ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΦΑΡΜΑΚΕΥΤΙΚΟΣ ΣΥΛΛΟΓΟΣ ΑΤΤΙΚΗΣ
Ν.Π.Δ.Δ.
Μυλλέρου 1 & Αγησιλάου - 104 36 ΑΘΗΝΑ,
ΤΗΛ. 210 5243186
ΦΑΞ. 210 5220721 – Email: grfsa@fsa.gr
Πληρ. Κατερίνα Νιάρχου
Αριθ. Πρωτ.5040 ΑΘΗΝΑ 19.11.2026

ΠΡΟΣ ΤΙΣ ΕΦΗΜΕΡΙΔΕΣ
1.- ΓΕΝΙΚΗ ΔΗΜΟΠΡΑΣΙΩΝ 2.- ΝΑΥΤΕΜΠΟΡΙΚΗ 3.- ΗΧΩ ΔΗΜΟΠΡΑΣΙΩΝ 4.- ΔΗΜΟΠΡΑΣΙΩΝ ΚΑΙ ΠΛΕΙΣΤΗΡΙΑΣΜΩΝ

ΠΡΟΣΚΛΗΣΗ ΕΝΔΙΑΦΕΡΟΝΤΟΣ
ΓΙΑ IT SUPPORT ΜΕ ΣΥΜΒΑΣΗ ΔΥΟ ΧΡΟΝΩΝ ΓΙΑ ΤΙΣ ΥΠΗΡΕΣΙΕΣ ΤΟΥ Φ.Σ.Α
(περιλαμβάνει θέματα hardware & αναβαθμίσεων)

Ο Φαρμακευτικός Σύλλογος Αττικής (Φ.Σ.Α.) είναι νομικό πρόσωπο δημοσίου δικαίου, σωματειακής μορφής σύμφωνα με τον ν.5041/2023, το οποίο δεν ανήκει στο δημόσιο τομέα κατά την έννοια της περ. α) της παρ. 1 του άρθρου 14 του ν. 4270/2014 (Α' 143) και απολαμβάνει πλήρους διοικητικής και περιουσιακής αυτοτέλειας. Επομένως δεν χρηματοδοτείται από τον Κρατικό Προϋπολογισμό και δεν αποτελεί αναθέτουσα αρχή ή αναθέτοντα φορέα, κατά την έννοια των υποπερ. α) και β) της περ. 1 της παρ. 1 του άρθρου 2 του ν. 4412/2016 (Α' 147), ούτε οργανισμό δημοσίου δικαίου, κατά την έννοια της περ. 4) της παρ.1 του άρθρου 2 ου ιδίου νόμου. Επίσης σύμφωνα με τη παρ.2 το άρθρο 43 του ν. 5041/2023 δύναται να προβαίνει στη σύναψη συμβάσεων παροχής υπηρεσιών ή/και έργου.

Ο Φαρμακευτικός Σύλλογος Αττικής αναζητά IT SUPPORT για τις υπηρεσίες του Φαρμακευτικού Συλλόγου Αττικής με σύναψη διετές σύμβασης.

Ειδικότερα η ζητούμενη παροχή αφορά :

1. Ασφαλές Δίκτυο

Η διασφάλιση της ακεραιότητας και ασφάλειας του δικτύου με εξασφάλιση υψηλής διαθεσιμότητας, προστασίας από κακόβουλες επιθέσεις, και αποτροπή ανεπιθύμητης πρόσβασης. Οι τεχνολογίες που θα χρησιμοποιηθούν πρέπει να περιλαμβάνουν τεχνολογίες όπως :

1.1 Cyber Security [End point]

- **Κεντρική Διαχείριση**: Ενιαίο ταμπλό ελέγχου (dashboard) που συγκεντρώνει δεδομένα από όλα τα υποσυστήματα, επιτρέποντας την παρακολούθηση, ανάλυση και αναφορά σε πραγματικό χρόνο.
- **Ενοποίηση με Υφιστάμενα Συστήματα**: Δυνατότητα ενσωμάτωσης με υπάρχουσες λύσεις ασφαλείας και ITSM μέσω API, διευκολύνοντας την κεντρική διαχείριση και αναφορά.
- **Νέας γενιάς Antivirus με πολυδιάστατη ανίχνευση**. Συνδυασμός τοπικής ανίχνευσης, ανάλυσης συμπεριφοράς, cloud scanning και sandboxing για ανίχνευση προηγμένων απειλών.
- **Αντιμετώπιση Brute Force**: Ενισχυμένη προστασία κατά επιθέσεων brute force, μειώνοντας τον κίνδυνο διαρροής δεδομένων.

- **Ανίχνευση και Πρόληψη Απειλών (IDS/IPS)**: Παροχή συνεχούς ανίχνευσης και πρόληψης απειλών, με προηγμένα εργαλεία για ανίχνευση κακόβουλων επιθέσεων σε πραγματικό χρόνο.
- **Διαχείριση Ασφαλείας Συσκευών**: Ενσωμάτωση προστασίας από ιούς, κακόβουλο λογισμικό και άλλες διαδικτυακές απειλές σε όλες τις συσκευές του δικτύου.
- **Διαχείριση Δικτύου και Αξιολόγηση Ασφαλείας**: Ανάλυση και αναφορά για το επίπεδο ασφαλείας του δικτύου και των συσκευών, παρέχοντας προτάσεις για βελτιστοποίηση της προστασίας.
- **Ανίχνευση και Αποτροπή Κρυπτογράφησης**: Προστασία από κακόβουλες προσπάθειες κρυπτογράφησης κατά τη διάρκεια επιθέσεων ransomware, χωρίς την ανάγκη υπογραφών.
- **Προστασία Δικτύου με DNS Filtering**: Φιλτράρισμα DNS για τον εντοπισμό και την αποτροπή κακόβουλης κίνησης πριν φτάσει στα endpoints.
- **Κάλυψη Συσκευών IoT και BYOD**: Προστασία όλων των συσκευών που συνδέονται στο δίκτυο, συμπεριλαμβανομένων συσκευών IoT και προσωπικών συσκευών χρηστών (BYOD).
- **Καταγραφή Δικτυακής Κίνησης**: Εκτενής καταγραφή δραστηριότητας δικτύου, επιτρέποντας την ανάλυση και την ανίχνευση απειλών σε πραγματικό χρόνο.
- Προστασία από Απάτες μέσω Ηλεκτρονικού Ταχυδρομείου

1.2 Firewall [Περιμετρική ασφάλεια]

- **Τείχος Προστασίας**: Εφαρμογή πολιτικών πρόσβασης για την αποτελεσματική διαχείριση της κυκλοφορίας, επιτρέποντας ή αποκλείοντας συγκεκριμένες συνδέσεις βάσει IP, θύρας, ή πρωτοκόλλου.
- **Δρομολόγηση και Failover**: Υποστήριξη πολλαπλών WAN για την εξασφάλιση συνεχιζόμενης σύνδεσης στο δίκτυο, με δυνατότητες load balancing και failover για αυξημένη αξιοπιστία.
- **VPN (Virtual Private Network)**: Διαχείριση απομακρυσμένων συνδέσεων μέσω πρωτοκόλλων VPN όπως OpenVPN και IPsec για ασφαλή σύνδεση απομακρυσμένων χρηστών και συσκευών.
- **Διαχείριση Χρηστών VPN**: Δημιουργία και διαχείριση χρηστών VPN με δυνατότητες ελέγχου πρόσβασης και πολιτικών ασφαλείας.
- **Ασφαλής Πρόσβαση και Προστασία Δικτύου**: Ενσωμάτωση επιπλέον μηχανισμών για την προστασία από επιθέσεις, όπως brute force, DDoS και άλλες κυβερνοεπιθέσεις.
- **Διαχείριση Πακέτων**: Επέκταση λειτουργικότητας μέσω της εγκατάστασης επιπλέον πακέτων όπως Snort (IDS/IPS) και pfBlockerNG για φιλτράρισμα περιεχομένου και αυξημένη ασφάλεια.
- **Δρομολόγηση Πολυάριθμων WAN**: Υποστήριξη για πολλαπλές συνδέσεις WAN, επιτρέποντας load balancing και failover για αυξημένη αξιοπιστία.
- **Διαχείριση Κυκλοφορίας (Traffic Shaping)**: Εφαρμογή περιορισμών και προτεραιοτήτων στην κυκλοφορία δικτύου για βελτιστοποίηση της απόδοσης και της ποιότητας υπηρεσίας
- **Υποστήριξη Πακέτων**: Δυνατότητα εγκατάστασης και διαχείρισης πρόσθετων πακέτων για επέκταση της λειτουργικότητας, όπως Snort για IDS/IPS, Squid για proxy, και pfBlockerNG για φιλτράρισμα περιεχομένου.

- **Γραφήματα RRD**: Παρακολούθηση της απόδοσης του συστήματος μέσω γραφημάτων RRD που απεικονίζουν στοιχεία όπως χρήση CPU, κυκλοφορία δικτύου, και κατάσταση firewall.
- Perpetual [εφάπαξ] προμήθεια , χωρίς ετήσιες ανανεώσεις

2. Παρακολούθηση Εξοπλισμού και Υποστήριξη

Συνεχής παρακολούθηση του εξοπλισμού και έγκαιρης ανταπόκριση σε προβλήματα για τη διατήρηση της επιχειρησιακής συνέχειας και την αποφυγή downtime. Η λύση που θα χρησιμοποιηθεί για την παρακολούθηση του εξοπλισμού και την υποστήριξη των χρηστών, θα πρέπει να παρέχει :

- **Παρακολούθηση Συσκευών σε Πραγματικό Χρόνο**: Παρακολούθηση των συστημάτων (υπολογιστές, διακομιστές, και δίκτυο) σε πραγματικό χρόνο, με ειδοποιήσεις για οποιαδήποτε ανωμαλία ή πρόβλημα στη λειτουργία τους.
- **Αυτοματοποιημένες Ενημερώσεις (Patch Management)**: Αυτόματη εφαρμογή κρίσιμων ενημερώσεων για τα λειτουργικά συστήματα και το λογισμικό, ελαχιστοποιώντας τις ευπάθειες και αυξάνοντας την ασφάλεια.
- **Ανάλυση Απόδοσης και Αναφορές**: Παροχή αναφορών σχετικά με τη χρήση πόρων, την απόδοση των συσκευών, τη συμμόρφωση με τις πολιτικές ασφαλείας και τη γενική υγεία των συστημάτων.
- **Αυτοματισμός Εργασιών IT**: Δυνατότητα δημιουργίας αυτοματοποιημένων εργασιών για τη συντήρηση και βελτιστοποίηση των συστημάτων, μέσω scripting και χρήσης τεχνητής νοημοσύνης.
- **Απομακρυσμένη Υποστήριξη και Πρόσβαση**: Παροχή εργαλείων για απομακρυσμένη πρόσβαση σε συσκευές μέσω εργαλείων όπως AnyDesk και Splashtop για άμεση υποστήριξη και αποκατάσταση προβλημάτων.
- **Σύστημα Ticketing**: Διαχείριση αιτημάτων υποστήριξης μέσω συστήματος ticketing, που επιτρέπει την παρακολούθηση και την επίλυση προβλημάτων με υψηλή προτεραιότητα.
- **Δυνατότητα ευέλικτου ωραρίου**. Δυνατότητα προσαρμογής ωραρίου υποστήριξης ως και 24 x 7 x 365

3. Δημιουργία DISASTER RECOVERY PLAN

- **Αυτόματα Αντίγραφα Ασφαλείας (Backup Scheduling):** Η λύση backup πρέπει να υποστηρίζει πλήρη και τοπικά αντίγραφα ασφαλείας σε τακτική βάση (π.χ., καθημερινά ή εβδομαδιαία), με δυνατότητες incremental ή differential backups για τη μείωση του χρόνου και του αποθηκευτικού χώρου.
- **Αναπαραγωγή Δεδομένων (Replication):** Η λύση backup πρέπει να επιτρέπει την αναπαραγωγή των δεδομένων σε απομακρυσμένο διακομιστή ή το cloud, εξασφαλίζοντας συνεχιζόμενη διαθεσιμότητα των υπηρεσιών σε περίπτωση καταστροφής.
- **Επαλήθευση Αντιγράφων Ασφαλείας:** Η διαδικασία ανάκτησης από το backup πρέπει να περιλαμβάνει τη δυνατότητα επαλήθευσης της ορθότητας των αντιγράφων ασφαλείας, εξασφαλίζοντας ότι τα αντίγραφα είναι πλήρη και ακέραια.
- **Ασφάλεια και Κρυπτογράφηση:** Η λύση backup πρέπει να περιλαμβάνει δυνατότητες κρυπτογράφησης τόσο κατά τη διάρκεια της αποθήκευσης όσο και κατά τη διάρκεια της

μεταφοράς των δεδομένων, διασφαλίζοντας την προστασία των ευαίσθητων δεδομένων από μη εξουσιοδοτημένη πρόσβαση.

- **Ανακτήσεις και Διαχείριση Recovery:** Η λύση πρέπει να υποστηρίζει γρήγορη ανάκτηση των δεδομένων και εύκολη αποκατάσταση σε περίπτωση απώλειας δεδομένων ή καταστροφής, με δυνατότητες για πλήρη και μερική αποκατάσταση, όπως ανάκτηση ολόκληρου του συστήματος ή συγκεκριμένων αρχείων/φακέλων.
- **Υποστήριξη για Virtual Environments:** Η λύση backup θα πρέπει να υποστηρίζει την αναπαραγωγή και αποκατάσταση δεδομένων σε εικονικά περιβάλλοντα (π.χ., VMware, Hyper-V), επιτρέποντας εύκολη διαχείριση για εταιρικές υποδομές εικονικοποίησης.

4. Γενικές προδιαγραφές Υπηρεσιών

- Η λύση που θα σχεδιαστεί και θα προσφερθεί, θα πρέπει να μπορεί να διατηρηθεί ενεργή για την επόμενη πενταετία
- Η εκάστοτε υποστήριξη σε συστήματα και προγράμματα θα αφορά όλο το έτος 2027
- Η προσφορά θα πρέπει να έχει ανάλυση του ποσού, σύμφωνα με τα ζητούμενα στην παρούσα πρόσκληση
- Ο πάροχος της υπηρεσίας ,θα πρέπει να διατηρεί ενεργές πιστοποιήσεις ISO9001, ISO27001 και ISO27701 καθώς ο οργανισμός διατηρεί στοιχεία πελατών.

Οι προσφορές θα ανοιχθούν από την επιτροπή του ΦΣΑ και η επιλογή παρόχου/-ων θα γίνει εντός ευλόγου χρόνου μετά την λήξη προθεσμίας υποβολής των προσφορών κατά την απόλυτη κρίση του Δ.Σ. του Φ.Σ.Α.

Ο Φαρμακευτικός Σύλλογος Αττικής διατηρεί επίσης το δικαίωμα να ακυρώσει ή να κηρύξει άγονο τον διαγωνισμό ή ακόμα και να αποκλείσει οιονδήποτε ενδιαφερόμενο, ακόμα και τον μειοδότη, εάν το κρίνει απαραίτητο, με αιτιολογημένη απάντησή του.

Οι προσφορές θα πρέπει να κατατεθούν στα γραφεία του Συλλόγου έως 11-12-2026, ημέρα Παρασκευή, σε κλειστό φάκελο που θα φέρει την σφραγίδα και υπογραφή του εκπροσώπου της εταιρείας στο κλείσιμο του φακέλου.

Οι ενδιαφερόμενοι πιθανόν να κληθούν να δώσουν διευκρινήσεις από την επιτροπή του ΦΣΑ.

Για το Δ.Σ. του Φ.Σ,Α,

Ο ΠΡΟΕΔΡΟΣ
ΗΛΙΑΣ ΒΑΣΙΛΑΔΙΩΤΗΣ

Ο ΓΡΑΜΜΑΤΕΑΣ
ΣΤΥΛΙΑΝΟΣ ΚΑΛΟΓΕΡΟΠΟΥΛΟΣ