πρέπει να είναι συμβατά και να μη δημιουργούν προβλήματα δια-λειτουργικότητας με την υπάρχουσα υποδομή της Ελληνικής Αστυνομίας.</p> <p>Επισημαίνεται ιδιαίτερα η απαίτηση διαλειτουργικότητας με τα λογισμικά χρήσης των έξυπνων καρτών (smart cards) NetiD client version 5.3.2.32 και RSA Authentication client version 2.0.1 για τη προσωποποιημένη σύνδεση - πρόσβαση (αυθεντικοποίηση) των τελικών χρηστών στο πληροφοριακό σύστημα της Ελληνικής Αστυνομίας (Police On Line) με τη χρήση των έξυπνων καρτών RSA Smart Card 5200 και Smart Card SLE 66CX322P, καθώς και με το λογισμικό Trend Micro Antivirus που έχουν εγκατασταθεί στους Η/Υ των τελικών χρηστών.</p>	ΝΑΙ		
1.15.	Η εγκατάσταση των υπό προμήθεια λογισμικών θα πραγματοποιηθεί στους προσφερόμενους εξυπηρετητές σε εικονικό περιβάλλον VM Ware, που θα	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>πρέπει επίσης να προσφερθεί, επεκτείνοντας την υφιστάμενη υποδομή εικονικοποίησης της Ελληνικής Αστυνομίας. Ο Υποψήφιος Ανάδοχος υποχρεούται να υποβάλλει με την προσφορά του την αρχιτεκτονική εγκατάσταση και τα τεχνικά χαρακτηριστικά των εικονικών εξυπηρετητών που θα απαιτηθούν. Οι απαιτούμενες άδειες όλων των προσφερόμενων λογισμικών και λειτουργικών συστημάτων θα προσφέρονται από τον Ανάδοχο.</p>			
1.16.	<p>Από την παρούσα διακήρυξη δεν απαιτείται η προσφορά συστήματος DLP περιμετρικής προστασίας για το Intranet της Ελληνικής Αστυνομίας. Ωστόσο η ταυτόχρονη προσφορά του, ή η ενδεχόμενη δυνατότητα ενεργοποίησής του βάσει των προσφερόμενων αδειών χρήσης δεν αποτελεί απόκλιση από τις απαιτήσεις της διακήρυξης.</p>	<p>ΝΑΙ</p>		
1.17.	<p>Ο Ανάδοχος υποχρεούται να παραδώσει, μαζί με τα υπό προμήθεια υλικά και λογισμικά, εγχειρίδια χρήσης αυτών τουλάχιστον στην αγγλική γλώσσα.</p>	<p>ΝΑΙ</p>		
1.18.	<p>Ο Ανάδοχος προ της οριστικής παραλαβής του συνόλου των ειδών είναι υποχρεωμένος να παραδώσει, χωρίς πρόσθετο κόστος, σε ηλεκτρονικό αρχείο τα serial numbers όλου του εξοπλισμού Η/Υ & λογισμικού S/W.</p>	<p>ΝΑΙ</p>		
1.19.	<p>Για τη διαθεσιμότητα όλου του υπό προμήθεια συστήματος και τις ρήτρες που εφαρμόζονται ισχύουν όλοι οι όροι που αναφέρονται στην παρούσα, Κεφ. «ΔΙΑΘΕΣΙΜΟΤΗΤΑ-ΡΗΤΡΕΣ».</p>	<p>ΝΑΙ</p>		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.20	Ο ανάδοχος οφείλει να συμμορφώνεται με όλους τους όρους που αναφέρονται στην παρούσα, Κεφ. «ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ».	ΝΑΙ		

2. ΤΕΧΝΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

A/A	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
A)	ΕΞΟΠΛΙΣΜΟΣ Η/W			
2.1	Εξυπηρετητές Συστήματος			
2.1.1	Αριθμός Υπολογιστικών Συστημάτων	2		
2.1.2	Τα επί μέρους τμήματα που συνθέτουν το προσφερόμενο σύστημα (πλακέτες, σκληροί δίσκοι, οδηγόι δισκέτας, κάρτες, κλπ.) να είναι συναρμολογημένα από το εργοστάσιο κατασκευής του εξυπηρετητή.	ΝΑΙ		
2.1.3	Οι εξυπηρετητές θα πρέπει να δύνανται να εγκατασταθούν σε υφιστάμενα 42U racks 19 ιντσών, με εφαρμογή των βέλτιστων πρακτικών και υλικών (π.χ. μπράτσα οδηγών κλπ) για τη διαχείριση των καλωδίων και την εύκολη τεχνική υποστήριξη χωρίς την ανάγκη αποσύνδεσης του εξυπηρετητή.	ΝΑΙ		
2.1.4	Δυνατότητα εγκατάστασης και τεχνικής υποστήριξης δίχως χρήση εργαλείων (tool-free).	ΝΑΙ		
2.1.5	<p>Τεχνολογία επεξεργαστή Intel Xeon E7-2820 ή μεταγενέστερη (ισοδύναμη ή καλύτερη).</p> <p>Σε κάθε περίπτωση θα πρέπει να υπάρχει πλήρης συμβατότητα με την υφιστάμενη υποδομή που βασίζεται σε IBM 3690 X5 – 7147ZHU, 16 CPU Intel®Xeon® E7-2820@2GHz με 256GB RAM σε συνδυασμό με VMware ESXi v.5.1.0. και VMware vSphere Client v.5.1.0.</p> <p>Η συμβατότητα θα πρέπει να προκύπτει από τον επίσημο οδηγό συμβατότητας της VMWare (VMWare compatibility guide), που θα περιλαμβάνεται στην τεκμηρίωση</p>	ΝΑΙ		

A/A	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	της προσφοράς.			
2.1.6	Να υποστηρίζεται λειτουργία "Live Migration" των εικονικών μηχανών με την υφιστάμενη υποδομή εικονικοποίησης της Ελληνικής Αστυνομίας.	ΝΑΙ		
2.1.7	Συνολικός αριθμός πυρήνων (cores) ανά εξυπηρετητή	≥ 16		
2.1.8	Συνολικός αριθμός νημάτων (threads) ανά εξυπηρετητή	≥ 32		
2.1.9	Μνήμη Cache ανά CPU Socket	≥ 18 Mb		
2.1.10	Αρχιτεκτονική 64bit	ΝΑΙ		
2.1.11	Ονομαστικός χρονισμός των προσφερόμενων επεξεργαστών	≥ 2 GHz		
2.1.12	Πλήρης υποστήριξη hardware assisted virtualization με τα κατάλληλα extensions	ΝΑΙ		
2.1.13	Τύπος Μνήμης DDR3 ή DDR4	ΝΑΙ		
2.1.14	Ταχύτητα μνήμης	≥1066 MHz		
2.1.15	Συνολική χωρητικότητα προσφερόμενης μνήμης ανά εξυπηρετητή	≥ 256 GB		
2.1.16	Να μπορεί να αναβαθμιστεί στα 512GB στο προσφερόμενο σασί, χωρίς την αντικατάσταση των προσφερόμενων μνημών.	ΝΑΙ		
2.1.17	Να περιγραφεί η διάταξη (Αριθμός και είδος Dimm module ανά περίπτωση) για να επιτευχθούν οι ανωτέρω προδιαγραφές (2.1.15, 2.1.16).	ΝΑΙ		
2.1.18	Hardware RAID controller με RAID 0, 1, 10.	ΝΑΙ		
2.1.19	Πλήθος προσφερόμενων μονάδων εσωτερικών δίσκων ανά Σύστημα.	≥2		
2.1.20	Πλήθος υποστηριζόμενων μονάδων	ΝΑΙ		

A/A	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	εσωτερικών δίσκων ανά Σύστημα (μέγιστος αριθμός). Να αναφερθεί.			
2.1.21	Διάταξη προσφερόμενων μονάδων εσωτερικών δίσκων RAID 1.	ΝΑΙ		
2.1.22	Μονάδες εσωτερικών HDD ή SSD τεχνολογίας SAS. Το ενδεχόμενο προσφοράς SSD αξιολογείται θετικά.	ΝΑΙ		
2.1.23	Ταχύτητα περιστροφής σε περίπτωση HDD.	≥ 10 Krpm		
2.1.24	Χωρητικότητα εκάστου HDD ή SSD.	≥ 500 GB		
2.1.25	Να αναφερθεί το φυσικό μέγεθος των HDD ή SDD σε ίντσες.	ΝΑΙ		
2.1.26	Αναγνώστης οπτικών ψηφιακών δίσκων (CD/DVD).	ΝΑΙ		
2.1.27	Θύρες PCI Express.	≥ 5		
2.1.28	Να διαθέτει Hot-swap μονάδες τροφοδοσίας.	≥ 2		
2.1.29	Να διαθέτει Hot-swap μονάδες ψύξης.	ΝΑΙ		
2.1.30	Ο εξυπηρετητής να διαθέτει onboard diagnostics panel με indicators καλής λειτουργίας – να αναφερθούν αναλυτικά.	ΝΑΙ		
2.1.31	Να γίνει αναφορά σε άλλα χαρακτηριστικά του server που δύναται να βελτιώσουν τη διαθεσιμότητά του (βλ. Κεφάλαιο «ΔΙΑΘΕΣΙΜΟΤΗΤΑ-ΡΗΤΡΕΣ») π.χ. πρόγνωση βλαβών.	ΝΑΙ		
2.1.32	Συνολικός αριθμός θυρών (ports) Gigabit Ethernet (RJ-45) ή καλύτερων.	≥ 8		
2.1.33	Αριθμός θυρών Οπτικής Ίνας (Fibre Channel) ανά εξυπηρετητή.	≥ 2		
2.1.34	Ταχύτητα επικοινωνίας θυρών Fibre Channel.	≥ 4 Gbps		

A/A	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
2.1.35	Ο Ανάδοχος σε κάθε περίπτωση εγγυάται την ομαλή εκκίνηση του συστήματος με όλα τα προσφερόμενα περιφερειακά συνδεδεμένα σε αυτόν και σε πλήρη λειτουργία.	ΝΑΙ		
2.1.36	Παροχή των εγχειριδίων χρήσης - διαχείρισης σε ηλεκτρονική μορφή ή/και σε έντυπη μορφή.	ΝΑΙ		
2.1.37	Πιστοποίηση CE ή άλλη ισοδύναμη (συνοδευόμενη από έγγραφη τεκμηρίωση ισοδυναμίας).	ΝΑΙ		
2.1.38	Να αναφερθούν πιστοποιήσεις ISO και λοιπά κατασκευαστικά standards.	ΝΑΙ		
2.2	FC SAN Switches			
2.2.1	FC SAN Switches Rack Mounted με τα παρακάτω χαρακτηριστικά έκαστο:	2		
2.2.2	Να αναφερθεί η εταιρεία κατασκευής και το προσφερόμενο μοντέλο.	ΝΑΙ		
2.2.3	Να αναφερθεί το ύψος σε U του προσφερόμενου προϊόντος.	ΝΑΙ		
2.2.4	Εγκατάσταση σε διάταξη υψηλής διαθεσιμότητας (failover).	ΝΑΙ		
2.2.5	Τρόπος διάταξης (active-active).	ΝΑΙ		
2.2.6	Να συνοδεύεται από όλα τα απαιτούμενα για την εγκατάσταση υλικά (μπράτσα οδηγών κ.λ.π.) στο ικρίωμα (rack).	ΝΑΙ		
2.2.7	Να διατεθεί όλος ο εξοπλισμός που απαιτείται για την εγκατάσταση των συσκευών (καλώδια ρευματοδοσίας κ.λ.π.).	ΝΑΙ		
2.2.8	Αριθμός οπτικών SFP θυρών.	≥ 16		
2.2.9	Αριθμός ενεργών οπτικών SFP θυρών.	≥ 16		

A/A	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
2.2.10	Αριθμός Transceiver modules SFP-LC 8Gbps.	≥ 16		
2.2.11	Οπτικές ίνες LC-LC μήκους τουλάχιστον 10 μέτρων.	16		
2.2.12	Οπτικές ίνες LC-LC μήκους τουλάχιστον 3 μέτρων.	16		
2.2.13	Αριθμός θυρών διαχείρισης Ethernet (RJ45).	≥ 1		
2.2.14	Λογισμικό παρακολούθησης, ελέγχου, διαχείρισης, και αρχείων καταγραφής (logs) μέσω HTTP, SSH2, CLI και SNMP.	ΝΑΙ		
2.2.15	Αυτόματη ανίχνευση ταχύτητας θυρών.	ΝΑΙ		
2.2.16	Υποστήριξη ταχυτήτων τουλάχιστον 2 και 4 Gbps. Να αναφερθεί τυχόν υποστήριξη υψηλότερων ταχυτήτων.	ΝΑΙ		
2.2.17	Αθροιστικό bandwidth συσκευής.	≥ 64 Gbps		
2.2.18	Θύρα USB.	≥ 1		
2.2.19	Υποστήριξη τεχνολογίας VSAN.	ΝΑΙ		
2.2.20	Να αναφερθούν οι υποστηριζόμενες τεχνικές ασφάλισης ποιότητας (QoS).	ΝΑΙ		
2.2.21	Υποστήριξη πρωτοκόλλων όπως TACACS+, RADIUS κ.λ.π.	ΝΑΙ		
2.2.22	Υποστήριξη ISL Trunking.	ΝΑΙ		
B)	ΛΟΓΙΣΜΙΚΑ S/W			
2.3	Λογισμικό Εικονικοποίησης ESXi			
2.3.1	Να προσφερθεί η κατάλληλη έκδοση του λογισμικού εικονικοποίησης VMWare ESXi με όλες τις απαραίτητες άδειες χρήσης για τους υπό προμήθεια εξυπηρετητές προκειμένου να επιτυγχάνεται η ένταξη και η πλήρης συμβατότητα με την υφιστάμενη υποδομή εικονικοποίησης.	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Να αναφερθεί η προσφερόμενη έκδοση και ο αριθμός των αδειών.			
2.4	Λειτουργικά Συστήματα			
2.4.1	<p>Να προσφερθούν όλες οι πλέον πρόσφατες συνιστώμενες εκδόσεις των απαραίτητων Λειτουργικών Συστημάτων και οι άδειες χρήσης τους για την εγκατάσταση και λειτουργία όλων των εικονικών εξυπηρετητών που θα δημιουργηθούν για τις ανάγκες λειτουργίας και διαχείρισης του ολοκληρωμένου συστήματος.</p> <p>Μεταξύ αυτών περιλαμβάνονται:</p> <ul style="list-style-type: none"> • Τα λειτουργικά συστήματα των Active Directory Servers • Τα λειτουργικά συστήματα των εξυπηρετητών του υποσυστήματος DLP. • Τα λειτουργικά συστήματα των τυχόν επιπλέον εξυπηρετητών κεντρικής διαχείρισης του ολοκληρωμένου συστήματος. <p>Να αναφερθούν όλοι οι τυχόν απαραίτητοι εξυπηρετητές που θα δημιουργηθούν και τα προσφερόμενα Λειτουργικά Συστήματα αυτών.</p>	ΝΑΙ		
2.4.2	Οι προσφερόμενες εκδόσεις (άδειες) των Λειτουργικών Συστημάτων θα πρέπει να υποστηρίζουν τη λειτουργία όλων των εικονικών εξυπηρετητών σε ένα φυσικό μηχάνημα σε περίπτωση δυσλειτουργίας του άλλου.	ΝΑΙ		
2.4.3	Ειδικότερα για το Active Directory Server, ο Ανάδοχος θα πρέπει να εγκαταστήσει την πλέον πρόσφατη έκδοση που κυκλοφορεί κατά το χρόνο υλοποίησης της εγκατάστασης, με τα απαραίτητα CALS (εφόσον υπάρχουν), χωρίς επιπλέον κόστος.	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
2.5	Λογισμικό υποσυστήματος DLP			
2.5.1	<p>Να προσφερθούν όλα τα απαραίτητα λογισμικά και οι άδειες χρήσης τους για την εγκατάσταση και λειτουργία του υποσυστήματος DLP, τόσο για:</p> <p>Τους εξυπηρετητές του συστήματος</p> <p>Τις κονσόλες διαχείρισης και</p> <p>Τους πελάτες (clients) του συστήματος.</p> <p>Να αναφερθούν όλοι οι τυχόν απαραίτητοι εξυπηρετητές που θα δημιουργηθούν για τα προσφερόμενα λογισμικά του υποσυστήματος DLP και να περιγραφεί η χρήση τους.</p>	ΝΑΙ		
2.5.2	<p>Να αναφερθούν τα εκτιμώμενα απαιτούμενα χαρακτηριστικά πόρων των εξυπηρετητών του υποσυστήματος DLP για την κάλυψη των αναγκών του έργου.</p>	ΝΑΙ		
2.5.3	<p>Αριθμός προσφερόμενων αδειών χρήσης για σταθμούς εργασίας υπό προστασία.</p>	≥ 250		
2.5.3.1.	<p>Να αναφερθεί αν ο/οι εξυπηρετητής/ές του DLP απαιτούν ξεχωριστή άδεια χρήσης ή αν παρέχονται δωρεάν με τις άδειες των σταθμών εργασίας από τον κατασκευαστή (χωρίς να αναφέρεται στην τεχνική προσφορά τυχόν κόστος).</p>	ΝΑΙ		
2.5.4	<p>Να αναφερθούν τα επιμέρους προϊόντα και ο κατασκευαστής της προσφερόμενης λύσης.</p> <p>Τα λογισμικά θα εγκατασταθούν στους σταθμούς εργασίας που θα υποδειχθούν από τη Δ/νση Πληροφορικής του Αρχηγείου της Ελληνικής Αστυνομίας.</p> <p>Υποστήριξη των ακόλουθων λειτουργικών της Microsoft:</p>	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>Windows XP, 7, 8, 10, Windows Server 2000, Windows Server 2003, Windows Server 2008 (R2), Windows Server 2012 (R2).</p> <p>Να αναφερθεί τυχόν υποστήριξη άλλων λειτουργικών συστημάτων.</p>			
2.5.4.1.	<p>Η προσφερόμενη λύση θα πρέπει να παρέχει λογισμικό αποτροπής διαρροής πληροφοριών, για σταθμούς εργασίας και εξυπηρετητές κοινής χρήσης αρχείων (File Servers), με πλήρη υποστήριξη ελληνικών.</p> <p>Εφόσον για τη λειτουργία αυτή απαιτείται διαφορετική αδειοδότηση λογισμικού, να αναφερθεί και να προσφέρονται τουλάχιστον 20 άδειες για εξυπηρετητές από τις 250 συνολικές άδειες που αναφέρθηκαν παραπάνω.</p>	ΝΑΙ		
2.5.4.2.	<p>Η προσφερόμενη λύση θα πρέπει να παρέχει λογισμικό κατηγοριοποίησης (data classification), για σταθμούς εργασίας και εξυπηρετητές κοινής χρήσης αρχείων, με πλήρη υποστήριξη ελληνικών.</p> <p>Η εν λόγω λειτουργικότητα δύναται να είναι ενσωματωμένη στο λογισμικό αποτροπής διαρροής πληροφοριών ή να παρέχεται από άλλο λογισμικό.</p>	ΝΑΙ		
2.5.4.3.	<p>Η προσφερόμενη λύση θα πρέπει να παρέχει λογισμικό κρυπτογράφησης (data encryption), για σταθμούς εργασίας και εξυπηρετητές κοινής χρήσης αρχείων.</p> <p>Η εν λόγω λειτουργικότητα δύναται να είναι ενσωματωμένη στο λογισμικό αποτροπής διαρροής πληροφοριών ή να παρέχεται από άλλο λογισμικό.</p>	ΝΑΙ		
2.5.5	<p>Να περιγραφεί ο τρόπος επικοινωνίας του συστήματος με τους Η/Υ που έχει ενεργοποιηθεί η</p>	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	προστασία αποτροπής διαρροής πληροφοριών.			
2.5.6	<p>Δυνατότητα ελέγχου, καταγραφής και αποτροπής της χρήσης ευαίσθητων δεδομένων στα τερματικά των χρηστών καλύπτοντας κατ' ελάχιστον τα ακόλουθα:</p> <ul style="list-style-type: none"> • ενέργειες σε αρχεία (open, read, edit, write, move, copy, rename, delete, print), • αντιγραφή/επικόλληση δεδομένων (copy/paste), • εξαγωγή δεδομένων από εφαρμογές (export, save as, print κ.α.), • εκκίνηση διεργασιών (process launch), • αποστολή δεδομένων μέσω δικτύου (FTP, network share, κτλ) ανεξαρτήτως πρωτοκόλλου, • αποστολή δεδομένων μέσω email (ως επισυναπτόμενο αρχείο ή μέσα στο κυρίως μέρος του μηνύματος - message body), • αποθήκευση δεδομένων σε εξωτερικά αποθηκευτικά μέσα (USB Stick, HDD, SSD, φορητές συσκευές τηλεφώνων ή tablets), • εγγραφή σε CD/DVD, • Εντοπισμός και αποτροπή Clipboard operations και Print Screen. 	ΝΑΙ		
2.5.7	Δυνατότητα εξαιρέσης επιλεγμένων συσκευών από τις εφαρμοζόμενες πολιτικές.	ΝΑΙ		
2.5.8	Δυνατότητα αποτροπής του χρήστη από τροποποίηση της λειτουργίας του λογισμικού.	ΝΑΙ		
2.5.9	Δυνατότητα παραγωγής παραμετροποιημένων μηνυμάτων προς τους χρήστες.	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
2.5.10	<p>Δυνατότητα εφαρμογής πολιτικών αποτροπής διαρροής πληροφοριών βάσει:</p> <ul style="list-style-type: none"> • Μηχανήματος (Η/Υ). • Χρήστη (Η/Υ). <p>Να περιγραφεί εν συντομία ο τρόπος και οι απαραίτητες προϋποθέσεις εφαρμογής.</p>	ΝΑΙ		
2.5.11	<p>Να περιγραφεί ο τρόπος διαχείρισης των συσκευών μόνο ανάγνωσης (read only devices).</p>	ΝΑΙ		
2.5.12	<p>Υποστήριξη συσκευών αποθήκευσης δεδομένων (repository) χωρίς την ανάγκη εγκατάστασης σ' αυτές λογισμικού DLP server ή client.</p> <p>Να αναφερθεί ο τρόπος προστασίας των δεδομένων τους.</p>	ΝΑΙ		
2.5.13	<p>Να αναφερθούν οι τεχνικές-μέθοδοι και δυνατότητες ανάλυσης-κατηγοριοποίησης δεδομένων που χρησιμοποιεί το προσφερόμενο λογισμικό.</p>	ΝΑΙ		
2.5.14	<p>Δυνατότητα κατηγοριοποίησης δεδομένων βάσει κανονικών εκφράσεων (regular expressions).</p>	ΝΑΙ		
2.5.15	<p>Δυνατότητα αναγνώρισης και διαχωρισμού τύπων προσωπικών ή ευαίσθητων προσωπικών δεδομένων (τηλεφωνικά νούμερα, ΑΜΚΑ κλπ.).</p>	ΝΑΙ		
2.5.16	<p>Να αναφερθεί αν το προσφερόμενο λογισμικό έχει δυνατότητα αναγνώρισης και διαχείρισης Ψηφιακών Πνευματικών Δικαιωμάτων.</p> <p>Να αναφερθούν οι δυνατότητες διαχείρισής τους.</p>	ΝΑΙ		
2.5.17	<p>Να αναφερθούν όλοι οι τύποι δεδομένων που υποστηρίζονται από το προσφερόμενο λογισμικό χωρίς επιπλέον κόστος, τα οποία θα πρέπει να είναι κατ' ελάχιστον doc, docx,</p>	ΝΑΙ		

A/A	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	txt, pdf, pdf/a, xls, xlsx, accdb, jpg.			
2.5.18	Να αναφερθούν τυχόν επιπλέον τύποι δεδομένων που υποστηρίζονται από το λογισμικό με επιπλέον χρέωση.	ΝΑΙ		
2.5.19	Δυνατότητα αναγνώρισης εφαρμογών ανεξαρτήτου θύρας (application port) λειτουργίας.	ΝΑΙ		
2.5.20	Να αναφερθούν τα υποστηριζόμενα πρωτόκολλα εφαρμογών.	ΝΑΙ		
2.5.21	Δυνατότητα δημιουργίας πολιτικών με λογικά AND/OR και εξαιρέσεις.	ΝΑΙ		
2.5.22	Δυνατότητα δημιουργίας συνδυασμών πολιτικών.	ΝΑΙ		
2.5.23	Να αναφερθούν τα είδη των περιεχομένων (π.χ. παραλήπτης, πρωτόκολλο, όνομα αρχείου) που μπορεί να περιέχονται στους κανόνες των πολιτικών.	ΝΑΙ		
2.5.24	Δυνατότητα εφαρμογής διαφορετικών πολιτικών αντίδρασης του συστήματος ανάλογα με τον εντοπιζόμενο βαθμό επικινδυνότητας ενός περιστατικού, με συνυπολογισμό και των ταυτόχρονων παραβιαζόμενων κανόνων.	ΝΑΙ		
2.5.25	Το υποσύστημα του λογισμικού DLP θα πρέπει να μπορεί να ενσωματώσει λειτουργία αναγνώρισης χρηστών από Active Directory.	ΝΑΙ		
2.5.26	Να αναφερθούν τα τυχόν υποστηριζόμενα εργαλεία κατηγοριοποίησης δεδομένων τρίτων κατασκευαστών.	ΝΑΙ		
2.5.27	Να αναφερθεί τυχόν δυνατότητα να συνεργαστεί το προσφερόμενο σύστημα DLP με Υποσύστημα DLP περιμετρικής προστασίας (Network	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	DLP). Να αναφερθούν συμβατές συσκευές (Network DLP) και οι πρόσθετες δυνατότητες που παρέχονται κατά τη συνεργασία τους, εφόσον δε λειτουργούν ανεξάρτητα.			
2.5.28	Δυνατότητα παραγωγής αυτόματων περιοδικών και κατ' απαίτηση τεχνικών και διοικητικών αναφορών αποτροπής περιστατικών διαρροής δεδομένων.	ΝΑΙ		
2.5.29	Να αναφερθεί τυχόν δυνατότητα αποστολής των τεχνικών και διοικητικών αναφορών αποτροπής περιστατικών μέσω e-mail.	ΝΑΙ		
2.5.30	Δυνατότητα για online update του λογισμικού των Η/Υ από τον εξυπηρετητή του συστήματος.	ΝΑΙ		
2.5.31	Δυνατότητα για online update του εξυπηρετητή του συστήματος DLP από το Διαδίκτυο, μέσω Proxy.	ΝΑΙ		
2.5.32	<p>Να αναφερθούν οι δυνατές ενέργειες κατά την ανίχνευση απόπειρας διαρροής των υπό προστασία δεδομένων που εφαρμόζονται αυτόματα από το λογισμικό ή εμφανίζονται ως ειδοποιήσεις ή επιλογές στο χρήστη ή στο διαχειριστή.</p> <p>Ελάχιστα απαιτούνται:</p> <ul style="list-style-type: none"> • Απλή καταγραφή ενέργειας, • Αποτροπή ενέργειας, • Ειδοποίηση χρήστη και αποτροπή ενέργειας, • Ειδοποίηση χρήστη με δυνατότητα συνέχισης ενέργειας, • Ειδοποίηση χρήστη με δυνατότητα συνέχισης ενέργειας κατόπιν εξουσιοδότησης, • Αποτροπή με ειδοποίηση προϊσταμένου, 	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<ul style="list-style-type: none"> Δυνατότητα συνέχισης ενέργειας με ειδοποίηση προϊσταμένου. <p>Σε κάθε περίπτωση θα πρέπει να υπάρχει δυνατότητα καταγραφής όλων των ενεργειών.</p>			
2.5.33	Αυτόματη κατηγοριοποίηση και χαρακτηρισμός των δεδομένων βάσει του περιεχομένου τους ή μέρους αυτού (content inspection / pattern-matching).	ΝΑΙ		
2.5.34	<p>Αυτόματη κατηγοριοποίηση και χαρακτηρισμός των δεδομένων ανάλογα με την προέλευσή τους όπως:</p> <ul style="list-style-type: none"> Διεύθυνση IP εξυπηρετητή, Διαδρομή URL, client εφαρμογή, όνομα κοινόχρηστου πόρου (network share name), Φάκελος αποθήκευσης. <p>Να αναφερθούν τυχόν περισσότερες υποστηριζόμενες προελεύσεις.</p>	ΝΑΙ		
2.5.35	Δυνατότητα αυτόματης ανίχνευσης και κατηγοριοποίησης των ευαίσθητων δεδομένων που υπάρχουν ήδη σε κοινόχρηστους καταλόγους (file shares), τοπικούς δίσκους (local drives), φορητά αποθηκευτικά μέσα (removable drives) και άλλα συστήματα.	ΝΑΙ		
2.5.36	Να αναφερθεί τυχόν δυνατότητα ανάλυσης και αναγνώρισης ευαίσθητων δεδομένων στο περιεχόμενο συμπιεσμένων αρχείων, καθώς και τα είδη των υποστηριζόμενων συμπιεσμένων αρχείων.	ΝΑΙ		
2.5.37	Δυνατότητα κατηγοριοποίησης αρχείων από τον τελικό χρήστη.	ΝΑΙ		
2.5.38	Περιορισμός της αποθήκευσης κατηγοριοποιημένων δεδομένων στο	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>τερματικό του χρήστη σε προκαθορισμένη μόνο τοποθεσία (κατάλογο) στην οποία θα εφαρμόζονται οι κατάλληλες πολιτικές ορθής χρήσης.</p> <p>Κάθε προσπάθεια αποθήκευσης κατηγοριοποιημένων δεδομένων σε τοποθεσία, μη προκαθορισμένη από την πολιτική, θα αποτρέπεται.</p>			
2.5.39	<p>Έλεγχος ή/και απαγόρευση της εξαγωγής ευαίσθητων δεδομένων από βάσεις δεδομένων, όταν η πρόσβαση γίνεται μέσω εφαρμογών όπως Toad, SQL Enterprise κτλ.</p> <p>Σε περιπτώσεις που η εξαγωγή ευαίσθητων δεδομένων είναι επιθυμητή, η αποθήκευσή τους θα πρέπει να γίνεται σε προκαθορισμένες και μόνο τοποθεσίες στα τερματικά των χρηστών, στις οποίες θα εφαρμόζονται οι κατάλληλες πολιτικές, όπως αυτές θα καθοριστούν κατά τη μελέτη εφαρμογής.</p>	ΝΑΙ		
2.5.40	<p>Έλεγχος, της αποθήκευσης ευαίσθητων δεδομένων σε φορητά αποθηκευτικά μέσα, εφαρμόζοντας κατάλληλες πολιτικές με δυνατότητα καταγραφής ή και απαγόρευσης εκτέλεσης της ενέργειας.</p>	ΝΑΙ		
2.5.41	<p>Αποτροπή της διαρροής ευαίσθητων δεδομένων μέσω ηλεκτρονικής ταχυδρομείου με χρήση τόσο webmail όσο και email client, ελέγχοντας ενέργειες όπως επισύναψη αρχείου, επικόλληση στο κυρίως σώμα του μηνύματος, απευθείας προώθηση κτλ. εφαρμόζοντας κατάλληλες πολιτικές ανά διεύθυνση αποστολέα/παραλήπτη, domain κτλ.</p>	ΝΑΙ		
2.5.42	<p>Δυνατότητα αυτόματης κρυπτογράφησης των ευαίσθητων δεδομένων κατά την αποθήκευση</p>	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>τους:</p> <ul style="list-style-type: none"> σε προκαθορισμένη τοποθεσία στο τερματικό του χρήστη, σε φορητά αποθηκευτικά μέσα, ως e-mail attachment, <p>με δυνατότητα ανάκτησης μόνο σε τερματικό στο οποίο είναι εγκατεστημένος ο αντίστοιχος μηχανισμός (DLP agent).</p>			
2.5.43	<p>Αποτροπή διαρροής ευαίσθητων δεδομένων μέσω client εφαρμογής (π.χ. IM, P2P, social media, cloud storage κ.α.), IP διεύθυνση / πόρτα προορισμού, δικτυακή τοποθεσία, URL/UNC path, τύπος δικτύου (ενσύρματο, ασύρματο, Bluetooth κ.α.) κτλ.</p>	<p>ΝΑΙ</p>		
2.6	<p>Λογισμικό υποσυστήματος Active Directory</p>			
2.6.1	<p>Active Directory Server στην πλέον πρόσφατη διαθέσιμη έκδοση.</p> <p>Να αναφερθούν το Όνομα – Έκδοση – Κατασκευαστής – Τύπος – Χρονολογία διάθεσης του προσφερόμενου λογισμικού.</p>	<p>ΝΑΙ</p>		
2.6.2	<p>Αριθμός εξυπηρετητών που θα εγκατασταθούν στην υπό προμήθεια υποδομή VM, με τις αντίστοιχες άδειες για οργανισμούς του Δημοσίου.</p>	<p>≥ 2</p>		
2.6.3	<p>Αριθμός προσφερόμενων Αδειών χρήσης για οργανισμούς του Δημοσίου Active Directory για συσκευές (CALs per device) που θα ενταχθούν στο Domain (per device).</p>	<p>≥ 1000</p>		
2.6.4	<p>Δυνατότητα περιορισμού της πρόσβασης σε servers που αποθηκεύουν ευαίσθητα δεδομένα μόνο σε τερματικά που διαθέτουν τον αντίστοιχο DLP agent.</p>	<p>ΝΑΙ</p>		

A/A	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
2.6.5	Λειτουργία Single Sign On με τις υφιστάμενες Web εφαρμογές της Ελληνικής Αστυνομίας.	ΝΑΙ		
2.6.6	Το υποσύστημα του λογισμικού DLP θα πρέπει να μπορεί να ενσωματωθεί πλήρως στην αρχιτεκτονική του υπό προμήθεια συστήματος Active Directory.	ΝΑΙ		
2.6.7	Δυνατότητα δημιουργίας Domains και Subdomains.	ΝΑΙ		
2.6.8	Δυνατότητα δημιουργίας εμπιστοσύνης (Trust) από και προς συστήματα MS Active Directory και Samba Active Directory.	ΝΑΙ		
2.6.9	Εγγενής δυνατότητα διαχείρισης των MS Windows συσκευών που έχουν ενταχθεί στο Domain του.	ΝΑΙ		
2.6.10	Δυνατότητα δημιουργίας "Group Policy Preferences".	ΝΑΙ		
2.6.11	Δυνατότητα δημιουργίας "Security Silos".	ΝΑΙ		
2.6.12	Εγγενής δυνατότητα διανομής και εγκατάστασης λογισμικού στους Η/Υ που έχουν ενταχθεί στο Domain του.	ΝΑΙ		
2.6.13	Συμβατότητα με LDAP.	ΝΑΙ		
2.6.14	Δυνατότητα ένταξης εξυπηρετητών αρχείων στο Domain.	ΝΑΙ		
	ΚΕΝΤΡΙΚΗ ΚΟΝΣΟΛΑ ΔΙΑΧΕΙΡΙΣΗΣ			
2.7	Οι προσφερόμενες λύσεις θα πρέπει να διαθέτουν γραφικό περιβάλλον διεπαφής του διαχειριστή, με μορφή κεντρικής κονσόλας, με τα ακόλουθα χαρακτηριστικά:	ΝΑΙ		
2.7.1	Να υποστηρίζεται, μεμονωμένα ή συνδυαστικά, η δυνατότητα αυτόματης και χειροκίνητης	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	απομακρυσμένης εγκατάστασης λογισμικού για τους περιφερειακούς σταθμούς (clients) αδιαφανώς για το χρήστη (transparent installation).			
2.7.2	Να παρέχεται, μεμονωμένα ή συνδυαστικά, η δυνατότητα απομακρυσμένης απεγκατάστασης υφιστάμενων λογισμικών DLP, Antivirus ή Firewalls, συμπεριλαμβανομένων κρυμμένων rootkits και κατάλοιπων λύσεων τρίτων κατασκευαστών.	ΝΑΙ		
2.7.3	Να παρέχεται, μεμονωμένα ή συνδυαστικά, η δυνατότητα απομακρυσμένης εκτέλεσης scripts στους περιφερειακούς σταθμούς.	ΝΑΙ		
2.7.4	Να υποστηρίζεται αυτοματοποιημένος τρόπος ανανέωσης των ενημερώσεων, καθώς και των προγραμμάτων (software updates) που αφορούν τα λογισμικά του DLP με τη μέθοδο προώθησης (push) από τον κεντρικό εξυπηρετητή.	ΝΑΙ		
2.7.5	Να υποστηρίζεται η δυνατότητα εντοπισμού περιφερειακών σταθμών που δεν έχουν λάβει τις πιο πρόσφατες ενημερώσεις. Για το σύνολο των σταθμών ή/και κάθε ένα ξεχωριστά να προσφέρεται τουλάχιστον η δυνατότητα απευθείας εγκατάστασης (push) των ενημερώσεων αδιαφανώς για τους χρήστες.	ΝΑΙ		
2.7.6	Να υποστηρίζεται η δυνατότητα ειδοποίησης του διαχειριστή σε επιλεγόμενες κατηγορίες συμβάντων ή απαγορευμένης ενέργειας. Να αναφερθεί ο τρόπος ειδοποίησης και η δυνατότητα αυτοματοποίησης περαιτέρω ενεργειών του διαχειριστή.	ΝΑΙ		

3. ΥΠΗΡΕΣΙΕΣ ΥΛΟΠΟΙΗΣΗΣ ΕΓΚΑΤΑΣΤΑΣΗΣ ΚΑΙ ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗΣ

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
3.1.	<p>Η προσφερόμενη λύση θα πρέπει να εγκατασταθεί στο προσφερόμενο υλικό σε εικονικό περιβάλλον (virtual environment) που θα δημιουργηθεί από τον Ανάδοχο για το σκοπό αυτόν. Ο Ανάδοχος υποχρεούται να τεκμηριώσει στη Μελέτη Εφαρμογής την προτεινόμενη αρχιτεκτονική εγκατάσταση για την προσφερόμενη λύση λαμβάνοντας υπ' όψη τα χαρακτηριστικά του δικτύου της Ελληνικής Αστυνομίας (βάσει της υπάρχουσας υποδομής που περιγράφεται στην παρούσα διακήρυξη).</p>	ΝΑΙ		
3.2.	<p>Ο Ανάδοχος υποχρεούται εντός 30 ημερών από την υπογραφή της Σύμβασης και κατόπιν συνεντεύξεων με στελέχη της Δ/σης Πληροφορικής /Α.Ε.Α. και των Υπηρεσιών στις οποίες θα ενεργοποιηθεί η χρήση του συστήματος, να παραδώσει τεύχος Μελέτης Εφαρμογής, το οποίο θα πρέπει να γίνει αποδεκτό από τη Διεύθυνση Πληροφορικής της Ελληνικής Αστυνομίας, πριν την έναρξη της υλοποίησης.</p> <p>Η Μελέτη Εφαρμογής επιδέχεται τροποποιήσεων μόνο κατόπιν έγκρισης ή κατ' απαίτηση του Αγοραστή, ακόμα και μετά την έναρξη της υλοποίησης, χωρίς επιπλέον χρέωση (εξαιρείται η άσκηση του δικαιώματος κατά τρόπο που υπερβαίνει τα όρια της καλής πίστης).</p> <p>Στη Μελέτη Εφαρμογής θα</p>	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	περιλαμβάνονται κατ' ελάχιστον:			
3.2.1.	<p>Οριστικοποίηση του αριθμού, των ειδών και των χαρακτηριστικών (πυρήνες, μέγεθος μνήμης, χωρητικότητα σκληρών δίσκων, κάρτες δικτύου) των εξυπηρετητών και των λογισμικών που θα απαιτηθούν για την εγκατάσταση του συστήματος σε εικονικό περιβάλλον λαμβάνοντας υπόψη:</p> <ul style="list-style-type: none"> ο Τis υφιστάμενες υποδομές της Ελληνικής Αστυνομίας, ο Τη διασφάλιση υψηλής διαθεσιμότητας, ο Τη διασφάλιση της Ασφάλειας του συστήματος, ο Τη δυνατότητα επαναφοράς του συστήματος σε προγενέστερη κατάσταση, ο Τη δυνατότητα επέκτασης του συστήματος. 	ΝΑΙ		
3.2.2.	<p>Όλη την Αρχιτεκτονική των υπό εγκατάσταση υποσυστημάτων – εξυπηρετητών του Συστήματος με σχεδιαγράμματα, τις αποστρατικοποιημένες ζώνες (DMZ) των υφιστάμενων Firewalls στις οποίες θα ενταχθούν τα υποσυστήματα στο Server Farm της Ελληνικής Αστυνομίας, το πλάνο διευθυνσιοδότησης IP που θα χρησιμοποιηθεί (σε συμφωνία με το υπάρχον), τις διεπαφές με άλλα συστήματα της Ελληνικής Αστυνομίας και τους κανόνες που θα εφαρμοστούν.</p>	ΝΑΙ		
3.2.3.	<p>Καταγραφή των αναγκαίων θυρών και κατευθύνσεων επικοινωνίας εκάστου εξυπηρετητή των Υποσυστημάτων και των περιφερειακών σταθμών που θα</p>	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	εγκατασταθεί το DLP.			
3.2.4.	Καταγραφή των απαραίτητων ρυθμίσεων και εγκαταστάσεων λογισμικών που θα πρέπει να διενεργηθούν στους σταθμούς εργασίας.	ΝΑΙ		
3.3.	Ο Ανάδοχος θα εγκαταστήσει τους εξυπηρετητές σε υφιστάμενα 42U racks 19 ιντσών στο Data Center της Δ/σης Πληροφορικής της Ελληνικής Αστυνομίας.	ΝΑΙ		
3.4.	Ο Ανάδοχος θα εγκαταστήσει τα προσφερόμενα FC Switches σε υφιστάμενα racks στο Data Center της Δ/σης Πληροφορικής της Ελληνικής Αστυνομίας.	ΝΑΙ		
3.5.	Ο Ανάδοχος θα υλοποιήσει τις διασυνδέσεις και παραμετροποιήσεις για συνεργασία με το υπάρχον Σύστημα Εξωτερικών Δίσκων μέσω των καρτών οπτικών ινών (Fibre Channel), με υψηλή διαθεσιμότητα ενεργού-παθητικού (active-passive) στις θύρες.	ΝΑΙ		
3.6.	Ο Ανάδοχος θα προβεί στην παραμετροποίηση και διασύνδεση όλου του υπό προμήθεια εξοπλισμού με την υπάρχουσα υποδομή (ESXi, VMWare Sphere, παραμετροποίηση εξυπηρετητών, δίκτυο δεδομένων, VLANs, δρομολόγηση, κλπ). Όλα τα απαιτούμενα VMs θα φιλοξενοούνται στο υφιστάμενο Storage της Ελληνικής Αστυνομίας.	ΝΑΙ		
3.7.	Ο Ανάδοχος θα προβεί στην παραμετροποίηση και δημιουργία της δομής Active Directory του φορέα	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	στους Active Directory Servers σύμφωνα με τα παρακάτω:			
3.7.1.	Δημιουργία του οργανογράμματος του φορέα μέσω αυτοματοποιημένης διαδικασίας, η οποία δύναται να προκύπτει από την υφιστάμενη Βάση Δεδομένων που χρησιμοποιούν και ενημερώνουν οι εφαρμογές της Ελληνικής Αστυνομίας.	ΝΑΙ		
3.7.2.	Εισαγωγή όλων των χρηστών της Ελληνικής Αστυνομίας στο ανωτέρω δέντρο οργανογράμματος του νέου Active Directory με την παραπάνω αυτοματοποιημένη διαδικασία.	ΝΑΙ		
3.7.3.	Αυτοματοποιημένη περιοδική ενημέρωση του οργανογράμματος, δημιουργίας, διαγραφής, μετακίνησης και απενεργοποίησης χρηστών στο δέντρο του νέου Active Directory σε συγχρονισμό με την υπάρχουσα Βάση Δεδομένων που χρησιμοποιούν και ενημερώνουν οι εφαρμογές της Ελληνικής Αστυνομίας.	ΝΑΙ		
3.7.4.	Ο ανάδοχος θα πρέπει να υλοποιήσει λειτουργία Single Sign On (SSO) μεταξύ του υπό εγκατάσταση υποσυστήματος Active Directory και του υφιστάμενου συστήματος εξουσιοδότησης χρηστών της Ελληνικής Αστυνομίας (Tivoli Access/Identification Manager).	ΝΑΙ		
3.8.	Ο Ανάδοχος θα προβεί σε σχεδιασμό και υλοποίηση της παραμετροποίησης του Συστήματος DLP για κατηγορίες δεδομένων, πολιτικές προστασίας, Η/Υ και χρήστες, ως ακολούθως:	ΝΑΙ		
3.8.1.	Ο Ανάδοχος θα πρέπει να παραδώσει καταγραφή με τις κατηγοριοποιήσεις	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>πληροφοριών και τις αντίστοιχες πολιτικές DLP που θα εφαρμόσει σε αυτές, οι οποίες θα προκύψουν από τις συνεντεύξεις με στελέχη των Υπηρεσιών της Ελληνικής Αστυνομίας στις οποίες θα εγκατασταθεί η προστασία του συστήματος και θα περιλαμβάνει:</p> <ul style="list-style-type: none"> • Προτεινόμενες από τον Ανάδοχο κατηγοριοποιήσεις πληροφοριών και προτεινόμενες πολιτικές DLP, βάσει διεθνών προτύπων και βέλτιστων πρακτικών. • Επιθυμητές κατηγοριοποιήσεις πληροφοριών και πολιτικές DLP, κατά την κρίση των Υπηρεσιών της Ελληνικής Αστυνομίας στις οποίες θα εγκατασταθεί η προστασία του συστήματος. <p>Στις προτεινόμενες από τον Ανάδοχο πολιτικές θα πρέπει κατ' ελάχιστον να περιλαμβάνονται οι απαιτούμενες από την παρούσα ελάχιστες δυνατότητες του συστήματος.</p>			
3.8.2.	<p>Κατ' ελάχιστον θα δημιουργηθούν 3 κατηγορίες δεδομένων με κλιμακούμενες εφαρμοζόμενες πολιτικές ως εξής:</p> <p>Κατηγορία 1: Πληροφορία που εμπίπτει στην κατηγορία της περιορισμένης χρήσης ή προσωπικά δεδομένα, τοπικά αρχεία Η/Υ, αρχεία δικτυακών χώρων αποθήκευσης,</p> <p>Πολιτική: Καταγραφή κάθε ενέργειας των χρηστών.</p> <p>Κατηγορία 2: Πληροφορία που εμπίπτει στην κατηγορία του</p>	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>εμπιστευτικού ή ευαίσθητα προσωπικά δεδομένα, τοπικά αρχεία Η/Υ, αρχεία δικτυακών χώρων αποθήκευσης.</p> <p>Πολιτική: Αποτροπή αποστολής με e-mail σε εξυπηρετητή εκτός της Ελληνικής Αστυνομίας. Καταγραφή κάθε ενέργειας χρηστών.</p> <p>Κατηγορία 3: Πληροφορία που εμπίπτει στην κατηγορία μη ηλεκτρονικά διακινούμενης, τοπικά αρχεία Η/Υ, αρχεία δικτυακών χώρων αποθήκευσης.</p> <p>Πολιτική: Αποτροπή αποθήκευσης σε διαδρομές πέραν των προκαθορισμένων, αποτροπή εξαγωγής σε φορητή μονάδα αποθήκευσης, αποτροπή αποστολής με e-mail, καταγραφή κάθε ενέργειας, ειδοποίηση διαχειριστή και προϊσταμένου.</p> <p>Οι παραπάνω κατηγορίες και πολιτικές δύναται να αναπροσαρμοστούν κατά τις απαιτήσεις της προηγούμενης παραγράφου (3.8.1).</p>			
3.9.	<p>Ο Ανάδοχος θα προβεί στην:</p> <ul style="list-style-type: none"> • απένταξη περίπου 200 υφιστάμενων Η/Υ Υπηρεσιών της Ελληνικής Αστυνομίας από το υπάρχον Samba Active Directory και ένταξή τους στο νέο Active Directory, • εγκατάσταση και παραμετροποίηση του συστήματος DLP στους ανωτέρω Η/Υ. <p>Οι ανωτέρω εργασίες θα</p>	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	πραγματοποιηθούν με κατανομή περίπου 160 Η/Υ στο νομό Αττικής και 40 Η/Υ στο νομό Θεσσαλονίκης.			
3.9.1.	<p>Κατά την ένταξη των Η/Υ στο νέο Active Directory, ο Ανάδοχος υποχρεούται να προβεί σε όλες τις απαραίτητες ρυθμίσεις του νέου περιβάλλοντος χρήστη, ώστε να επιτυγχάνονται τουλάχιστον οι προηγούμενες λειτουργικότητες, για ένα μέσο όρο 3 χρηστών ανά Η/Υ, τουλάχιστον για τα παρακάτω:</p> <ol style="list-style-type: none"> 1. Μεταφορά τοπικών αρχείων χρηστών (user files), 2. Μεταφορά συντομεύσεων πρόσβασης σε δικτυακούς πόρους, 3. Μεταφορά Αγαπημένων χρήστη, 4. Επιλογή προεπιλεγμένου εκτυπωτή, 5. Μεταφορά δεδομένων και ρυθμίσεων MS Outlook. 	ΝΑΙ		
3.9.2.	Ο Ανάδοχος θα παραδώσει στη Δ/νση Πληροφορικής/Α.Ε.Α. πλάνο μετάπτωσης με τις εκτιμώμενες ημερομηνίες, τα στοιχεία των τεχνικών του και περιγραφή των εργασιών της μετάπτωσης στις Αστυνομικές Υπηρεσίες, προκειμένου η Δ/νση Πληροφορικής να εκδώσει τις σχετικές διαταγές ενημέρωσης των εμπλεκόμενων Υπηρεσιών.	ΝΑΙ		

4. ΕΚΠΑΙΔΕΥΣΕΙΣ

A/A	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
4.1	Στην προσφορά θα συμπεριλαμβάνονται 3 κατηγορίες εκπαιδεύσεων ως ακολούθως:	ΝΑΙ		
4.1.1.	<p>Παροχή εκπαίδευσης για την κεντρική διαχείριση όλων των εξυπηρετητών, του συστήματος Active Directory και του συστήματος DLP, σε 6 άτομα, προσωπικό της Δ/νσης Πληροφορικής /Α.Ε.Α. που θα περιλαμβάνει τουλάχιστον:</p> <ul style="list-style-type: none"> • 1 ημέρα για την παρουσίαση της συγκεκριμένης υλοποίησης, τη διαχείριση όλων των Εξυπηρετητών των δύο υποσυστημάτων (Active Directory και DLP). • 2 ημέρες για τη διαχείριση του Active Directory. • 2 ημέρες για τη δημιουργία και τροποποίηση πολιτικών ασφαλείας, δημιουργία και διαχείριση groups κλπ. <p>Η διάρκεια της προσφερόμενης εκπαίδευσης θα αναφέρεται σε ημέρες/άτομο.</p>	≥ 5		
4.1.2.	<p>Παροχή εκπαίδευσης για τη μερική – περιφερειακή διαχείριση των κατηγοριών και πολιτικών ασφαλείας του συστήματος DLP ανά Υπηρεσία εγκατάστασης, σε 30 άτομα, προσωπικό της Δ/νσης Πληροφορικής και των Υπηρεσιών εγκατάστασης του συστήματος, που θα αφορά τη διαχείριση του συστήματος DLP, δημιουργία ομάδων και διαχειριστών αυτών, διαχείριση των Clients του συστήματος από τους περιφερειακούς</p>	≥ 3		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>διαχειριστές, δημιουργία και εισαγωγή κανόνων, φίλτρων κατηγοριοποίησης, τροποποίησης πολιτικών, διαχείριση των Η/Υ και χρηστών του συστήματος, επισκόπηση των αρχείων καταγραφής και των ενεργειών των χρηστών σε πραγματικό χρόνο, προτεινόμενες ενέργειες σε βασικές κατηγορίες events, επίλυση δυσλειτουργιών με δημιουργία νέων κανόνων κλπ.</p> <p>Η διάρκεια της προσφερόμενης εκπαίδευσης θα αναφέρεται σε ημέρες/άτομο.</p>			
4.1.3.	<p>Παροχή εκπαίδευσης τελικών χρηστών διάρκειας 1 ημέρας/άτομο σε 50 άτομα, προσωπικό της Ελληνικής Αστυνομίας, για τη χρήση του συστήματος και θα περιλαμβάνει παρουσίαση του υλοποιημένου συστήματος στο επίπεδο που αφορά τους τελικούς χρήστες, αναφορά στους βασικούς κανόνες εντοπισμού ενδιαφέρουσας δραστηριότητας που έχουν υλοποιηθεί, λειτουργίες κατηγοριοποίησης των δεδομένων χρήστη κλπ.</p>	ΝΑΙ		
4.2	<p>Κατά τη διενέργεια των εκπαιδεύσεων θα πρέπει να παρασχεθεί εκπαιδευτικό υλικό σε έντυπη και σε ηλεκτρονική μορφή, τόσο για τους διαχειριστές όσο και για τους τελικούς χρήστες στην ελληνική γλώσσα.</p> <ul style="list-style-type: none"> - Το εκπαιδευτικό υλικό θα πρέπει να είναι προσαρμοσμένο στην υλοποίηση του παρόντος έργου περιγράφοντας τους κανόνες και τη λειτουργικότητα η οποία έχει υλοποιηθεί και εφαρμόζεται στα πλαίσια αυτού. - Το εκπαιδευτικό υλικό θα 	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>περιλαμβάνει αναλυτική περιγραφή ενεργειών & διαδικασιών <u>για τους διαχειριστές</u> για όλες τις τακτικές λειτουργίες και διαδικασίες οι οποίες θα πρέπει να εκτελούνται τόσο κεντρικά, όσο και από τους περιφερειακούς (ανά Υπηρεσία) διαχειριστές του συστήματος DLP, προκειμένου να επιτυγχάνεται η πλήρης διαχείριση και εκμετάλλευση των δυνατοτήτων του συστήματος.</p> <p>- Το εκπαιδευτικό υλικό για τους τελικούς χρήστες πρέπει να περιέχει συνοπτικές οδηγίες για τη σωστή λειτουργία και την προστασία των δεδομένων στους σταθμούς που είναι εγκατεστημένο το λογισμικό αποτροπής διαρροής πληροφοριών.</p>			
4.3	<p>Η εκπαίδευση για τους κεντρικούς διαχειριστές του συστήματος θα πραγματοποιηθεί στο εγκατεστημένο σύστημα (σε χώρους του Αρχηγείου της Ελληνικής Αστυνομίας), από τεχνικούς του Αναδόχου που ενεπλάκησαν στην υλοποίηση και θα περιλαμβάνει παρουσίαση της συγκεκριμένης υλοποίησης.</p>	ΝΑΙ		
4.4	<p>Η εκπαίδευση για τους περιφερειακούς διαχειριστές του συστήματος DLP και τους τελικούς χρήστες θα πραγματοποιηθεί σε χώρους του Αναδόχου, όπου θα εξασφαλίζεται η πρόσβαση σε Η/Υ κατ' άτομο.</p>	ΝΑΙ		
4.5	<p>Όσον αφορά τις εκπαιδεύσεις των περιφερειακών διαχειριστών και των τελικών χρηστών σημειώνεται ότι:</p> <ul style="list-style-type: none"> • 8 περιφερειακοί διαχειριστές και 8 τελικοί χρήστες θα πρέπει να εκπαιδευτούν στο νομό Θεσσαλονίκης, 	ΝΑΙ		

A/A	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<ul style="list-style-type: none"> • οι υπόλοιπες εκπαιδεύσεις θα λάβουν χώρα στο νομό Αττικής. 			
4.6	Η διάρκεια της εκπαιδευτικής ημέρας θα είναι 6 ώρες/ημέρα.	ΝΑΙ		
4.7	Στην προσφορά του Υποψηφίου Αναδόχου να περιλαμβάνεται πίνακας εκπαιδεύσεων που θα αναφέρονται οι τομείς των εκπαιδεύσεων, οι ώρες-ημέρες και ο αριθμός των εκπαιδευομένων.	ΝΑΙ		
4.8	Με το πέρας των εκπαιδεύσεων ο Ανάδοχος θα παραδώσει Αναφορά αξιολόγησης αποτελεσμάτων των εκπαιδεύσεων.	ΝΑΙ		

5. ΔΩΡΕΑΝ ΕΓΓΥΗΣΗ ΚΑΙ ΤΕΧΝΙΚΗ ΥΠΟΣΤΗΡΙΞΗ

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
5.1	<p>Χρονικό διάστημα σε έτη από την ημερομηνία οριστικής παραλαβής του Έργου, για το οποίο ο Ανάδοχος αναλαμβάνει την υποχρέωση εγγύησης και τεχνικής υποστήριξης καλής λειτουργίας όλων των προσφερόμενων ειδών και επισκευής κάθε βλάβης όλων των ειδών της Σύμβασης.</p> <p>Να αναφερθεί ο τυχόν περισσότερος δωρεάν παρεχόμενος χρόνος εγγύησης και τεχνικής υποστήριξης του Έργου.</p>	≥ 5 έτη		
5.2	<p>Ο Ανάδοχος πρέπει να διαθέτει μηχανισμό για την αναγγελία βλαβών (helpdesk) σε 24ωρη βάση, καθ' όλη τη διάρκεια του έτους. Να περιγραφεί ο μηχανισμός αναγγελίας βλαβών (helpdesk).</p>	ΝΑΙ		
5.3	<p>Κατά το διάστημα της εγγύησης και τεχνικής υποστήριξης όλες οι εργασίες αποκατάστασης και τα ανταλλακτικά θα βαρύνουν αποκλειστικά τον Ανάδοχο.</p>	ΝΑΙ		
5.4	<p>Οι υπηρεσίες της περιόδου εγγύησης και τεχνικής υποστήριξης αφορούν στην εξασφάλιση της καλής λειτουργίας του συστήματος και στην αποκατάσταση όλων των τύπων βλαβών και δυσλειτουργιών υλικού και λογισμικού που ενδεχομένως προκύπτουν επηρεάζοντας την ομαλή λειτουργία του δικτύου της Ελληνικής Αστυνομίας.</p>	ΝΑΙ		
5.5	<p>Οι υπηρεσίες της περιόδου εγγύησης και τεχνικής υποστήριξης θα πρέπει να καλύπτουν όλες τις απαραίτητες άδειες χρήσης για τη νόμιμη χρήση των ζητούμενων λειτουργιών, την αδιάλειπτη υποστήριξη των σταθμών εργασίας για την ενημέρωση με νέες εκδόσεις και την αυτόματη ενημέρωση των λογισμικών του Έργου.</p> <p>Η εγγύηση και τεχνική υποστήριξη θα έχει ημερομηνία έναρξης από την</p>	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	επόμενη ημέρα της οριστικής παραλαβής.			
5.6	Υποχρέωση δωρεάν αναβάθμισης όλων των προσφερόμενων λογισμικών και λειτουργικών συστημάτων εφόσον υπάρξει νέα έκδοση (version) κατά την περίοδο εγγύησης και τεχνικής υποστήριξης. Σημειώνεται ότι σε περίπτωση αλλαγής version ή release του S/W θα πρέπει να μη δημιουργούνται διενέξεις – δυσλειτουργίες (conflicts) στο σύνολο του υπάρχοντος εξοπλισμού και λογισμικού. Για οποιαδήποτε ενέργεια αυτού του τύπου θα πρέπει να προηγηθεί έγκριση από τη Δ/ση Πληροφορικής / Α.Ε.Α.	ΝΑΙ		
5.7	<p>Ο Ανάδοχος στα πλαίσια των συμβατικών υποχρεώσεων της εγγύησης και τεχνικής υποστήριξης έχει την ευθύνη για τα ακόλουθα:</p> <ol style="list-style-type: none"> 1. Τον εντοπισμό των βλαβών ή δυσλειτουργιών του προσφερόμενου Η/Υ ή/και S/W, την αποκατάστασή τους και την παράδοση του εξοπλισμού σε πλήρη λειτουργία, τόσο για αυτά που είχαν προσφερθεί κατά την προσφορά, είτε με κόστος είτε δωρεάν, όσο και για αυτά που η παροχή τους προέκυψε κατά την υλοποίηση. 2. Την αποκατάσταση λαθών όλου του προσφερόμενου λογισμικού (patches, ενημέρωση υπογραφών συστήματος, διαδικασία έκδοσης στατιστικών, παραμετροποίηση ενεργειών, κλπ). 3. Την ευθύνη για την παροχή βοήθειας για βελτιστοποίηση (Tuning) της απόδοσης του συστήματος προς επίλυση οποιοδήποτε προβλήματος – δυσλειτουργίας, η οποία δημιουργείται στο δίκτυο της Ελληνικής Αστυνομίας. 	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	4. Την εγκατάσταση κάθε απαραίτητου patch ή νέας version των λογισμικών του Έργου με σκοπό τη συμβατότητα λειτουργίας του Συστήματος με νέες version των Windows, java, Antivirus κπλ. που χρησιμοποιεί η Ελληνική Αστυνομία.			
5.8	<p>Υποχρέωση δωρεάν παροχής υποστήριξης των περιφερειακών διαχειριστών του DLP στις Υπηρεσίες που αυτό θα εγκατασταθεί (στο πλαίσιο του παρόντος έργου) με σκοπό τη συνδρομή τους στη διαχείριση πολιτικών DLP.</p> <p>Η εν λόγω υποχρέωση θα προσφέρεται σε ανθρωποώρες ανά μήνα, εντός Αττικής και Θεσσαλονίκης.</p> <p>Σε περίπτωση υπέρβασης των προσφερόμενων ανθρωποωρών, ο Ανάδοχος δε θα αποζημιώνεται και έχει το δικαίωμα άρνησης παροχής της εν λόγω υπηρεσίας για το υπόλοιπο του τρέχοντος μήνα.</p>	≥ 30		
5.9	Όλες οι παρεχόμενες υπηρεσίες που αφορούν σε προγραμματισμένες εργασίες εγγύησης και τεχνικής υποστήριξης του συστήματος, θα παρέχονται κατόπιν συνεννόησης όλες τις εργάσιμες ημέρες (Δευτέρα έως Παρασκευή) και ώρες (09:00 έως 17:00) της εβδομάδας, καθ' όλη τη διάρκεια του έτους πλην των επίσημων αργιών.	ΝΑΙ		
5.10	Για επείγουσες βλάβες, ο Ανάδοχος έχει υποχρέωση επίλυσης αυτών καθ' όλο το 24ωρο όλη τη διάρκεια του έτους.	ΝΑΙ		
5.11	Όλες οι κλήσεις παροχής υποστήριξης του Συστήματος θα πραγματοποιούνται μέσω της Δ/σης Πληροφορικής/ Α.Ε.Α.	ΝΑΙ		
5.12	Η εκτέλεση κάθε εργασίας του Αναδόχου, θα γίνεται σε συνεργασία με τον Αγοραστή, σε χώρους και με τρόπο που θα εγκρίνει ο τελευταίος ανά	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	περίπτωση, ενώ δε θα επιτρέπεται η απομακρυσμένη πρόσβαση μέσω Διαδικτύου.			
5.13	<p>Η διάγνωση και αποκατάσταση των βλαβών θα γίνεται στους χώρους της Ελληνικής Αστυνομίας. Σε εξαιρετικές περιπτώσεις, η επισκευή θα μπορεί να γίνει στα εργαστήρια του Αναδόχου κατόπιν σχετικής έγκρισης του Αγοραστή. Τα έξοδα μεταφοράς στην περίπτωση αυτή επιβαρύνουν τον Ανάδοχο. Επισημαίνεται πως σε κάθε περίπτωση που δε δύναται να αποκατασταθεί βλάβη μιας συσκευής στην οποία μπορεί να υπάρχουν αποθηκευμένα δεδομένα, τότε η οριστική καταστροφή της πραγματοποιείται παρουσία τεχνικών του Αγοραστή.</p>	<p>ΝΑΙ</p>		

6. ΣΥΝΤΗΡΗΣΗ

A/A	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
6.1	Υποχρέωση παροχής συντήρησης για το σύνολο των προσφερόμενων ειδών από τον Ανάδοχο με χρέωση, μετά τη λήξη της περιόδου εγγύησης και τεχνικής υποστήριξης, εάν το ζητήσει ο Αγοραστής [σε έτη].	≥ 2		
6.2	Ο Ανάδοχος στα πλαίσια των συμβατικών υποχρεώσεων συντήρησης, έχει όλες τις υποχρεώσεις της εγγύησης και τεχνικής υποστήριξης.	ΝΑΙ		
6.3	Στην ετήσια δαπάνη συντήρησης που θα δοθεί στον αναλυτικό πίνακα των προσφορών, περιλαμβάνονται: 1. Η αμοιβή για την αποκατάσταση λαθών, δυσλειτουργιών, την προληπτική συντήρηση και την βελτιστοποίηση (Tuning) της απόδοσης όλου του προσφερόμενου λογισμικού. 2. Η δαπάνη με το ετήσιο κόστος για την ανανέωση όλων των αδειών των προσφερόμενων λογισμικών και λειτουργικών συστημάτων.	ΝΑΙ		
6.4	Το ετήσιο / μηνιαίο κόστος συντήρησης και υποστήριξης θα δοθεί αναλυτικά στους Πίνακες της οικονομικής προσφοράς για κάθε προσφερόμενο είδος ανά μονάδα. Οι ίδιοι Πίνακες (για κάθε προσφερόμενο είδος ανά μονάδα), αλλά χωρίς τιμές θα υποβληθούν στην τεχνική προσφορά.	ΝΑΙ		
6.5	Το σύνολο του ετησίου κόστους συντήρησης, δε θα υπερβαίνει το 16.6% του συνολικού κόστους του παρόντος Έργου.	ΝΑΙ		
6.6	Το ετήσιο κόστος συντήρησης θα είναι σταθερό τουλάχιστον για τα 2 πρώτα	ΝΑΙ		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>έτη από την έναρξη καταβολής δαπανών συντήρησης, ενώ μετέπειτα θα μπορεί να αναπροσαρμοστεί ετησίως.</p> <p>Η ετήσια αναπροσαρμογή δεν θα υπερβαίνει τον ετήσιο δείκτη τιμών καταναλωτή του τελευταίου έτους.</p>			
6.7	<p>Ο Αγοραστής διατηρεί το δικαίωμα μονομερούς παράτασης της παροχής υπηρεσιών συντήρησης από τον Ανάδοχο, επανεξετάζοντας τις Υπηρεσιακές του ανάγκες, μετά τη λήξη του χρόνου εγγύησης και τεχνικής υποστήριξης και κάθε τυχούσας μετέπειτα παράτασης του χρόνου παροχής υπηρεσιών συντήρησης.</p>			
6.8	<p>Ο Αγοραστής, στα πλαίσια της συντήρησης, διατηρεί το δικαίωμα με έγγραφη και μονομερή δήλωσή του στον Ανάδοχο, να εξαιρεί ή να επανεντάσσει οποιοδήποτε είδος των υπό προμήθεια ειδών ή μέρους αυτών στο συμβόλαιο συντήρησης, αναπροσαρμόζοντας ανάλογα το κόστος συντήρησης. Σε περίπτωση επανένταξης στη συντήρηση κάποιου είδους που είχε εξαιρεθεί, τα συμβαλλόμενα μέρη εξακολουθούν να έχουν τις ίδιες υποχρεώσεις και δικαιώματα που θα είχαν εάν το συγκεκριμένο είδος δεν είχε ποτέ εξαιρεθεί από τη συντήρηση.</p>	ΝΑΙ		
6.9	<p>Τυχόν αμοιβές από πρόσθετες υπηρεσίες συντήρησης (όπως per call κλήσεις, αποκατάσταση βλαβών σε προϊόντα που έχουν εξαιρεθεί από τη συντήρηση κλπ.) τιμολογούνται με την ολοκλήρωση της παρεχόμενης υπηρεσίας.</p>	ΝΑΙ		
6.10	<p>Υποχρέωση δωρεάν παροχής υποστήριξης των περιφερειακών διαχειριστών του DLP στις Υπηρεσίες που αυτό θα εγκατασταθεί (στο πλαίσιο του παρόντος έργου) με σκοπό</p>	≥ 30		

Α/Α	ΚΡΙΤΗΡΙΟ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>τη συνδρομή τους στη διαχείριση πολιτικών DLP.</p> <p>Η εν λόγω υποχρέωση θα προσφέρεται σε ανθρωποώρες ανά μήνα, εντός Αττικής και Θεσσαλονίκης.</p> <p>Σε περίπτωση υπέρβασης των προσφερόμενων ανθρωποωρών, ο Ανάδοχος δε θα αποζημιώνεται και έχει το δικαίωμα άρνησης παροχής της εν λόγω υπηρεσίας για το υπόλοιπο του τρέχοντος μήνα.</p>			

Αθήνα, 20-09-2016

Η ΕΠΙΤΡΟΠΗ

Η ΠΡΟΕΔΡΟΣ

ΤΑ ΜΕΛΗ

1)

**ΖΙΩΓΑ ΕΛΙΣΣΑΒΕΤ
ΑΣΤΥΝΟΜΟΣ Β' Ε.Κ.**

**ΔΗΜΟΥΛΑΚΗΣ ΙΩΑΝΝΗΣ
ΥΠΑΣΤΥΝΟΜΟΣ Α'**

2)

**ΜΠΙΚΗΣ ΤΗΛΕΜΑΧΟΣ
ΥΠΑΣΤΥΝΟΜΟΣ Α'**

3)

**ΤΕΛΚΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ
ΑΝΟΥΠΑΣΤΥΝΟΜΟΣ**

4)

**ΠΑΠΑΣΑΒΒΑΣ ΑΔΑΜ
ΑΝΟΥΠΑΣΤΥΝΟΜΟΣ**